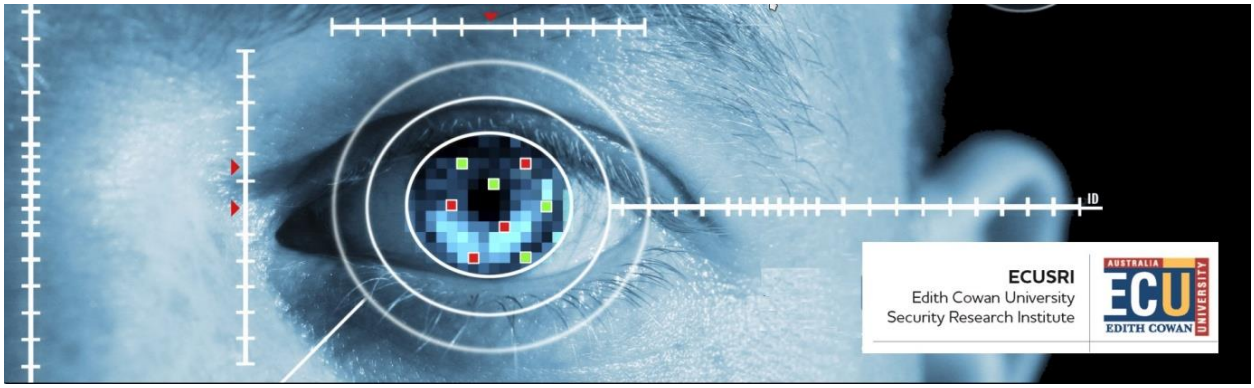
2016

The Proceedings of 14th Australian Information Security Management Conference, 5-6 December 2016, Edith Cowan University, Perth, Australia

Mike Johnstone
Security Research Institute, Edith Cowan University

DOI: 10.4225/75/58a69ee5afc30
Published as: Johnstone, M. (Ed.). (2016). *The Proceedings of 14th Australian* Information Security Management Conference*, 5-6 December 2016, Edith Cowan University, Perth, Australia.*



The Proceedings of

14th Australian Information Security Management Conference

5-6 December 2016

Edith Cowan University, Perth, Australia

AUSTRALIA ECU EDITH COWAN UNIVERSITY

Proceedings of the
14th Australian Information Security Management Conference

Published By
Security Research Institute
Edith Cowan University

Edited By
Dr Mike Johnstone
Security Research Institute
Edith Cowan University

ISBN 978-0-9946186-0-3

CRICOS Institution Provider Code 00279B

Sponsors

ECUSRI
Edith Cowan University
Security Research Institute

AUSTRALIA ECU EDITH COWAN UNIVERSITY

Secure Systems

CISCO

Supporters

AUSTRALIAN SECURITY MAGAZINE

acs AUSTRALIAN COMPUTER SOCIETY

Australian and New Zealand FORENSIC SCIENCE SOCIETY

Conference Foreword

The annual Security Congress, run by the Security Research Institute at Edith Cowan University, includes the Australian Information Security and Management Conference. Now in its fourteenth year, the conference remains popular for its diverse content and mixture of technical research and discussion papers. The area of information security and management continues to be varied, as is reflected by the wide variety of subject matter covered by the papers this year.

The conference has drawn interest and papers from within Australia and internationally. All submitted papers were subject to a double blind peer review process. Fifteen papers were submitted from Australia and overseas, of which ten were accepted for final presentation and publication.

We wish to thank the reviewers for kindly volunteering their time and expertise in support of this event. We would also like to thank the conference committee who have organised yet another successful congress. Events such as this are impossible without the tireless efforts of such people in reviewing and editing the conference papers, and assisting with the planning, organisation and execution of the conferences.

To our sponsors also a vote of thanks for both the financial and moral support provided to the conference. Finally, thank you to the administrative and technical staff, and students of the ECU Security Research Institute for their contributions to the running of the conference.

Yours sincerely

Conference Chair
Dr Mike Johnstone, Security Research Institute, Edith Cowan University

Congress Organising Committee

Congress Chair: Professor Craig Valli

Committee Members: Dr Zubair Baig
Mr David Cook
Mr Michael Crowley
Mr Peter Hannay
Professor Bill Hutchinson
Dr Ahmed Ibrahim
Dr Mike Johnstone
Dr Patryk Szewczyk
Dr Krishnun Sansurooah
Associate Professor Andrew Woodward

Congress Coordinator: Ms Emma Burke

Table of Contents

CELESTIAL SOURCES FOR RANDOM NUMBER GENERATION

Erin Chapman, Jerina Grewar, Tim Natusch
Digital Forensics Research Laboratories, Institute for Radio Astronomy and Space Research
Auckland University of Technology, Auckland, New Zealand
erinchapman@xtra.co.nz, jmgrewar@gmail.com

Abstract

In this paper, we present an alternative method of gathering seed data for random number generation (RNG) in cryptographic applications. Our proposed method utilises the inherent randomness of signal data from celestial sources in radio astronomy to provide seeds for RNG. The data sets were collected from two separate celestial sources, and run through the SHA-256 algorithm to deskew the data and produce random numbers with a uniform distribution. The resulting data sets pass all tests in the NIST Statistical Test Suite for random data, with a mean of 98.9% of the 512 total bitstreams from the two sources passing all tests in the NIST suite, as well as further testing in R. These results are on par with the control set generated using Java's SecureRandom function. An explanation of the sources, the data processing and detailed results of each of the tests are presented.

Keywords

Random number generation, RNG, random noise, NIST, seeds, cryptographic hash functions, SHA-256, secure hashing algorithm, radio astronomy, signal noise, data analysis, astronomy, analytics, random sequences

INTRODUCTION

The use of random number generators is a fundamental element of cryptographic systems. The creation of random initialisation vectors and keys are of utmost importance in security applications which utilise encryption on a day-to-day basis globally. The means by which these numbers are generated varies from application to application, however many are created through algorithmic processes, such as the Monte Carlo methods (Gentle, 2006). Many different options for producing truly random numbers through nature have been proposed, utilising the signal noise of lasers (Applegate et al., 2015), or implementing quantum chaotic generators (Akhshani, Akhavan, Mobaraki, Lim, & Hassan, 2014). In this paper we propose an alternative method for seeding RNGs which utilises the inherent randomness of the signal noise produced by radio telescopes, with a scheme which implements the Secure Hashing Algorithm (SHA) as a deskewing algorithm for randomness extraction. The output of this scheme passes statistical tests for randomness in both R and the NIST Statistical Test Suite (NIST STS), and offers a new method of collecting random numbers for use in seeding cryptographic applications. This research offers applications in the implementation of secure random number generators such as SHA-256 (Dang, 2015), which rely on irreproducible, statistically random seed data for security. The proposed scheme for gathering seed data could be utilised in the application of cryptographic protocols for secure systems, as our results show it presents a high-level of performance paired with rapid data collection.

The structure of this paper is as follows: in Part I relevant prior research is discussed briefly, and an overview of the area is given. In Part II the operation and theory of radio telescopes and the related signal noise is explained. Part III then offers our data sources and method for the collection of the output. Part IV enumerates the method by which the gathered data was processed using SHA-256 for deskewing purposes and our results based on the outcome of the statistical testing completed. Finally, Part V offers our conclusions and suggestions for further research.

RANDOM NUMBER GENERATION AND RANDOM SEEDS

The generation of random numbers for security applications is an ever-present concern. Utilising hardware to generate these numbers is a well-developed area, in which the main aim is to mitigate the statistical properties of the data, and to determine whether there is any way for an adversary to estimate the likely output of a particular system. As the algorithms used in these applications are themselves public knowledge, the security rests in the seed, for deterministic systems, and in the data source, for non-deterministic RNG.

Schemes such as the secure RNG developed by Lo Re, Milazzo, & Ortolani (2014) make use of the inherent properties of hardware components to collect data. In the system proposed by Lo Re et al. (2014) each node of the wireless sensor network is capable of generating random numbers, which are provided to the leader node.

Other systems have utilised the properties of quantum mechanics to implement RNGs. Lunghi et al. (2015) offered a quantum RNG which maintained consistent monitoring of the output to ensure continuing statistical randomness. Cicek, Pusan, & Dundar (2014) presented a method for True Random Number Generation (TRNG) through a chaos system, which gave excellent performance when tested by the NIST Statistical Test Suite, with the bitstream resulting from the scheme split into 1 Mbit blocks.

In generating random numbers for everyday use in cryptographic applications, most systems use pseudo-random number generators (PRNGs), which function through algorithmic means. This type of RNG requires a seed, which in itself should be statistically random and irreproducible, because if the seed is compromised, then the resulting random numbers are also compromised. Implementations such as the Java function call SecureRandom use a mixture of truly random and pseudorandom data, often starting with a TRN as the function seed. Other PRNGs use statistical methods such as Monte Carlo techniques, or Lorenz systems (Lynnyk, Sakamoto, & Celikovsky, 2015). In the case of Lynnyk, Nakamoto and Celikovsky (2015), a TRN was used to produce the seed for the algorithmic PRNG. In Barker and Kelsey (2015), the Secure Hash Algorithm (SHA) family is recommended for use in deterministic random number generation using irreproducible and statistically random seeds.

RADIO ASTRONOMY

Radio Astronomy is the discipline of science using antennae or radio telescopes to detect the emission of celestial sources in the electromagnetic frequency range of 10^6 Hz to 10^9 Hz (Shuch, 2013). Radio telescopes allow astronomers to peer through not only the layers of our atmosphere but in frequencies beyond the human eye's capability into interstellar clouds of particles, thereby determining the chemistry and physics behind the astronomical phenomena of our universe (Dougherty, 2011).

At 30.48 metres in diameter, the Warkworth 2 antennae was licensed from Telecom and converted in 2010 by the Institute for Radio Astronomy and Space Research (IRASR) of Auckland University of Technology (AUT) (Murphy, 2010). This took it from an international telecommunications satellite dish to a radio telescope as part of the Warkworth Radio Astronomical Observatory (WRAO). The telescope is a reflector on a wheel and track with a beam waveguide feed (Woodburn et al., 2015). NEC Corporation of Japan originally built the dish for the Post Office (later Telecom) in 1984 as part of Warkworth Satellite Earth Station, which is located 5 km south of Warkworth and 60 km north of Auckland, in New Zealand's North Island (Ministry of Culture and Heritage, 2013).

The majority of astronomical objects give off radiation for astronomers to detect, but some have much greater emissions including pulsars, quasars, certain nebulae, and radio galaxies (The Editors of Encyclopædia Britannica, 2016). In 1931, Karl Jansky worked on improving the operation of transoceanic radio links for Bell Laboratories. The "steady hiss static" that he recorded became the origin of radio astronomy, and now the strength, or spectral flux density of a radio source is measured in Janskys (Jy), where 1 Jy = 10-26 Wm-2Hz-1 (Jansky, 1979).

Radio astronomy signals are inherently random, "a specific property of astronomical observations is that they cannot be repeated under the exact same conditions" (Junklewitz, 2014, p.13). The astrophysical source signal and the telescope system noise are both Gaussian distributed (Burke and Graham-Smith, 2002). The signal available at the output of a radio telescope consists of the combination of system noise (internally generated noise), a 2.73 Kelvin component from Cosmic Microwave Background Radiation, noise power from the celestial source of interest (the "signal") and typically interference signals picked up from the surrounding terrain (Campbell, 2002). The influence of the amplifier increases the amplitude of both "signal" and noise whilst a linear (frequency independent) response of the receiving system will preserve the statistical distribution of the input signal and result in a Gaussian output signal (Haykin, 2009).

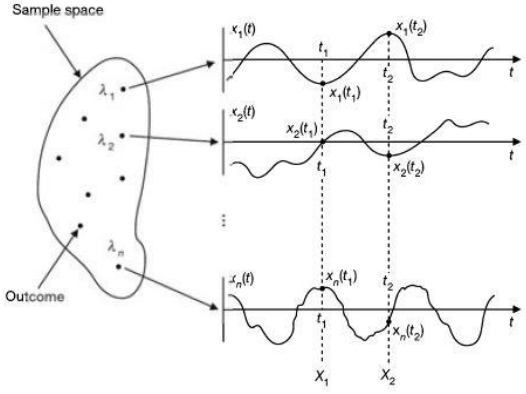


Figure a: Random Process (Hsu, 2013, p. 393)

Due to the random nature of all the processes contributing to the final receiver output signal it is not normally possible to distinguish between the various components from a study of the output signal. Using the sum of all these signals, and recognizing the implausibility of another party replicating the uniqueness of the system noise component(s) confers a distinct advantage for recording a unique source of randomly generated data (Burke and Graham-Smith, 2002). An illustrated example of how our recorded signal is a statistically random process is shown in *Figures A* and *B*.

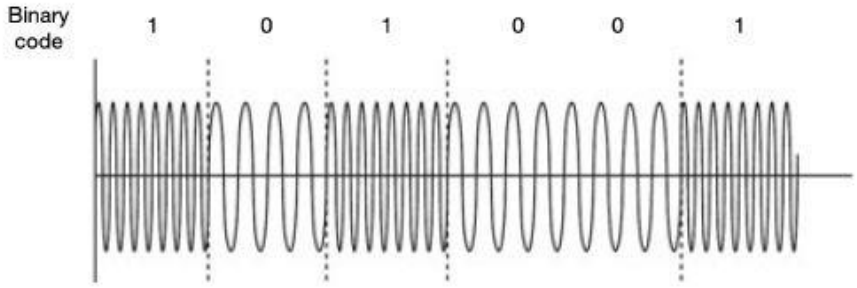


Figure b: Random sequence of data bits 1 or 0 produced by a Random Process (Hsu, 2013, p. 393)

DATA COLLECTION

The data used in this research was collected at the WRAO. The two sources chosen for data collection were the bright Maser 309.92+0.47, hereafter referred to as "G309" (coordinates 13h 50mins 41.78s RA and -61º 35' 10.2" DEC) and M17 (18h 20mins 26s RA and -16º 10' 36" DEC) from the J2000 epoch. G309 is a methanol maser; an interstellar cloud of methanol (CH_3OH) molecules that emits at a frequency of approximately 6.7 GHz (in the laboratory/rest frame). Photons are released when these particular molecules change their angular momentum via a transition between allowed quantum rotational states. In the J/A+A/432/737 General Catalogue of 6.7GHz Methanol Masers, G309 has a flux of approximately 780 Jy (Pestalozzi and Chrysostomou, 2005). The methanol maser is 5.3 kiloparsecs (kpc) or 17.2 kilo-lightyears (kly) distant from Earth (Phillips, Norris, Ellingsen, & McCulloch, 1998). M17 is a nebula containing an open cluster of stars called NGC6618. The cluster is an HII star-forming region, an ionised cloud of Hydrogen that radiates by a thermal emission process. M17 is at 1.6 kpc distance and observed total flux is some 687 Jy (Povich et al., 2007).

Signal from the right hand circular polarisation (RCP) of the telescopes C band receiver was processed by a chain of backend electronics consisting of a "front end" Low Noise Amplifier (LNA), a down-converter that selected and mixed a 6.5-6.8 GHz "RF/Sky" band of signal down to a 300 MHz wide band centred on 825 MHz and finally to an RTL-SDR for further filtering, amplification and digitisation of the signal. Down conversion to the Intermediate Frequency (IF) band at 825 MHz is achieved by selecting the lower side band result of mixing the RF/Sky band with a 5.8 GHz signal from a Local Oscillator (LO) locked to the WRAO Hydrogen Maser (Woodburn et al., 2015):

$$f_{IF} = f_{SKY} - f_{LO} = 6.675\ GHz - 5.85\ GHz = 0.825\ GHz\ or\ 825\ MHz$$

The down converted band was conveyed by a short length (≈0.5 m) of coaxial cable that also converted from the type N output connector of the C band downconverter to the MCX input of the RTL-SDR. Equipped with a RTL2838U chipset the RTL-SDR Software Defined Radio (SDR) dongle was plugged into a USB 2.0 port of a Unix based laptop (provided by IRASR) The dongle was tuned to 825 MHz and set to a gain of 40 dB by constructing a simple GUI interface in the free GNU Radio Companion (GRC) software package (West, 2006). The digitized 8 bit data was interleaved into in-phase (I) and quadrature phase (Q) streams produced by the dongle. The raw data streams were processed by a Fast Fourier Transform (FFT) GRC block to produce a spectrum for visual monitoring of the recorded signal. The LO was turned on and off, the response assured a signal was being recorded from *fsky*. The actual recording of signals was initiated using appropriate commands from the rtl_sdr driver package (obtained from git clone git://git.osmocom.org/rtl-sdr.git). Approximately 400MB of raw data was recorded from each of our sources, for ≈ 1 min each, into 2 binary seed files. This data was then pre-processed using hex dump into text files each containing a 128 bit line of received data in hexadecimal format.

As part of the process of determining correct operation of the system the telescope was first pointed at Centaurus A (NGC5128), a Seyfert galaxy (13h25m27.6s RA, -43d01m09s DEC). A pointing observation was run, stepping through a grid of 9 points offset from the nominal position in both azimuth and elevation. The received power levels obtained for all offset positions where then subjected to a least squares fit (Gaussian peak on a straight line

background) to determine offsets of the flux peak. Offsets of 0.04º in azimuth and 0.03º in elevation where determined and then applied to subsequent source observations. With calibration of pointing offsets applied the telescope was then focused on G309 and M17 in sequence and data files recorded for analysis as described above.

RESULTS

The data collected from the sources G309 and M17 was processed for testing using Java. All processing and testing was completed on a Unix-based machine configured with 16GB 1867 MHz DDR3 RAM and a 3.1 GHz Intel Core i7 processor. The Java code stripped the index numbering from the lines in the hex dump file, and removed all excess white space. Each of the 128-bit lines of data were then individually used as a seed for hashing into random numbers. As per the NIST recommendations (Barker & Kelsey, 2015), we utilised the SHA family of algorithms for the purpose of randomness extraction, specifically the SHA-256 algorithm (Dang, 2015). The output of this process was then written to a binary file for testing purposes.

The first set of tests performed on our data were completed in R, version 3.3.1, which offers several libraries for the analysis of random data. The *randtests* package created by Mateus & Caeiro (2014) offer tests which examine the vector data read through a binary file and offer a p-value as the output. A p-value of greater than then significance level $a = 0.05$ gives the sequence a pass, while a p-value of less than $a = 0.05$ means the test has rejected the null hypothesis. The binary file for each source was read into a vector of integer elements, with 2 bytes to each integer value. The data was subjected to the Bartels Rank Test (Bartels, 1982), the Cox Stuart Test (Cox & Stuart, 1955), the Difference Sign Test (Moore & Wallis, 1943), and the Wald-Wolfowitz Runs Test (Wald & Wolfovitz, 1940) for continuous data. In all tests, the p-value result was greater than a, meaning the data passed the test. In comparing the two data sets, we found that the data gathered from M17 offered better results than that gathered from G309. We speculate that this may be due to the inherent nature of each of the sources, as M17 is a weaker and more generally dispersed source than G309. Further investigation is required for a definitive resolution to this speculation.

Table 1 shows the results of the testing for both sources, as well as values generated through Java's SecureRandom function, used as our control group. The control data was similarly hashed with the SHA-256 algorithm, and read in to integer values 2 bytes at a time.

Table 1: Results of testing in R's randtests package (4 d.p.)

Test	*M17*	*G309*	*Control*
Bartel's rank test	0.5922	0.4317	0.5633
Cox Stuart test	0.7919	0.05636	0.138
Difference sign test	0.6885	0.4409	0.5945
Wald-Wolfowitz runs test	0.4372	0.2941	0.353

The hashed M17 data gave a better performance on the tests than the control group, of the hashed SecureRandom numbers, while G309 resulted in the worst performance of the test sets. Table 2 shows the entropy values of the data sets, both pre- and post-hashing, which were calculated using the Dirichlet-multinomial pseudo count model with Bayesian estimates using Laplace's prior (a=1) in the *entropy* R package (Hausser & Strimmer, 2009). The entropy value of the pre-hashed astronomical data in comparison with the control group of the data generated using the SecureRandom function suggests that the use of celestial sources provides data with a superior level of entropy for use in cryptographic functions.

Table 2: Data Entropy Values as per R's entropy package (5 d.p.)

Data set	*Entropy pre-processing*	*Entropy post-processing*
M17	16.11105	15.92491
G309	16.10822	15.92499
Control	15.89529	15.92493

The histograms for each of the data sets were also computed, both for the unprocessed stream received from the radio telescope, which presents a Gaussian distribution, and for the hashed data, which results in a visibly uniform distribution. *Figure C* shows the histogram for the unprocessed data gathered from M17, while *Figure D* shows the post-hashing data for M17 once it was fed through the SHA-256 algorithm. *Figure E* meanwhile displays the histogram for G309 pre-processing, and *Figure F* gives the histogram for G309 post-hashing.

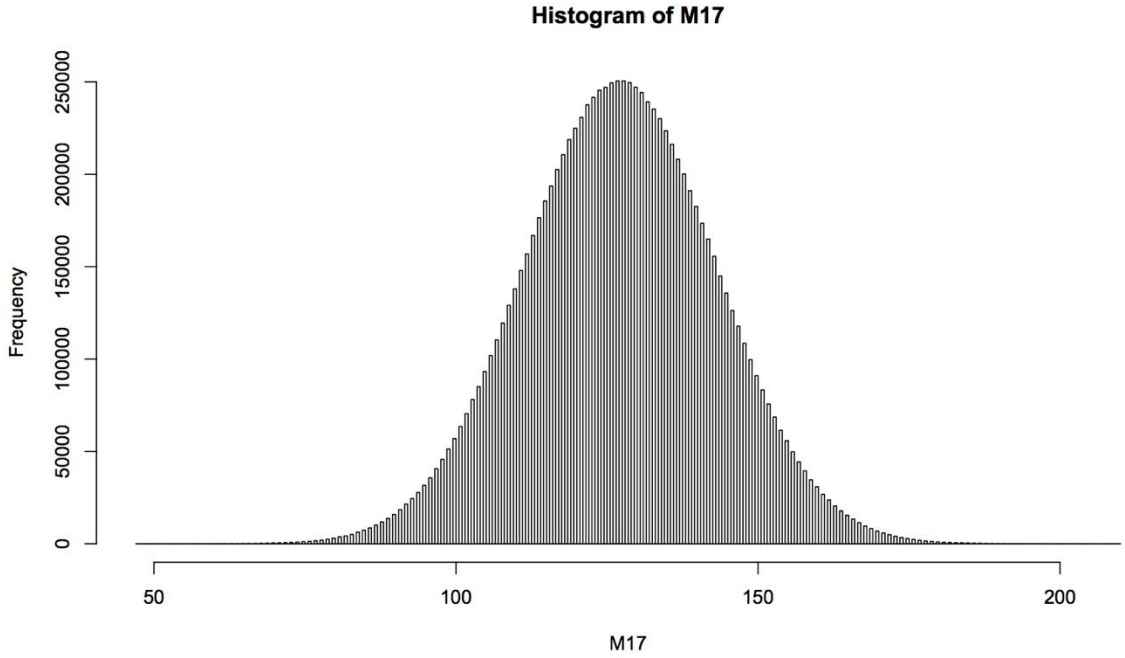


Figure c: M17 data distribution frequencies, per one million bits

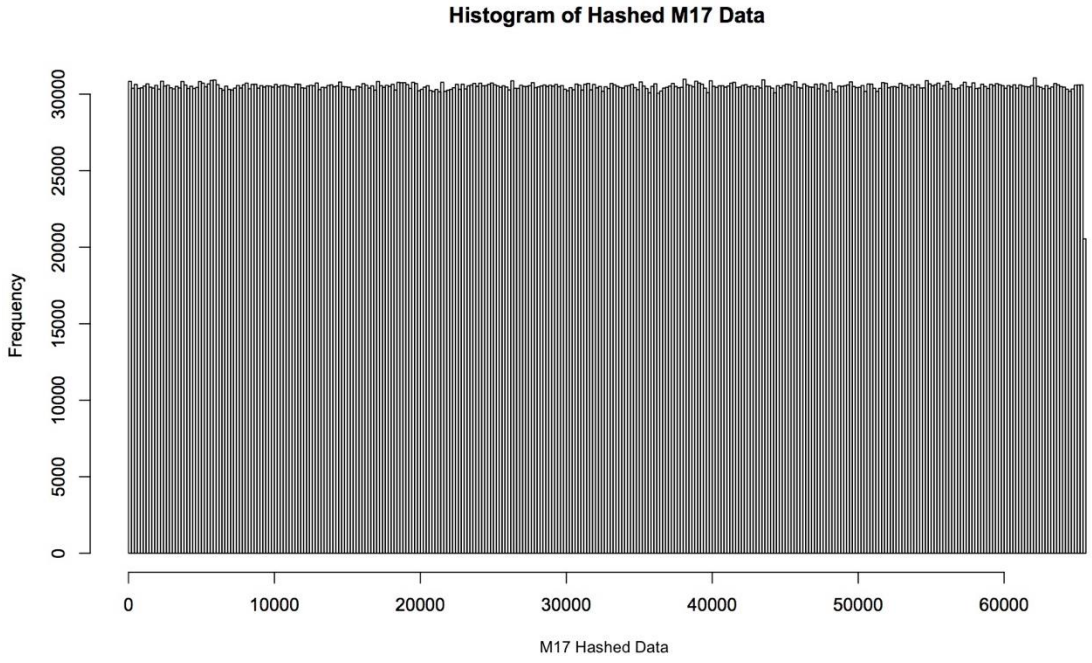


Figure d: Hashed M17 data distribution frequencies, per one million bits.

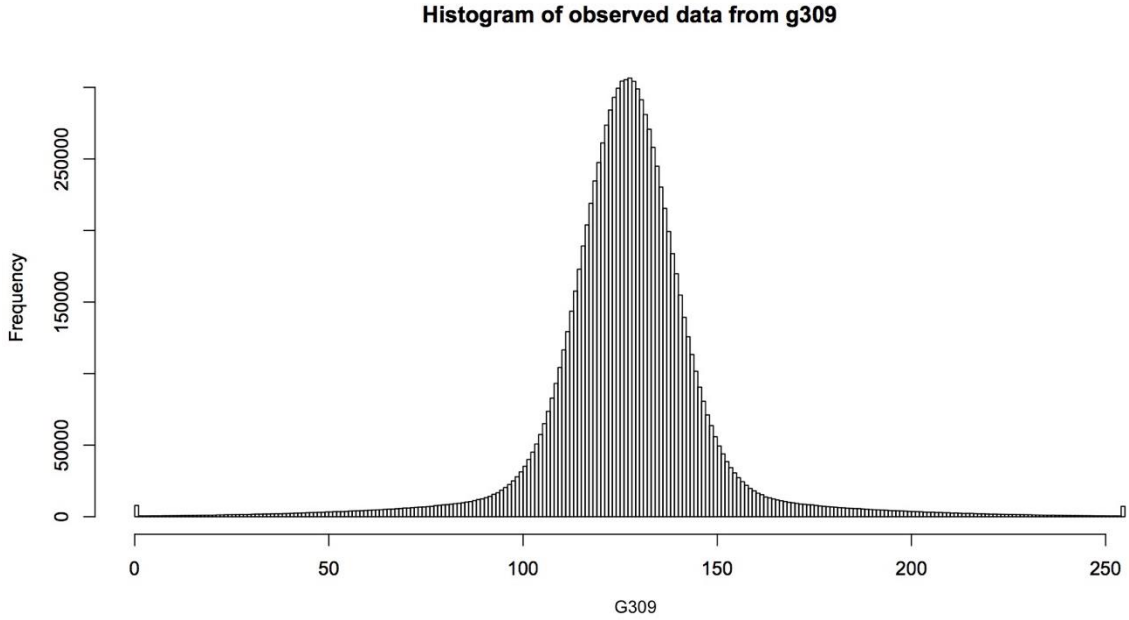


Figure e: G309 data distribution frequencies, per one million bits.

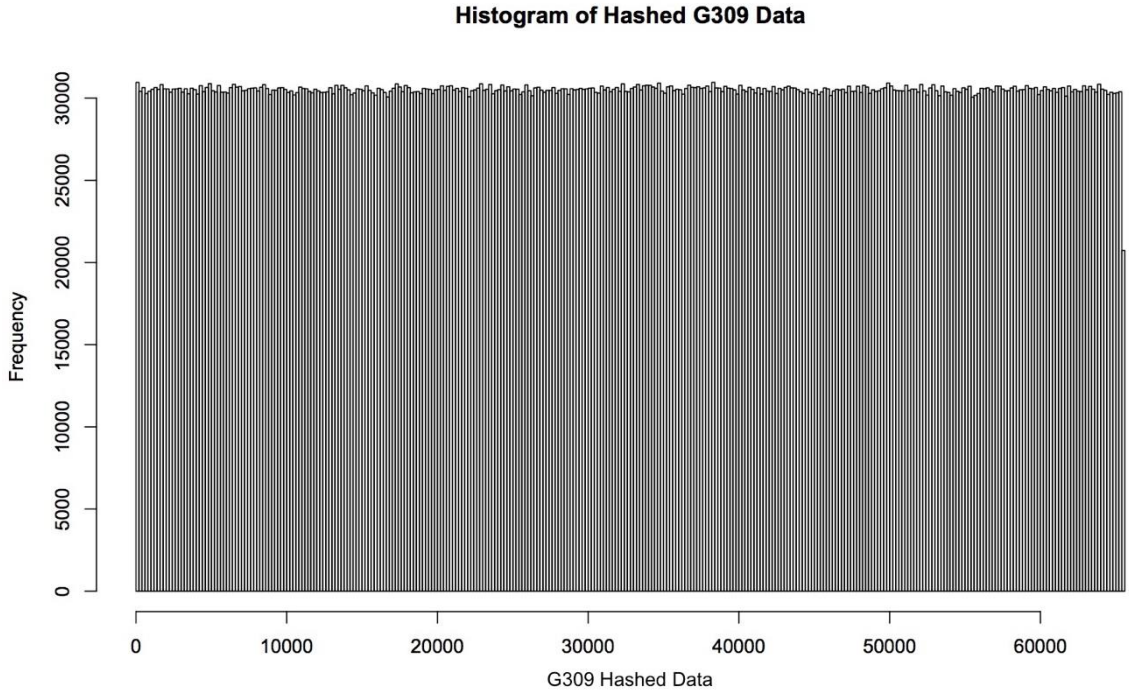


Figure f: Hashed G309 data distribution frequencies, per one million bits.

Based on the results of testing in the *randtests* suite, a second set of testing was conducted using the NIST Statistical Test Suite (Rukhin et al., 2010), which conducts 15 tests for randomness in binary data. The binary files input to this program were the same ones used for the testing in R, and the bitstream length was set to $n = 6{\times}10^6$ for 256 streams of data.

Table 3 gives the results of testing in the NIST STS. All data sets passed all 15 of the tests for randomness, with 97% or more of the streams passing each. For all data sets the results are within a few percentage points of one another, suggesting highly comparable values. For tests such as the non-periodic template matching test, which returned multiple results for each data set, the mean value was calculated from all returned values for that test.

Table 3: Results from testing in the NIST Statistical Test Suite (4 d.p.)

Test	*M17*		*G309*		*Control*	
	p-val	*%*	*p-val*	*%*	*p-val*	*%*
Frequency	0.7637	99.6094	0.6828	98.8281	0.0835	99.6093
Block Frequency	0.3012	98.0469	0.4484	98.4375	0.8237	98.8281
Cumulative Sums	0.7455	100	0.7065	99.2188	0.5834	99.4141
Runs	0.4711	98.8281	0.6993	98.4375	0.6993	98.8281
Longest Run of 1s	0.5022	97.2656	0.7637	99.2188	0.4559	100
Rank	0.9769	99.2188	0.5667	98.8281	0.1167	99.6093
DFT	0.1681	98.4375	0.2954	99.6094	0.0989	99.2188
Non-periodic Template Matching	0.4805	98.9627	0.4974	98.9390	0.5262	98.9733
Overlapping Template Matching	0.1038	98.0469	0.4788	99.2188	0.5194	98.0469
Universal Statistical	0.0815	99.2188	0.9114	99.2188	0.2320	98.4375
Approximate Entropy	0.3191	98.4375	0.5914	100	0.9114	97.6563
Random Excursions	0.5232	99.0783	0.5166	99.2477	0.4923	98.2981
Random Excursions Variant	0.4301	99.2832	0.6290	98.9712	0.4117	98.9306
Serial	0.3169	99.2188	0.6696	99.2188	0.4541	99.2188
Linear Complexity	0.5667	98.0469	0.8092	98.8281	0.2272	99.2188

Figure G gives the graphed percentages of the NIST STS results for each of the data sources. The overall mean of the percentage of bitstreams which pass the tests for the two celestial sources is within 0.02% of the control group, with 98.9% of the 512 bitstreams passing the tests.

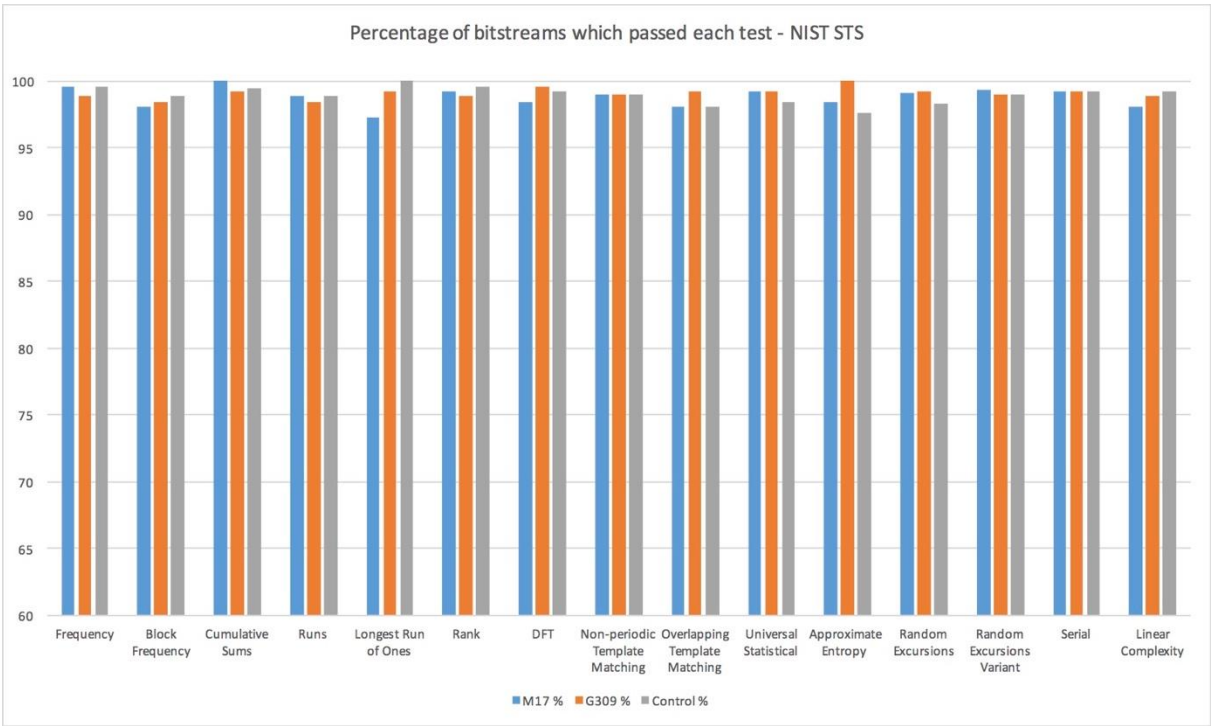


Figure g: Percentage of bitstreams which passed the NIST testing for each data source.

The results of the testing suggest that data gathered through radio astronomy may present a viable option for use as seeds for cryptographic application. The wide variety in data due to fluctuations in machinery, inconsistent

radiation from sources, and interference from satellites and other space junk offers a continuous stream of irreproducible random bits. The time taken to gather the data used in the testing, approximately 400MB worth for each source, was approximately one minute per source. The resulting performance of the data with the SHA-256 algorithm shows it may be a viable option for security applications. As such, it offers a new, rapid and efficient method of gathering irreproducible seeding for random number generation.

CONCLUSION

In this paper we have presented an alternative method for the collection of seed data for random number generators. Utilising the inherent randomness and irreproducibility of radio signal data from celestial sources presents what our results appear to show is a viable method for collecting vast amounts of seed data for use in RNG. The data sets tested all offered high performance levels in the statistical tests for randomness, over long period bitstreams. This suggests that astronomical data retrieved from celestial sources presents a viable option for use in implementing secure systems, and cryptographic functions such as SHA-256. With the ever increasing demand for secure systems, the need for seed data for random numbers is growing rapidly and our results suggest the large volume of data that is available through radio astronomy offers a scheme for addressing this growing demand.

Further research is necessary to determine the most effective use of this type of astronomical data in cryptographic applications. Examination of other sources to examine the best types of celestial events to collect seed data from, as well as collecting and comparing data from other radio telescopes, would be a prudent next step, as would testing the astronomical data with multiple different RNGs for performance. However, the data presented in this paper offers a feasible beginning to such research.

Acknowledgements

We would like to thank the Institute for Radio Astronomy and Space Research at Auckland University of Technology, for the use of the 30m Warkworth Radio Telescope for the collection of the data used in this research.

REFERENCES

Akhshani, A., Akhavan, A., Mobaraki, A., Lim, S. ., & Hassan, Z. (2014). Pseudo random number generator based on quantum chaotic map. *Communications in Nonlinear Science and Numerical Simulation*, *19*(1), 101–111. doi:10.1016/j.cnsns.2013.06.017

Applegate, M. J., Thomas, O., Dynes, J. F., Yuan, Z. L., Ritchie, D. A., & Shields, A. J. (2015). Efficient and robust quantum random number generation by photon number detection. *Applied Physics Letters*, *107*(7), 071106. doi:10.1063/1.4928732

Bartels, R. (1982). The rank version of von Neumann's ratio test for randomness. *Journal of the American Statistical Association*, *77*(377), 40-46.

Burke, B. F., & Graham-Smith, F. (2002). *An introduction to radio astronomy 2ed* (2nd ed.). Cambridge, UK: Cambridge University Press.

Barker, E. B., & Kelsey, J. M. (2015). *Recommendation for random number generation using deterministic random bit generators, (NIST 800-90A rev1)*. Retrieved September 3, 2016, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

Campbell, D. B. (2002). Measurement in Radio Astronomy. *Single-Dish Radio Astronomy: Techniques and Applications*, *278*, 84–85. Retrieved September 17, 2016 from http://adsabs.harvard.edu/full/2002ASPC..278...81C

Cicek, I., Pusane, A. E., & Dundar, G. (2014). A novel design method for discrete time chaos based true random number generators. *Integration, the VLSI Journal*, *47*(1), 38–47. doi:10.1016/j.vlsi.2013.06.003

Cox, D. R., & Stuart, A. (1955). Some quick sign tests for trend in location and dispersion. *Biometrika*, *42*(1/2), 80-95.

Dang, Q. H. (2015). *Secure hash standard (FIPS 180)* (4). Retrieved August 18, 2016, from http://csrc.nist.gov/publications/ fips/fips180-4/fips-180-4.pdf

Dougherty, S. (2011). *Fundamentals of radio astronomy*. Retrieved September 17, 2016, from http://chime.phas.ubc.ca/workshop_penticton/dougherty_Fundementals_2011.pdf

The Editors of Encyclopædia Britannica (2016). Radio source | astronomy. In *Encyclopædia Britannica*. Retrieved September 17, 2016, from https://www.britannica.com/topic/radio-source

Gentle, J. E. (2006). *Random number generation and Monte Carlo methods*.

Haykin, S. (2009). *Communication systems* (4th ed.). New York: John Wiley & Sons.

Hausser, J., & Strimmer, K. (2009). Entropy inference and the James-Stein Estimator, with application to Nonlinear Gene Association networks. *Journal of Machine Learning Research*, *10*(Jul), 1469–1484. Retrieved September 18, 2016, from http://www.jmlr.org/papers/v10/hausser09a.html

Hsu, H. P. (2013). *Schaum's outline of signals and systems, 3rd edition* (Third ed.). United States: McGraw-Hill Professional.

Jansky, C. M., Jr. (1979). My Brother Karl Jansky and his Discovery of Radio Waves from Beyond the Earth. *Cosmic Search*, *1*(4), 12. Retrieved September 16, 2016, from http://www.bigear.org/CSMO/HTML/CS04/cs04p12.htm

Junklewitz, H. (2014). *Statistical inference in Radio Astronomy*. Retrieved September 18, 2016, from https://edoc.ub.uni-muenchen.de/17745/1/Junklewitz_Henrik.pdf

Lo Re, G., Milazzo, F., & Ortolani, M. (2014). Secure random number generation in wireless sensor networks. *Concurrency and Computation: Practice and Experience*, *27*(15), 3842–3862. doi:10.1002/cpe.3311

Lunghi, T., Brask, J. B., Lim, C. C. W., Lavigne, Q., Bowles, J., Martin, A., … Brunner, N. (2015). Self-testing quantum random number generator. *Physical Review Letters*, *114*(15), doi:10.1103/physrevlett.114.150501

Lynnyk, V., Sakamoto, N., & Čelikovský, S. (2015). Pseudo random number generator based on the generalized Lorenz chaotic system. *4th IFAC Conference on Analysis and Control of Chaotic Systems CHAOS 2015*, *48*(18), 257–261. doi:10.1016/j.ifacol.2015.11.046

Mateus, A., & Caeiro, F. (2014). An R implementation of several Randomness Tests. *AIP Conf. Proc*, *1618*, 531–534.

McLean, G., & Ministry of Culture and Heritage. (2013, September 3). Warkworth Satellite Earth Station. Retrieved September 18, 2016, from NZ History, http://www.nzhistory.net.nz/media/photo/warkworth-satellite-earth-station

Moore, G. H., & Wallis, W. A. (1943). Time series significance tests based on signs of differences. *Journal of the American Statistical Association*, *38*(222), 153-164.

Murphy, K. (2010, November 19). New Recipe for Famous Dish. Retrieved September 18, 2016, from Telecom NZ Media Releases, https://archive.is/oYVP

Pestalozzi, A. M. R., & Chrysostomou. (2005). *The General Catalogue of 6.7 GHz Methanol Masers in the Galaxy*. Retrieved September 18, 2016, from http://www.lpi.usra.edu/meetings/ppv2005/pdf/8130.pdf

Phillips, C. J., Norris, R. P., Ellingsen, S. P., & McCulloch, P. M. (1998). Methanol masers and their environment at high resolution. *Monthly Notices of the Royal Astronomical Society*, *300*(4), 1131–1157. doi:10.1046/j.1365-8711.1998.t01-1-01979.x

Povich, M. S., Stone, J. M., Churchwell, E., Zweibel, E. G., Wolfire, M. G., Babler, B. L., … Whitney, B. A. (2007). A Multiwavelength study of M17: The spectral energy distribution and PAH emission morphology of a massive Star Formation region. *The Astrophysical Journal*, *660*(1), 346–362. doi:10.1086/513073

Rukhin, A., Sota, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., … Vo, S. (2010, April). *A statistical test suite for random and pseudorandom number generators for cryptographic applications* (1a). Retrieved August 10, 2016, from http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf

Shuch, P. H. (2013, August 9). Significant radio astronomy frequencies. Retrieved September 20, 2016, from http://www.setileague.org/articles/protectd.htm

Wald, A., & Wolfowitz, J. (1940). On a test whether two samples are from the same population. *The Annals of Mathematical Statistics*, *11*(2), 147-162.

West, N. (2006). GNU Radio Companion (GRC). Retrieved August 8, 2016, from http://gnuradio.org/redmine/projects/gnuradio/wiki/GNURadioCompanion

Woodburn, L., Natusch, T., Weston, S., Thomasson, P., Godwin, M., Granet, C., & Gulyaev, S. (2015). Conversion of a New Zealand 30-Metre telecommunications antenna into a radio telescope | Cambridge core. *Publications of the Astronomical Society of Australia*, *32*, doi:10.1017/pasa.2015.13

A PRIVACY GAP AROUND THE INTERNET OF THINGS FOR OPEN-SOURCE PROJECTS

Brian Cusack, Reza Khaleghparast
Digital Forensic Research Laboratories, AUT
brian.cusack@aut.ac.nz, reza.khaleghparast @aut.ac.nz

Abstract

The Internet of Things (IoT) is having a more important role in the everyday lives of people. The distribution of connectivity across social and personal interaction discloses personalised information and gives access to a sphere of sensitivities that were previously masked. Privacy measures and security to protect personal sensitivities are weak and in their infancy. In this paper we review the issue of privacy in the context of IoT open-source projects, and the IoT security concerns. A proposal is made to create a privacy bubble around the interoperability of devices and systems and a filter layer to mitigate the exploitation of personal and private information by marketing companies.

Keywords:
IoT, Privacy, Security, Risk, Mitigation

INTRODUCTION

The rapid development of technical capability to sponsor the Internet of Things (IoT) has also impacted the daily lives of millions of people. The ability for devices and applications to provide personal services for millions of people on a moment by moment basis, has also removed immediately barriers from personal choices, behaviours and habits. The rich information around individuals opens new marketing opportunities and information opportunities for third-party exploitation. The question of privacy, concerns access to personal information. In the case of IoT private information has the same status as any information and can become readily available to multiple layers of interested parties (Weber, 2010). The bigger issue is that much of this information can be collected unknown to the end user of the IoT. The concept of the smart home, the smart car, the smart phone and other technologies, has introduced a relationship where the gap between the human and the technology is narrowed. Every movement, motion and breath of life of the human can be monitored by sensor networks and transmitted across multiple layers of interested parties. In a medical applications this may be immensely beneficial (Wan et al., 2013). However, the human may resist when they are bombarded by multiple advertising campaigns driven by harvested data from behavioural sensors and the invitation materialize in their weakest and strongest emotional moments. Privacy and privacy protection is hence a central concern when developing open source projects.

Challenges however arise in terms of scalability. IoT applications that require large numbers of devices are often difficult to implement because of the restrictions on time, memory, processing, and energy constraints (Tan, 2011). For example, calculation of daily temperature variations around all of the country may require millions of devices and result in unmanageable amounts of data. The deployment of hardware in IoT often has different operating characteristics, such as sampling rates and error distributions, interoperability protocols and complex sensors and actuators components. All of these factors contribute to the formation of the heterogeneous network of IoT in which the data of IoT will also be heterogeneous and require a multiplicity of management systems. IoT not only has the same security issues as sensor networks, mobile communications networks and the Internet, but also has its other vulnerabilities such as privacy protection, different authentication compliance, access control network configuration issues, information storage and management problems, and so on. Data and privacy protection is one of the application challenges of IoT (Chen et al, 2009). One risk is of the IoT security is from itself, and the other one comes from the related technology of construction and implementation of the network functions. IoT itself is the integration of multiple heterogeneous networks. There are compatibility issues between different networks and they are prone to security issues. For example, it is difficult to establish the junction of relationship as the relationship of trust between nodes is constantly changing and this requires a dynamic solution (Jing et al., 2014). The application of IoT directly connects with people's everyday lives and has application in many different fields, for example: patient's remote monitoring, energy consumption control, traffic control, smart parking systems, inventory management, production chains, customization of the shopping at the supermarket, and civil protection. For all of the uses, users require the protection of their personal information related to their movements, habits and

interactions with other people. They also require their privacy be guaranteed. In the literature, there are some attempts to address such problems (eg. Fabian and Gunther, 2009).

VULNERABILITIES OF IoT

IoT must ensure the security of all layers. In addition, IoT security should also include the security of whole system crossing the perception layer, transportation layer and application layer. The Perception layer includes RFID security, WSNs security, RSN security and any others. Transportation layer includes access network security, core network security and local network security. In addition there are application layer security concerns such as, 3G access network security, Ad-Hoc network security, WiFi security and so on. Different network transmission has different technology. The Application layer includes the application support layer and specific IoT applications. The security in the support layer includes middleware technology security, cloud computing platform security and so on. IoT applications in different industries have different application requirements but each requires similar diligence for protective mechanisms (Suo et al., 2013).
IoT divides into three layers: the perception layer, the transportation layer and the application layer (Tsai et al., 2014). Each of these layers further resolves into layer elements that differentiate the service provided. In figure 1 a full summary is made of the security architecture for IoT.

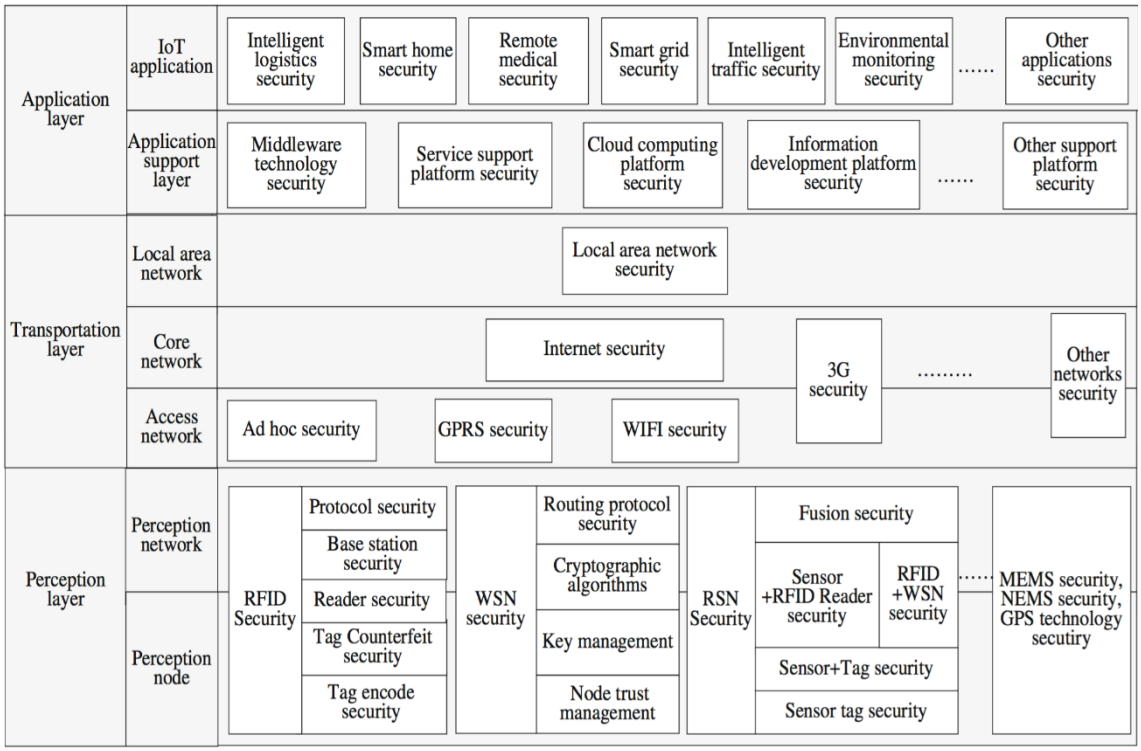


Figure 1. Security architecture of IoT (Tsai et al., 2014).

The technical architecture of the IoT has an impact on the security and privacy of the participating stakeholders. Privacy includes the concealment of personal information as well as the ability to control what happens with the information (De Turck et al., 2002; Tan and Han, 2011). The right to privacy can be considered as either a basic and inalienable human right, or as a personal right or possession. The attribution of tags to objects may not be known to users, and there may not be an acoustic or visual signal to draw the attention of the object's user. Thereby, individuals can be followed without them knowing. Electronic traces are left of their data and movement that remain in memory and in cyber- space. Further aggravating the problem (Ukil et al., 2014), it is not anymore only the authorities that are interested in collecting the respective data, but also private actors such as marketing enterprises. Since business processes are concerned, a high degree of reliability is needed. In the literature, the following security and privacy requirements are described (Akyildiz et al., 2002; Evans and Eyers, 2012):

- Resilience to attacks: The system has to avoid single points of failure and should adjust itself to node failures.

- Data authentication: As a principle, retrieved address and object information must be authenticated.
- Access control: Information providers must be able to implement access control on the data provided.
- Client privacy: Measures need to be taken that only the information provider is able to infer from observing the use of the lookup system related to a specific customer; at least, inference should be very hard to conduct.

These requirements begin to shape the design of a bubble of protection that can be created around a participant in an IoT environment. However further work is required to have policies for the erasure of data that relates to personal activity, and the protection of all data from parties who wish to exploit it for economic gain (Juels, 2006; Aleaide et al., 2013).

PRIVACY CONCERNS OF IoT

The fulfilment of customer privacy requirements is a challenging problem. A number of technologies have been developed in order to achieve information privacy goals. These Privacy Enhancing Technologies (PET) can be described in short as follows (Fabian et al., 2007; Haitao and Ting, 2012):

- Virtual Private Networks (VPN) are extranets established by close groups of business partners. As only partners have access, they promise to be confidential and have integrity. However, this solution does not allow for a dynamic global information exchange and is impractical with regard to third parties beyond the borders of the extranet.
- Transport Layer Security (TLS), based on an appropriate global trust structure, could also improve confidentiality and integrity of the IoT. However, as each ONS delegation step requires a new TLS connection, the search of information would be negatively affected by many additional layers.
- DNS Security Extensions (DNSSEC) make use of public-key cryptography to sign resource records in order to guarantee origin authenticity and integrity of delivered information. However, DNSSEC could only assure global ONS information authenticity if the entire Internet community adopts it.
- Onion Routing encrypts and mixes Internet traffic from many different sources, i.e. data is wrapped into multiple encryption layers, using the public keys of the onion routers on the transmission path. This process would impede matching a particular Internet Protocol packet to a particular source. However, onion routing increases waiting times and thereby results in performance issues.
- Private Information Retrieval (PIR) systems conceal which customer is interested in which information, once the EPCIS have been located. However, problems of scalability and key management, as well as performance issues would arise in a globally accessible system such as the ONS, which makes this method impractical.
- A further method to increase security and privacy are Peer- to-Peer (P2P) systems, which generally show good scalability and performance in the applications.

The following are reviewed literature provides further information regarding the privacy elements in a security bubble for an IoT user. In Gurses et al. (2006) a data tagging for managing privacy in IoT is proposed. Using techniques taken from the Information Flow Control, data representing network events can be tagged with several privacy properties; such tags allow the system to reason about the flows of data and preserve the privacy of individuals. Although exploiting tagging within resource-constrained sensor nodes may not be a viable solution because tags may be too large with respect to the data size and sensitivity, therefore they generate an excessive overhead. Clearly, in this case it is not suitable for IoT. In Huang et al. (2012) a user-controlled privacy-preserved access control protocol is proposed, based on context-aware and anonymity privacy policies. The privacy protection mechanisms are investigated in the research and the users can control which of their personal data is being collected and accessed, who is collecting and accessing such data, and when this happens. In Cao et al., (2011) it is presented Continuously Anonymizing streaming data via adaptive clustering (CASTLE). It is a cluster-based scheme which ensures anonymity, freshness, and delay constraints on data streams, thus enhancing those privacy preserving techniques (e.g., k-anonymity) that are designed for static data sets and not for continuous, unbounded, and transient streams.
In Aleaide (2013), the traditional privacy mechanisms are divided into two categories: Discretionary Access and Limited Access. The former addresses the minimum privacy risks, in order to prevent the disclosure or the cloning of sensitive data; whereas the latter aims at limiting the security access to avoid malicious unauthorized attacks.

Blass et al. (2011) analyses the privacy risk that occurs when a static domain name is assigned to a specified IoT node. In this work the authors propose a privacy protection enhanced DNS (Domain Name System) for smart devices, which can authenticate the original user's identity and reject illegal access to the smart device. The scheme is compatible with widely used DNS and DNSSEC (Domain Name System Security Extensions) protocols. In Elkhiyaoui et al., (2012) a fully decentralized anonymous authentication protocol for privacy-preserving target-driven IoT applications is presented. Such a proposal is based on a multi-show credential system where different showings of the same credential cannot be linked together, therefore avoiding the generating keys to be discovered. The system defines two possible roles for participant nodes. There are users, which represent the nodes originating the data, and data collectors, which are responsible for gathering the data from authorized users. Users can anonymously and unlinkably authenticate themselves in front of data collectors proving the owning of a valid Anonymous Access credential (AAC) encoding a particular set of attributes, established by the system itself. The protocol is divided in three phases: set-up, user registration, during which users obtain Anonymous Access Credentials, and Credential Proving, during which users prove the possession of a valid AAC to a data collector. Such a protocol guarantees: user anonymity, AAC un-linkability (no Data Collector or set of colluding Data Collectors can link two transactions to the same User), resistance to user impersonation, faulty and selfish nodes, nodes hindering the efficiency, and adversary controlling the Data Collectors. Moreover, such a system relies on a fully distributed approach, thus avoiding single point of failure issues. Sunmaker et al. (2010), starting from the privacy preserving data mining (PPDM) techniques, and aims at minimizing the sensitive data disclosure probability and the sensitive content analysis. In such a work, the user privacy awareness issue is addressed, proposing a privacy management scheme which enables the user to estimate the risk of sharing sensitive data. It also aims at developing a robust sensitivity detection system, able to quantify the privacy content of the information (Hachem et al., 2011).

USE CASES

Amazon Echo is a small hands-free wireless speaker that is controlled by voice. The voice command technology called "Alexa," that is inside Amazon Echo is now available on other devices, including the Amazon Fire TV and the Amazon Echo Dot and Amazon Tap. These devices exhibit state-of-the-art artificial intelligence that facilitates human requirements and human interaction. The concept is grown from a belief that all of human experience may be represented by artificial intelligence that is supported by information technology and physical devices. The information architecture shows voice command technology that allows the user to manage, control and demand personal experiences. The information requirements are managed by sensors, processes and mediating software to assure the end user has full connectivity. The IoT systems architecture is design for interoperability across different requirements so that the system may be implemented in a home, a motor vehicle, a business, or any other social situation. It allows artificial intelligence to control the requirements to satisfy the experience. The concept is that Alexa is a human friendly personification that access an access point to a multitude of systems and services. It only requires "invocation words" that tell Alexa what Skill or service that is to be activated. The communication requires a person to say things like "Alexa, ask Scout to arm my security system" or "Alexa, ask Fitbit what my resting heart rate is." (Wan et al., 2011).

These use cases of IoT are being developed as open source projects. The developers are working to make it easier for third-parties to create Skills that don't require invocation words at all. For instance, smart home gadgets that create Alexa Skills using Amazon's open application programming interface (API) will get to use existing code and standardized Alexa vocabulary for things like lights, switches, and thermostats. In this way the concept of the smart home can be built around an IoT plan and human experience may be captured within the technological confines. Software such as Alexa are leading the way for creative developers to design and implement this new future. To utilize these technologies the user says the word "Alexa," and from then on the automation monitors everything in around the human experience. The concept is strong but the privacy issues still remain. Questions arise regarding the supervision of these types of technologies. What happens if Echo is left unsupervised? The technologies are not only smart in the sense that they may be communicated to deliver actions services and experiences, but they also open the user to a global communication world through the IoT. The security wireless signals is notoriously vulnerable to external influence making the human experience vulnerable to unintended failures. Similarly the information generated regarding human behaviour may be recorded and transmitted for commercial interests. Marketing for example may become more targeted and better represent a requirement within the human life world. To some this may be a benefit but to others it may be deemed invasive (Wang and Wen, 2011).

Commercial interests are in the business of selling everything humans need from clothes to groceries, electronics goods, gifts and so on. To do that better and more efficiently, they need to know more about their users, their friends, their family and social networks. By knowing more about the users' information, they can better suggest new experiences for purchase, and to exactly time when to make the offer. Some of the characteristics collected by Alexa (through Echo) are:

- **Unique home occupants:** Echo is able to distinguish between the numbers of unique voices in a home and to map these voices onto registered users and images of people in the home.
- **Home visitors:** Echo can identify and monitor who comes to a home. This is for intended and unintended visitors, such as friends and burglars.
- **Gender and age:** From voice and photographic data trapped by Echo gender and age may be estimated.
- **Happiness, sadness, anger:** emotional states can be monitored and moods such as happiness and sadness, anger and delight, and so on can be instantaneously recorded and transmitted.
- **Who is home:** Echo can learn patterns of behaviour and detect movement within a home. From this learning real-time being is established and also all the interactions are accessible.
- **What we watch and listen to:** Echo can hear everything that is going on that includes preferences for television channels, music, statements about products being used, political statements, personal relationship statements, and so on, and so on. Such data provides up-to-date information on personal preferences although the human may not be conscious that these things are being recorded and matched against patterns.

To create a privacy bubble around the human some security features have already been built into Alexa. However the technology can do a lot if left unsupervised that not only includes cleaning the house but also being responsive to multiple layers of communication networks from outside of the home. One of the things that has been done to quell some of the automation fears is to add a variety of voice controls that put the technology into various sleep modes. These types of controls are necessary if the human is to maintain control over their private information that includes movements, locations, emotions, habits, and many other personalised information is that would not normally be made public. The intrusion of commercial interest into the spaces and the precision with which generalizations can be made is a new phenomenon. These are matters that the IoT has introduced (Yang and Fang, 2011; Jing et al., 2014).

Privacy security bubble

Our advocacy in this paper, after the review of the relevant literature, is to have a proximity around technology in which the user has protection for the use of their information. To achieve this the user must first be given the rights of ownership to their own information. At present within the multiple layers of system the content created within a word processor for example may have multiple ownership challenges. The user and creator of the content may not be aware of these competing digital rights that are behind what they are doing. In a similar sense people using robot vacuum cleaners, automated software on their mobile phone, motor vehicles, hospital services, financial services, and so on, may not be aware, and in effect may not have the digital rights to the content that they have created with the efficacy of their presence and actions. The privacy requirement in IoT is currently inadequately unaddressed and there is a wide set of research issues yet to be investigated. Privacy policies starting from a well-defined model and the correspondent development of policies that adequately deal with the scalability and the dynamic environment characterizes IoT scenarios are required. Capturing privacy requirements in the very early stages of project development is essential for creating public confidence and the adoption of novel IoT systems. Private enterprises using IoT technology will have to include these requirements into their risk management plans for governing the business activities in general.

The IoT is susceptible to intentional and unintentional compromise of information. The complexity of IoT security was shown in figure 1. Usual Internet services and other communication services are familiar with protection for the transport and application layers. However the IoT introduces the concept of the perception layer. The perception layer is made up of networks and nodes that are both social and machine. The mixing of these two elements in the perception concept introduces an ambiguity that cannot be easily addressed. The issues of ownership around information that is mediated and hosted by machines is much more difficult than the adjudication of common property rights. The owners of the machines can lay claim to content, the owners of the software can lay claim to content, and the user of the systems and the machines may not be in a position to realise that data has been created regarding their own behaviours. The user of IoT experiences and services may also not be in a position to challenge the owners of the technology and the hosted services. This therefore creates an imbalance of power that requires redress in the fashion that we suggest whereby the user and participant in the IoT environment is given a proximity measure in which they hold a primary ownership of the data. The management of such a privacy and security bubble can be done by honouring the proximity metric and enforcing it transaction by transaction. This will require the

partitioning of data into private and public categories at the point and within the modes of production. The proximity measure can be enforced as a contractual arrangement and all the other interested parties must negotiate with the human factor for access to any data created within the proximity boundary or from instances within the proximity boundary. At present such arrangements are not in place and there is no boundary for privacy. The privacy requirement in IoT is currently emerging issue by issue and it will only be when developers are impacted financially by end user resistance that the problem will be taken seriously. Consideration is required for building the privacy requirement into the front end of a project as a bubble of protection for the end-user. Suitable survey of potential end users and full HCI analysis are necessary components of every project. Human factor vulnerability and the potential exploitation of the personal data can be treated with these measures.

CONCLUSION

In this paper we have reviewed literature that addresses the security and privacy issues in the IoT. The use case of Amazon's Alexa devices illustrates open source projects that are currently active and developing. Our consideration is to assure that there is a bubble of security and privacy around the user experience so that they are adequately protected from exploitation and manipulation by multiple parties who may get access through the technology. It would be reasonable to have legislation that prescribes a proximity in terms of a physical metric around and IoT user, and anything within that proximity is owned by the user. This would mean that advertising companies and others who seek to exploit this information would have to gain permission from the owner of the information before they use it. In a hospital situation the patient already signs away these rights but with a mobile device or the sensor systems within a motor vehicle, the user is not aware of where their data is going, who was looking at it and who may have access to use it. Privacy rights advocates have called for limits on the information that companies can collect and use, but the truth is that our privacy is already being breached on a daily basis. However, that does not mean that we should voluntarily give up more of our privacy through the purchasing of devices such as the Alexa (Echo Dot), automated motor vehicles, or Pokémon applications.

REFERENCES

Akyildiz IF, Su W, Sankarasubramaniam Y, (2002). Wireless sensor networks: a survey. Computer networks 38:393-422 (2002)

Alcaide A, Palomar E, Montero-Castillo J et al. (2013). Anonymous authentication for privacy-preserving IoT target-driven applications. Computers & Security 37:111-123.

Blass E-O, Elkhiyaoui K, Molva R. (2011). Tracker: security and privacy for RFID-based supply chains. In: In NDSS'11, 18th Annual Network and Distributed System Security Symposium, 6-9 February.

Cao J, Carminati B, Ferrari E et al. Castle. (2011). Continuously anonymizing data streams. IEEE Transactions on Dependable and Secure Computing 8:337-352.

Chen M, Kwon T, Mao S. (2009). Spatial-Temporal relation-based Energy-Efficient Reliable routing protocol in wireless sensor networks. International Journal of Sensor Networks 5:129-141.

De Turck F, Vanhastel S, Volckaert B. (2002). A generic middleware-based platform for scalable cluster computing. Future Generation Computer Systems 18:549-560.

Elkhiyaoui K, Blass E-O, Molva R (2012). CHECKER: On-site checking in RFID-based supply chains. In: Proceedings of the fifth ACM conference on security and privacy in wireless and mobile networks. ACM, p 173-184.

Evans D, Eyers D. (2012). Efficient data tagging for managing privacy in the internet of things. In: Green Computing and Communications (GreenCom), 2012 IEEE International Conference on. IEEE, p 244-248.

Fabian B, Günther O. (2009). Security challenges of the EPCglobal network. Communications of the ACM 52:121-125.

Fabian B, Gunther O. (2007). Distributed ONS and its Impact on Privacy. In: 2007 IEEE International Conference on Communications. IEEE, p 1223-1228.

Gürses S, Berendt B, Santen T (2006). Multilateral security requirements analysis for preserving privacy in ubiquitous environments. In: Proceedings of the UKDU Workshop. p 51-64.

Hachem S, Teixeira T, Issarny V (2011). Ontologies for the internet of things. In: Proceedings of the 8th Middleware Doctoral Symposium. ACM, p 3.

Haitao LBCHW, Ying F (2012). Security Analysis and Security Model Research on IOT. Computer & Digital Engineering 11:006.

Hamad F, Smalov L, James A (2009). Energy-aware Security in M-Commerce and the Internet of Things. IETE Technical review 26:357-362.

Huang X, Fu R, Chen B et al. (2012) User interactive internet of things privacy preserved access control. In: Internet Technology and Secured Transactions, 2012 International Conference for. IEEE, p 597-602.
Itu-T Y (2009). Overview of ubiquitous networking and of its support in NGN. ITU-T Recommendation.
Jing Q, Vasilakos AV, Wan J. (2014). Security of the internet of things: Perspectives and challenges. Wireless Networks 20:2481-2501.
Juels A (2006). RFID security and privacy: A research survey. IEEE journal on selected areas in communications 24:381-394.
Sundmaeker H, Guillemin P, Friess P et al. (2010) Vision and challenges for realising the Internet of Things. Cluster of European Research Projects on the Internet of Things, European Commision.
Suo H, Liu Z, Wan J et al. (2013). Security and privacy in mobile cloud computing. In: 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE, p 655-659.
Tan Y, Han J (2011). Service-oriented middleware model for internet of things. Computer Science 38.
Tsai C-W, Lai C-F, Vasilakos AV (2014). Future Internet of Things: open issues and challenges. Wireless Networks 20:2201-2217.
Ukil A, Bandyopadhyay S, Pal A (2014). Iot-privacy: To be private or not to be private. In: Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on. IEEE, p 123-124.
Wan J, Chen M, Xia F et al. (2013). From machine-to-machine communications towards cyber-physical systems. Comput. Sci. Inf. Syst. 10:1105-1128.
Wan J, Yan H, Suo H et al. (2011). Advances in Cyber-Physical Systems Research. TIIS 5:1891-1908.
Wang Y, Wen Q (2011). A privacy enhanced dns scheme for the internet of things. In: Communication Technology and Application (ICCTA 2011), IET International Conference on. IET, p 699-702.
Weber R. (2010). Internet of Things–New security and privacy challenges. Computer Law & Security Review 26:23-30.
Yang J-C, Fang B-X (2011). Security model and key technologies for the Internet of things. The Journal of China Universities of Posts and Telecommunications 18:109-112.

AN ANALYSIS OF CHOSEN ALARM CODE PIN NUMBERS & THEIR WEAKNESS AGAINST A MODIFIED BRUTE FORCE ATTACK

Alastair Nisbet, Maria Kim
Security & Forensic Research Group
Auckland University of Technology, Auckland, New Zealand
alastair.nisbet@aut.ac.nz, Maria.Kim@corrections.govt.nz

Abstract

Home and commercial alarms are an integral physical security measure that have become so commonplace that little thought is given to the security that they may or may not provide. Whilst the focus has shifted from physical security in the past to cyber security in the present, physical security for protecting assets may be just as important for many business organisations. This research looks at 700 genuine alarm PIN codes chosen by users to arm and disarm alarm systems in a commercial environment. A comparison is made with a study of millions of PIN numbers unrelated to alarms to compare the results in order to allow a prediction of the alarm codes utilised in these systems. Results show that PIN number for alarm codes are often chosen differently than other PIN numbers and an analysis of the alarm codes gives an indication of how users choose codes. The codes are ranked in various groupings and results show that a non-sequential brute force attack against an alarm system using the results of this study greatly reduce the number of codes tried by an attacker before a disarming code is discovered. The results can be used to assist users in choosing codes that are less predictable than the codes that are often chosen today.

Keywords
alarm, PIN, security, crime, brute force attack

INTRODUCTION

Alarm systems are commonplace in business and domestic settings. Basic alarms to protect property have been recorded as early as 386 BC where animals were used to guard valuables and objects and were placed in positions so when disturbed would alert the occupants. Bellis (n.d) states that the history of locks date back approximately 4000 years where a lock was found by archaeologists in the Khorsabad near Nivenah. The use of alarm systems is twofold: to detect and alert the owners of property that a breach has occurred but equally to act as a deterrent to would be offenders. Advertising the presence of an alarm system has shown to be something of a deterrent to potential burglars, meaning often that the potential offenders will move on to a premises that does not have an alarm. The New Zealand Police report that approximately 143 burglaries are committed each day against business and domestic premises, but resolved cases only account for 13% of these break-ins. The effectiveness of an alarm system therefore derives from advertising its presence and ensuring its effectiveness if an offender is detected.

The most common method of authenticating to an alarm system is a code or PIN number. Most alarm systems require a PIN number of at least 4 numbers, with many allowing up to 10 numbers or more. Whilst some alarms have a lockout feature where multiple wrong codes will disable the keypad for a time or set off the alarm, many alarm systems either don't have this feature or do not have the feature enabled. Whilst longer codes are more secure from a brute force attack, most PIN numbers are found to be 4 digits as this is easier to remember than longer numbers and humans are incapable of choosing random numbers which leads to a level of predictability of those PIN numbers (Gutmann,A. Volkamer,M. Renaud,K. 2016). This research looks at the process of conducting an attack utilising a brute force method to find a PIN code for the alarm, but rather than utilising the usual sequential attack beginning at 0000 and incrementing the code by one until successful, known codes are analysed so that the attack can work through the more likely codes first and try the less likely codes last.

There are three different types of codes involved in an alarm system. These are the Master Code, Installer Code and the Standard User Code. According to the Alarm Forum (n.d), the Master Code is a code which is most commonly used and it acts as both a User code to arm and disarm the alarm and to enable resetting of user codes on the alarm system. This code allows full usage however without access right to the alarm system's control panel, which can be performed with Installer Code. This type of code would allow full programming access to change user codes if required (Monitoring Plus, 2006). This privilege is given to the Master code so the user does not need to call the security company every time modification of user codes is required. The standard

NZS2201:2007, the section 5.6.2 explicitly prohibits the reissue of the master code unless there is an extremely unavoidable situation to do so. The user code is the most basic code with very limited access rights and which is used to arm and disarm the system. This code has less privilege compared to the Master Code and the only function of it is to arm and disarm the system.

Figure 1: Standard Alarm System Keypad

Keypads do not place a restriction on using the same number multiple times. Therefore, there are 10,000 possible four digit PIN number combinations from 0000-9999. An intruder may be able to attempt multiple guesses of the PIN number before the alarm is activated. If a sensor is placed so that anyone gaining physical access to the keypad alerts the system by activating the sensor, the intruder may be given a very short time to enter a correct PIN number. This is often no more than 30 seconds before the alarm system responds with a siren and may also dial a predetermined phone number to alert the recipient of the alarm activation. If a keypad is placed where access can be gained without activating a sensor, as is often the case, the intruder may be able to try many thousands of PIN numbers without activating the system. The possibility of an intruder trying seemingly random numbers and finding a correct code in a short space of time is very unlikely. However, if numbers are not chosen randomly but have some meaning to the user or are chosen for reasons that may be common such as easy to remember combinations such as 1234, then the chances of success are greatly increased.

In his research into 3.4 million PIN number in a database constructed from a variety of PIN numbers released onto the Internet, Berry (2012) discovered certain numbers are chosen more frequently than others and argued that people are not particularly strong at choosing a difficult to guess PIN number. The most common numbers that are a variety of different PIN numbers but likely not alarm codes, as Berry was unable to ascertain exactly where they had come from, are shown in table 1. By identifying the most popularly used PIN numbers and performing a brute force attack to the system using these more common PIN numbers first, an intruder may successfully gain entry to the premise in a much shorter time than simply systematically trying every number from 0000 to 9999.

Table 1: Four digit PIN codes most commonly in use (Berry 2012)

Rank	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
PIN	1234	1111	0000	1212	7777	1004	2000	4444	2222	6969	9999	3333	5555	6666	1122	1313	8888	4321	2001	1010
Freq	10	6.0	1.9	1.2	0.75	0.66	0.61	0.53	0.52	0.51	0.45	0.42	0.39	0.39	0.37	0.30	0.30	0.29	0.29	0.28

The following section describes the process of analysing PIN numbers to identify the most common types of numbers and therefore predict what numbers are more likely to be chosen than others.

RESEARCH DESIGN

The researchers were able to obtain 700 genuine and freely chosen 4 digit alarm codes used in businesses in New Zealand and these were used as the dataset for analysis. Experiments by the researcher utilising an alarm keypad and stop watch found on average a person entering a 4 digit PIN number onto a keypad would take approximately 5 seconds per PIN number. If using a brute force attack against a 4 digit PIN number trying all possible 10,000 combinations, it would take an attacker approximately 50,000 seconds, which is 13.9 hours. If the PIN numbers are chosen genuinely at random, then on average the number will be located in half that time.

Rasmussen and Rudmin (2010) point out the problem of people's difficulty with memorising number codes causes problems. Although it is a well-known that longer and more complicated PIN codes are more difficult to guess or crack, the lack of users' ability to memorise more complex passcodes means a tendency to choose numbers that are easy for them to remember and thus easier to guess or predict. Rasmussen and Rudmin (2012) attempted to investigate people's common strategies and difficulties when memorising a PIN number including making a pattern on the keypad rather than remembering a series of numbers.

With this in mind, the focus becomes how best to predict a number or a method used by a user to choose as the code. Whilst some codes are more likely to occur than others, the purpose of this research was to identify what types of codes are more likely to be chosen, and therefore groups of 'likely' codes could be tried first. The brute force attack could therefore begin with the most likely group, move on to the next most likely group and so on until the final most unlikely group was the last to be tried. It was hoped that by analysing the 700 PIN codes, groups of codes could be established greatly speeding up the success of a brute force attack. The first task was to identify the PIN codes that were used multiple times. Initially the study by Berry was used to identify any correlation between his study's findings and the database of alarm codes. A comparison of these codes with the alarm code database found that there was some relationship between the Berry findings and the alarm codes but some specific codes had almost no relationship. For example, Berry found that the number '1234' was utilised over 10% of the time, whereas the alarm database found that it was used for 2 out of the 700 or 0.00314% of the time. However, the use of repeating numbers within the code did occur frequently in the database as Berry had found. Taking into consideration the study and findings of Berry (2012), his category of numbers was used along with two additional categories, those PIN numbers beginning with 19?? and 20?? which may indicate a year of significance to a user. Another category considered was a PIN number which is composed with a sequential number either ascending or descending order. This category was considered due to its relative simplicity for memorising PIN numbers in such characteristics and due to the fact that Berry (2012) has identified 1234 as the most popularly used PIN numbers. Due to this, certain PIN numbers may fall into two categories: such as PIN number 1999. This will fall into a category of a year, and also into a category of PIN number that is composed with two different digits only. The following categories were chosen.

- Category 1: PIN number is composed of four different digits
  - In this category, the code contains numbers that are all unique. That is, no number is repeated in the code but the four numbers will form a certain pattern on the keypad.
- Category 2: PIN number is composed of three different digits
  - In this category, 2 numbers are unique and one other number is repeated. On the keypad, this allows for a code that can fit on a line composed of 3 numbers wide by repeating a number.
- Category 3: PIN number is composed of two different digits
  - In this category there are only 2 numbers and either both are repeated once or one of those numbers is repeated 3 times.
- Category 4: PIN number is composed of one number only
  - In this category, a single number is used and repeated 4 times.
- Category 5: PIN number with 19 or 20
  - In this category, the user has apparently chosen a recent year of significance
- Category 6: PIN number with sequential numbering:
  - In this category, the user has chosen a PIN number with 4 digits in numerical ordering. This can be ascending or descending starting from any digit.

By utilising these 6 broad categories, the numbers that may fit into those categories can be identified and then their frequency in the database found. The first 3 categories focus on patterns that may be identified and therefore more easily remembered. It was noted that there may be some numbers chosen by users for some significance, but that coincidentally fit into a pattern such as a straight line. Additionally, some numbers will fit into more than one category. These are identified and guidelines used to ensure that all numbers appear once in the guideline and are not repeated. The next step in the process is to examine each category and construct more specific sub-categories based on the codes physical appearance on the keypad. The aim of category 1 and 2 is to identify all the possible patterns on a keypad that can be formed.

- Category 1: PIN number is composed of four different digits

1) Square (Four corners)
2) Four digits in the middle of the keypad making a vertical line
3) Diamond shape
4) Rectangle shape
5) L shape in any orientation
6) Reverse L shape in any orientation

7) Y shape

Table 2: Category 1 Number Groupings

Pattern	Number	PIN Number Combination
Square (Four Corners)	24	1397, 1379, 1793, 1739, 1937, 1973 3971, 3791, 3179, 3917, 3719, 3197 9713, 9137, 9317, 9173, 9371, 9731 7139, 7913, 7931, 7391, 7193, 7319
Four digits in middle vertical line	2	2580, 0852
Diamond shape	24	2684, 2648, 2486, 2468, 2846, 2864 6842, 6482, 6248, 6824, 6284, 6426 4268, 4826, 4862, 4683, 4628, 4268 8426, 8264, 8624, 8346, 8462, 842
Rectangle shape	24	1346, 1364, 1463, 1436, 1634, 1643 3461, 3641, 3146, 3614, 3416, 3164 4613, 4136, 4631, 4361, 4163, 4316 6134, 6413, 6314, 6143, 6341, 6431
L shape	16	1478, 2589, 3214, 6547, 9632, 8521, 7896, 4563 8741, 9852, 4123, 7456, 2369, 1258, 6987, 3654
Y shape	24	1358, 1385, 1538, 1583, 1853, 1835 3581, 3851, 3815, 3158, 3185, 3518 5813, 5138, 5381, 5831, 5318, 5183 8135, 8513, 8153, 8315, 8531, 8315
Reverse L shape	16	3698, 2587, 6541, 9874, 8523, 7412, 7896, 4563 8963, 7852, 1456, 4789, 3258, 2147, 6987, 3654

- Category 2: PIN number is composed of three different digits
  1) Vertical line
  2) Horizontal line
  3) Diagonal line

Table 3: Category 2 Number Groupings

Pattern	Number	PIN Number Combination
Vertical Line	24	1147, 1447, 1477, 2258, 2558, 2588, 3369, 3669, 3699 7411, 7441, 7741, 8522, 8552, 8852, 9633, 9663, 9963 5800, 5880, 5580, 2588, 2558, 2588
Horizontal Line	18	1123, 1223, 1233, 4456, 4556, 4566, 7789, 7889, 7899 3211, 3221, 3321, 6544, 6554, 6654, 9877, 9887, 9987
Diagonal Line	12	7753, 7553, 7533, 9951, 9551, 9511 3577, 3557, 3357, 1599, 1559, 1159

- Category 3 PIN number is composed of two different digits

There is no pattern for this category. However this category can be divided into two different sub categories for this category which are:

1) 2 digits are repeated twice (for example, 1212)
2) One digit is repeated three times (for example, 1112)

Table 4: Category 3 Number Groupings

Pattern	Number	PIN Number Combination
2 Digits Repeated twice	50 Times 9 (450)	11xx, 1x1x, x11x, x1x1, xx11 22xx, 2x2x, x22x, x2x2, xx22, 33xx, 3x3x, x33x, x3x3, xx33, 44xx, 4x4x, x44x, x4x4, xx44 55xx, 5x5x, x55x, x5x5, xx55 66xx, 6x6x, x66x, x6x6, xx66 77xx, 7x7x, x77x, x7x7, xx77 88xx, 8x8x, x88x, x8x8, xx88 99xx, 9x9x, x99x, x9x9, xx99 00xx, 0x0x, x00x, x0x0, xx00
2 Digits: 1 Repeated 3 Times	40 Times 9 (360)	111x, 11x1, 1x11, x111 222x, 22x2, 2x22, x222 333x, 33x3, 3x33, x333 444x, 44x4, 4x44, x444 555x, 55x5, 5x55, x555 666x, 66x6, 6x66, x666 777x, 77x7, 7x77, x777 888x, 88x8, 8x88, x888 999x, 99x9, 9x99, x999 000x, 00x0, 0x00, x000

- Category 4: PIN number is composed of one number only
  In this category, there is no pattern as a single digit is repeated 4 times.

Table 5: Category 4 Number Groupings

Pattern	Number	PIN Number Combination
1 Digit Repeated 4 times	10	1111, 2222, 3333, 4444, 5555 6666, 7777, 8888, 9999, 0000

- Category 5: PIN number with 19 or 20
  Whilst this does not represent a pattern, it would appear most likely that a date would have already past for it to be of some personal significance. Therefore it is expected that codes beginning 19 will be more frequent than those beginning with 20.

Table 6: Category 5 Number Groupings

Pattern	Number	PIN Number Combination
Begin 19	100	19xx
Begin 20	100	20xx

- Category 6: PIN number with sequential numbering
  This pattern is 4 digits in numerical ordering - the most basic of pins & therefore maybe occurring regularly as the sequence is easy to remember.

Table 7: Category 6 Number Groupings

Pattern	Number	PIN Number Combination
4 digits in numerical order	7	0123, 1234, 2345, 3456, 4567, 5678, 6789
4 digits in numerical order in	7	9876, 8765, 7654, 6543, 5432,

reverse		4321, 3210

- Category 7: 25 PIN numbers obtained from home alarm users.

Table 8: Test set of genuine alarm codes

Pattern	Number	PIN Number Combination
Test set of genuine alarm codes	30	0123, 0227, 0247, 0404, 0521, 0629, 0904, 1470, 1234, 1962, 2468, 2514, 2875, 3107, 4201, 4425, 4663, 4989, 4927, 5242, 5683, 7233, 7479, 7777, 7942, 8282, 8888, 8989, 9876, 9908

Once the categories of PIN numbers were chosen, the expectations of the analysis were then derived as follows: A large number of PIN numbers in the database will at least belong to one of six categories.

1) The analysis by Berry (2012) and the analysis of the 700 PIN numbers will indicate relative similarity.
2) A specific category will be noticeably more popular than other categories
3) It is expected that the percentage of PIN numbers than do not belong to a category will not exceed 50%, since most categories were identified and users are assumed to choose a PIN number according to its simplistic nature or a specific pattern
4) The specific most popular PIN number is expected to belong to one of the six categories
5) A brute force attack performed with the most popular PIN numbers and/or the most popular category will reduce time taken for a successful brute force attack to at least half.

RESULTS & DISCUSSION

The 700 PIN numbers present in the database were examined and analysed according to their distinctive characteristics including them into at least one of the categories. If a PIN number did not belong to at least one category of the six defined, it was to be defined as no category PIN number. As an assumption was that people would choose PIN numbers that were easy to memorise over random numbers, category 4 was the simplest category and was expected to occupy at least one-third of the database. Category 1 and 2 dealt with PIN numbers with a certain pattern, and since the initial assumption was that a significant percentage of users would draw certain pattern on a keypad to aid themselves with memorising as discussed by Rasmussen and Rudmin (2012), percentages of expected numbers of the 700 code dataset could be calculated and then measured against what was actually present. The results are shown in Table 9.

Table 9: Pin Numbers by Primary Category

Variance	Expected	Actual	over/under expected
Category 1	10%	1%	-9%
Category 2	10%	0%	-10%
Category 3	15%	8%	-7%
Category 4	30%	1%	-29%
Category 5	5%	4%	-1%
Category 6	15%	1%	-14%
No category	15%	85%	+70%
Total	**100%**	100%	

It was somewhat unexpected to observe that a large number of PIN numbers in the database did not belong to any one of the six categories. 85%, which accounts for 595 PIN numbers did not belong to a category which might hint that the alarm users were comfortable to select PIN numbers with no apparent pattern and memorise them. This significantly deviated from initial expectation and findings of previously research where ease of memorising the number in apparent patterns was a significant influencing factor. The aim of the research was to identify users' behaviour relating to choice of alarm codes and to show that a brute force attack would be significantly more efficient by taking into consideration people's behaviour. The initial results were tending

towards showing that the results of the alarm code choice were different than for other types of PIN codes and certainly greatly differed from the findings of Berry.

Expectation had been that category 1 would to compose about 10% of the database, that is, about 70 numbers were to be expected in this category. Despite only two possible combinations available, the four digits in the middle of the keypad were expected to appear more than other patterns in the category, due to its frequent occurrence at the study by Berry (2012). Although there were more available combinations existed, Y shape was not expected to appear as much due to more complicated nature of the pattern. For other patterns, at least half of the available combinations were expected to appear in the database.

Table 10: Pin Numbers Analysed In Category 1

Variance	**Expected**	**Actual**	**over/under expected**
Square	12	1	-11
Middle four digit	10	1	-9
Diamond shape	12	0	-12
Rectangle shape	12	0	-12
L shape	8	2	-6
Y shape	8	1	-7
Reverse L shape	8	3	-5
Total	**70**	**8**	

In general, all of the possible combinations in this category were heavily underestimated. The most distinctive pattern in this category was the shapes that related to 'L' shape, whether it is reverse or straight L shape. Against expectations, the middle four digits vertically down the keypad was not a common choice and appeared only once in the database. In category 2 it was expected that approximately 10% of PIN numbers or 70 PIN numbers would be present. However, none of the 700 PIN numbers in the database belonged to this category. In category 3 the initial expectation was that this category was to appear about 15%, which is about 105 PIN numbers. It was found that only 56 or fewer than half expected belonged to this category. In category 4 210 numbers were expected yet only 6 existed and in category 5, despite the simplicity involved in the numbers in the category, the result was heavily under expected. The result analysed in this category significantly differed from the analysis by Berry (2012), where all the PIN number combinations in this category were apparent in his top ten most popular 4-digit PIN numbers. A noticeable behaviour is that the PIN numbers 1111 and 6666 are not present in the database. These PIN numbers may avoided for most people due to concern of the PIN number 1111 or 1234 or superstition relating to 666. It is also interesting to note that PIN 0000 was not present which may indicate that the commercial nature of the dataset had led to a requirement to change the default codes, something that may not occur always on home alarm systems. The results are shown in figure 2.

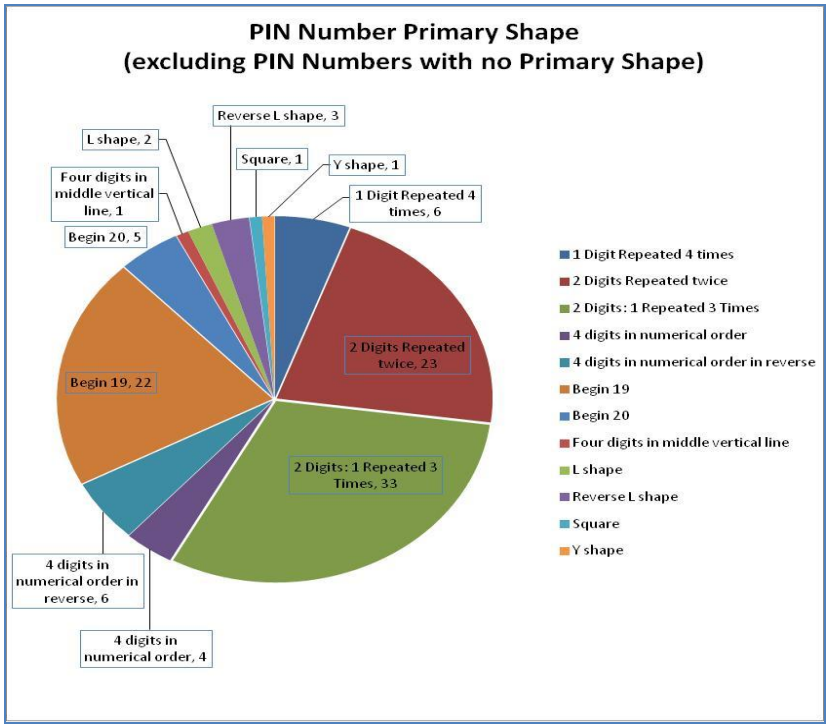


Figure 2: Most commonly chosen PIN numbers

It was decided to use these 12 categories as the test categories. Added to this at the head of the list is a 13th category, one number repeated twice. Whilst this does not form a pattern, it was found to be the most common approach to choosing a number. Finally, the 30 test PIN numbers were analysed utilising the standard sequential brute force attack and this was compared with the modified brute force attack. These 30 test PINs were obtained by asking people known to the researcher, and who had home alarm systems, what numbers they had used in the past or currently used. The purpose is to test the modified attack on a distinct dataset to show that it is more efficient than the standard attack. The process is to work through the categories of PIN numbers from most likely to least likely and once all numbers in the categories have been exhausted, revert to a sequential brute force attack on the remaining numbers. Table 11 shows the number of codes in each of the 13 categories.

Table 11: The 13 categories for the modified attack

Category	1	2	3	4	5	6	7	8	9	10	11	12	13
Number	320	10	45	36	7	7	100	100	2	8	8	112	20

The problem of including shapes formed but out of sequence highlights the necessity to look carefully through the chosen codes and plot them on the keypad. Selecting these numbers allows for easier memorisation but makes it more difficult for the attacker unless they are aware of this type of behaviour.

Table 12: Standard v Modified brute force attack

Category	**Code**
1	0227 0904 4425 4663 4989 5242 7233 7479 9908
3	0404 8282 8989
5	0123 1234
6	9876
7	1962
11	2875
12	2514
NIL	0247 0521 0629 1470 2468 3107 4201 4927 5683 7777 7942 8888

The total number of PIN codes that could possibly fall into one of these 13 categories is 767 out of 10 000 codes which equates to 7.67% of the codes. With 30 codes in the test dataset, it would therefore be expected that 2.3

codes would be expected to be into one of these categories if chosen randomly. Results show that 18 of the 30 codes or 60% fell into these categories. This shows the effectiveness of the new attack with a well over 50% chance that the code will be found in the first 767 codes attempted rather than 5000 attempts with the standard brute force attack. However, it is not always the case that a code will be found more quickly with the modified attack. Rather, on average the code will be found more quickly with the new attack. Overall the modified attack is likely to lead to the code being found in much fewer attempts than the standard attack and therefore in a quicker time on average of approximately 767 attempts multiplied by 5 seconds per attempt equates to 3835 seconds or just over one hour as opposed to almost 7 hours with the standard attack. This research shows that the choosing PIN codes for alarms should be a robust process rather than allowing users to choose their own codes where personal influences may lead to simplified attacks. These attacks can be mitigated by choosing random numbers and by ensuring codes longer than 4 numbers are chosen. The preference should be for 6 numbers selected randomly to increase the time of this attack from just over one hour to 690 hours, or over 4 days with a manual attack and to place a sensor in sight of all keypads so that an attacker cannot enjoy the luxury of time when mounting this attack, even when automated with the use of a computer.

CONCLUSION

The purpose of this study was to determine whether alarm code PIN numbers were predictable by pattern of frequency of chosen numbers. The study by Berry in 2012 of 3.4 million different PIN codes released on the Internet was used as a basis for comparing the 700 genuine alarm codes obtained from a single source. Analysis found that alarm code PIN number choice varies from PIN numbers utilised in other systems requiring a 4 digit PIN number. However, some unique features were determined which would allow a brute force attack against an alarm code to be simplified by trying more likely types of PIN numbers first and leaving the least likely PIN number to last. While the results did not closely follow the Berry findings, this study has highlighted the necessity for users to choose PIN number that are not easily predicted and utilise methods to memorise PIN numbers that cannot be predicted by an attacker. Further research is planned where a physical implementation of the attack will be performed utilising a laptop computer, an alarm system and a file of 10 000 Pin codes listed from most to least likely. These will be read one at a time and tried against the alarm system so that the improvement in speed in locating a number can be demonstrated. This research forms the basis of a guideline on how users should select PIN numbers that are more secure than the numbers that are currently being chosen.

REFERENCES

Alarm Forum. (n.d). How do I determine how many zones are needed on my security alarm? Retrieved from http://www.diyalarmforum.com/diy-alarm-faq18/

Bellis, M. (n.d). History of locks. Retrieved from http://inventors.about.com/library/inventors/bllock.htm

Berry, N. (2012). PIN Analysis. Retrieved from http://www.datagenetics.com/blog/september32012/

Berry, S. (2010). One in five use birthday as PIN number. Retrieved from http://www.telegraph.co.uk/finance/personalfinance/borrowing/creditcards/8089674/One-in-five-use-birthday-as-PIN-number.html

Gutmann,A. Volkamer,M. Renaud,K. (2016) “Memorable and Secure: How Do You Choose Your PIN?” Proceedongs of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016).

Krebs on Security, (2013). Does your Alarm have a Default Duress Code? Retrieved from http://krebsonsecurity.com/2013/01/does-your-alarm-have-a-default-duress-code/

Monitoring Plus. (2006). Get the most from your burglar alarm. Retrieved from https://www.monitoringplus.co.nz/

Rasmussen, M. and Rudmin, F. (2010). The coming PIN code epidemic: A survey study of memory of numeric security codes. Electronic Journal of Applied Psychology. 6(2):5-9. Retrieved 19 March, 2012, from http://ojs.lib.swin.edu.au/index.php/ejap/article/viewPDFInterstitial/182/220

Standards New Zealand (2007). Standard NZS2201.1:2007. Retrieved 8th November 2016 from https://shop.standards.govt.nz/catalog/2201.1%3A2007%28AS%7CNZS%29/view

USING GRAPHIC METHODS TO CHALLENGE CRYPTOGRAPHIC PERFORMANCE

Brian Cusack, Erin Chapman
Digital Forensic Research Laboratories, AUT
brian.cusack@aut.ac.nz, erinchapman@xtra.co.nz

Abstract

Block and stream ciphers have formed the traditional basis for the standardisation of commercial ciphers in the DES, AES, RC4, and so on. More recently alternative graphic methods such as Elliptic Curve Cryptography (ECC) have been adopted for performance gains. In this research we reviewed a range of graphic and non-graphic methods and then designed our own cipher system based on several graphic methods, including Visual Cryptography (VC). We then tested our cipher against RC4 and the AES algorithms for performance and security. The results showed that a graphics based construct may deliver comparable or improved security and performance in many of the required areas. These findings offer potential alternative avenues for post-quantum cryptographic research.

Keywords
Cryptography, performance, security, graphs, testing, word-oriented ciphers

INTRODUCTION

The demand for cryptographic methods has always been strong. The ever-expanding use of technology for communications, banking and financial transactions of diverse types, secure communications, and many other Internet applications is driving current demand for security and performance. The consumers of cryptography products require ever-increasing protection at lower cost (Thakur et al., 2011). Algorithms must maintain the confidentiality of communications, the integrity of the messages, and the accessibility of information to the users. The requirement for privacy of information has become increasingly challenging, caught in inter-jurisdictional debates of legality and the ability of developers to provide the levels of protection required (Bhat et al., 2015). The implementation of cryptographic algorithms in modern networked systems is crucial to ensure the users of information are satisfied with the service they receive. Many standardised algorithms have come and gone as vulnerabilities have been exploited to make algorithms unusable in the current cryptographic climate.
Events such as the theoretical cracking of the data encryption standard (DES), revisions including triple DES, and the major competition that resulted in the adoption of the Advanced Encryption Standard (AES) (Fluhrer et al., 2011; Singhal & Raina, 2011), illustrate the constant evolution of cryptography. While much research has been done to improve the security of traditional ciphers such as the AES and the now-defunct Rivest Cipher 4 (RC4) (Klien, 2008), there are opportunities for the development and improvement of alternative ciphers (Ustimenko, 2007). Our research focused on the potential of graphic methods. Encryption using Visual Cryptography (VC) and Elliptic Curve Cryptography (ECC), is well-established and has been shown to give high levels of security, improved performance, and reduced resource requirements. It also shows that that alternative competitors can be found in graphic schemes. To demonstrate that there are alternative approaches to achieve secure methods for the ever-expanding online world we constructed a word-oriented symmetric stream cipher. It was tested against AES, RC4, ECC, and VC algorithms, and the results demonstrated that alternatives are possible using graphic schemes.

The proposed system was termed Coordinate Matrix Encryption (CME) to reflect the graphic construct behind the algorithm (Galbraith & Menezes, 2005; Hou et al., 2014). It was implemented in Java along with the four competing algorithms, and we tested both graphic-based and traditional cryptographic algorithms against our construct. The algorithms were all tested for security, efficiency and resource consumption. The comparative results show the high levels of security achievable by alternative graphic-based ciphers and the potential for alternative innovations. The resistance of the proposed 8-bit CME system to brute force attacks was shown to be 157,899 orders of magnitude higher than that of a 128-bit key in traditional ciphers such as AES. Examination of the avalanche effect of the CME scheme showed that less than 0.5% of all bytes within the cipher text remained in the same position when a single bit of the plaintext was altered. While the RC4 scheme offered the best efficiency in terms of time required to encrypt and decrypt the data, it has been proven vulnerable; and the CME comparison showed lower memory requirements and faster setup execution. This offers the potential for research, testing and implementation of different approaches to make traditional cryptography adaptable to the new high-speed cyber connected world (Vigila et al., 2009; Tawalbeh et al., 2013).

GRAPHIC METHODS

Graphic-based systems rely on group theory and graph theory to create secure algorithms for encryption. Some of the more popular graphic-based methods are ECC (Akhter, 2015) and VC (Blundo et al., 2006). However, there are other algorithms that take advantage of the innate properties of group theory and families of graphs (Cohn, 2000; Polak et al., 2013). These graphic methods for encryption exploit particular traits of certain types of graphs, such as those using families of graphs of large girth, for example Cayley graphs. A Cayley graph is defined as a graph G(G,S) where S is a non-empty subgroup of the group G, such that S is equal to its own inverse $(S = S^{-1})$, and the set of vertices is equal to G, V=G, and the set of edge elements is:

$$E = \{\{x,y\} : x,y \in G, \exists s \in S : y = xs\}$$

A Cayley graph constructed in this manner is a regular graph, and the underlying algebraic structures of the family of Cayley graphs can be exploited for use in encryption (Priyadarsini, 2015).

Another family of graphs providing a possible route for cryptographic research is the family of directed graphs of large girth. The fact that there are only three families of undirected graphs of arbitrarily large girth limits their use, however there are infinite numbers of algebraically constructed families of such graphs. These can be converted to equivalent Turing machines of basic construction. The basic finite automaton is equitable to a directed graph, if the memory component is ignored. These graphs are part of the expander family of graphs. Cayley graphs can be used to describe a linear automata, while other graph families can be used to result in non-linear systems for encryption. Encryption systems based around groups of graphs such as Cayley or expander families use sequences of vertices or graph-colourings to create a cipher text. Others opt for using strongly regular graphs to generate a Hadamard matrix for encoding images (Davidoff et al., 2003). Some systems use the vertices to represent the plaintext space and the path within the graph becomes the password. Systems such as these based around walks along graph edges can be used in the construction of stream ciphers. Expander graphs are also of interest in cryptography; they are sparse, finite, and highly connected. Ramanujan graphs are a brand of expander graphs that are often used for encryption (Agnarsson & Greenlaw, 2007).

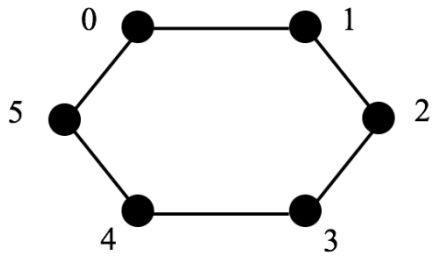


Figure 1. A simple Cayley graph described by G=Z/6Z,S={1,-1}

New systems have been proposed that utilise group theory and rings to create encryption that relies on the combining of two group elements. The reversing of these processes is impossible and hence establishes their cryptographic value. Multivariate cryptography is the set of cryptosystems which use polynomials and finite commutative rings for encryption, and these are part of the post-quantum cryptography movement (Ustimenko & Romanczuk, 2013). The concepts of quantum cryptography have been used and applied to theoretically break many standard cryptographic algorithms including the RSA. Post-quantum cryptography involves systems that are theoretically resistant to adversaries using quantum attacks. Graphic methods have hence been explored as possibilities in the post-quantum world, with the potential to define non-standard cryptographic methods that are better and stronger than the new adversaries. New developments in graphic methods have used the injection of algebraic geometry into the field of multivariate public key cryptosystems with outstanding effect (Blakley & Kabatiansky, 2011). The structures are a set of multivariate quadratic polynomial equations over finite fields and parameterised matrices for systems of para-unitary equations that deliver the cryptographic solution. Multivariate polynomials are a solution to the problems of RSA and an alternative to systems like ECC, using multivariate systems of equations over small fields, such as $GF(2^m)$ where m is some small number. The use of multivariate polynomials is a proposed solution to the issues with key size and set up time, both of which are high in computational complexity and require large amounts of data to communicate. Multivariate systems generally use quadratic polynomial fields. The multivariate systems rely on their own version of the one-way problem, in this case called the MQ problem, based on the computational complexity of solving many different quadratic equations over multiple different fields using many different variables (Chen et al., 2012; Sutter et al., 2013). The complexity of the MQ problem has led to these graphic methods being proposed as a possible quantum-resistant encryption method.

ISSUES WITH GRAPHIC METHODS

Encryption systems that use graphs for encoding, like those based around VC, can have very high computational overhead, due to the size of the graphs required to achieve the required levels of security (Klein & Wessler, 2007). Also, those encryption methods that base themselves around the special colourings of vertices and edges are vulnerable to cubical linearization attacks, which make decryption possible, and are costly in practice. For those graph-based systems that also rely on the DLP, the same vulnerabilities encountered by ECC encryption apply. The biggest problem within graph based systems is implementation challenges. Representing a graph within a computer program can be broken down into four possible objects for management: the adjacency list; the adjacency matrix; the incidence list; and the incidence matrix. Each object lists either vertices or edges, and they are either enumerated fully – in a matrix – or only where a connection occurs. These implementations affect the use of a particular system, especially with larger connected graphs, with many entries in its matrix or list (Riaz & Ali, 2011).
The security of ECC relies on computational complexity to assure that it is intractable to compute the Elliptic Curve Discrete Logarithm Problem (ECDLP) (Yan, 2008). This reliance means that the security would be severely compromised should the ever-increasing speed of technology provide a method of computing the solution to the ECDLP in less than the current exponential time. On the realization of quantum computers, the Elliptic Curve Discrete Logarithm problem will no longer be computationally infeasible to compute and exposing the algorithm to an intractable vulnerability (Kramer, 2015). The weakness surrounding ECC in a post-quantum world is based on Shor's algorithm, operating on a quantum computer, which is capable of solving problems such as discrete logarithms in minimal time. Aside from the possibility of breaking the Discrete Logarithm Problem, ECC also has disadvantages in its implementation. It is highly complex to implement, and the resulting cipher text message is increased in length from the original plaintext significantly (Akhier, 2015).

Advances in fields such as index calculus and number-field sieves have shown possible weaknesses in systems based around the problem of computing discrete logarithms (Joux & Vitse, 2012). Index calculus, as a method of computing discrete logarithms using probability and field arithmetic, which has been used by mathematicians to exploit characteristics of groups and to then solve the original discrete logarithm problem (Agnarsson & Greenlaw, 2007). While classic index calculus has not been implemented successfully against general ECC systems, and exponential time square root attacks are more efficient against these general ECC algorithms, the reduction in computing time for solving the discrete logarithm problem in other systems may suggest weakness in the overall computational complexity of DLP-based systems.

VC schemes encounter difficulties due to pixel expansion, the number of subpixels required to encode the correct level of contrast in each share (Shyu et al., 2007). This expansion greatly affects the required overhead of VC schemes, and as such is the target of much research. While there have been schemes proposed that give a constant pixel expansion, such as graph-based extended VC (Lu et al., 2011), many schemes require linear, or even polynomial pixel expansion based on the number of nodes within the scheme, making them infeasible for larger implementations. Within the schemes which ensure pixel expansion remains constant, the overhead for the encoding of the shares is still computationally high for large images with a greater numbers of pixels. These systems which constrain pixel expansion also degrade the contrast of an image, as there are fewer subpixels differentiating dark and light in the image, making it more difficult for the human eye to visually decode. Once multiple colours are introduced to the scheme, pixel expansion becomes even more complex, and overall image contrast is lowered further (Liu et al., 2008). A colour VC scheme will also require higher overall time complexity, as each colour within the image must have a different threshold for contrast.

VC is also open to malicious man-in-the-middle attacks, during the transfer of shares to participants. If the shares are intercepted, the malicious intermediary could keep the original share, and forward a new, false share to the intended participant. The interception of the share would as such result in the security of the scheme being completely undermined. Attacking a VC scheme in this manner is generally referred to as cheating. While this risk can be decreased by the implementation of a filter where each participant is assigned a specific target image, cheating is still possible, by a malicious participant. Cheating prevention VC schemes have been proposed that use specific basis matrices in the generation of both the secret shares, and a set of verification shares, to counter the ability to generate fake shares. These matrices add an extra column to the original matrices and hence extra cost. The problem still remains however, that these basis matrix schemes are not immune to cheating. To prevent this type of cheating, it is necessary to introduce multiple extra zero columns into the basis matrices that adds further costs. As a result, cheating prevention VC schemes result in higher overheads and increased pixel expansion when compared regular VC algorithms, which delivers a lower level of utility in real-world application. The proposal of adding tags to individual shares to allow for the identification of false or forged shares may offer additional protection against cheating, however it is still vulnerable to attack if an attacker is in possession of a genuine share, and can therefore find and replicate the security tag (Wang & Hsu, 2011).

ALGORITHM DESIGN

The algorithm design for the CME scheme was based around a square coordinate matrix and transformations in a finite Galois field $F(2^n)$ (Martin, 2012; Martinez & Encinas, 2013). The coordinate matrix design was structured by the concepts delivered in error-correcting codes, in which sparse matrices and code words are used to eliminate noise from the transmissions. In addition, security principles from VC were applied. The main encryption process uses a randomized coin toss style procedure, which is similar to the VC method of choosing whether a given pixel is black or white. This coin toss decides if the next section of the cipher text is to be a blank padding section, or if it is the next section of the plaintext message. If it is a blank padding section, one of the locations containing an empty entry is picked at random from a blank list, and the binary or integer coordinates (depending on the implementation) of that location are then input as the next part of the cipher text. Else, if the section is a part of the plaintext message, then a location containing that bit string is randomly chosen from the list of locations for the string. The location is then translated into the corresponding coordinates and concatenated to the cipher text. The scheme involves the addition of exactly the same number of blank coordinates as enciphered message coordinates. As a result of the addition of padding characters, the resulting cipher text is exactly four times the length of the plaintext, with two coordinates for every message or padding character, and exactly the same number of padding and message characters. The style of encryption means that the total length of the outputted cipher text is fixed at exactly four times the length of the plaintext, which may prove to result in undesirable overheads for transmission.

```
Total strings: 8
Number of occupied spaces: 32
Number of blank spaces: 32
Total matrix size: [8,8]
[---][---][101][---][---][---][---][---]
[---][010][011][---][---][---][000][---]
[000][111][---][001][---][101][---][---]
[110][000][001][---][---][---][---][111]
[---][---][---][010][111][100][100][---]
[010][100][001][---][---][100][101][011]
[---][---][101][010][---][110][---][---]
[110][---][011][011][111][000][001][110]
Set up complete, time taken: 19 ms.
Total memory used: 0.43109130859375 MB
```

Figure 2: A randomly generated key matrix for a 3-bit coordinate CME matrix scheme.

The use of multiple locations for each bit string and the addition of an equal number of padding coordinates at random locations in the ciphertext provide resistance to cryptanalysis, and particularly to known and chosen plaintext attacks, as the encryption process therefore results in a non-singular mapping. This non-singular mapping means each plaintext input has many possible ciphertext outputs for any one key matrix. The multiple locations also result in far more of the overall matrix being taken up by bit strings than would be the case if each string appeared only once. Again, this helps prevent cryptanalytic attacks, as it increases the likely occurrence of the same of padding coordinates appearing more than once, which is helpful in further confusing any analysis of the resulting data. A sample of a 16-bit plaintext and the corresponding 64-bit ciphertext resulting from encryption using a 4-bit coordinate matrix scheme is shown in Figure 3.

```
Plaintext:
0101000110111011
Ciphertext:
1110011001001011101101001100010001100111101100111010010000000010
```

Figure 3. Example plaintext ciphertext pair output from a 4-bit CME scheme.

The decryption process uses the same key matrix as in the encryption process and looks up each of the coordinates. If a given coordinate is an empty padding variable, it is discarded. If not, the value of the coordinate is combined with the next character of the key string using exclusive-OR, and the resulting value is added to the plaintext output. In this manner, the extra noise generated by the encryption process to ensure security is efficiently removed during decryption. Because each step of the decryption process consists only of simple entry check and exclusive-OR operation, the overall efficiency for decrypting the ciphertext is theoretically higher than that of the encryption

process.

TESTING AND RESULTS

The algorithm implementations were tested using Java, on an Intel i7 3.1GHz machine with 16GB of RAM. All algorithms were tested for resistance to brute force, avalanche effect, set up requirements and encryption/decryption time. Equation 1 shows the brute force analysis based on the key space for traditional 128-bit keys, while Equation 2 compares the resistance of the CME 8 and 4 bit schemes, based on the key space of the relevant matrix sizes. The results of avalanche effect testing showed that when the 8-bit CME algorithm was trialled against RC4 and AES it not only performed very well but outperformed the traditional algorithms, demonstrating the resilience of the CME algorithm, shown in Table 1. Table 2 shows the results of avalanche testing of 4-bit CME against VC, in which both algorithms achieved the maximum Hamming distance. Table 3 shows the set up time and memory requirements for ECC, 8-bit CME, AES, RC4, and Table 4 shows the set up time and memory for VC and 4-bit CME. Encryption/decryption times are given in Table 6 for AES, RC4, and 8-bit CME, and in Table 6 for 4-bit CME and VC. These results appear to show CME as a potential competitor for streaming encryption.

Equation 1 $$brute\ force_{128-bit} \approx 1.7014118 \times 10^{38}$$

Equation 2 $$brute\ force_{8-bit\ CME} \approx 1.19162785 \times 10^{157937}$$

Table 1: Comparative avalanche effect results with AES and RC4

Data Size (bits)	**Same Bytes (%)**			**Same Position (%)**		
	RC4	AES	CME	RC4	AES	CME
304	97.668	37.767	44.839	97.368	24.779	0.414
928	99.472	62.777	84.026	99.145	38.905	0.388
3024	99.940	87.935	99.713	99.735	45.857	0.422
4408	99.979	94.276	99.984	99.819	48.227	0.404
8144	99.997	99.100	100	99.902	48.593	0.395

Table 2: Comparative avalanche effect results with 4-bit CME and VC

Data Size (bits)	**% of Bits Unchanged**	
	VC	**CME 4-bit**
16	49.275	50.319
32	50.169	50.619
64	50.005	50.499
128	49.934	50.286
256	49.981	50.337
512	50.072	50.120

Table 3: Set up and memory requirements for 8-bit CME, AES, ECC and RC4

	ECC	CME	AES	RC4
Time taken (ms):	359.5	80.13	409	258.5
Memory used (MB):	1.192	1.217	2.364	2.340

Table 4: Set up and memory requirements for 4-bit CME and VC

	4-bit CME	VC
Memory used (MB):	0.448	0.456
Time taken (ms):	21.44	0

Table 5: Encryption/decryption time for AES, RC4 and 8-bit CME

Data Size (bits)	Encryption (ms)			Decryption (ms)		
	AES	Byte CME	RC4	AES	Byte CME	RC4
304	0.199	0.031	0.014	0.17	0.012	0.022
928	0.142	0.059	0.027	0.182	0.023	0.025
3024	0.173	0.136	0.023	0.179	0.065	0.016
4408	0.185	0.173	0.02	0.196	0.05	0.045
8144	0.148	0.262	0.024	0.25	0.093	0.032

Table 6: Encryption/decryption times for 4-bit CME and VC schemes

Bit String Length	Encryption (ms)		Decryption (ms)	
	VC	4-bit CME	VC	4-bit CME
16	0.056	0.02	0.01	0.02
32	0.08	0.066	0.014	0.036
64	0.196	0.104	0.052	0.06
128	0.368	0.214	0.088	0.074
256	0.868	0.369	0.214	0.136
512	2.822	1.13	0.492	0.328

CONCLUSION AND FURTHER RESEARCH

Further research into alternative graphic methods is required to explore the applications of alternative systems such as CME. The security offered by the proposed CME scheme makes it a potential candidate for post-quantum cryptographic research. The system's alternative key structure and non-singular mapping allow for resistance to a large key space and superb avalanche effect, while maintaining competitive efficiency. These features require further exploration. Comparative analysis between traditional and graphic-based ciphers is required to determine whether alternative graphic methods are able to offer higher security for lower overheads. Optimization of these schemes requires further research to ensure a lasting competitive advantage, and suitability for implementation in application development. There is currently little standardisation in stream ciphers to replace RC4, and as such the opportunity exists for an optimized version of CME to assist in this particular space in applications such as TLS that utilize stream ciphers for encryption on a day-to-day basis.

REFERENCES

Agnarsson, G., & Greenlaw, R. (2007). *Graph Theory: Modelling, Applications, and Algorithms*. New Jersey: Pearson Education Ltd.

Akhter, F. (2015). A novel Elliptic Curve Cryptography scheme using random sequence. Paper presented at the 2015 International Conference on Computer and Information Engineering (ICCIE).

Bhat, B., Ali, A. W., & Gupta, A. (2015). DES and AES performance evaluation. Paper presented at the International Conference on Computing, Communication & Automation (ICCCA), 2015.

Blakley, G. R., & Kabatiansky, G. (2011). Secret Sharing Schemes. In H. A. van Tilborg & S. Jajodia (Eds.), *Encyclopedia of Cryptography and Security* (pp. 1095-1097): Springer US.

Blundo, C., Cimato, S., & De Santis, A. (2006). Visual cryptography schemes with optimal pixel expansion. *Theoretical Computer Science*, 369(1–3), 169-182.

Chen, Y. C., Horng, G., & Tsai, D. S. (2012). Comment on Cheating Prevention in Visual Cryptography. *IEEE Transactions on Image Processing*, 21(7), 3319-3323.

Cohn, P. M. (2000). *Introduction to ring theory*. Springer Science & Business Media.

Davidoff, G., Sarnak, P., & Valette, A. (2003). *Elementary number theory, group theory and Ramanujan graphs* (Vol. 55): Cambridge University Press.

Fluhrer, S., Mantin, I., & Shamir, A. (2011). Weaknesses in the key scheduling algorithm of RC4. Paper presented at the International Workshop on Selected Areas in Cryptography.

Galbraith, S., & Menezes, A. (2005). Algebraic curves and cryptography. *Finite Fields and Their Applications*, 11(3), 544-577.

Hou, Y. C., Wei, S. C., & Lin, C. Y. (2014). Random-Grid-Based Visual Cryptography Schemes. *IEEE Transactions on Circuits and Systems for Video Technology*, 24(5), 733-744.

Joux, A., & Vitse, V. (2012). Cover and decomposition index calculus on elliptic curves made practical *Advances in Cryptology–EUROCRYPT 2012* (pp. 9-26): Springer.

Klein, A. (2008). Attacks on the RC4 stream cipher. *Designs, Codes and Cryptography*, 48(3), 269-286.

Krämer, J. (2015). *Why Cryptography Should Not Rely on Physical Attack Complexity*. Singapore: Springer.

Liu, F., Wu, C. K., & Lin, X. J. (2008). Colour visual cryptography schemes. *Information Security, IET, 2*(4), 151-165.

Lu, S., Manchala, D., & Ostrovsky, R. (2011). Visual cryptography on graphs. *J. Comb. Optim., 21*(1), 47-66.

Martin, K. M. (2012). *Everyday Cryptography: Fundamental Principles & Applications*. New York: Oxford University Press.

Martinez, V. G., & Encinas, L. H. (2013). Implementing ECC with Java Standard Edition 7. *International Journal of Computer Science and Artificial Intelligence*, 3(4), 134.

Polak, M., Romańczuk, U., Ustimenko, V., & Wróblewska, A. (2013). On the applications of Extremal Graph Theory to Coding Theory and Cryptography. *Electronic Notes in Discrete Mathematics*, 43, 329-342.

Priyadarsini, P. L. K. (2015). A Survey on some Applications of Graph Theory in Cryptography. *Journal of Discrete Mathematical Sciences and Cryptography*, 18(3), 209-217.

Riaz, F., & Ali, K. M. (2011, 26-28 July 2011). *Applications of Graph Theory in Computer Science.* Paper presented at the Third International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), 2011.

Shyu, S. J., Huang, S.-Y., Lee, Y.-K., Wang, R.-Z., & Chen, K. (2007). Sharing multiple secrets in visual cryptography. *Pattern Recognition*, 40(12), 3633-3651.

Singhal, N., & Raina, J. (2011). Comparative analysis of AES and RC4 algorithms for better utilization. International *Journal of Computer Trends and Technology*, 2(6), 177-181.

Sutter, G. D., Deschamps, J. P., & Imana, J. L. (2013). Efficient Elliptic Curve Point Multiplication Using Digit-Serial Binary Field Operations. *IEEE Transactions on Industrial Electronics*, 60(1), 217-225.

Tawalbeh, L., Mowafi, M., & Aljoby, W. (2013). Use of elliptic curve cryptography for multimedia encryption. *IET Information Security*, 7(2), 67-74.

Thakur, J., & Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. *International Journal of Emerging Technology and Advanced Engineering*, 1(2), 6-12.

Ustimenko, V. (2007). On Graph-Based Cryptography and Symbolic Computations. *Serdica Journal of Computing*, 1(2), 131-156.

Ustimenko, V., & Romańczuk, U. (2013). *On extremal graph theory, explicit algebraic constructions of extremal graphs and corresponding Turing encryption machines Artificial Intelligence*, *Evolutionary Computing and Metaheuristics* (pp. 257-285). Heidelberg, Germany: Springer.

Vigila, S., & Muneeswaran, K. (2009). Implementation of text based cryptosystem using Elliptic Curve Cryptography. Paper presented at the First International Conference on Advanced Computing, 2009. ICAC 2009.

Wang, R. Z., & Hsu, S. F. (2011). Tagged Visual Cryptography. *IEEE Signal Processing Letters*, 18(11), 627-630

Yan, S. Y. (2008). *Cryptanalytic attacks on RSA*. New York, USA: Springer US.

A HYBRID BEHAVIOUR RECOGNITION AND INTRUSION DETECTION METHOD FOR MOBILE DEVICES

Ashley Woodiss-Field
School of Science, Edith Cowan University, Perth, Australia
awoodiss@our.ecu.edu.au

Abstract

Behaviour-based authorisation is a technique that assesses the user of a device for authenticity by comparing their activities to previously established behaviour profiles. Passwords and other point of entry authorisation techniques are often inadequate for protecting mobile device security as they only provide an initial barrier to usage and do not operate continuously. Behaviour-based authorisation continuously assesses user authorisation, using the device owner's profile for authentication. This research improves upon behaviour-based authorisation performance by applying a hybridised intrusion detection method. The constituent intrusion detection methods that were applied include context-awareness and self-correction. Performance of a behaviour-based authorisation method can be measured as either an increase in intrusion detection, without significantly increasing false positives or a decrease in false positives without totally compromising intrusion detection. This research found that an increase in performance can be achieved by the addition of intrusion detection components.

Keywords
Behaviour-based authorisation, intrusion detection, context-awareness, self-correction, hybrid intrusion detection, artificial neural network, mobile security

INTRODUCTION

Mobile devices facilitate a range of multimedia applications, many of which are driven by user data. This user data has become sensitive in nature, including personal information, login credentials, and business data (Li, Clarke, Papadaki, & Dowland, 2013). Mobile device theft rates have been recorded:

- Approximately 1.6% of mobile phone owners experienced mobile phone theft in England and Wales during 2012/2013 (Home-Office, 2014).
- Collected US law enforcement data combined with FBI crime data indicates an estimate of 1/10th of all theft for 2013 in the US is associated with the theft of a mobile device. According to a consumer report's survey, 3.1 million smartphone thefts occurred in 2013 (Federal-Communications-Commission, 2014; Tapellini, 2014).

Credent (cited by Li et al., 2013) found that 40% of participants in a survey failed to utilise personal identification numbers (PIN). PIN-based approaches are also often misused when they are weak, rarely changed, or shared with others. A fundamental weakness is that it does not seek to validate a user once they know the PIN (Li et al., 2013).

Behaviour-based authorisation is a technique that assesses the user of a device for authenticity by comparing their activities to previously established behaviour profiles. A benefit of behaviour-based authorisation is active authentication wherein if an intruder somehow bypassed standard point of entry techniques, such as PINs or passwords, they will still be under scrutiny (Li et al., 2013).

The research goal was to ascertain whether or not a combined intrusion detection method can be applied to behaviour-based authorisation on mobile devices, with the purpose of performance improvement. The performance improvement was measured by an increase in intrusion detection accuracy without significantly increasing false positives or a reduction of false positives without totally compromising the intrusion detection rate. Intrusion detection methods that were experimented with include contextual-awareness, adapting a system's assessment metrics based on the apparent situation, and self-correction, altering assessment results through internal determination based on known information without additional external assistance.

RESEARCH BACKGROUND

Approaches to Behavioural Profiling and Authorisation

Multiple approaches to behaviour profiling, including such approaches for the purpose of authorisation, have been made. These approaches include different types of artificial neural networks, rule-based methods, specially designed frameworks, and clustering methods.

Artificial Neural Networks

Artificial neural networks (ANNs) are dynamic systems of interconnected parts. They are made up of artificial neurons which each take in a set of inputs. Inputs are regulated by weight values and activation functions. A training algorithm is applied to an ANN and the weights for all inputs are adjusted to improve the accuracy of the output. ANNs are able to detect non-linear relationships and interactions among variables (Anandarajan, 2002; Wasserman, 1989b).

Li et al. (2013) experimented a radial basis function (RBF) ANN. The activation functions in an RBF ANN are RBFs, which are used to determine the Euclidean distance of the inputs from certain points, known as centres. Using this, the mapping relationship between the input and desired output can be obtained (Chang, Cheng, & Yu-Feng, 2010; Li et al., 2013).

Li et al. (2013) also ran experiments with a feed-forward multi-layered perceptron (FF MLP) network. FF MLP ANNs pass values in one direction, from input to output, typically using the sigmoid function or hyperbolic tangent function as their activation function. The activation functions scale the outputs of each neuron which are passed to further neurons in the network (Anandarajan, 2002; Li et al., 2013; Wasserman, 1989b).

A simple recurrent network (SRN) was experimented with by Anandarajan (2002) for the purpose of classifying user behaviour in terms of workplace internet activity. An SRN has a small amount of additional neurons in the input layer, known as context units that receive feedback signals from the hidden layers, allowing the ANN to record the outputs of the hidden layers. This allows for past values to influence present values going into the ANN meaning that the ANN can learn faster than a standard feed-forward ANN (Anandarajan, 2002; Krenker, Kos, & Bešter, 2011).

It was found that ANN based systems, particularly RBF ANNs, would deliver a greater performance in terms of correctly profiling user behaviour, at the cost of being more resource intensive, using twice the amount of computational power of that of a rule-based method (Li et al., 2013).

Rule-Based and Fuzzy Systems

A dynamic rule-based approach was devised by Li et al. (2013) based on the idea that recent historical usage can be used to predict the probability of a present event. As shown in Equation 1 the approach would provide a mechanism to have all recorded outputs bounded between 0 and 1 to help determine a threshold. If a singular output breaches the threshold, then the event is deemed to have breached the rule-set (Li et al., 2013).

$$1 - \frac{\sum_{i=1}^{N}\left(\frac{O_{ix}}{\sum_{x}^{M} O_{ix}}\right)}{N} \geq t(1)$$

Equation 1 Where: i = the features of one chosen application, x = the value of $Feature_i$, M = total number of values for $Feature_i$ N = total number of features, t = predefined Threshold, O_{ix} = feature occurrence (Li et al., 2013).

Sood, Mehmi, and Dogra (2015) conducted experimentation with a fuzzy system applying a user profiling system for cloud computing. Fuzzy systems work by representing data in degrees rather than as booleans in a linguistic way. Fuzzy systems are ideal for solutions where the problem is non-linear or hard to define. Fuzzy logic is rule-based and determines what degree values are in relation to their variables. Variables that have had their fuzzy values determined are weighted and aggregated to develop a crisp output (Sood et al., 2015).

Rule-based methods appear to be able to distinguish user activity from different users through behaviour profiling, but at a lesser rate of some machine learning methods as RBF ANNs (Li et al., 2013).

Other methods of user profiling

Majeed, Jing, Novakovic, and Ouazzane (2014) applied K-means clustering as a means to establish a user profile with which to compare future user behaviour for legitimacy. K-means clustering is used to create a usage profile from the input data gathered by a feature extractor. Once the usage profile is created the feature extractor compares new user data to determine deviation. If a persistent deviation occurs, an alert is made (Majeed et al., 2014).

Shi, Niu, Jakobsson, and Chow (2011) developed a machine learning framework based around modelling independent features. The user model is developed as a combination of the probability density of all features, based on time of occurrence. Selected features were based on good events, bad events and location. Good events would be those conducted with known contacts, bad events are those with unknown contacts. When in training, frequency and time between certain events would be used to establish feature probability. Using the Gaussian mixture model (GMM) the probability of user being at a certain location at a certain time would also be calculated (Shi et al., 2011).

The research conducted by Shi et al. (2011) provide a set of concise features that behaviour-based authorisation can be tested on, including calls made, texts made, internet activity, and user location (Shi et al., 2011).

Of the methods of behaviour-based profiling and authorisation, ANNs and rule-based methods appear to produce effective results, being able to identify most intrusive activity records during various experiments. However, the problem of false positives remains among these methods. Work done by Li, Wheeler, and Clarke (2014) based on that from Li et al. (2013) found that while illegitimate users were denied application access 95.83% of the time, their developed framework allowed legitimate users access only 87.09% of time (Li et al., 2014).

Intrusion detection methods for reducing false positives

False positive reduction is important to intrusion detection as false positives make it more difficult to identify intrusive activity and can cause resource intensive false alarms that discourage the use of the intrusion detection system altogether.

Cluster-based Intrusion Detection Methods

Yassin, Udzir, Muda, and Sulaiman (2013) used K-means clustering and Naïve Bayes classification methods combined to minimise false alarms generated by anomaly-based intrusions detection systems. K-means clustering is used to separate activity data, normal or intrusive, into separately identifiable partitions. Naïve Bayes Classification uses a set of attributes assigned to a set of classes and calculates the probability of activity belonging to one class (normal activity) to another (intrusive activity) by assessing the occurrence of attributes with the given activity. The combination of K-means clustering and Naïve Bayes classification performed greater, in terms of reducing false positives, than either of the two methods standalone, demonstrating the advantages of hybrid approaches (Yassin et al., 2013).

Hybrid frequency and relation-based Intrusion Detection Methods

Spathoulas and Katsikas (2010) discuss and experiment with a system with three components:

- Neighbouring Related Alerts (NRA)
- High Alert Frequency (HAF)
- Usual False positives (UFP)

The NRA method relies on the assumption that most attacks have a group of alerts related to it. NRA works by counting the amount of neighbours that exist in a time window, that have the same source and destination addresses (Spathoulas & Katsikas, 2010).

HAF is based on how often an alert with a certain signature appears within a certain time window. Each existing signature is given an average frequency which establishes the general distribution of signatures. After that, every

time a signature occurs, the minimum amount of time for reoccurrence is established. If reoccurrence of a signature appears before it should several times it will cause an alert (Spathoulas & Katsikas, 2010).

UFP is designed based on the idea that patterns of common false positives are related to topology problems or misconfigured services. The frequency for the signature during an attack-free period is made. During actual deployment, if a number of common frequencies occur more than expected, it may be a true positive and an alert is made if an established limit is breached.

Each component acts independently to one another before combining their individual verdicts on whether or not a given alert is true. This allows for the strengths and weaknesses of each component to complement and mitigate each other (Spathoulas & Katsikas, 2010).

System security status level

Part of the research conducted by Li et al. (2013) involved the development of a framework that could facilitate behaviour-based authorisation. The framework was developed to take into account different error rates experienced by different sets of application usage data. A System security status (SSS) level is kept between -3 and +3 where -3 is low security and +3 is high security. SSS level is determined by the performance of a given application based on equal error rate (EER) and the verification result, which can be a pass or fail. A verification test is when user behaviour is matched to what is expected. If the verification is successful, it is added to the SSS level. If verification fails, it is subtracted. The SSS also decreases over time through lack of usage. The SSS framework allows for a given base behaviour-based authorisation method to produce initially incorrect results but for corrections to be made if necessary based on further results (Li et al., 2013).

CHOSEN BEHAVIOUR-BASED AUTHORISATION METHOD

Artificial Neural Network

The behaviour-based authorisation method chosen as a baseline for this research was an ANN. The ANN was built using pybrain, a python module that allows customisable ANNs to be built and applied to datasets. The ANN was built with a configuration of four inputs, one output neuron and a variable amount of hidden neurons. The input values were the day of the week for a given activity record, the time of the day for a given activity record, the type of activity recorded and the details of the activity record. The output of the ANN would be a single number, where the closer to one the value was, the more likely the record would be that of a legitimate user.

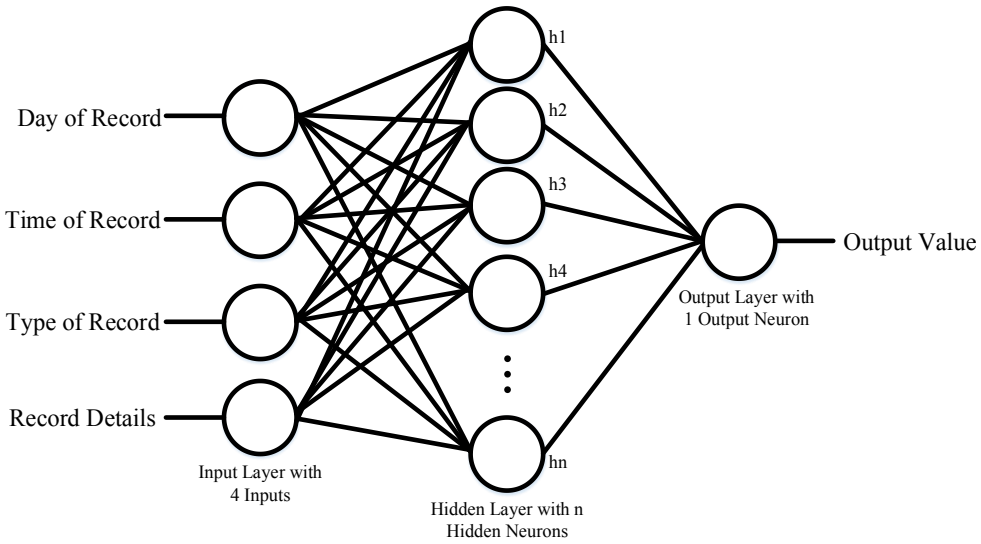


Figure 1 ANN configuration for Behaviour-Based Authorisation Diagram, the number of hidden neurons (n) is a configurable amount that had been experimented on.

The ANN configuration in Figure 1 receives four input values in the input layer and produces one output. The output value is a number that is tested by examining whether or not it comes between an established pair of

threshold values. If the output value falls outside the threshold values, it is designated as an intrusion, if it falls between the threshold values it is designated as legitimate activity. The ANN was trained using the supervised method of backwards propagation, as provided by the pybrain module (Wasserman, 1989a). Only legitimate user behaviour could be used to train the ANN as intrusive behaviour would be unknown.

Chosen Behavioural Attributes

Partly based on the research conducted by Shi et al. (2011), for this experiment the following mobile device attributes were used as independent/control variables to measure accuracy of the improved behaviour based authorisation method:

- calls made to known contacts
- calls made to unknown contacts
- text messages sent to known contacts
- texts messages sent to unknown contacts
- packet data sent to and from the device
- location of the mobile device
- day of the week and time of day activity occurs

INTRUSION DETECTION COMPONENTS

Self-correction using surrounding data

Self-correction provides a form of improvement that doesn't require user intervention (Patel et al., 2011). Because self-correction must be conducted without external intervention, it must be able to determine a correction only using internal factors (Schmeck, Müller-Schloer, Çakar, Mnif, & Richter, 2010; Yang et al., 2013). Surrounding data describes the records that occur before and after a given timeline record. Using surrounding data, a given record can be reassessed and potentially corrected if required. This works by assessing the surrounding data of a record. If a certain amount of the surrounding data records are assessed as intrusive, then it is concluded that the surrounded record is also intrusive. If a certain amount of the surrounding data records are not intrusive, the surrounded record will be determined to be a legitimate record.

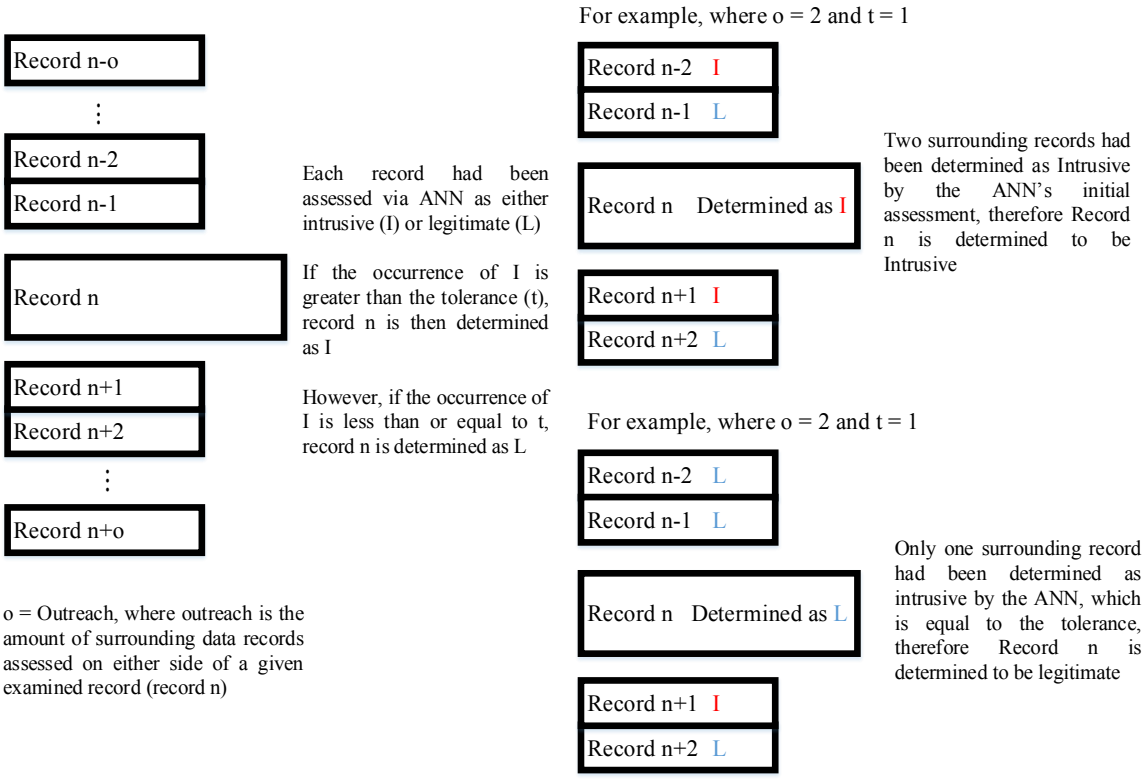


Figure 2 Diagram describing self-correction via surrounding data records

The self-correction process works by examining records that occur before and after a current record, based on a configurable outreach, and adjusts an initial assessment of a record, whether it is intrusive or legitimate, by examining the initial assessments of the surrounding records. If the numbers of records surrounding the examined record, within the given outreach, that is different to the examined record exceed a threshold value, which is also configurable, the examined record is changed to match the different records.

Adjusting self-correction through context awareness

Different conditions that include erratic user behaviour, overtrained ANNs or less distinguishable intruders require different approaches to mitigate (Piotrowski & Napiorkowski, 2013; Tetko, Livingstone, & Luik, 1995). A dynamic approach that can apply changes to assessment when required will allow a given problem to be mitigated without causing another problem.

Context awareness was applied to self-correction to allow for the tolerance of potential false assessments to be adjusted. If false positives occur frequently, tolerance was increased so that false positives that would otherwise remain incorrect can be changed. In the same way that false positives can be accounted for, false negatives that would evade the self-correction process can be caught by adjusting the tolerance to be lower. The context-awareness component adjusts tolerance whenever a false positive or false negative was identified and corrected using self-correction. Whenever a record was not identified as false, the tolerance was changed to be closer to the default.

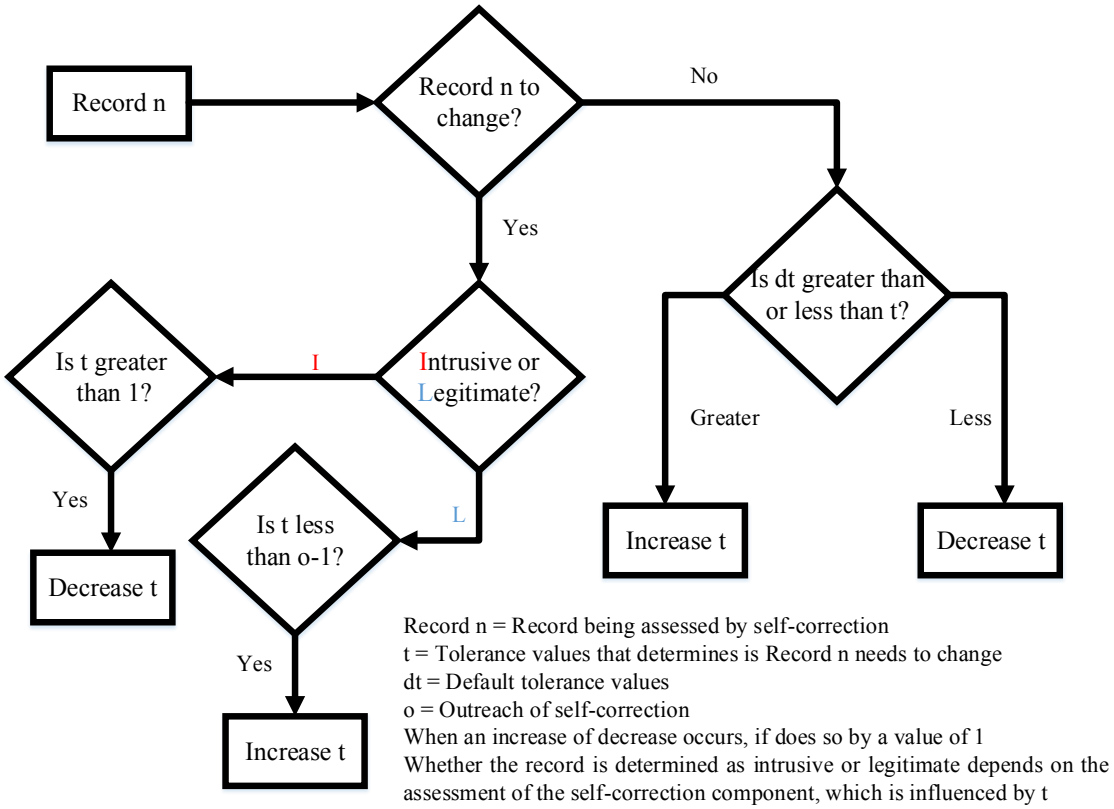


Figure 3 Flowchart of the context-aware component working with the self-correction component

The context-aware component adjusts the threshold of the self-correction component to be either more restrictive when false negative has recently been detected and changed or less restrictive when a false positive has recently been detected and changed. If no changes had been made due to caught false positives or false negatives, the context-aware component either does nothing or changes to be closer to the default self-correction threshold.

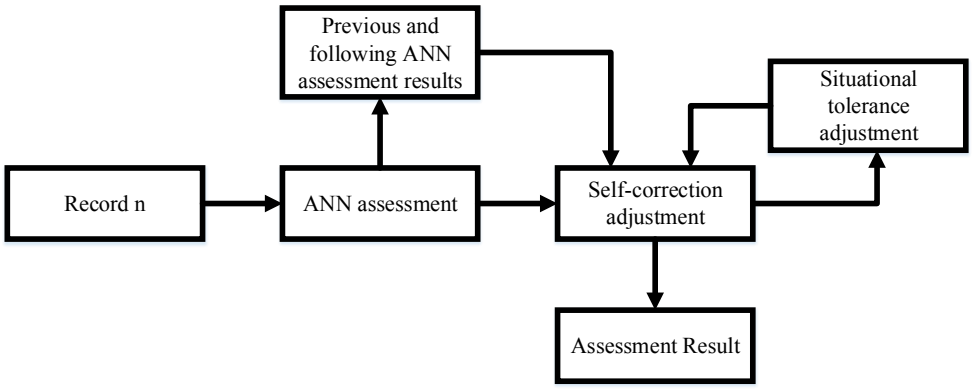


Figure 4 Overview of a record being processed through ANN combined with both intrusion detection components.

The overall process, as described by Figure 4, examines each record which are assessed by the ANN, previous and following assessments are also retrieved. The self-correction component adjusts the assessment of the ANN based on the previous and following record assessment, the ANN's assessment and the threshold adjustment made by the context-aware component. The self-correction component sends the result to the context-aware component which, based on the situation, will make a tolerance threshold adjustment to the self-correction component for the next record. The result from the self-correction component is also the final result for the record.

EXPERIMENT RESULTS

To test the capabilities of the applied intrusion detection methods of improving behaviour-based authorisation performance, three systems were developed. The base ANN (treatment script 1) served as the baseline for experimentation and the ANN with a self-correction component and context-awareness (treatment script 3) component served as the end-line. The base ANN with only the self-correction component was also assessed (treatment script 2). Each system was tested on 14 user pair datasets, where each pair consisted of training data from a legitimate user, test data from a legitimate user and test data from an intrusive user. Data for these 14 datasets was produced from the MIT reality mining dataset (Eagle & Pentland, 2006).The mean overall accuracies, false positive rates and true positives rates for each system applied to each dataset were examined.

The overall accuracy of a behaviour-based authorisation method depends on the rate that it can determine intrusive activity, as well as the rate that it produces false positives from legitimate activity. Overall accuracy did not always increase, but did for four of the 14 datasets demonstrating its capability to do so. Examining the mean result for all datasets together found that the overall accuracy did increase but not significantly.

False positives are legitimate activities mistaken for intrusive activities. Overall, the mean false positive rate was reduced when the intrusion detection components were applied. With the exception of two datasets, the behaviour-based authorisation method with intrusion detection concepts applied was able decrease false positives to below 5%.

True positives are intrusive activities correctly identified as intrusive. Overall the mean true positives rate was found to be less when both intrusion detection concepts had been applied. The self-correction component significantly increased the true positive rate, but this was always reduced with the application context-awareness. It was also found that if the base ANN had a true positive below 10%, the behaviour-based authorisation method with both intrusion detection concepts would perform at a rate below 5%, in most cases 0%.

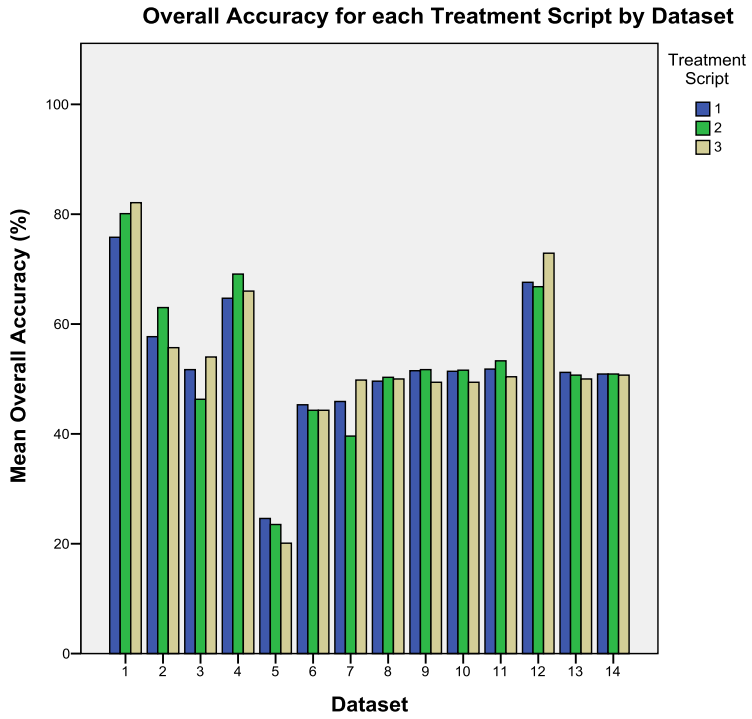


Figure 5 Bar chart of different mean overall accuracies separated by Dataset and Treatment Script, with datasets 1 through to 14 being plotted across treatment scripts 1, 2 and 3.

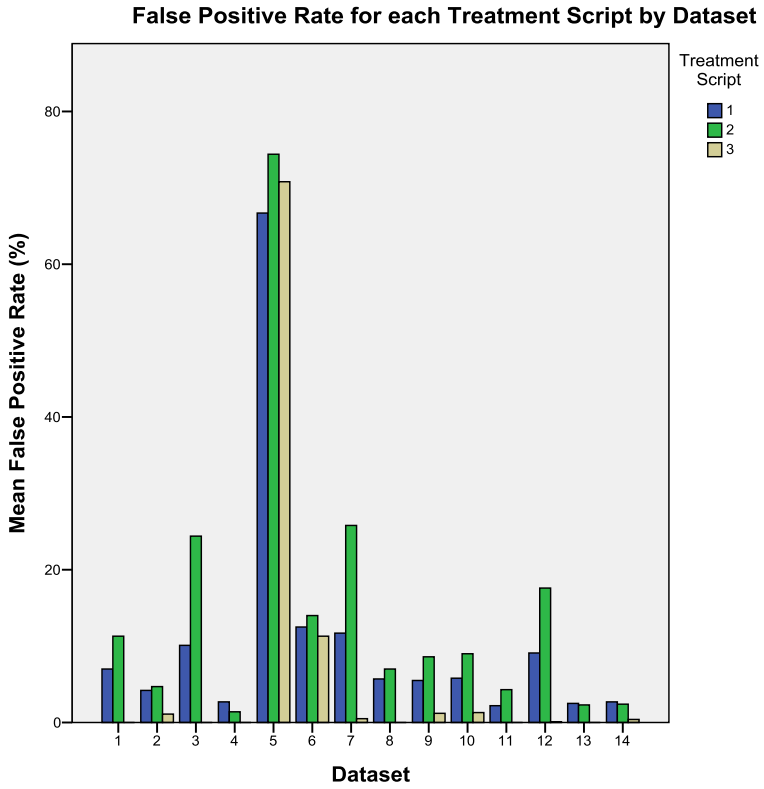


Figure 6 Bar chart of different mean false positive rates separated by Dataset and Treatment Script, with datasets 1 through to 14 being plotted across treatment scripts 1, 2 and 3.

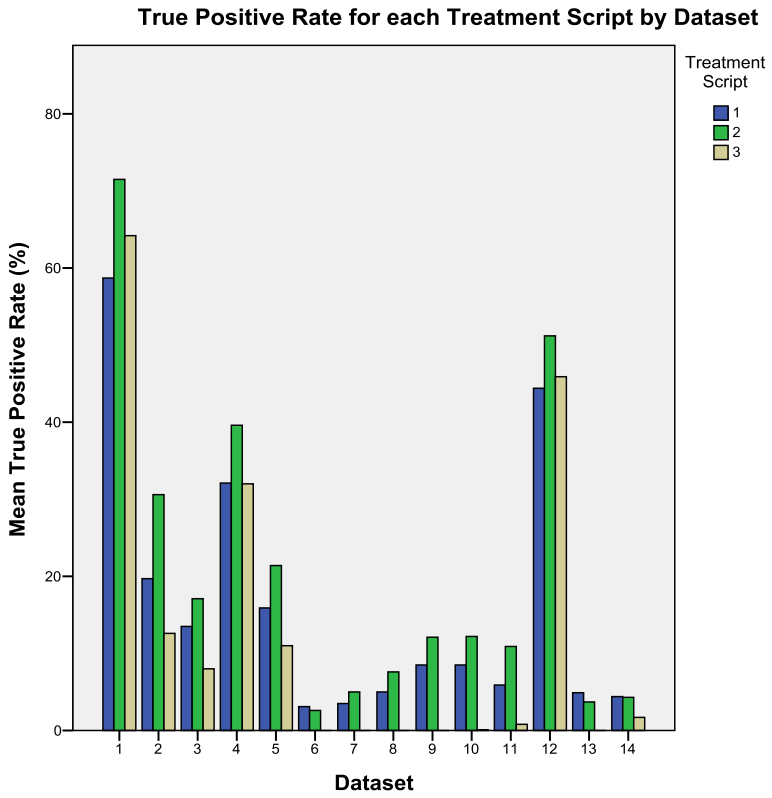


Figure 7 Bar chart of different mean true positive rates separated by Dataset and Treatment Script, with datasets 1 through to 14 being plotted across treatment scripts 1, 2 and 3

CONCLUSION

This research involved the development of modular components based on intrusion detection methods to find out whether or not said intrusion detection methods can improve the performance of behaviour-based authorisation on mobile devices. The intrusion detection methods were based around:

- Self-correction
- Context awareness
- Hybridisation

The results of experimentation found that the performance of a behaviour-based authorisation method for mobile devices can be improved by applying a hybrid self-correction and context-aware intrusion detection component, but only if the initial base behaviour-based authorisation method can detect intrusions at a rate of at least 10%. The self-correction intrusion detection component, when added, improved intrusion detection rates but increased the rate of false alarms. The hybrid self-correction and context-aware components, when applied, reduced false alarms to an average rate of below 5%, many producing a rate of 0%. However, the hybrid self-correction and context-aware components also reduced true positive (intrusion detection) rates for most datasets. Although the false positive reduction indicates an increase in performance, if the intrusion detection rate falls to 0, the performance of a behaviour-based authorisation method is also effectively 0. The experiments found that if the base behaviour-based authorisation method's intrusion detection rate was at least 10%, the intrusion detection rate would not fall to 0 when the hybrid self-correction and context-aware components are applied.

A reduction in false positives indicates an improvement of performance for a behaviour-based authorisation method, as it maintains the accessibility of a device while potentially preventing breaches of privacy and integrity. However if the ability to detect intrusions does not exist, the performance of a behaviour-based authorisation method also does not exist, regardless of lower false positive rates. As an improvement to the performance of the behaviour-based authorisation method only appears to occur when the initial method has an

intrusion detection rate of 10% or higher, future research should focus on experimenting with other behaviour-based authorisation methods that are capable of fulfilling the requirements for improvement.

REFERENCES

Anandarajan, M. (2002). Profiling Web Usage in the Workplace: A Behavior-Based Artificial Intelligence Approach. *Journal of Management Information Systems, 19*(1), 243-266. doi: 10.2307/40398573

Chang, G. W., Cheng, I. C., & Yu-Feng, T. (2010). Radial-Basis-Function-Based Neural Network for Harmonic Detection. *Industrial Electronics, IEEE Transactions on, 57*(6), 2171-2179. doi: 10.1109/TIE.2009.2034681

Eagle, N., & Pentland, A. (2006). Reality mining: sensing complex social systems. *Personal and Ubiquitous Computing 10*(4), 255-268. doi: 10.1007/s00779-005-0046-3

Federal-Communications-Commission. (2014). *Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP)*. US: Technological Advisory Council.Retrieved from https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12414/TAC-MDTP-Report-v1.0-FINAL-TAC-version.pdf

Home-Office. (2014). Reducing Mobile Phone Theft and Improving Security. *The Behavioural Insights Team.* Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/390901/HO_Mobile_theft_paper_Dec_14_WEB.PDF

Krenker, A., Kos, A., & Bešter, J. (2011). *Introduction to the artificial neural networks*: INTECH Open Access Publisher.

Li, F., Clarke, N., Papadaki, M., & Dowland, P. (2013). Active authentication for mobile devices utilising behaviour profiling. *International journal of information security, 13*(3), 229-244. doi: 10.1007/s10207-013-0209-6

Li, F., Wheeler, R., & Clarke, N. (2014). An Evaluation of Behavioural Profiling on Mobile Devices *Human Aspects of Information Security, Privacy, and Trust* (pp. 330-339): Springer. doi: 10.1007/978-3-319-07620-1_29

Majeed, K., Jing, Y., Novakovic, D., & Ouazzane, K. (2014). Behaviour Based Anomaly Detection for Smartphones Using Machine Learning Algorithm*International conference on Computer Science and Information Systems*, *held in Dubai (UAE),* 17th-18th October 2014: International Institute of Engineers.

Patel, A., Qassim, Q., Shukor, Z., Nogueira, J., Júnior, J., Wills, C., & Federal, P. (2011). *Autonomic agent-based self-managed intrusion detection and prevention system.* Paper presented at the Proceedings of the South African Information Security Multi-Conference (SAISMC 2010), Port Elizabeth, South Africa

Piotrowski, A. P., & Napiorkowski, J. J. (2013). A comparison of methods to avoid overfitting in neural networks training in the case of catchment runoff modelling. *Journal of Hydrology, 476*, 97-111.

Schmeck, H., Müller-Schloer, C., Çakar, E., Mnif, M., & Richter, U. (2010). Adaptivity and self-organization in organic computing systems. *ACM Transactions on Autonomous and Adaptive Systems (TAAS), 5*(3), 10. doi: 10.1145/1837909.1837911

Shi, E., Niu, Y., Jakobsson, M., & Chow, R. (2011, 25th October 2010). *Implicit authentication through learning user behavior.* Paper presented at the Proceedings of the 13th international conference on Information security, Boca Raton, FL, USA. doi: 10.1007/978-3-642-18178-8_9

Sood, S., Mehmi, S., & Dogra, S. (2015, 19th-20th March 2015). *Artificial intelligence for designing user profiling system for cloud computing security: Experiment.* Paper presented at the Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in, Ghaziabad, India. doi: 10.1109/ICACEA.2015.7164645

Spathoulas, G. P., & Katsikas, S. K. (2010). Reducing false positives in intrusion detection systems. *Computers & Security, 29*(1), 35-44. doi: http://dx.doi.org/10.1016/j.cose.2009.07.008

Tapellini, D. (2014). Smart phone thefts rose to 3.1 million in 2013. *Consumer Reports.* Retrieved from http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm

Tetko, I. V., Livingstone, D. J., & Luik, A. I. (1995). Neural network studies. 1. Comparison of overfitting and overtraining. *Journal of Chemical Information and Computer Sciences, 35*(5), 826-833. doi: 10.1021/ci00027a006

Wasserman, P. (1989a). The Backpropagation Training Algorithm *Neural Computing: Theory and Practice* (pp. 44-54). New York: Van Rostrand Reinhold.

Wasserman, P. (1989b). Fundamentals of Artificial Neural Networks *Neural Computing: Theory and Practice* (pp. 11-26). New York: Van Rostrand Reinhold.

Yang, Q.-L., Lv, J., Tao, X.-P., Ma, X.-X., Xing, J.-C., & Song, W. (2013). Fuzzy self-adaptation of mission-critical software under uncertainty. *Journal of Computer Science and Technology, 28*(1), 165-187. doi: 10.1007/s11390-013-1321-9

Yassin, W., Udzir, N. I., Muda, Z., & Sulaiman, M. N. (2013). *Anomaly-Based Intrusion Detection through K-Means Clustering and Naives Bayes Classification.* Paper presented at the Proceedings of the 4th International Conference on Computing and Informatics (ICOCI), Sarawak, Malaysia. doi: 10.1109/CITA.2011.5999520

UNDERSTANDING AND COMBATTING TERRORIST NETWORKS: COUPLING SOCIAL MEDIA MINING WITH SOCIAL NETWORK ANALYSIS

Benn Van Den Ende
School of Science, Edith Cowan University, Perth, Australia
bvandene@our.ecu.edu.au

Abstract

Throughout the past decade the methods employed by terrorist organisations have changed drastically. One of these key changes has been associated with the rise of social media such as Facebook, Twitter, YouTube and blogging in general. Terrorist organisations appear to be using the wide reach and vast network capabilities created by social media to disseminate propaganda, radicalise susceptible individuals, recruit potential fighters and communicate strategic and operational objectives. However, this growing terrorist presence on Social Media can also offer invaluable insights into the social networks of terrorist organisations through the use of Social Media Mining and Social Network Analysis. By coupling these two techniques together, researchers can gain a greater understanding of how to combat and possibly destabilise complex terrorist social networks and aid in the fight against radicalisation and terrorism.

Keywords
Terrorism, National Security, Social Network Services, Social Groups, Social Network Analysis, Social Media

INTRODUCTION

Throughout the past decade the nature of terrorism has changed enormously. Through the changing global economy, to the universal issues facing all nations today such as climate change, the face of terrorism is a very different, and as many would observe, a more frightening one. While the core of terrorism may be tenacious in its changeability, with political, religious and ideological violence still the most common claims to terrorist action, arguably the biggest change has come from Social Media. Social Media has opened up new ways for radical thinkers to communicate, network, plan and operate. Social media sites such as Facebook, Twitter, YouTube, Myspace, and Blogging sites in general, have fundamentally and irrevocably changed the platform for terrorist networking in the 21st century. While social media has opened up extraordinary avenues for socialising, sharing information, rallying for political and social causes, and identity formation, it has also made combatting terrorism exponentially more difficult due to the sheer magnitude of data exchanged and retained . With a change in the medium of terrorist networking and organisation, so too must there be a change in the way we investigate, understand and counter terrorist networks – and Social Network Analysis (SNA) coupled with Social Media itself, may have the answer. This paper will explore how SNA can be used to analyse data collected through Social Media Mining to help map out and analyse terrorist networks. This coupling can be immensely helpful for future researchers studying terrorist networks, as well as law enforcement and intelligence agencies.

Social network analysis and terrorism

Social Network Analysis was developed in the 1950's as a methodology for investigating relations between actors. Where traditional social science methods focused predominantly on the individual as the primary source of social data, SNA re-directed the focus on the relations *between* the actors rather than on the actors themselves (Knoke & Yang, 2008). By doing this, SNA practitioners could observe the nuanced dynamics between individuals, groups, corporations, nation-states, etc. often providing a rich source of meaningful information not obtainable through traditional social science research methods. SNA was then quickly adopted in many different disciplines including: criminology, where it was/is used to map criminal organisation structure and analyse the power dynamics, distribution and crime patterns of its key players. Anthropology, where tribal, urban and informal groups are mapped to aid in understanding the formal and informal social structures. And the health sciences, where diseases such as Avian flu and HIV/AIDS can be geographically mapped and better prevented through the focus on interactions between infected individuals. With the many benefits of SNA presenting themselves in various disciplines, recently, scholars have begun unleashing SNA's unique analytic capabilities on the study of terrorism, and more specifically, terrorist networks (these scholars' works will be explored later).

As Perliger and Pedahuzer (2011) note students appear to be reluctant in using SNA as "the majority of political violence students have very limited acquaintance with the rationale, main concepts, and methodological tools of SNA… and consequently tend to express doubt in regard to its efficiency and relevance for the study of complex social phenomena" (Perliger and Pedahuzer, 2011, pp:45). This unfortunate point leads to an oversight in the important, rich and meaningful results, that can be obtained in terrorism studies through the use of SNA. SNA is a research tool that is rarely included as part of the curriculum in social science departments at universities, with most students not even hearing about it well into their post-graduate studies. With the advances in technology, specifically the personal computer, there was a sharp ascent in SNA popularity which was the direct result of the development of SNA software, most notably UCINET, Pajek, NetMiner, STRUCTURE and MultiNet (Knoke & Yang, 2008). However, SNA remained a relatively nuanced research methodology within Terrorism and Security Studies, not often practiced by scholars. Having said this, there has been a small group of academics who have completed research in terrorism studies using SNA methodologies.

Scholar Karl Van Meter, following the 9/11 terrorist attacks in New York City used SNA, specifically Link Analysis to describe various forms of network research including adversary networks and traffic analysis in relation to phone surveillance. Van Meter's study examined this topic by focusing on the US Army from World War II to the late 1960s, against the IRA in Northern Ireland in the 1970s and well into the modern era (Van-Meter, 2001). By using SNA in the study of terrorism, Van Meter was able to identify weaknesses in certain terrorist networks which would otherwise not have been uncovered through traditional social science approaches. Going one step further, Kathleen Carley specifically targeted her research at destabilising covert networks. Through SNA networks she was able to identify weaknesses in the social networks and accurately develop strategies to combat and destabilise them (Carley, 2006). Similar to Carley (2006), Krebs (2002) points out the difficulty in mapping covert terrorist cells and offers insights into how SNA can be used in future research for this purpose (Krebs, 2002). However, as Perliger and Pedahuzer note, "even though their [post September 11 SNA scholars] studies showed strong potential in providing significant insights into the structures and internal processes of terrorist groups, the use of SNA in the study of political violence has remained quite limited and still amounts to only a small fraction of the research in the field" (Perliger & Pedahzur, 2011). One of the reasons scholars of Terrorism and Security studies have not been inclined to use SNA techniques is due to the assumption that Social Network Analysis is often hindered by difficulties in data collection. However, the rise of social media may be a solution to this problem.

Social Media as a Data Source for SNA

The use of Social Media as a data source in SNA has been growing over the last decade, since the rise of Social Media in general. The data is often gathered through data mining, using software specifically designed to pinpoint keywords, to more laborious methods, such as manually scouring hashtags, as in the case of twitter. However, with the large number of individuals participating in social media, creating, engaging with and disseminating networks, social media makes an excellent source for SNA data collection.

Data collection methods vary from site to site; however common approaches can be identified. Sites such as Twitter and Instagram allow data to be collected directly from the application programming interface (API), such as the method used by Community Studies scholars Wayne Williamson and Kristian Ruming (Williamson & Ruming, 2016). Data collection through the API is also possible for the social network site Facebook, however recent important changes to the privacy permissions of the application have barred access to specific data such as the sharing of 'Friend's' information. However, core data sets are still accessible within the Facebook API, allowing the researcher access to useful network data Networks can also be traced and linked through hashtags, a type of metadata label which works similarly to a hyperlink but with a broader focus on social interaction (Chang & Iyer, 2012). Blogging works similarly in that social interaction and 'sharing' are key to the function of the site, allowing a data collector or researcher access to already established digital networks. Scholars have taken advantage of these large amounts of accessible data for research in varying disciplines such as Community Studies, Political Science, Psychology and Pedagogy. See (Norman, Nordin, Din, Ally, & Dogan, 2015), (Fu, Cheng, Wong, & Yip, 2013), (Williamson & Ruming, 2016) and (Lucente & Wilson, 2013). Having said this there has been little use of Social Media data combined with SNA techniques in the study of terrorism.

While data collected through social media has been used in terrorism studies, it has rarely been integrated and analysed through SNA. It is well documented that terrorist propaganda, social networks and recruitment processes are disseminated through social media. However, the overwhelming majority of literature featuring the key words "Social Media" and "Terrorism" is concerned with the use of social media by terrorist organisations, rather than using social media as a data gathering tool to aid in the understanding and combat of terrorism. See (Dean, Bell, & Newman, 2012), (Marhu & Balteanu, 2014) and (Markon, 2016). Many academics, including the

above authors have documented the use of social media by terrorist organisations and how this creates a risk of online radicalisation to susceptible individuals. They also address the international network potential of terrorist groups and organisational prowess made possible by social media. However, as mentioned above there appears to be very little research that takes advantage of the relatively large radical and terrorist presence on social media as a data source for combatting terrorism and extremism.

This paper identifies 3 key advantages of using Social Media data with SNA in terrorism studies

1. International terrorist networks are easier to link together: While other methods of research into terrorist networks may be somewhat effective at identifying primitive links between key actors, they are rarely useful in mapping international connectedness.
2. The majority of Social Media data is open-source: Due to the covert and confidential nature of terrorism, data collection is often limited to news reports and declassified government documents, which are often outdated and no longer relevant. Social Media data, for the most part, is open to any individual with the abilities to mine it. This coupled with the large use of Social Media by terrorist organisations exposes a gold-mine of terrorist network data
3. Social Media Mining circumvents the risks of field research: Due to the violent nature of terrorist groups, ethnographic field research often comes with great risks to the researcher's well-being. While this method of research offers extensive and important ethnographic data, it is often very dangerous and thus rarely undertaken. Social Network data mining and SNA can be completed externally, with extra protection possibilities provided through secure servers and networks. This method of research eliminates the dangers experienced by the field researcher and allows for more varied and automated data gathering techniques.

With this in mind, it is also important to outline the disadvantages of using Social Media data with SNA in terrorism studies. SNA being a quantitative research methodology misses out on the detailed subject centred approach that qualitative studies offer. Ethnographic studies for example while limited in their scope, offer a much more detailed analysis of the human experience involved in terrorism. The other key disadvantage evident is the fact that not all terrorist organisations use social media. This can lead to a gap in data, which can cause misleading analyses. Having said this, specific research methods should not be used in isolation. SNA and Social Media Mining should be used as a complimentary research approach. Combining qualitative and quantitative research methods can lead to a more rounded approach to studying terrorism, therefore the disadvantages of SNA and Social Media Mining should not be seen as a problem when appropriately complimented.
These above mentioned three key advantages of coupling Social Media Mining with SNA as a research methodology position the researcher at a key advantage to others in the field of terrorism studies.

IMPLICATIONS

Data gathered from social media sites and applications can be integrated in SNA to produce insightful analyses into various aspects of extremism and terrorism. This coupling can provide invaluable insights into the network, power relations, distribution patterns and radicalisation trends of terrorist networks. Additionally, the advantages are not limited to analysis and understanding, they also offer integral practical applications. Through understanding the structure and most importantly, the key relations within terrorist social networks, researchers and security agencies will be able to effectively identify vulnerabilities in the network, which could ultimately expose opportunities to destabilise networks as a counter-offensive tactic. Thus, the use of Social Media data in SNA can be employed in counter-terrorism as well. Several variables must be addressed during the planning and operational stage of such research; therefore, this paper will not publish such results here. However, this paper hopefully exposes important and useful techniques in understanding terrorist networks for future research to explore, allowing for a more in depth discussion on the analytical capabilities of the coupling of SNA with social media mining.

CONCLUSION

The analytic capabilities of SNA in Terrorism Studies are invaluable, however there is a peculiar lack of research done using SNA techniques. This appears to come down to a lack of in-depth conceptual understanding of the methodology. However, by combining the data mining resources of Social Media, a domain which is populated by many terrorist organisations, with the relation focused analytic capabilities of Social Network Analysis, we may be able to better understand and ultimately combat terrorist networks which threaten national and global security. This article offers only a brief outline of the capabilities of the proposed research method, but hopefully illuminates possible approaches to terrorism that may be adopted by future researchers as well as law enforcement and intelligence agencies.

REFERENCES

Carley, K. (2006). Destabilization of covert networks. *Computational and Mathematical Organization Theory, 12*(1).

Chang, H.-C., & Iyer, H. (2012). Trends in Twitter Hashtag Applications: Design Features for Value-Added Dimensions to Future Library Catalogues. *Library Trends, 61*(1), 248-258. doi: 10.1353/lib.2012.0024

Dean, G., Bell, P., & Newman, J. (2012). The Dark Side of Social Media: Review of Online Terrorism. *Pakistan Journal of Criminology, 4*(2).

Fu, K.-w., Cheng, Q., Wong, P. W. C., & Yip, P. S. F. (2013). Responses to a Self-Presented Suicide Attempt in Social Media. *Crisis, 34*(6), 406-412. doi: 10.1027/0227-5910/a000221

Knoke, D., & Yang, S. (2008). *Social Network Analysis* (2 ed.). Illinois: Sage Publications.

Krebs, V. (2002). Mapping Networks of Terrorist Cells. *Connections, 24*(3).

Lucente, S., & Wilson, G. (2013). Crossing the Red Line: Social Media and Social Network Analysis for Unconventional Campaign Planning. *Special Warfare*, 20-26.

Marhu, M., & Balteanu, C. (2014). SOCIAL MEDIA-A REAL SOURCE OF PROLIFERATION OF INTERNATIONAL TERRORISM. *Annales Universitatis Apulensis, 16*(1), 162-169.

Markon, J. (2016). Homeland security to amp up social media screening to stop terrorism, johnson says, *The Washington Post*.

Norman, H., Nordin, N., Din, R., Ally, M., & Dogan, H. (2015). Exploring the Roles of Social Participation in Mobile Social Media Learning: A Social Network Analysis. *International Review of Research in Open and Distributed Learning, 16*(4), 205-224.

Perliger, A., & Pedahzur, A. (2011). Social Network Analysis in the Study of Terrorism and Political Violence. *Political Science and Politics, 44*(1).

Van-Meter, K. (2001). Terrorists/Liberators: Researching and Dealing with Adversary Social Networks. *Connections, 24*(3).

Williamson, W., & Ruming, K. (2016). Using Social Network Analysis to Visualize the Social-Media Networks of Community Groups: Two Case Studies from Sydney. *Journal of Urban Technology*. doi: 10.1080/10630732.2016.1197490

FUTURE OF AUSTRALIA'S ETP: SCRIPT EXCHANGE, SCRIPT VAULT OR SECURE MOBILE ALTERNATIVE

Kyaw Kyaw Htat[1], Patricia A H Williams[2], Vincent McCauley[3]
[1]Edith Cowan University, [2]Flinders University, [3]McCauley Software
khtat@our.ecu.edu.au, patricia.williams@flinders.edu.au, vincem@mccauleysoftware.com

Abstract
Electronic transfer of prescriptions is an essential element of electronic medications management. Unfortunately, current manual and preliminary electronic transfer of prescription methods are not patient focussed, leading to a suboptimal solution for the patient. This is increasingly relevant in the push for more patient engagement in their own healthcare. The area is highly controlled by legislation and regulation. Through research and an analysis of the possible methods to improve and personalise electronic transfer of prescriptions, this paper provides an overview of these conclusions, and presents an alternative technical solution. The solution has been derived from a number of experiments in data transfer techniques using a mobile phone. The paper explains how this meets the current regulations and legislation, as well as providing a patient centred approach to the problem. Ultimately, healthcare outcomes will improve where patients are given the opportunity and the tools to better engage in their own healthcare management, and secure electronic transfer of prescriptions with patient access to their own medication lists may improve compliance and reduce healthcare costs.

Keywords
ePrescription transfer, ePrescription security, mobile transfer of ePrescription, eTP, mobile eTP

INTRODUCTION

The use of electronic prescription (eTP) is the lifeblood of eHealth and in improving quality of care through better medication compliance, improved prescribing accuracy and efficiency while reducing the adverse drug events. In fact, electronic prescribing is an essential initial step of the electronic Medication Management (eMM) program which primarily focuses on improving medication-related outcomes through better quality and availability of medications-related healthcare information ("NEHTA Blueprint V2", 2011). Having an effective medication management system in place improves medication compliance and reduces adverse drug events. A recent study indicates almost 70,000 hospital admissions per year are associated with adverse drug events and poor medication compliance/adherence. This significantly contributes to having undesirable patient outcomes such as hospital readmission or even loss of life (White, 2015). The use of eTP enables eMM to reduce these undesirable outcomes and to prevent excessive use of healthcare expenditure while providing better patient safety.

Current eTP implementation converts the conventional manual prescription process/model to a digital equivalent using two Prescription Exchange Services (PES), *Script Exchange* from *eRx* and *Script Vault* from *MediSecure* (Htat, Williams, & McCauley, 2015a). Using these PES services, prescribers can upload the electronic copy of the prescription for later download and dispense by the pharmacies. The use of electronic prescription exchange not only connects the two major healthcare providers such as clinicians and pharmacists, but it also paves the way to create a national medication repository. Such a repository would allow clinicians, pharmacists, aged care facilities and hospitals to see a combined list of prescribed and dispensed medications regardless of how many different doctors and pharmacies the patient has visited. However, current implementation of eTP is an expensive operation to maintain as an ongoing process for the nation. The associated electronic prescription fees for each prescription downloaded from PES used to be as much as AU$ 0.85 prior to achieving the interoperability between the two PES services. Some negotiations and cooperation between the Commonwealth, the Pharmacy Guild and the two PES operators managed to reduce the electronic prescription fees to AU$ 0.15 per eligible prescription. This electronic prescription fees has, so far, been subsidised by the Commonwealth through a series of Community Pharmacy Agreements (CPA). However, the section 6.1.3 and Appendix-B of the current agreement, Sixth Community Pharmacy Agreement (6CPA), states that funding from 1st July 2016 and onwards will be subject to a cost-effectiveness assessment by an independent health technology assessment body as determined by the Minister ("The Pharmacy Guild of Australia", 2015). Since the eligibility criteria for this subsidy can be tightened or amended to the disadvantages of the pharmacies (i.e. current eTP implementation being a pharmacy user-pay system) ("FAQs", 2016), exploration of cheaper alternatives with comparable security measures to the current use of eTP is commendable.

WHAT ETP STANDARDS AND SPECIFICATIONS MANDATES VS CURRENT ETPIMPLEMENTATION

There are numerous standards and mandates regulating the management of medications in Australia. These include the Electronic Transaction Act (ETA) and various Acts and Regulations governing the Poisons and Therapeutic Goods. They have been repealed and/or amended at the Commonwealth as well as State and Territory level to accommodate the implementation of eTP in Australian healthcare. Figure 1 briefly depicts how these Acts and Regulations fit together to enable the current eTP implementation. It also demonstrates how the legislation and regulations in Australia are constructed and the complexity of this construction for eTP. The outermost circle represents the encompassing regulation for the entire nation. The next inner circle defines the regulations for each State and Territory amended as per jurisdictional legislative requirements. These two circles enable the use of electronic transactions at national, state and territory levels thus making the use of eTP and other electronic transactions possible. The third circle lists Acts and Regulations governing the Poisons and Therapeutic Goods for each jurisdiction which play a major role in enabling the use of eTP. The centre circle contains various standards and specifications developed reflecting those national and jurisdictional legislative requirements. It is named Dante's 4 circles of eTP as the closer the circle is to the centre of the diagram the more eTP specific it becomes in a similar way the 14th century poet Dante Alighieri's depiction of nine circles of hell (i.e. lower circles are for more severe sins).

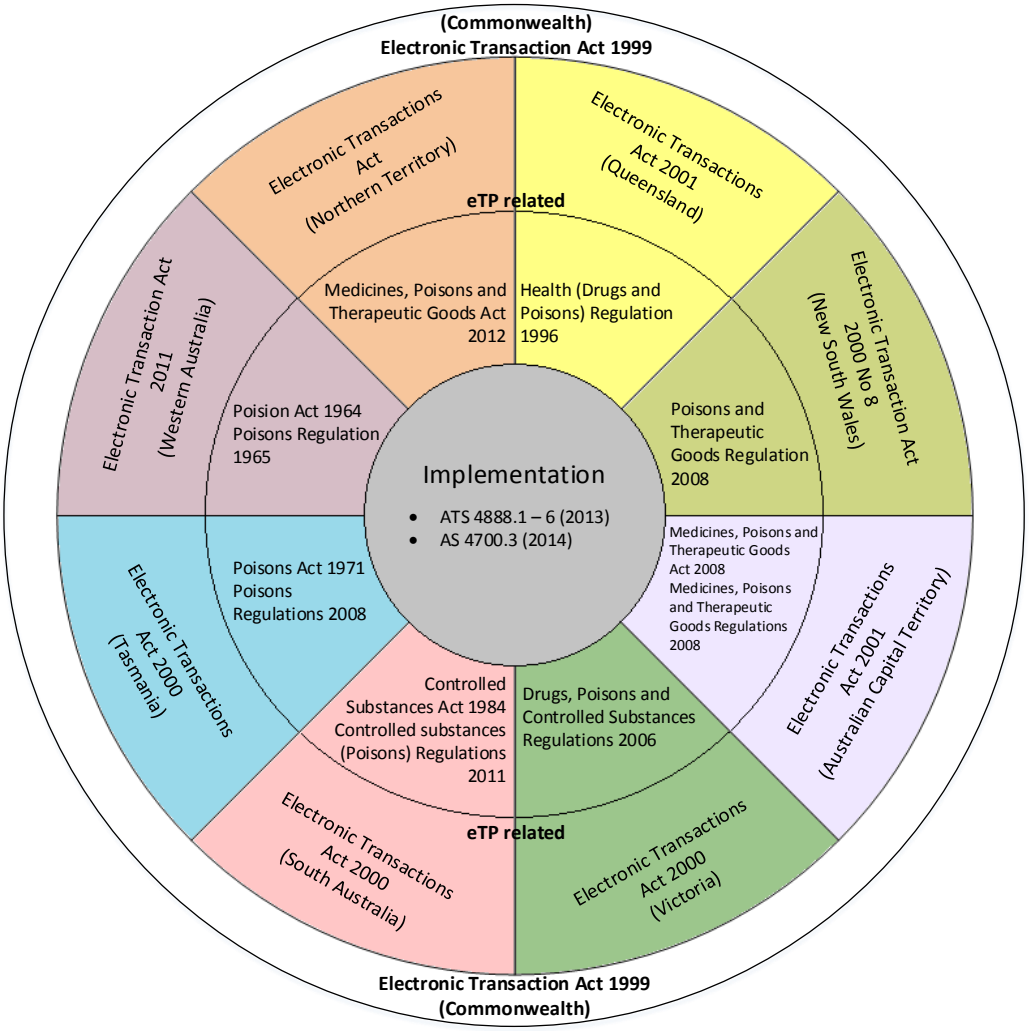


Figure 1. Dante's 4 circles of eTP

The Commonwealth Electronic Transaction Act 1999 facilitates the use of electronic means and enables the use of electronic communications in dealings with government, business and community for the future economic and social prosperity of Australia. Various States and Territories amend/adopt this overarching Act to suit their jurisdictional legislative requirements. This jurisdictional ETA and various Acts and Regulations governing the Poisons and Therapeutic Goods for each jurisdiction dictate the requirements for eTP implementation in that jurisdiction. After all the eTP requirements of all jurisdictions have been considered, various standards and

specifications have been developed reflecting those requirements. Among these related standards and specifications, ATS4888 series and AS4700.3 primarily govern the implementation of eTP. Current eTP implementation developed in compliance with these standards and specifications is briefly depicted in Figure 2.

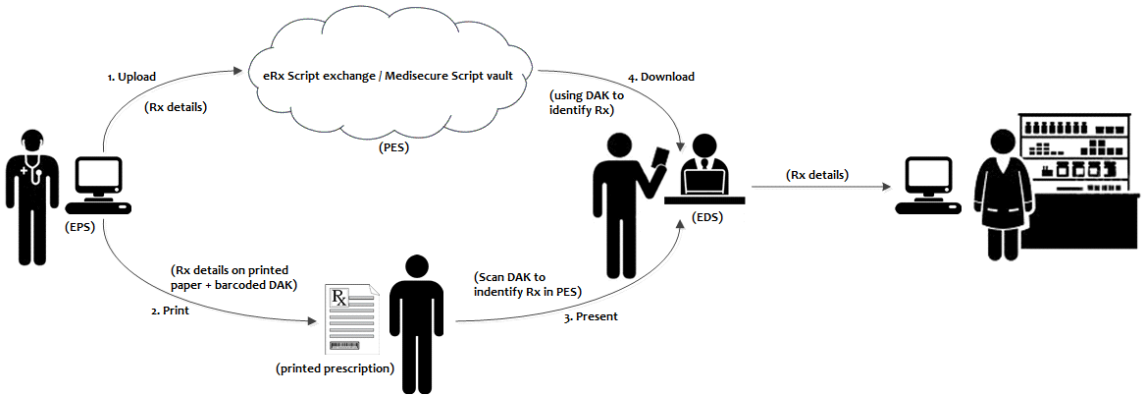


Figure 2: Current electronic prescription transfer model using PES (Htat, Williams, & McCauley, 2015a)

Although ATS4888.2 of the ATS4888 series particularly emphasizes on the platform independent model, it also includes specific details on securing electronic prescription information from the security of the data-at-rest perspective. It mandates that the electronic prescription to be encrypted using a symmetric key derived from the Document Access Key (DAK) before being stored on PES. DAK is the barcode printed on the paper prescription created by any eTP enabled electronic prescribing system. The current eTP implementation also makes use of DAK for authorizing access to the prescription stored on the PES and decrypting it after being downloaded from PES. In addition, section 7.3.3 of the ATS4888.2 strictly prohibits storing of DAK or any of its derived key on any stable storage (i.e. non-volatile storage) unless they have been encrypted using 128 bit encryption. Further details on securing electronic prescription from the security of data-at-rest perspective can be found in sections 5.3.3 - 5.3.4, 5.3.6 - 5.3.7 and 7.3.3 of the ATS4888.2. These sections provide an overview of the security mechanism implemented using the DAK for safeguarding prescription information. Figure 3 briefly illustrates how this security mechanism works.

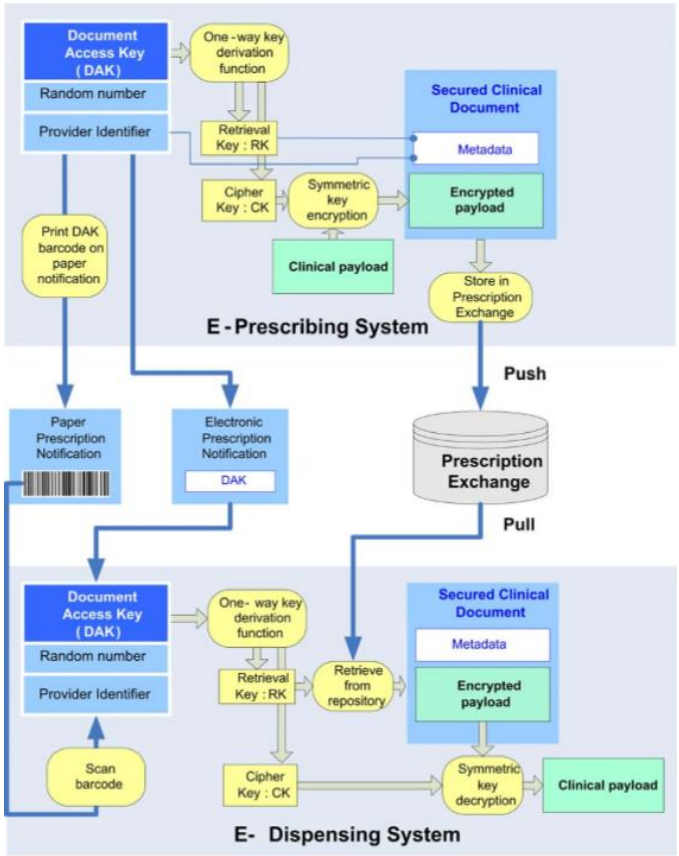


Figure 3: DAK usage for storage and retrieval of prescription with PES (Standards Australia, 2013, Figure 19)

On the other hand, although ATS4888.2 contains specific details on securing prescription information from security of data-at-rest perspective, it mentions very little on securing the prescription information from data-in-transit (i.e. data in motion) perspective. Both sections 5.3.5 and 7.3.3 of ATS4888.2 mention that securing prescription information from data-in-transit perspective entirely relies on the security and encryption mechanism of the implementation platform and the eTP technical specification for that platform. Research on eTP to date has not encountered any other standard or specification which includes further details on securing prescription information from data-in-transit perspective. Security in this context appears to be solely relying on existing industrial standards and best practices. Current implementation of eTP (i.e. both PES services) implements the simple Subscriber-Provider pattern instead of publishing their service endpoints using Endpoint Location Services (ELS) service infrastructure (Htat, Williams, & McCauley, 2016). Moreover, current eTP implementation does not utilize other eHealth infrastructural components such as Health Identifiers (HI) Services. Unfortunately, this leaves current eTP implementation considerable room for future improvement from security perspective.

Another disadvantage of the current eTP is its associated ongoing cost, the electronic prescription fees. Although the combined effort of the Commonwealth, the Pharmacy Guild and the two PES operators could reduce the fees to AU$ 0.15 per eligible prescription, it is still a taxing expenditure for the nation on the long run. A recent survey by eRx found that pharmacies using eRx are dispensing 753,000 electronic prescriptions per day with up to 25 prescriptions per second during peak periods. When dispensing 753,000 prescriptions per day, it will cost the nation AU$ 112,950 a day for electronic prescription fees alone.

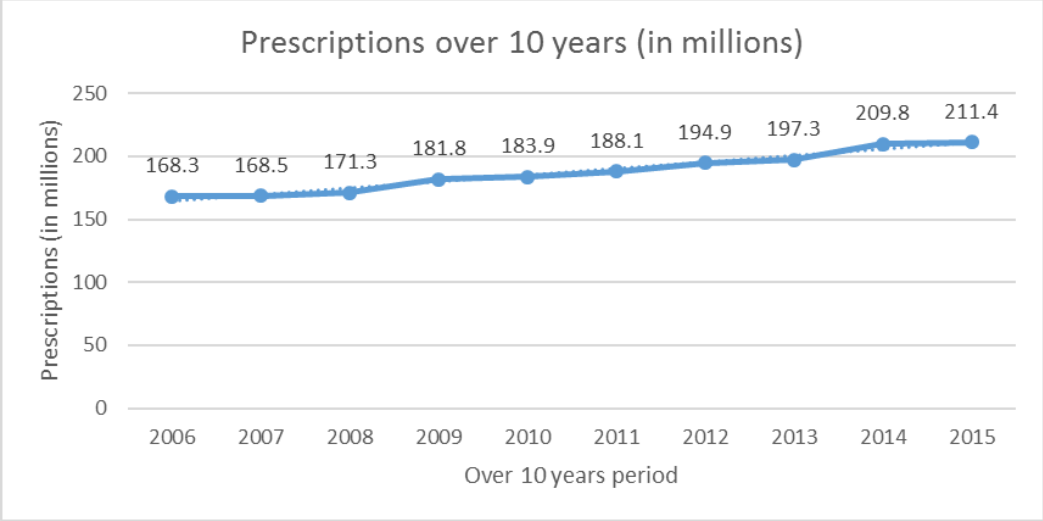


Figure 4. Number of prescriptions over 10 year's period

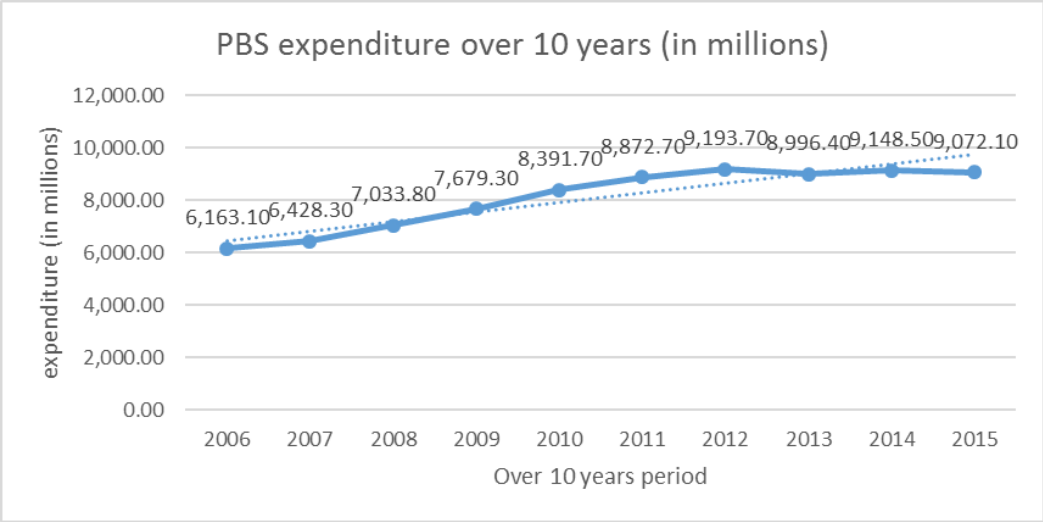


Figure 5. PBS expenditure over 10 year's period

Using statistics from the Pharmaceutical Benefits Scheme website, figure 4 and 5 depicts the number of prescriptions and PBS expenditure over the past 10 years. Based on figure 4 and 5, it is evident that although the PBS expenditure fluctuate slightly, the number of prescriptions increased steadily over the decade. Unfortunately, this indicates that unless less expensive alternatives are explored and utilized, the on-going expense associated with the use of electronic prescription will only cost more in future with increase in volume. At present, electronic prescription fees has been subsidised by the Commonwealth through a series of Community Pharmacy Agreements. However, despite the fact that current eTP implementation being designed as a pharmacy user-pay system ("FAQs", 2016), which party (among prescriber, dispenser and patient) will actually be liable to pay for this on-going cost when it is no longer subsidised by the Commonwealth and the ramification of this potential change is yet to be witnessed.

PROPOSED ALTERNATIVE MOBILE SOLUTION

The proposed mobile electronic prescription transfer application was designed to be a cheaper, if not completely cost-free, alternative with comparable security measures to the current eTP implementation using PES. This proposed solution makes use of the patient's smartphone as the secured transfer mechanism for transferring electronic prescription instead of using PES. Figure 6 roughly depicts how this model works and its simplified operations using the patient's smartphone in place of PES services whilst the rest of the operations remain the same as in the current eTP system.

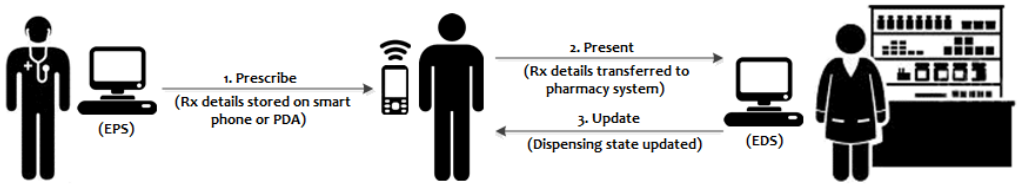


Figure 6: Electronic prescription transfer model using smartphones (Htat, Williams, & McCauley, 2015a)

In securing the prescription information from the security of data-at-rest perspective, this model also makes use of DAK for encrypting the electronic prescription prior to transfer (i.e. to the patient's mobile device) and decrypting at the pharmacy end. However, in this model, the prescriber's Electronic Prescribing System (EPS) also transfers the DAK together with the electronic prescription to the patient's smartphone for storage and transportation instead of using PES. The DAK is then encrypted using a 128 bit symmetric encryption, in compliance with the section 7.3.3 of the ATS4888.2, by the mobile electronic prescription transfer application prior to being stored on the smartphone. Upon arriving at the pharmacy, the mobile electronic prescription transfer application on the smartphone decrypts the DAK and transfers it together with the electronic prescription to the pharmacy's eTP enabled Electronic Dispensing System (EDS). This transfer is to be done via Bluetooth communication although earlier research was conducted with the intention of using NFC technology instead. Once both the DAK and electronic prescription have been transferred to the pharmacy's EDS system, the rest of the eTP operations such as decrypting the prescription using DAK, dispensing the medication and updating the National Prescriptions and Dispense Repository (NPDR) will continue in the same way as if in the current eTP implementation (Htat, Williams, & McCauley, 2015b). For the repeat prescription scenario, the pharmacy's EDS will update the prescription information on the smartphone via the mobile electronic prescription transfer application. This model is designed to have minimal impact on the prescriber's EPS and dispenser's EDS systems in straightforward operations (i.e. simple prescribe and dispense scenario with no script-owing or script-request). How this proposed model's security mechanism works and how it differs from the one using PES can be seen in Figure 7.

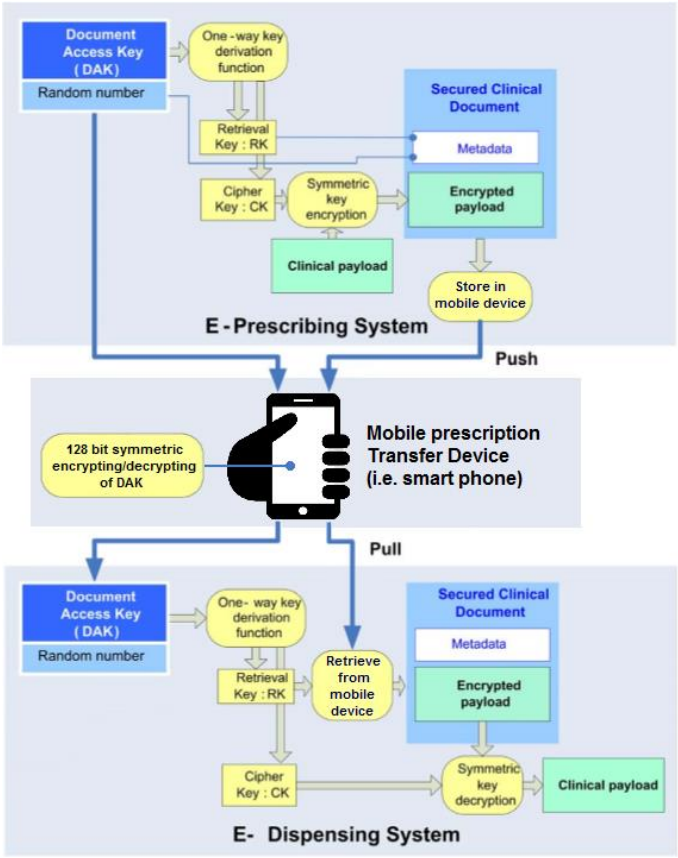


Figure 7: DAK usage for storage and retrieval of prescription in proposed approach (Htat, Williams, & McCauley, 2015b)

Since the prescription information is stored on the patient's smartphone, despite both the DAK and the electronic prescription being securely encrypted, it is still vulnerable to loss due to loss of the device on which it is stored. To ensure this sensitive information does not fall into the wrong hand, the remote data-wipe feature can be implemented as part of the mobile electronic prescription transfer application using Cloud-to-Device-Messaging (C2DM) from Google on Android platform, Google Cloud Messaging (GCM) on iOS platform and Windows Push Notification Services (WNS) on Windows phone platform. This will enable the device owner to remotely delete the prescription data stored on the device. Currently all major mobile OS platforms such as Android, iOS and Windows support remote wipe features for scenario like this.

From the security of the data-in-transit perspective, this proposed model relies on the Bluetooth's inbuilt security measures and governing standards for securing the prescription information in a very similar way current PES implementation relies on the implementation platform and its relevant standards for the security of the data in transit (Htat, Williams, & McCauley, 2015b).

DISCUSSION

The primary objective of the proposed mobile solution is to provide a cheaper, if not completely cost-free, alternative with comparable security measures. Therefore, the proposed alternative mobile solution intends to achieve the same level of security assurance as the current eTP implementation using PES by fulfilling the same security requirements mandated by the same standards and specifications.

Being a national eHealth facility, current implementation of eTP using PES is considered to have complied with the legislative requirements of all the jurisdictions within Australia. However, the study on how it complies with those requirements and to which extent it complies with those requirements leads to interesting findings. For instance, whilst sections 32A, 32B and Appendix-K of the Western Australia's Poisons Regulation 1965 describes the fairly detailed criteria of an approved electronic prescribing system by CEO, the clause "in a manner of writing approved by the Secretary." in section 26 (1) (b) of the Victoria's Drugs, Poisons and Controlled Substances Regulations 2006 implies the use of electronic prescribing without further details on it.

Moreover, whilst the sections 37 (1A) (1B) and 51 (1A) (1B) (1C) of the Western Australia's Poisons Regulation 1965 explicitly state the exemption from the requirement of prescriber's signature on electronic prescriptions, sections 33 (5) and 34 (3) of the South Australia's Controlled Substances (Poisons) Regulations 2011 only mention that prescribers with adequate arrangements for the electronic transmission of prescriptions are permitted to transmit prescriptions electronically and it will be deemed to have been signed. Whilst one Act or regulation dictates something explicitly, the others imply the same meaning using somewhat catch-all statements and vice versa. Therefore, from the legislative approval/acceptance perspective, it is expected that the proposed mobile solution will be accepted as a viable alternative if it complies with all the same standards and specifications as the current eTP using PES.

From the security of the data-at-rest perspective, the proposed solution also makes use of the symmetric encryption key derived from the DAK for securing the electronic prescription in the same way current eTP implementation using PES services does. This limits the impact of the change in transfer mechanism (i.e. patient's smartphone instead PES) on other components of the eTP process such as prescribing, dispensing and updating NPDR etc. Then, in the proposed solution, the DAK is encrypted using a 128 bit symmetric encryption according to section 7.3.3 (i.e. Data Security Conformance Points) of the ATS4888.2 before being stored on the mobile device (Htat, Williams, & McCauley, 2015b). Since the proposed solution uses the same DAK for securing the electronic prescription and the DAK itself is stored encrypted according to the relevant security mandates, the proposed solution's security measures are so far comparable to those of the current approach using PES. Moreover, in the same way the DAK scanned from the paper prescription is used for authorizing the pharmacy access to the prescription stored on the PES in the current eTP implementation, the DAK transferred from the mobile electronic prescription transfer application (i.e. the application from patient smartphone to the pharmacy's EDS) authorizes the pharmacy to access the electronic prescription stored on the patient's smartphone. Therefore, this authorisation mechanism of the proposed solution is also comparable to the current one being used.

From the security of the data-in-transit perspective, the Bluetooth's inbuilt security measures and governing standards upon which this proposed model depends on for securing the prescription information are well accepted by the industry and strictly governed by the Bluetooth Special Interest Group (SIG) and IEEE standard 802.15.1-2005. With strict governance by these two reputable authority bodies (i.e. Bluetooth SIG and IEEE), the implementation platform specific security measures of the proposed model (i.e. using Bluetooth) can be considered comparable to those of the current eTP implementation using the Internet.

Current eTP implementation using PES does not use any of the existing eHealth infrastructural components such as SMD, ELS and HI services although they can be effectively incorporated for better security, identification mechanism, consistency and reliability. Since the current approach using PES does not set very high standards for the proposed prescription transfer approach to live up to, this makes the proposed solution easier to implement and more acceptable to the industry. Although the primary objective of the proposed solution is to be a cheaper alternative with comparable security measures to the current approach using PES, it also has a few additional advantages over the current approach. First, this proposed solution puts the user in control of their sensitive information and allows them to prevent undesirable secondary use of that information by third parties. In addition, some useful features such as prescription expiration alert, last repeat alert, drug allergy alert and alert for harmful doses can also be implemented as part of the mobile electronic prescription transfer application. The ability to transfer the full history of patient's medication from the patient's mobile phone directly into the hospital system (i.e. once the interface has been implemented to integrate this mobile solution with the hospital information system) is just another benefit of this solution. Furthermore, without the requirement for the supporting network infrastructure this proposed solution will also be suitable for the remote regions of Australia where the network availability is limited or unreliable.

CONCLUSION

Before the 6CPA was officially signed, there were concerns and various speculations regarding what the new eligibility criteria will be for electronic prescription fees and how the subsidy will continue. Among them, eRx persuaded users with the no cost policy even for non-eligible scripts. But, some of its publications mention that it may not be able to maintain the cost neutral policy indefinitely but users would be given at least two month notice prior to any change being implemented to the price structure ("eRx slashes e-script pricing", 2010; O'Donoghue, 2012). So, effectively it does not even promise the users that it will remain cost neutral even with the current Commonwealth's AU$ 0.15 contribution for each electronic prescription. How the use eTP will continue without the Commonwealth subsidy is rather an alarming thought. On the other hand, MediSecure seems to try using a scare tactics on users by implying that the eligibility criteria for electronic prescription fees will likely to be stricter in future ("How electronic prescription fee payment works?", 2015). For instance, from

certain point in time during the 6CPA agreement period, the Commonwealth's AU$ 0.15 subsidy will only be applicable if the PES can share data with other eHealth components such as PCEHR and NPDR. From that aspect, only their product, Script Vault, is capable of such enhancement with minimal disruption to the services as it is the only PES service that fully complies with various eHealth and HL7 standards. When the 6CPA was officially signed, the section 6.1.3 and Appendix B of the agreement state that from 1st July 2016 and onwards this funding will be subject to a cost-effectiveness assessment by an independent health technology assessment body as determined by the Minister ("The Pharmacy Guild of Australia", 2015). Therefore, instead of living in fear of the potential change in the Commonwealth's subsidy for the electronic prescription fees, this paper proposed a cheaper (i.e. potentially cost-free) alternative with comparable security measures to the options currently available.

REFERENCES

eRx slashes e-script pricing (2010). Retrieved October 17, 2016 from Pharmacy Daily: http://erx.com.au/wp-content/uploads/2013/09/eRx_Newsletter_May_2010.pdf

FAQs. (2016). Retrieved from eRx Script Exchange: http://www.erx.com.au/support/faqs/

How electronic prescription fee payment works? (2015). Retrieved October 17, 2016 from SlideShare: http://www.slideshare.net/medisecure/how-electronic-prescription-fee-payment-works

Htat, K. K., Williams, P. A. H., & McCauley, V. (2015a). The Hare and the Hortoise [sic]: The Potential Versus the Reality of eTP Implementation. In Proceedings of the 23rd Australian national Health Informatics Conference 2015 (pp. 114-120). Brisbane, Australia.

Htat, K. K., Williams, P. A. H., & McCauley, V. (2015b). Security of ePrescription: Security of data at rest in Prescription Exchange Services vs on Mobile Devices. In Proceedings of the 4th Australian eHealth Informatics and Security Conference 2015. Perth, Australia.

Htat, K. K., Williams, P. A. H., & McCauley, V. (2016). *Security of ePrescriptions: Data in Transit Comparison Using Existing and Mobile Device Services*. Manuscript submitted for publication.

NEHTA Blueprint V2. (2011). Retrieved July 21, 2016 from Australian Digital Health Agency: https://www.nehta.gov.au/implementation-resources/ehealth-foundations/nehta-blueprint

O'Donoghue, N. (2012). Real-time claiming set to ease pharmacy red tape. Retrieved October 17, 2016 from Pharmacy News: http://www.pharmacynews.com.au/news/latest-news/real-time-claiming-set-to-ease-pharmacy-red-tape?t=636112320827921123

The Pharmacy Guild of Australia. (2015). Sixth Community Pharmacy Agreement (2015-2020). Retrieved from https://www.guild.org.au/the-guild/community-pharmacy-agreement

White, J. (2015). Benefits of e-prescribing for hospitals. Retrieved October 17, 2016 from Healthcare Business & Technology: http://www.healthcarebusinesstech.com/e-prescribing-hospitals/

ACCELERATING NTRUEncrypt FOR IN-BROWSER CRYPTOGRAPHY UTILISING GRAPHICAL PROCESSING UNITS AND WEBGL

Dajne Win, Seth Hall, Alastair Nisbet
Security & Forensics Research Group, Auckland University of Technology,
Auckland, New Zealand
dwin@aut.ac.nz, shall@aut.ac.nz, anisbet@aut.ac.nz

Abstract

One of the challenges encryption faces is it is computationally intensive and therefore slow, it is vital to find faster methods to accelerate modern encryption algorithms to keep performance high whilst also preserving information security. Users often do not want to wait for applications to become responsive, applications on limited devices such as mobiles often compromise security in order to keep execution times quick. Often they use algorithms and key sizes which are not considered cryptographically secure in order to maintain a smooth user experience. Emerging approaches have begun using a devices Graphics Processing Unit (GPU) to offload some of the computational burden from the Central Processing Unit (CPU) in an effort to parallelize and accelerate the encryption algorithms. Programming for a GPU often involves the use of CUDA or OpenCL programming, however these approaches are platform dependant. This research focuses on utilizing a GPU to perform in-browser cryptography using WebGL and JavaScript. This allows any GPU-enabled device capable of launching an OpenGL compatible browser to perform GPU accelerated cryptography. A GPU based implementation of the NTRUEncrypt algorithm was created and tested against a CPU based version on a range of hardware devices with results, challenges and limitations discussed.

Keywords
NTRUEncrypt, GPU, browser, cryptography, encryption, WebGL.

INTRODUCTION

Cryptography is one of the tools available to facilitate secure communication between two parties. Whilst cryptography provides confidentiality of communications between the two parties, it also, when applied correctly, allows for integrity, authentication and non-repudiation (Rivest 1990). One issue with cryptography on mobile devices is that it is computationally expensive meaning when high speed networking is utilised the encryption and decryption of messages on the device can become a bottleneck for the message exchanges, slowing down the communication exchange.

Whilst developments in cryptography has seen greatly improved security of cryptography with more sophisticated and robust encryption algorithms developed in the last few decades, the speed of encryption and decryption has suffered from the increased complexity of the cryptographic processes (Kapoor, Pandya et al. 2011). The Central Processing Unit (CPU) of a device is fixed hardware that must handle complex calculations for the processing of many functions on the devices. The design of the CPU on mobile devices is deliberately conservative as it must be small, consume little battery power and produce minimal heat. It therefore tends towards being designed to provide high speed processing but at its limit of available processing power. This leaves little available processing power when complex additional computations are required for cryptographic processes.

The GPU on a mobile device is required to deal with processing of graphical images which may at times require only a small percentage of the available processing power that the unit is capable of handling. This, along with the multiple processes within a single GPU mean that much additional processing power is available but generally not utilised. The ability to direct this additional processing power towards cryptographic requirements therefore has considerable benefits in permitting the most secure cryptographic algorithms to be utilised at high speed for message exchanges (Harrison and Waldron 2010). Whilst the idea of utilising the GPU of a device for processing of non-graphical requirements is not new, the restrictions that have been imposed by previous designs means that only a select few devices are capable of implementing this technology and reaping the benefits of the additional GPU processing power. This paper describes the development of a GPU accelerated NTRU Encrypt algorithm used for in-browser cryptography. It uses the WebGL and Three.js libraries for the purpose of trying to utilise the algorithm on any browser enabled device.

STATE OF THE ART

The Data Encryption Standard ratified in 1977 provided a robust and reliable symmetric encryption algorithm suitable for public and government use. With only 56 bit encryption permitted to comply with the contemporary laws restricting encryption to this key size, Data Encryption Standard (DES) remained suitable until technology surpassed the protection afforded by such a small key length. Triple DES (3DES) acted as an intermediary fix to provide significantly stronger encryption without the need for an entirely new algorithm. However, 3DES was computationally expensive and with security weakening as computer processing increased rapidly, the Advanced Encryption Standard (AES) was developed in 1998 as a result of a competition for a replacement for DES and 3DES (Daemen and Rijmen 2003). Both 3DES and AES are commonplace and whilst AES is much preferred, 3DES remains as the encryption algorithm of choice for many banking applications. AES is computationally expensive which for computer applications is suitable but for mobile devices with much less processing power can slow message exchanges in some circumstances.

In 2015, National Institute of Standards and Technology (NIST) announced that it could no longer support continued use of the 2 key 3DES version and recommended utilising 3 key 3DES or move to AES (Barker and Barker 2004). The banking industry has been slow to respond and 2 key 3DES remains in many banking communications, however the move to AES seems inevitable as more and more research into the insecurity of DES in all varieties appears.

The need to accelerate AES and other encryption processing on these devices has seen some improvements through new processes but so far all restrict the new processes to specific hardware. In 2007, experiments with accelerating AES by utilising a GPU showed significant improvements with bulk processing of AES (Harrison and Waldron 2007). The same year saw further experiments with AES and DES which achieved improvements of over 100% throughput with a GPU compared to a high performance CPU (Yang and Goodman 2007). In both of these experiments the limiting factor for improved processing was found to be the memory bandwidth rather than the GPU processing units on each card as each card required the same number of memory fetch units. In 2012 experiments by Chesebrough and Conlon showed a significant increase in cryptographic processing of AES-NI of 5 times greater than previous experiments (Chesebrough and Conlon 2012).

The move to parallel computing has seen great benefits in processing speed but at the expense of heat generation (Oancea, Andrei et al. 2014). Technology has moved rapidly from the original 8086 processer with 29 000 transistors to the Intel core i7-920 released in 2014 with 731 000 000 transistors to 1.9 billion transistors by 2015, all within approximately the same sized footprint of the CPU (Kowaliski 2015). Whilst multiple cores have somewhat alleviated the heat generation problems, the computing power requirements have increased at a greater rate than development so that higher performance from software remains ahead of the CPU development (Oancea, Andrei et al. 2014).

The area for greatly improved processing power at little cost is in Graphical Processing Unit utilisation as a defacto CPU. Nvidia GPUs utilise Single Instruction Multiple Data (SIMD) stream architecture which has the advantage over Single Instruction Single Data (SISD) of providing natural parallelism and therefore processes data simultaneously (Nvidia 2008). Nvidia's modification of SIMD is termed Streaming Multiprocessors (SM) and places emphasis on ease of development by reducing the complexity of the design. This has seen significant research in the area of GPU accelerated cryptography tied to Nvidia's hardware because of the simplicity with which developers can utilise development platforms such as Compute Unified Device Architecture by NVidia (CUDA), (Yang and Goodman 2007).

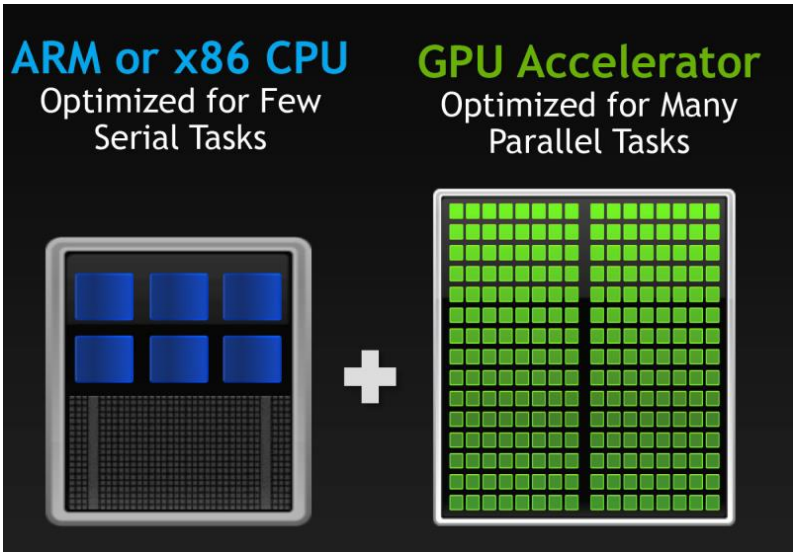


Figure 1: CPU v GPU processors (Nvidia, 2008)

As illustrated in Figure 1, the main difference in processing of a CPU compared to a GPU is that a CPU may consist of several cores with a control bus for communication meaning that the CPU does not perform in a truly parallel manner. The GPU is made up of many floating point units, with each unit dedicated to performing arithmetic tasks and when combined in a truly parallel manner produce a truly SIMD architecture which is considerable faster than the CPU. In 2008 an Nvidia 8800 GTX was utilised as it allowed for the use of DirectX 10, CUDA and a 32 bit integer processor (Harrison and Waldron 2009). They noted the necessity of taking into account different memory architectures to improve performance as whilst there is some local storage available, most is off-chip making transfers comparably slower. The competing architecture is OpenCL (Open Computing Language) and there has been significant research into utilising GPU's of each type but specific to the type being accelerated. This emphasis on writing software to accelerate the Nvidia architecture or the OpenCL architecture has meant that developments work for one technology but not the other.

Accelerated programming has become a necessity not just because of the increased speed of computing applications but because of the greatly increased expectations of the users. In 1994, Nielson's research found that 0.1 seconds of latency after performing a task such as selecting a key on a keyboard or dragging the mouse pointer across a screen could be considered instantaneous. Similar research by Ritter et al in 2015 found that 300 milliseconds was acceptable as a maximum latency with 170 milliseconds required for more urgent tasks (Ritter, Kempter et al. 2015).

The issue with acceleration of processing by utilising the GPU has potential to be overcome by the implementation of acceleration in JavaScript. All modern web browsers support the use of JavaScript (Flanagan 2011) and with the introduction of HTML5 JavaScript has moved from a simple scripting language to an efficient programming language. With a doubling of Internet connected devices occurring every two years (Gartner 2015) , the motivation to improve processing speeds on mobile devices becomes very apparent. An early attempt in 2012 to implement JavaScript on a GPU utilising OpenCL rather than the Nvidia architecture on an Intel i7 processor proved unsuccessful at accelerating the processing but did prove that it was technically possible to at least do so (Nicholls 2012). One benefit of a successful implementation is that client side acceleration of processing functions could occur efficiently, alleviating some of the burden of the processing from the servers. The first investigation into utilising the GPU for accelerating cryptographic functions using JavaScript occurred in 2006 (Cook and Keromytis 2006). Their experiments targeted the AES algorithm but problems were experienced in the areas of a lack of modular arithmetic, unsigned integers, branching and large integers. Yang and Goodman directly furthered the experiments and gained some positive results primarily because of the development of the technology in the 1 year period (Yang and Goodman 2007). In that time, branching and unsigned integers no longer proved difficult to handle but large integers remained a problem. Two years later, experiments of a similar nature but with asymmetric cryptography also showed some positive success but with some limitations (Harrison and Waldron 2009). Their research involved accelerating 1024 bit RSA encryption and they were able to show higher throughput and decreased latency by utilising the Nvidia GPU. Since 2010, little advancements have been made in accelerated cryptography utilising the GPU although hardware advances have made the area far more promising for success.

This issue with all of these previous experiments remained that they were all targeted to a particular type of GPU architecture, either Nvidia or OpenCL but not both. To be universally beneficial, what is clearly needed is software in JavaScript that will accelerate cryptography in both architectures. The following section outlines the research design for the software development.

RESEARCH DESIGN

This research used an experimental research design methodology which allows for control over the variables defined in the experiment, allowing more accurate results to determine relationships between sets of data. The purpose of running experiments with software that is developed to improve performance over currently available software is to show that the new scheme has benefits over previous schemes. A performance benchmark of what is currently available is one method of showing that improvements have been made with the new scheme by way of comparison between the older and the new scheme. Crypto++ has been chosen as the cryptographic scheme to be used in the comparison. Crypto++ is an open source library of several cryptographic algorithms and the version that is used in this research provides for AES encryption. Utilising the JavaScript software and RSA (Rivest, Shamir et al. 1978) cryptography as well as Elliptic Curve Cryptography (ECC) (Koblitz 1987). The JavaScript is run encrypting NTRUEncrypt and the resulting data used to compare against previous schemes. The hardware utilised for the testing can be divided into 3 distinct types, mobile, desktop and laptop, and server. These are shown in the following tables (Table 1 and 2) as well as the CPU, GPU, RAM and operating systems used.

Table 1: Mobile platforms tested

	Samsung Galaxy S2	ASUS Zenfone 2	Samsung Tab 10.1	Nvidia TK1
CPU	Dual Core 1.2 GHz Cortex A9	Quad Core 2.3 GHz Intel Atom Z3580	Dual Core 1 GHz Cortex A9	Quad Core ARM Cortex A15
GPU	Mali 400 GPU	PowerVR G6430 GPU	Nvidia Tegra 2 T20 ULP Geforce	Nvidia Kepler, 192 CUDA Cores
RAM	1 GB	4 GB	1 GB	2 GB
OS	Android 4.1.2	Android 5.0	Android 3.1	Ubuntu Desktop 14.04 LTS

Table 2: PC desktop platforms tested

	Custom Desktop	HP Desktop	Toshiba Thinkpad
CPU	Quad-Core 3 4 GHz Intel i5 3570k	Quad-Core 3 2 GHz Intel i5 4570	Dual-Core 2 53 GHz Intel Core 2 Duo T9400
GPU	Nvidia 660 GTX	AMD Radeon R7 360	Intel GMA 4500MHD
RAM	16 GB	16 GB	2 GB
OS	Windows 10	Ubuntu Desktop 14 04 LTS	Lubuntu 14 04

Initial tests were run to check that the systems were working as expected and results were being correctly recorded. Once this was satisfied, the experiments could begin.

TESTING & RESULTS

This research focused on utilizing the GPU in an attempt to optimize NTRUEncrypt (Hoffstein, Pipher et al. 1998) algorithm for in-browser cryptography. In order to target a variety of different devices, a Javascript version of NTRUEncrypt was developed using Three.js, which is a cross-browser library using WebGL and is primarily used for computer graphics. The experiments compared both Javascript CPU and GPU implementations of NTRU encrypt to test whether it could be beneficial to utilize the GPU for in-browser cryptography. Average throughput results after 500 iterations for each version of NTRU on the various platforms were recorded and compared. Porting an algorithm to GPU brings a number of challenges in order to port the algorithm to be more suitable for the GPU pipeline such as reducing code branching, fixing float values to between 0-1 within the GPU, and floating point precision errors. There is also limits on the buffer sizes and number of uniform values that are passed into the each shader. NTRUEncrypt is was used as it is considered to be fast compared to other asymmetric encryption algorithms (Hermans, Vercauteren et al. 2010) with comparable security settings and “quantum resistant” (Perlner and Cooper 2009), making it an ideal choice for future cryptography systems.

The algorithm was first tested with small set NTRU parameters (N=11) and progressing upwards to higher sets (N=1499, ees1499ep1) which become more computationally intensive to encrypt. The following values represent NTRU parameter sets considered to be cryptographically secure (Figure 2) (Inc 2014).

	N	q	p
Moderate Security	167	128	3
Standard Security	251	128	3
High Security	347	128	3
Highest Security	503	256	3

Figure 2: Recommended NTRU parameter steps

The following GPU pipeline diagram (Figure 3) shows the parts to the implemented algorithm. The first stage of the pipeline takes in the public key and blinding values as byte arrays into the convolution shader. The output of which is then fed into the second shader where a polynomial addition modulo by the value q is performed on the plaintext to get its corresponding ciphertext.

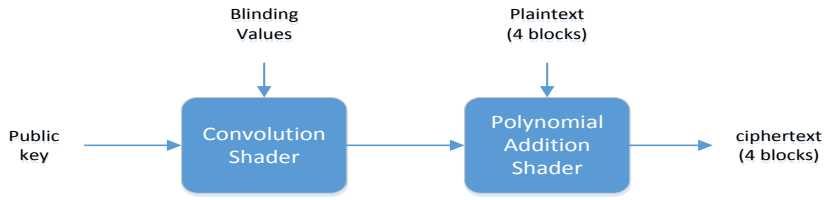


Figure 3: NTRUEncrypt GPU pipeline model

Because of the SIMD nature of GPU, the algorithm utilized vec4 operations within the GPU meaning that processing four blocks of plaintext can be converted to four ciphertext blocks with little to no extra computational cost over simply converting one block. The GPU implementation of NTRUEncrypt was tested and compared to a pure CPU implementation also implemented in Javascript and used as a benchmark comparison. The following table (Table 3) shows the results for the ees401ep1 parameter set on custom desktop.

Table 3: GPU vs CPU average throughput results in milliseconds for ees401ep1

Encryptrion Operation	NTRUEncrypt.js	NTRUEncrypt-GPU.js
Convolution	0.928	23.42
Addition	0.274	9.28
Total	2.104	230.5

Unfortunately it appears that no outright acceleration was achieved and in fact the algorithm execution time was significantly slower. This is because the nature of the algorithm for NTRU is difficult to parallelize, in particular the polynomial addition part of the algorithm. The algorithm took on average 2.1mS to encrypt one block of plaintext for the CPU implementation whereas the GPU implementation took on average 230.5mS to encrypt four blocks of plaintext held inside a vec4 buffer. Custom desktop was only able to handle ees401ep1 parameters due to the restrictions of OpenGL set on the GPU. The results are also affected by the setup time for Three.js and overhead on WebGL calling shader instances as it is simply meant to be a graphics library and not intended for high performance computing and cryptography. Furthermore hardware issues affected results due to their poor implementation of WebGL as although it is stated that it is OpenGL compliant, not all the standards are met. Furthermore the mobile devices tested also failed to perform the algorithm correctly due to lack of float buffer support.

However the following graph (Figure 4) shows results performed on the HP Elite desktop and demonstrates that, utilizing the GPU becomes advantageous when using the ees1449ep1 parameter sets for higher security levels as using a pure CPU approach becomes computationally burdensome using parameter sets over ees887ep1. Interestingly using very low spec parameters for NTRU on the GPU was slow compared to higher specification parameters, this is due to under-utilization of GPU cores. Furthermore only the original NTRUEncrypt algorithm was implemented, (Inc 2014) has suggested several enhancements to the algorithm which may be advantageous for reducing computation time for encryption/decryption on GPU.

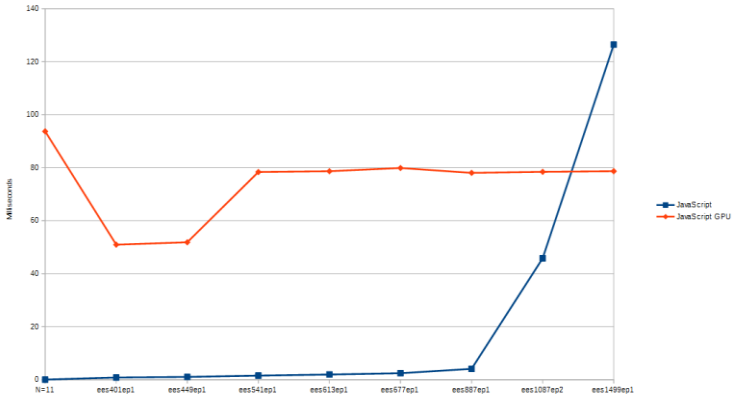


Figure 4: CPU vs GPU average throughput results on HP Elite desktop for increasing NTRU parameter sets

CONCLUSIONS

The ability to accelerate cryptography on limited devices is essential in order for applications to use encryption schemes which are considered cryptographically secure whilst still maintaining a smooth user experience. This paper looked at utilizing the GPU for in-browser cryptography using NTRUEncrypt as a case study. Not all the hardware platforms tested were able to accelerate the NTRUEncrypt algorithm, however the HP Elite Desktop was able to achieve GPU acceleration with the ees1449ep1 parameter set. Browsers poor implementations of WebGL affect performance in calling shaders for non-graphics purposes, however with the rise of GPU implementing compute shader pipelines then using GPU for non-graphics purposes could become more commonplace. Modern browsers will see the implementation of WebGL 2.1 in the near future which will have direct support for compute shaders (Jackson and Gilbert 2015). Using compute shaders is more useful for utilizing the GPU for non-graphics tasks such as high performance computing and cryptography. Future work will investigate using compute shader further by trying to improve throughput performance of a GPU-based NTRUEncrypt algorithm. A preliminary C++ implementation with the full OpenGL pipeline, utilizing compute shaders has been developed with beta results that are promising. The implementation was able to process four blocks of plaintext using the ees1499ep1 parameters in 18mS on the HP Elite Desktop. This is a significant improvement compared to the 80mS shown in this papers in-browser GPU JavaScript version. This shows that the ability to use GPU to accelerate cryptography algorithms has the potential to increase security and intelligence capabilities. However there is still a long way to go in order for it to be fully supported by browsers so it can be then used for in-browser cryptography. For now applications could still benefit from GPU acceleration by creating a direct port into the compute shader pipeline or using platform dependant alternatives such as CUDA or Open CL.

REFERENCES

Barker, W. C. and E. Barker (2004). Recommendation for the triple data encryption algorithm (TDEA) block cipher, US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

Chesebrough, R. and C. Conlon (2012). Implementation and Performance of AES-NI in CyaSSL Embedded SSL.

Cook, D. and A. D. Keromytis (2006). Cryptographics: exploiting graphics cards for security, Springer Science \& Business Media.

Daemen, J. and V. Rijmen (2003). "AES Proposal: Rijndael. htt p." csrc. nist. gov/archive/aes/rijndael/Rijndael-ammended. pdf.

Flanagan, D. (2011). JavaScript: The Definitive Guide: Activate Your Web Pages, O'Reilly Media.

Gartner (2015). Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015.

Harrison, O. and J. Waldron (2007). "AES Encryption Implementation and Analysis on Commodity Graphics Processing Units." 4727: 209-226.

Harrison, O. and J. Waldron (2009). "Efficient Acceleration of Asymmetric Cryptography on Graphics Hardware." 5580: 350-367.

Harrison, O. and J. Waldron (2010). "GPU Accelerated Cryptography as an OS Service." 6480: 104-130.
Hermans, J., F. Vercauteren, et al. (2010). Speed records for NTRU. Topics in Cryptology-CT-RSA 2010, Springer: 73-88.
Hoffstein, J., J. Pipher, et al. (1998). NTRU: A ring-based public key cryptosystem. Algorithmic number theory, Springer: 267-288.
Inc, S. I. (2014). "NTRU Enhancements 1." Retrieved 1 Ocotober 2016, from https://assets.securityinnovation.com/static/downloads/NTRU/resources/NTRU-Enhancements-1.pdf.
Inc, S. I. (2014). "NTRU PKCS Tutorial." Retrieved 1 October 2016, from https://assets.securityinnovation.com/static/downloads/NTRU/resources/NTRU-PKCS-Tutorial.pdf.
Jackson, D. and J. Gilbert. (2015). "WebGL 2 Specification." from https://www.khronos.org/registry/webgl/specs/latest/2.0/.
Kapoor, B., P. Pandya, et al. (2011). "Cryptography." Kybernetes 40(9/10): 1422-1439.
Koblitz, N. (1987). "Elliptic curve cryptosystems." Mathematics of computation 48(177): 203-209.
Kowaliski, C. (2015). Intel's Broadwell-U arrives aboard 15W, 28W mobile processors.
Nicholls, J. (2012). JavaScript on the GPU.
Nvidia (2008). CUDA Programming Guide.
Oancea, B., T. Andrei, et al. (2014). "GPGPU Computing." arXiv preprint arXiv:1408.6923.
Perlner, R. A. and D. A. Cooper (2009). Quantum Resistant Public Key Cryptography: A Survey. Proceedings of the 8th Symposium on Identity and Trust on the Internet, New York, NY, USA, ACM.
Ritter, W., G. Kempter, et al. (2015). User-Acceptance of Latency in Touch Interactions. Universal Access in Human-Computer Interaction. Access to Interaction. M. Antona and C. Stephanidis, Springer International Publishing. 9176: 139-147.
Rivest, R. L. (1990). Cryptography. Handbook of Theoretical Computer Science. J. V. Leeuwen, Elsevier. 1: 717-755.
Rivest, R. L., A. Shamir, et al. (1978). "A Method for Obtaining Digital Signatures and Public-key Cryptosystems." Commun. ACM 21(2): 120-126.
Yang, J. and J. Goodman (2007). "Symmetric Key Cryptography on Modern Graphics Hardware." 4833: 249-264.

A SURVEY OF SOCIAL MEDIA USERS PRIVACY SETTINGS & INFORMATION DISCLOSURE

Mashael Aljohani[1,2], Alastair Nisbet[1,2], Kelly Blincoe[2],
[1]Security & Forensic Research Group, [2]Auckland University of Technology
Auckland, New Zealand
mashaeljohani@gmail.com, alastair.nisbet@aut.ac.nz, k.blincoe@auckland.ac.nz

Abstract

This research utilises a comprehensive survey to ascertain the level of social networking site personal information disclosure by members at the time of joining the membership and their subsequent postings to the sites. Areas examined are the type of information they reveal, their level of knowledge and awareness regarding how their information is protected by SNSs and the awareness of risks that over-sharing may pose. Additionally, this research studies the effect of gender, age, education, and level of privacy concern on the amount and kind of personal information disclosure and privacy settings applied. A social experiment was then run for 3 months that tested SNSs users' reaction to a profile access request by a stranger. The research focused on four different social networks: Facebook, Twitter, Instagram,and Snapchat. The results of the survey and experiment found that there is a significant amount of personal information disclosure, but that the level differs between social networks. It is reveals that gender, age, and education have significant influences on information disclosure and user's privacy settings and that on most sites over 50% of friend requests were readily accepted. These results are a selection from a comprehensive study of some of the more revealing facts about SNS user ship covering 3 months of data collection and almost 500 responses.

Keywords
privacy, security, social networks

INTRODUCTION

Social media and social networking sites (SNS) are now utilised by a large majority of Internet connected people around the world. With the benefit of almost instant communication to potentially billions of other people, the temptation may be to connect as simply and as quickly as possible to enjoy the benefits of social media. With benefits, there are often drawbacks and the recent publicity of privacy breaches, identity theft and the dangers of over-sharing, social media users signing up for and utilising the sites' service should be wary of just how much information they disclose. Of the many SNS's available to consumers, Facebook, Twitter, Snapchat and Instagram are currently the most heavily visited sites. Each site has a user's conditions that are available to be read when a new user creates an account with the site. Often, these agreements may not be fully read or fully understood yet many users agree to the terms and continue to enter personal details to create their account. Some sites have publicly available areas where non-members r general members who have had no prior contact with a user's page can view information posted by the member. At times, this information may be of a personal nature that some members may wish to keep private or may be sufficient information to identify a person, a place of residence or other uniquely identifying feature. It has been argued that advances in communication technology have made people more tolerant and more willing to share information about themselves in a way that renounces the value of privacy in order to be more connected and traceable, specifically among younger generations (Tubaro, Casilli & Sarabi, 2014). Whilst much data exists regarding the numbers of people utilising social media, often on a daily basis, the makeup of the users in relation to their privacy settings and disclosure has been rarely examined.

LITERATURE REVIEW

Technological advancement has become less focused on connecting computers and more concerned about connecting people. A main contributor to this evolution is the use of social networking sites (SNS), which has seen explosive growth in use in the last couple of years (Zheleva, Terzi, & Getoor, 2012). As of August 2016, there are more than 2.22 billion users of SNSs (Statista, 2016). Due to the increasing popularity of SNSs and the drive to reach customers, more than 70% of businesses are now using SNSs (McKinsey Global Institute, 2012). Although SNSs provide a powerful tool to engage people over the web, they can be a source of possible threats to users' privacy and security because users routinely and voluntarily provide personal information (Cross, 2016).

Social networks initially started as websites where users only access to them was with a laptop or a desktop. However, with the advancement of smartphones, social networks released mobile application versions of their sites and other social networks developed mobile standalone applications for access. This development made it easier and more convenient for users to access their online profiles and update more actively and in real time (Aldhafferi, Watson, & Sajeev, 2013). However, the more accessible the social network, the easier it is to be used and the more information the user tends to share (Coyle & Vaughn, 2008). SNSs have unquestionably a strong social impact and the line between a person's virtual and offline life may for some, become blurred.

SNSs have evolved over the years and have gone through many phases of development to reach their current state (Hendricks, 2013). The first recognisable form of SNS that encouraged users to include personal information about themselves for the purpose of social networking emerged in 1997 with a site called SixDegrees (Boyd & Ellison, 2007). It allowed users to open personal accounts and create a list of friends. SixDegrees attracted over a million subscribers at its peak (Chapman, 2009). However, although SixDegrees managed to become popular and attract large numbers of subscribers, the site was not able to maintain its popularity (Boyd & Ellison, 2007). In 2001, SixDegrees.com was shut down. According to the founder of SixDegrees, the failure of his website was due to the fact that SixDegrees was ahead of its time: at that time, not many people had friends who were online and the idea of being online friends with strangers had not yet gained universal acceptance (Prall, 2010).

The concept of creating a virtual SNS inspired other developers (Liu, 2014). In the early 2000s, more people started to have Internet access, hence the target audience became much broader. This helped the success and increased the popularity of SNSs such as Friendster, which has attracted more than 90 million users. It introduced the ability for users to discover their friends and then friends-of-friends, and thus expand their networks and share more information with others.

The vast spread of SNSs started to occur at the start of 2003, initially when Myspace was launched, which grew to be the most popular SNS in the world at that time (Boyd & Ellison, 2007). Myspace differentiated itself from other competitors by giving users the freedom to customise the look of their profiles. In 2004, Facebook was launched initially as a Harvard-only social network and became the most popular SNS in 2008, overtaking Myspace. As of the second quarter of 2015, Facebook has 1.49 billion monthly active users (Statista, 2016). Facebook managed to maintain its success by constantly improving the site and by adding new features (Hendricks, 2013).

At the present time, hundreds of SNSs have emerged, each designed to serve a different audience or have a different style that distinguishes it from other SNSs. Figure 1 shows the vast growth of SNSs from 2006 to 2012.

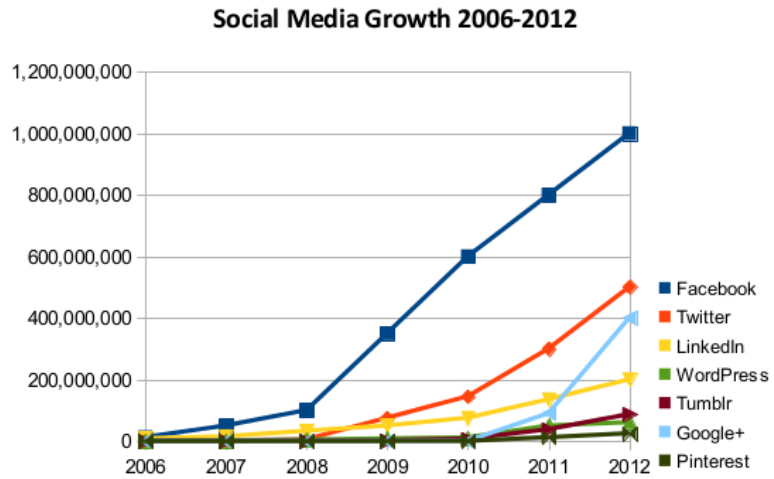


Figure 1: Growth of Online Social Networks, 2006-2012. (Source: White, 2013)

As of August 2016, there are over 2.34 billion social network users globally. This number is expected to increase and reach 2.95 billion social networks users by 2020, which is close to a third of the world's entire population (Statista, 2016). The last decade has witnessed a rapid growth in the number of individuals using SNSs. For instance, as of June 2016, Facebook was regarded as the third most used website globally after

Google and YouTube (Alexa, 2016). Although SNSs provide many benefits for individuals such as keeping in touch with friends and family, privacy and security is regarded as a critical issue that can threaten the users of SNSs (Donath, 2007). This is mainly because SNSs encourage their users to reveal a great deal of personal information about themselves by promising them a better user experience if they do so (Luo, Liu, Liu, & Fan, 2009). For example when users first sign up to Facebook, they will be constantly asked and reminded by Facebook to update their profile with more personal information such as date of birth, hometown, workplace, and/or school in order to find more friends and enjoy the experience better (Lewis, n.d.). The growing popularity of SNSs and the fact that they contain enormous amounts of information make these websites an attractive target for malicious hackers. It is therefore vital that users are aware of the risks of disclosure of personal information and how the information they disclose can be used by unscrupulous individuals to commit crimes such as Fraud and other scams.

The following section discusses the research phases including design of the questionnaire.

RESEARCH DESIGN

The aim of this research is to shed the light on SNS user's personal information disclosure behaviours, their privacy protection settings, privacy policies and users SNS privacy knowledge and awareness. The study was conducted to identify the effect of gender, education status, and age on the degree of personal information disclosure and protective privacy settings applied by the user, using factor analysis. Four most common SNS sites were selected as a cross section of social media sites, each giving a different purpose for the members and viewers of the sites, from primarily text based to primary video and graphics based sites. These sites are Facebook, Twitter, Instagram and Snapchat. An online survey was conducted which aimed to answer the following proposed research questions.

Q1: What are the personal attributes that can have an influence on information disclosure and privacy settings of SNS users?

Q2: Do users' levels of privacy concern have an effect on the amount of information they disclose in social networking sites?

Q3: Are users aware of how their information is protected by SNS providers according to the privacy policies that the users have agreed to?

In addition, a further experiment was conducted to test how users react to stranger's friendship of follow requests. In this experiments, requests were sent to people the requestor had no prior personal knowledge of to ascertain how likely it was that the friend request would be accepted.

Initially an online form was created with the link to the form posted on each of the four sites. In Twitter, for example, the link for the survey was tweeted with trending hash-tags in order to ensure it had wide exposure. In the post, there was a brief description of the survey in order to encourage users to take part in it. For the social experiment, users were selected randomly from their participation in public pages such as newspapers or public figures' pages by either liking a post or commenting on a post. With a population of the four sites combined reaching approximately 1.5 billion users, the confidence level of 95% and margin of error of 5% was found to be appropriate. This meant that a minimum of 385 responses would be required for the survey to have this validity.

Two stages of analysis were used in this research to derive the main findings.

1) Exploratory data analysis (EDA): In this stage, the data files are viewed before completion of the data collection in order to get some ideas about the initial results. The purpose of this stage is that it may indicate further data are required: for instance, there may be more female responses than male responses, which could affect the accuracy of the results. This preliminary stage ensured that any imbalances and limitations in the data were resolved before the end of the data collection period. This stage overlaps with data cleaning because anomalies can become evident. Therefore, in an optimal situation, before the end of this stage, there should be a clean dataset that is ready for the next stage of analysis.

2) Deriving the main findings: This stage generates a summary of the findings, relationships, trends, interpretations and narratives. When analysing the data, the type of questions dictate the type of analysis. However, in general, two tools are used together to analyse the data. The first tool is filtering,

which is provided by Survey Monkey to help break down the results in order to focus on a specific data subset. It allows viewing specific respondents' answers to specific questions. For instance, it allows viewing of all the answers of male respondents who are between the ages of 20-24 years and who answered that they do not trust SNS providers with their information. Secondly, the information is transferred into SPSS in order to analyse it statistically. Factor analysis has been conducted. Separate chi-square tests of contingencies were conducted in order to understand and determine the differences in user privacy setting behaviours and personal information disclosure variables with gender, age, education, and privacy rating for each of the four social networks. All chi-squares were interpreted at a conservative alpha of .01 to control for multiple tests. The chi-square analysis helps to determine whether two discrete variables have any statistical association and whether there is a statistical significance between the variables.

RESULTS

The survey was run from January 2016 to March of that year and 415 people completed the survey. The first question in the survey was: Which of the following Social Networking sites do you currently have an active account with and use? (Check all that apply). The purpose of having this question at the start was to disqualify any non-SNS users and to identify what SNSs the survey participant was currently using. The results revealed that Snapchat was the dominant SNS among the four networks, with a response rate of 69.6%. Snapchat is the newest social network between the other three networks. Facebook, which is one of the oldest SNSs, had the lowest percentage of users in this survey at 55.9%. Table 1 represents the findings and the rankings of the SNSs by the survey participants.

Table 1: Chosen SNSs by the users in the sample

Answer Choices	Responses
Facebook	55.90% N=*232*
Twitter	56.87% N=236
Instagram	60.96% N=253
Snapchat	69.64% N=*289*
None	3.37% N=*14*
Total Respondents: 415	

The next results looked at the membership of the four sites broken down into gender to identify if gender played a role in choice of sites to join. Figure 2 shows that a majority of males (75.52%) in this sample used Facebook; however, females used Facebook the least and Snapchat the most with 79.02%.

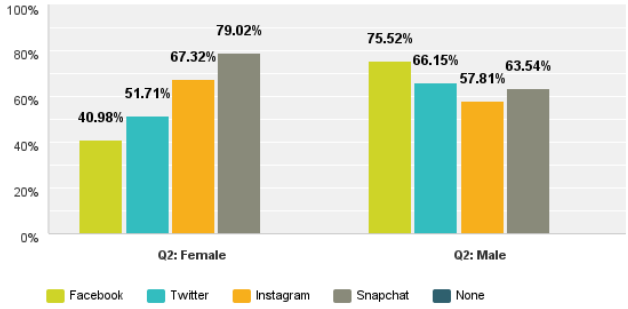


Figure 4.1 Male vs. Female Choice of SNS

One question was designed to determine the reason behind a user becoming a member of the site. With the growing acceptance of SNS's, this question looked at why people joined and was useful for also inferring why many people who are regular Internet users continue to resist joining sites.

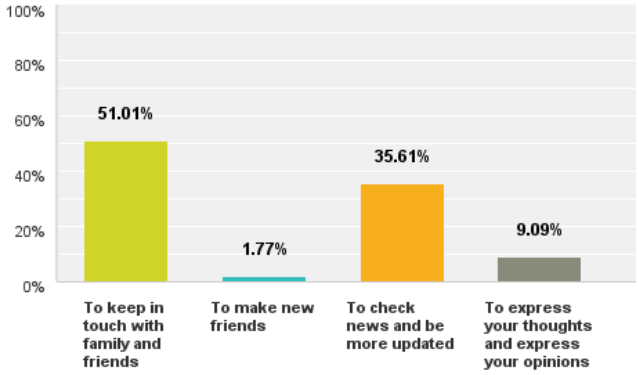


Figure 3: Motivation for using sites

Figure 4 displays the frequency of SNS use by the survey participants. It shows that most of the members are frequent users of SNSs, with 82.9% being daily users.

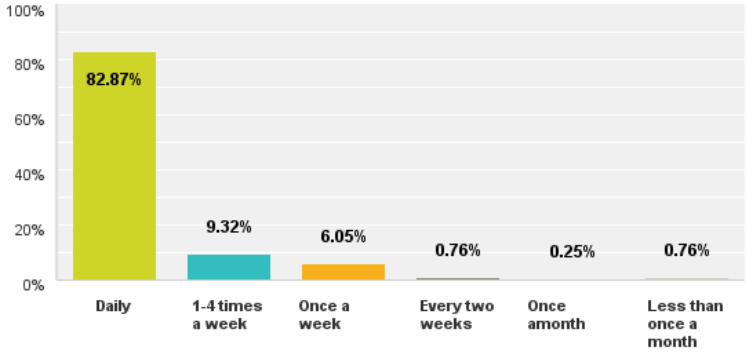


Figure 4: Frequency of site visits

Figure 5 presents the findings of the question "Is the privacy of your information on Social Networking sites a major concern for you?" The purpose of this question was to establish the value of online privacy for the user, which can affect their answers to other questions. For instance, if someone is not very concerned about the privacy of their information online, they will likely not be so stringent in applying protective privacy and security settings to avoid leakage of information. In addition, people who value their privacy and are more concerned about their information will probably not share as much personal information compared to those who are less worried about privacy.

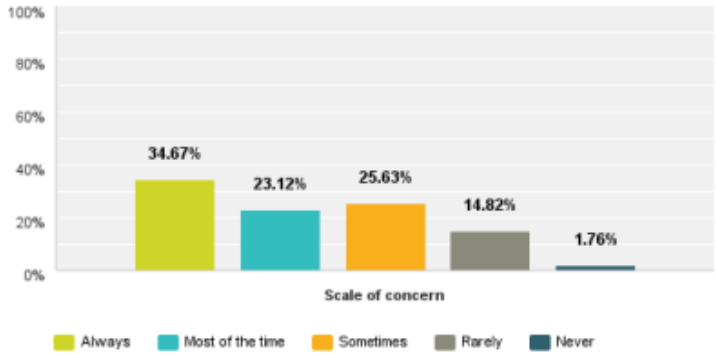


Figure 5:Scale of concern over privacy

The results showed that there was a lack of trust in SNS providers with regard to storage and protection of users' information, as 66.3% of the survey respondents answered that they did not trust their providers with their information. These findings will be used later in this chapter to compare users' actual actions with their levels of

personal information disclosure and examine the ways they apply privacy settings to protect their information and online identity. If users are disclosing personal information, then one method to hinder the use of information by unscrupulous individuals is to use fake or partially fake identities. Figure 6 shows the percentage of members who use their genuine name, fake name or partially fake name such as a genuine first name with a fake surname.

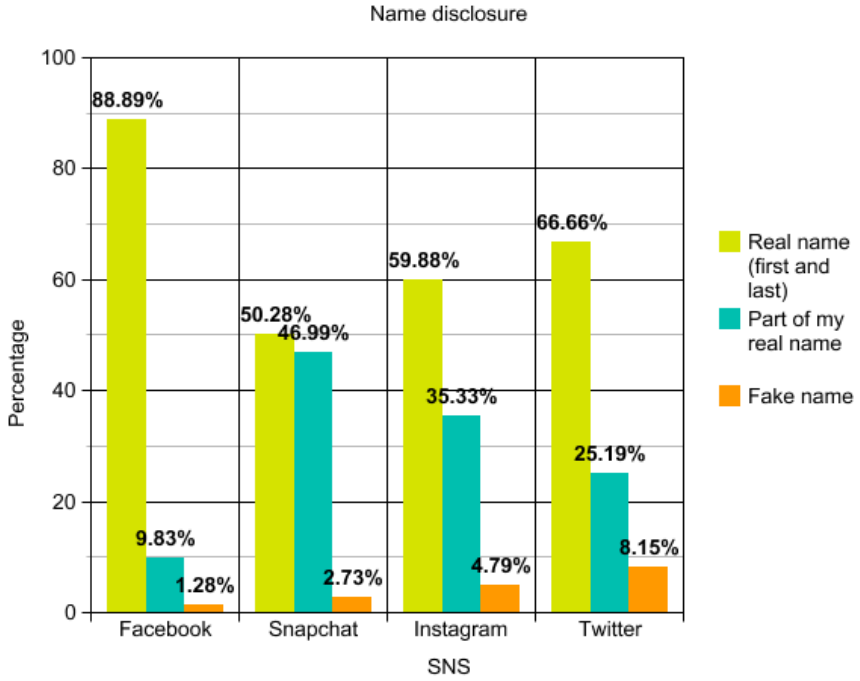


Figure 6: Name disclosure in Facebook, Snapchat, Instagram and Twitter.

The next results looked at the information disclosure and privacy settings members used on the four sites. The Facebook results are indicative of the four sites and indicate the varying level of disclosure people are willing to make. More personal information tends to be kept private on the sites and more generic information such as the city of residence tends to be more freely disclosed.

Table 2: Facebook: Personal information disclosure and privacy settings

	Public	Friends	Customised group of friends	I don't share this information with others	Total Respondents
Hometown	53.9%	36.0%	3.9%	6.1%	228
Current city	52.8%	36.7%	4.8%	5.7%	229
Family members	24.9%	52.8%	7.4%	14.8%	229
Relationship status	29.3%	50.7%	4.8%	15.3%	229
Birthday	41.3%	47.8%	3.5%	7.4%	230
Education	44.5%	45.4%	3.5%	6.6%	227
Events	26.3%	59.2%	5.7%	8.8%	228
Locations visited	24.3%	55.7%	4.3%	15.7%	230
Friends List	26.8%	54.8%	6.6%	11.8%	228
Contact Information	22.2%	50.0%	7.0%	20.9%	230

Instagram is a site dedicated to allowing members to post pictures and videos. The site allows for a brief description of the graphic or video allowing members a choice of how much information about the posting they wish to disclose. Table 3 shows the results for this site.

Table 3: Instagram: Types of personal information posted

	Yes	No	Total
I post pictures/videos of myself	55.7%	44.3%	271
I post pictures/videos of family members/friends	58.7%	41.3%	269
I include the real location of my pictures/videos	69.4%	30.6%	271
Sometimes I post a photo with my house location in the map	39.8%	60.2%	269
I include contact information in my profile	59.6%	40.4%	270
Does your profile picture contain a picture of yourself?	60.0%	40.0%	160

The next series of questions in the survey focuses on the awareness of users of the security policy wordings and the implications of accepting the site's agreements. Much research has been done on users' lack of careful reading of acceptance policies and the results in table 4 indicate that users generally trust that the site will protect their personal information. Careful reading of the policies tends to indicate otherwise in many cases with some sites quite clear that any information, graphics or videos can be reproduced by the site or passed on for any reason without the users permission.

Table 4: Facebook privacy policy awareness question: response frequency

Statement	Proportion of survey participants who do not believe that this statement is true
Collect and use all the information they receive about you to suggest advertisements for you	78 (33.6%)
Track your web surfing anytime you're logged into the site	43 (18.5%)
Use your public information, such as your profile picture, in ads without asking you first and without any compensation to you	45 (19.4%)
Collect information about your device locations, including specific geographic locations, through GPS, Bluetooth, or WiFi signals	59 (25.4%)
None of the above	132 (56.9%)

With the increasing publicity about the risks of over-disclosure of personal information to strangers, many SNS sites are responding by providing much tighter privacy settings for their users. Several sites now prevent graphics searchers to their sites so that a simple search for a picture found on the Internet, even directly downloaded from one of these sites, will often result in no matches on the site. These types of additional security are designed to protect their users from stalking and identity theft. However, these measures only provide greater resistance to these types of criminal acts if users are cautious about whom they permit to view their private information reserved for 'accepted' friends. Table 5 shows the results from setting up a fake profile and then requesting to 'friend' these strangers. Strangers were chosen as randomly as possible by selecting pages during browsing of users' sites. Results show that acceptance rates vary between sites but that 3 out of the 4 sites have greater than 50% acceptance of these fake friends.

Table 5: Acceptance rate for fake profiles on Snapchat, Facebook, Twitter and Instagram

	Users added	Users accepted the add	Frequency of acceptance
Snapchat	400	120	30%
Facebook	400	245	61.25%
Twitter	400	233	58%
Instagram	400	224	56%

The next point of interest was designed to ascertain generilastions from the four sites about whether gender played a significant role in how much personal information was disclosed. As an example which is representative of all sites, Facebook results are shown in table 6. These results indicate that gender does play a role in personal information disclosure with males more likely to disclose personal information than females in

every category. One interesting result from the survey is that in most cases there is no difference between the genders on accepting friend requests. It would appear from this result that the sociability of the members is something accepted by males and females equally.

Table 6: Facebook: Gender Chi-square description of results

Attribute	Results of cross -tabs and Chi Square analysis
Hometown	- Males more likely than females to be public - Females more likely than males to be friends - Females more likely than males to be "don't share
Current City	- Males more likely than females to be public - Females more likely than males to be friends - Females more likely than males to be "don't share"
Family members	- Males more likely to be public than females - Females more likely to "not share' than males
Relationship status	- Males more likely to be public than females - Females more likely to "not share' than males
Birthday	- Males more likely than females to be public - Females more likely than males to be friends
Education	- Males more likely than females to be public - Females more likely than males to be friends - Females more likely than males to "not share"
Events	- Males more likely than females to be public - No difference on friends - Females more likely to "not share"
Locations visited	- Males more likely than females to be public - No difference on friends - Females more likely to "not share"
Friends list	- Males more likely than females to be public - No difference on friends - Females more likely to "not share"
Contact information	- Males more likely than females to be public - No difference on friends - Females more likely to "not share"

Finally, Snapchat results are shown in figure 6 for posting of personal photos and videos. Snapchat promises to permanently delete these photos and videos after a short time but there has been a greater public awareness recently that they are in fact quite easily recoverable from devices that have viewed these items and that the site owners generally retail rights to these often very personal photographs. Results indicate that females are much more likely to post pictures of friends and family members and that younger people tend to be much less concerned by posting these types of personal family and friend pictures and videos.

Table 6: Snapchat Chi-square analysis results for posting pictures/videos that include family members/friends

		Yes	No
Gender	Male	74(56.9%)	56(43.1%)
	Female	122(77.7%)	35(22.3%)
Age	16-24	119(75.8%)	38(24.2%)
	25-34	61(62.9%)	36(37.1%)
	35+	16(47.1%)	18(59.9%)
Education	High school	41(83.7%)	8(16.3%)
	Bachelor	104(68%)	49(32%)
	Masters	42(59.2%)	29(40.8%)
	Doctoral	9(60%)	6(40%)
Privacy	Rarely/Never	42(84.0%)	8(16%)
	Sometimes	46(60.5%)	30(39.5%)
	Mostly	44(67.7%)	21(32.3%)
	Always	64(66%)	33(34%)

CONCLUSION

The results from the survey are a selection of several of the more interesting points taken from the findings. The questionnaire comprised of over 30 different questions with many diverse areas of SNS privacy investigated. This selection of results shows that many factors comprise the profile decisions of users and those who choose to join as members. The publicity over the risks of disclosing private information that may be used to construct fake profiles, stalking and other nefarious activity seems to have had little effect on many SNS users. The desire to be part of a community, often with hundreds of friends, most of which the person will never meet and who themselves may be using fake identities, seems to have only a modest effect on the users' sense of caution. The results indicate that people are generally willing to use real names, disclose personal attributes such as dates of birth and hometown locations and often post personal pictures that could identify themselves, family members and friends. The use of privacy settings where only 'friends' can view posts, videos or pictures is largely negated by the ready acceptance of both males and females to accept friend requests from people whom they have no prior knowledge of and no method to ascertain the genuineness of the identity or desire to follow them. These results indicate that whilst the messages about the risks of over-disclosure are regularly repeated, most social networking site users are making their own decisions about what they wish to disclose and often these decisions are not fully informed by the reading the user agreements and are putting users at risk because of their desire to belong to these communities and share their information with strangers.

REFERENCES

Aldhafferi, N., Watson, C., & Sajeev, A. (2013). Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices. *International Journal of Security, Privacy and Trust Management*, *2*(2), 1-17. doi:10.5121/ijsptm.2013.2201

Alexa. (2016). Alexa Top 500 Global Sites. Retrieved from http://www.alexa.com/topsites

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: definition, history and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210-230. doi:10.1109/EMR.2010.5559139

Chapman, C. (2009, October 7). The history and evolution of social media. Retrieved from http://www.webdesignerdepot.com/2009/10/the-history-and-evolution-of-social-media/

Donath, J. (2007). Signals in social supernets. *Journal of Computer-Mediated Communication*, *13*(1), 231-251. doi:10.1111/j.1083-6101.2007.00394.x

Cross, M. (2014). *Social media security: Leveraging social networking while mitigating risk*. Rockland, MA: Syngress (Elsevier Science).

Lewis, K. (n.d.). How social media networks facilitate identity theft and fraud. Retrieved from https://www.eonetwork.org/octane-magazine/special-features/social-media-networks-facilitate-identity-theft-fraud

Luo, W., Liu, J., Liu, J., & Fan, C. (2009). *An analysis of security in social networks.* Paper presented at the Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 12-14 December, Chengdu. doi:10.1109/DASC.2009.100

Prall, L. (2010, September 20). SixDegrees - social networking in its infancy. Retrieved from http://eziniearticles.com/?SixDegrees---Social-Networking-In-Its-Infancy&id=5064109

Statista. (2015). Facebook: monthly active users 2015 | Statistic. Retrieved from http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Tubaro, P., Casilli, A. A., & Sarabi, Y. (2014). Against the hypothesis of the end of privacy: An agent-based modelling approach to social media. SpringerBriefs in Digital Spaces, DOI: 10.1007/978-3-319-02456-1_1.

Zheleva, E. M., Terzi, E., & Getoor, L. (2012). *Privacy in social networks*. San Rafael, CA: Morgan & Claypool.

AN INVESTIGATION OF POTENTIAL WIRELESS SECURITY ISSUES IN TRAFFIC LIGHTS

Brian Bettany[1], Michael N. Johnstone[1, 2], Matthew Peacock[1, 2]
[1]School of Science, [2]Security Research Institute
Edith Cowan University, Perth, Australia
bbettany@our.ecu.edu.au, m.johnstone@ecu.edu.au, m.peacock@ecu.edu.au

Abstract

The purpose of automated traffic light systems is to safely and effectively manage the flow of vehicles through (usually) urban environments. Through the use of wireless-based communication protocols, sets of traffic lights are increasingly being connected to larger systems and also being remotely accessed for management purposes, both for monitoring and emergency purposes. These protocols, however, were not designed with security as a primary requirement, thus systems may operate with sub-standard or non-existent security implementations. This research aims to test if the same issues and vulnerabilities that appear to be present in traffic light systems in the USA are prevalent in Australia, specifically, Perth. There is evidence of weaknesses in traffic systems in Eastern Australia and by undertaking this research the conjecture that the same weaknesses may be present in Perth traffic systems can be answered. While none of three common wireless protocols (ZigBee, Bluetooth or Wi-Fi) were found to be in-use, the discovery of a large, consistent network pulse warranted further investigation at one specific intersection.

Keywords
Wireless Protocol, Critical Infrastructure, Cyber Security

INTRODUCTION

Traffic lights have existed in some form for over a century, with the first coloured signal light system appearing in 1914 in London, England (Helmer, Meth, & Young, 2015), consisting of two semaphore arms lit by gas lights. Mueller (1970) notes that by 1915 parts of America were trialling a similar system except it incorporated electric lights and contained a small rotary compressor to blow a whistle, a method well-established at the time by on-duty policemen to control traffic. In 1920 the first three-light (Red, Amber and Green) system was installed in Detroit, Michigan and represents the beginning of what would be conventionally recognised as the modern traffic light.

These early lights are somewhat unsophisticated compared to the traffic lights in use today. Mladenovic (2012) states that traffic lights are now part of a much larger system that is controlled by a central computer using programs such as SCATS (Sydney Coordinated Adaptive Traffic System) or SCOOT (Split Cycle Offset Optimisation Technique). These systems can measure traffic volumes used in road sensors and adjust light timings to allow for the most efficient flow of traffic, not only in a single set of traffic lights, but throughout a whole city.

The motivation for efficient movement of traffic is simple: traffic jams cost time and therefore money. Hodson (2014) estimates that the combined economic loss from traffic congestion for France, the UK, Germany and the USA will increase from USD $200 billion in 2013 to $293 billion by 2030. The total economic losses equate to $4.4 trillion over this 17 year period. These figures represent both the direct (cost of fuel and time wasted) and indirect costs (increased cost of doing business) caused by traffic congestion. The study predicts that the average hours wasted in traffic will increase by 6% by 2030. It also highlighted the environmental cost of this congestion, suggesting that in the four countries studied, idling vehicles released 15,434 kilotons of CO_2 into the atmosphere and that this figure will increase to 17,959 kilotons by 2030. Therefore, any attack (cyber-based or otherwise) on systems that control traffic need only be moderately successful to have a large impact on the economic well-being of a country.

Traffic systems are a vital part of the critical infrastructure of any city, and a city's economic and social well-being is dependent on the smooth movement of people and freight. It could therefore be assumed that any disruption to this system will have some form of impact. This does not have to be a major disruption to have a

potentially devastating effect, for example consider emergency vehicles not being able to get to where they have to be because they are caught in a traffic jam caused by a traffic system failure (Kelly, 2001).

Cerrudo (2014) claims to able to hack into the traffic lights in several United States cities, including Washington DC and New York City, and potentially alter the timings of the signals. Cerrudo (2014) showed how to intercept the wireless signals that were being transmitted from a sensor node in the roadway to a traffic controller located on the road-side using commercial off the shelf tools. The specific system in question is produced and marketed by Sensys Networks which, according to their sales literature, is used extensively around the world including Australia (Ford, 2015).

This research aims to test if the same identified issues and vulnerabilities that appear to be present in traffic light systems in the USA are prevalent in Australia, specifically, in the city of Perth. The remainder of the paper describes some specific instances of traffic or traffic-related attacks, defines the experimental methodology used and discusses the findings of the research.

SECURITY ISSUES IN TRAFFIC LIGHT SYSTEMS

Much like the advancement of other service-based systems, traffic lights were not designed with security as a principal requirement. Early security of these systems revolved around physical isolation and proprietary protocols. However, with increased connectivity for remote management and operation, and the use of common protocols for interoperability, the security through obscurity paradigm no longer applies to these critical systems.

There is limited peer-reviewed research on the security of traffic lights. Estrin (2013) reports that in September 2013 cyber-terrorists attacked the traffic system in the Israeli city of Haifa, targeting the security camera network on the Carmel Tunnels toll road with what was believed to be a Trojan malware programme. The attack was carried out sporadically over two days, resulting in the roadway being shut down during the peak hour period, and remaining shut for a period of eight hours on the second day. The resulting traffic jam not only caused long delays to the commuters caught in it, but could have other less visible flow-on effects. These include the cost of any type of traffic congestion to business and risk to life should emergency vehicles be stopped or delayed by the traffic jam (Bernasek, 2014; Kelly, 2001, Schrank, Eisele, & Lomax, 2012). While this attack was an extreme case, with driverless cars currently in the trial phase, security issues in traffic light systems are a risk that will need to be managed, given the increased automated interaction between driverless cars and traffic light systems (Petit & Shladover, 2014). There has been limited research into the vulnerabilities of these systems carried out in the USA (Cerrudo, 2014; Ghena, et al., 2014), with very little consideration of whether these same vulnerabilities are present in systems used in Australia.

A team from the University of Michigan (Ghena et al., 2014) investigated local traffic light systems. In the Michigan area, traffic light systems use induction loops below the ground to detect cars, which then communicate using wireless signals between the traffic controllers and the central server. The central server is capable of making modifications to the light timings dependent on the information it receives from the induction loop sensors, to dynamically avoid or alleviate traffic congestion. Each traffic intersection is treated as an individual isolated system, with communication and coordination between intersections undertaken using a central server. The protocol used for these wireless communications is a proprietary protocol similar to 802.11 Wi-Fi; which presents an SSID visible from a normal laptop or smartphone.

With the cooperation of a road agency in Michigan, Ghena et al (2014) went on to show that it was possible to compromise traffic lights in Michigan by using the communication radio signals used by the network. These fell into two ranges, 5.8GHz for short distance in-line signals and 900MHz for longer distances blocked by buildings or other obstacles. They found three major problems with these traffic communications:

1. Wireless signals were not encrypted
2. Default usernames and passwords were used
3. Known exploits could be used

These weaknesses allowed for attacks such as Denial of Service (DoS), timing manipulations to cause congestion and the ability to exploit these weaknesses while driving to ensure a green light wherever you go.

It was shown that at least in these types of traffic controllers the more extreme claims of deaths or accidents resulting from all the lights turning green are highly unlikely unless physical access to the traffic control box can be achieved, because a hardware system is in place which stops this event happening.

Government Audits

Similar to the US, there is little publicly-available information about the security of traffic systems in Australia. There have, however, been two Australian State Governments that have run audits on their traffic systems in the past five years, with both identifying a number of weaknesses (Gaskell et al., 2015; QUA, 2013).

The Queensland Government audit undertaken before the 2014 G20 conference in Brisbane identified a lack of security understanding, and a wide range of security issues. The report states, "The traffic management systems for the Brisbane metropolitan area were not secure. If the systems were specifically targeted, hackers could access the system and potentially cause traffic congestion, public inconvenience and affect emergency response times. Such attacks could also cause appreciable economic consequences in terms of lost productivity. It was identified that these issues were caused due to increased connectivity between control systems and the Internet for remote management purposes" (QUA, 2013). A similar audit, released by the Audit Office of New South Wales in 2015 also found significant security issues in the traffic management system, stating that the risk management process put in place had covered the Transport Management Centre infrastructure, but the scope did not include the traffic network. Of note was one particular section of the road network, which had an identified lack of security and could lead to traffic disruptions, avoidable accidents or even the loss of life (Gaskell et al., 2015). These audits did not disclose specific details of the vulnerabilities discovered, but it is clear from the findings that there were concerns as to the security of the traffic system at a holistic level. In response to these audits the relevant government departments of both states have stated that they have made, or are making the necessary changes to the systems, security practices and security education and awareness training for staff. At this time there is no evidence the WA government has audited the traffic control systems in Perth, in relation to their susceptibility to cyber-attack. The aim of this research is thus to investigate if wireless security issues of traffic sensors, identified in the US, and in operation in Eastern Australia, are in use and/or prevalent in Perth.

RESEARCH METHOD

The research was designed as a number of field experiments, where a combination of appropriate hardware and software resources were used to try and detect, capture and then analyse specific wireless communication used by a selection of traffic lights in Perth. Each step (hypothesis, defined in Table 1) is dependent on its precursor.

The initial focus of this research was to ascertain if the same wireless security issues described by Cerrudo (2014) were present in traffic systems used in Perth. There was evidence that these systems are in use in Melbourne ("M80 FWY Management System", 2012; "Sensys networks freeway solutions, Melbourne", 2010), so there was a possibility that they could also be in use here in Perth.

To answer the key research question, viz. *"Could the same security concerns highlighted in America in regard to ZigBee be present in the traffic systems here in Perth?"*, a number of hypotheses were proposed and are presented in Table 1.

The research was focused on the way traffic light systems communicate at the intersection level and whether specific wireless communications, namely ZigBee, are used. ZigBee was selected because, whilst Cerrudo, (2014) did not specify the protocol he examined, it is clear from the evidence he presented that he protocol was ZigBee. The field experiments to examine these communications were undertaken between March and June 2016 at multiple traffic intersections in Perth. These intersections were chosen because they allowed easy and safe access and represented a cross section of the traffic lights in the eastern and western suburbs of Perth.

Table 1: Hypotheses to be tested

Hypotheses
H_1: ZigBee can be detected in use for wireless communication by traffic lights in Perth.
H_2: The ZigBee packets used by the traffic lights can be captured for analysis.
H_3: The ZigBee traffic used by the traffic lights is encrypted.
H_4: Default settings for authentication are being used by ZigBee traffic systems.
H_5: ZigBee traffic is susceptible to attack with the KillerBee framework.
H_6: New nodes can connect to the traffic system using zbassocflood to a point where the system overloads.
H_7: Legitimate commands can be sent to the traffic system using zbreplay and accepted.
H_8: Legitimate commands are accepted and can be used to change the timings of the traffic lights.

Materials

The initial aim of capturing transmitted packets involved passively sniffing at the traffic intersection; to do this the following equipment was used:

1. HP Laptop (Pavillion dv6) with Windows 8.1 (64 bit) operating system
2. VMware Workstation 12 Player virtual machine running Kali-linux-2016.1-amd64
3. Wireshark version 2.0.1 installed as part of Kali-linux-2016.1-amd64
4. Atmel RZUSBstick antenna configured to work with the ZigBee protocol
5. KillerBee 1.0 Framework running on Kali-linux-2016.1-amd64

ANALYSIS AND DISCUSSION

According to Main Roads WA, Perth has over 850 sets of traffic lights in use throughout the metropolitan area ("Traffic Signals", 2015). These traffic lights are controlled using SCATS and a typical layout for the overall system is shown in Figure 1, whilst Figure 2 shows a typical intersection layout.

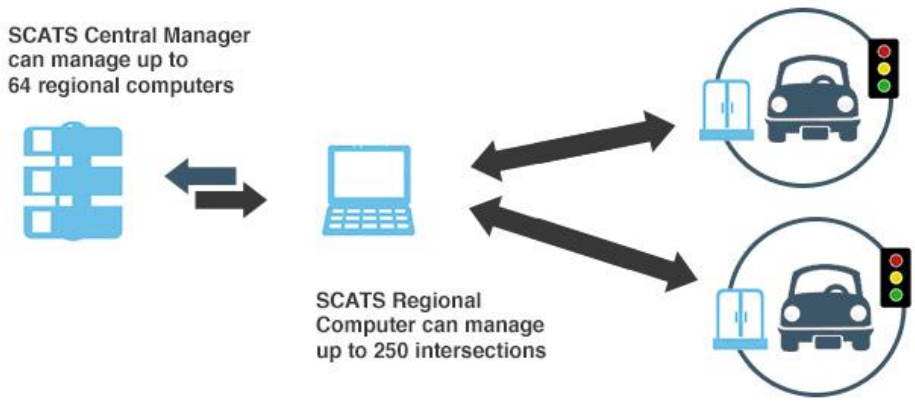


Figure 1: SCATS Control Hierarchy Layout.

The intersections examined consisted of a series of in-road sensors (induction loops) that are connected to a road side control box, which is subsequently connected to both the traffic lights and the regional control centre.

A car moving down the road is picked up by the in-road sensor, which sends this information to the roadside control box. The information is then sent back to the regional computer that performs an analysis, consisting of all the information provided by the other intersections in the area that it controls. The stated configuration gives the regional controller an overview of traffic conditions in a wide area, allowing intelligent decisions to be made to adjust traffic light times accordingly. The most appropriate timings are then sent back to the roadside controller, which then implements the timings through control of the associated traffic lights (Dineen & Cahill, 2001). A central control centre manages the regional controllers, allowing oversight and manual manipulation of the system when necessary, such as in emergencies.

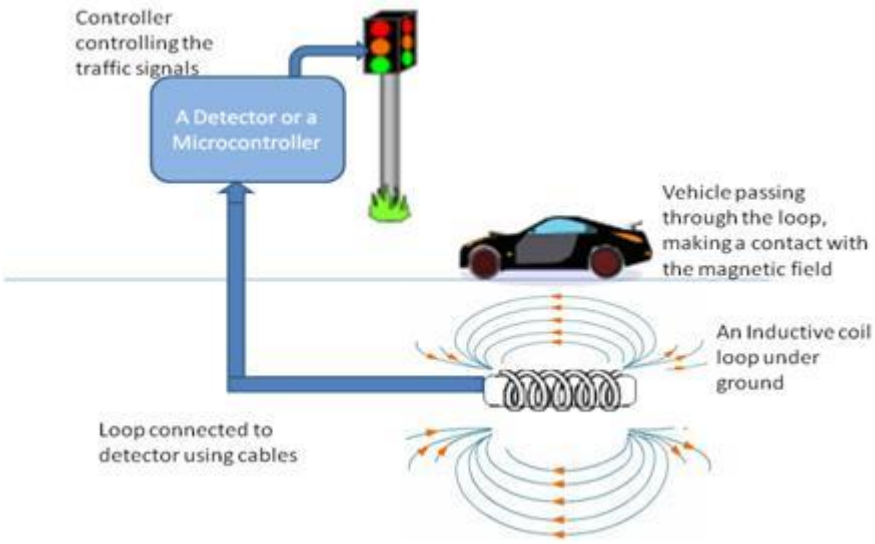


Figure 2: Typical Traffic Light Road layout, retrieved from Agarwal (2013)

Captures of the ZigBee protocol were attempted at ten different intersections in Perth, these tests being attempted on two separate occasions at each intersection and when possible, on different days and times. No traffic was detected on any channel, thus disproving H_1 and effectively invalidating the remaining hypotheses defined in Table 1. This result led to a re-focusing and re-evaluation of the research goal whereby other common wireless protocols were examined. The research question was re-framed as:

"*Is there any evidence that other wireless communication protocols are being used to transmit data between the components that make up an intersection set of traffic lights in Perth, specifically:*

a. Is Bluetooth (IEEE 802.15.1) used in the majority of traffic lights in Perth?

b. Is Wi-Fi (IEEE 802.11) used in the majority of traffic lights in Perth?"

Additional appropriate hypotheses were developed accordingly, to test the revised research question.

In addition to the materials described in the previous section, extra hardware (an Ubertooth One antenna 2015-10-R1) and software (Spectools -2015-10-R1) were utilised to enable detection and capture of these identified protocols.

Testing was undertaken at the same intersections as the ZigBee testing. A Spectools scan using the Ubertooth One was run at each intersection- a typical example being shown in Figure . The green line represents Bluetooth transmissions while the white lines are Wi-Fi.

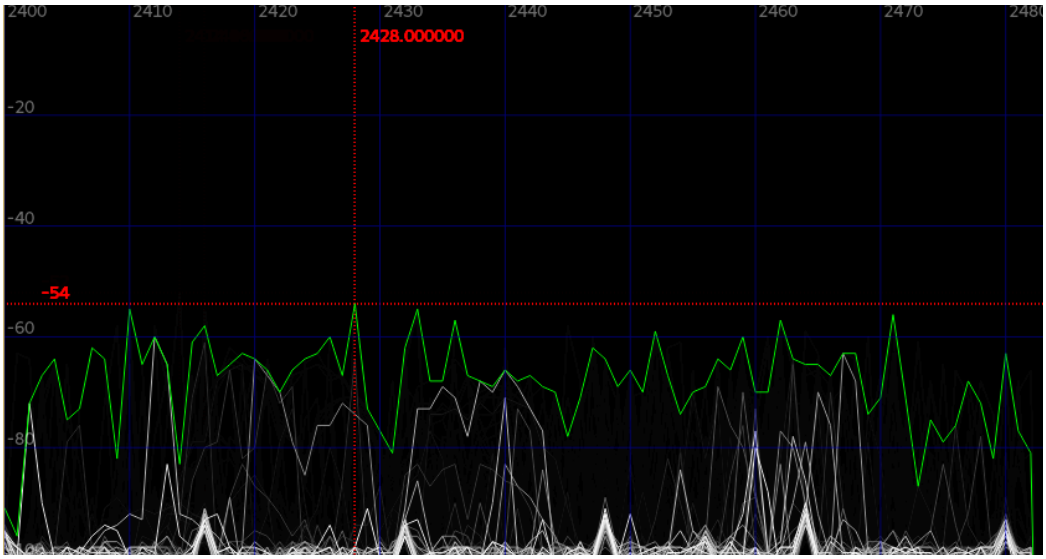


Figure 3: Ubertooth spectral analysis, depicting Wi-Fi and Bluetooth Activity

The Ubertooth One proved to be a useful spectrum analysis tool. It detected both protocols in the 2.4GHz range and displayed the traffic effectively. Although there were many transient devices at each intersection that were using Bluetooth (representing in-car systems and mobile phones used by pedestrians), there were no identified stationary Bluetooth devices at the traffic intersections (as the Bluetooth traffic did not have a static underlying pattern) based on the variable BD_ADDR identifiers detected during analysis.

Similarly, the Wi-Fi signals found were identified as nearby houses or businesses from their SSIDs and signal strength. There was no evidence to suggest that the 802.11 protocol was being used by the traffic lights to communicate to either another intersection or the roadside control box.

However, of note was a consistently identified network traffic pulse at one specific intersection. Upon further inspection of the surrounding traffic management infrastructure, a large antenna attached to the traffic light was identified as the source of the pulse. Spectral analysis was conducted on the pulse, but similar to other intersections, the pulse could not be classified as one of the investigated protocols, (ZigBee, Bluetooth or Wi-Fi), and thus was not captured or classified. The pulse occurred regularly at one-minute intervals, and was identifiable on two separate visits to the intersection, at similar times of day/days of week and peak traffic conditions. A third visit to the intersection resulted in no pulse being identified. While circumstantial, it should be noted that traffic conditions were much lighter during the third visit, which was conducted at a different time of day/day of week, compared to the previous two visits.

CONCLUSION

This research set out to look for the security flaws highlighted by Cerrudo (2014), in a traffic system that used in-road sensors connected via a wireless signal, namely ZigBee. As was outlined previously, there is some evidence that these systems are in use in Melbourne, but no such evidence was found in regard to the intersections investigated in Perth. The fact that there was no information on whether these systems were in service in Perth needed to be examined. The tools necessary for this examination were procured and testing was undertaken, however it became apparent that this protocol was not in use at the intersections tested. This result is a good outcome from a security viewpoint, considering traffic lights in Perth; if ZigBee is not being used it means it cannot be attacked via the methods outlined in Cerrudo (2014). This meant that the research project needed to be re-evaluated and modified to test a wider array of wireless protocols. Bluetooth and Wi-Fi were tested at the same intersections, using appropriate spectral analysis hardware and software. Similarly, there was no evidence of either Bluetooth or Wi-Fi being used by the traffic lights.

Finally, the discovery of a large, consistent network pulse warranted further investigation to one specific intersection. Further examination using the spectral analyser showed that none of the common wireless protocols (ZigBee, Bluetooth or Wi-Fi) were in use, similar to in other intersections investigated. Whilst purely circumstantial, the change in traffic conditions and related change in signal emission does add some weight to the argument that the identified pulse signal is being used by the traffic lights to transmit information during peak traffic periods. This is clearly an avenue for further research.

REFERENCES

Agarwal, T. (2013). Dynamic road traffic signal control system. Retrieved from https://www.elprocus.com/dynamic-road-traffic-signal-control/

Bernasek, A. (2014). The cost of getting stuck in traffic. *Newsweek*, 163.

Cerrudo, C. (2014). Hacking traffic control systems (U.S, UK, Australia, France, etc.). *DEF CON 22*, Las Vegas. Retrieved from https://www.youtube.com/watch?v=_j9lELCSZQw

Dineen, M., & Cahill, V. (2001). Towards an open architecture for Real-time Traffic Information Management. *Proceedings of the 8th World Congress on Intelligent Transport Systems*. Sydney, Australia

Estrin, D. (2013). Experts: Israeli tunnel hit by cyber attack. *Telegraph – Herald.* Retrieved from http://search.proquest.com/docview/144604498?

Ford, S. (2015). Audit project to evaluate vulnerability of traffic lights to cyber attacks. Retrieved from http://wjla.com/news/local/audit-project-to-evaluate-vulnerability-of-traffic-lights-to-cyber-attacks-114819#ixzz3dJSbTm2c

Gaskell, G., Avery, N., Crumlin, S., & Lo, K. (2015). New South Wales Auditor-General's report performance audit security of critical IT infrastructure. Retrieved from . https://www.audit.nsw.gov.au/ArticleDocuments/354/01_Security_of_Critical_IT_Infrastructure_Full_Report.pdf.aspx?Embed=Y

Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., & Halderman, A. (2014). Green Lights Forever: Analyzing the Security of Traffic Infrastructure. *Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT'14)*. Retrieved from https://www.usenix.org/system/files/conference/woot14/woot14-ghena.pdf

Helmer, J., Meth, G., & Young, S. (2015). Sustainable traffic signal development. *ITE Journal*, 85(5), 14-19.

Hodson, H. (2014). Gridlock alert. *New Scientist, 223*(2981), 20. doi: http://dx.doi.org/10.1016/S0262-4079(14)61532-3

Kelly, D. (2001 Mar 12). Traffic jam + ambulance = total chaos. *Austin American Statesman*, p. B1. Retrieved from http://kx7gx4pm8t.search.serialssolutions.com/

M80 FWY Management System. (2012). Vicroads.

Mladenovic, M. (2012). Large scale analysis of traffic control systems. *Traffic Engineering & Control*, 53, 26+

Mueller, E. A. (1970). Aspects of the history of traffic signals. *IEEE Transactions on Vehicular Technology*, 19(1), 6-17. doi: 10.1109/T-VT.1970.23426

Petit, J., & Shladover, S. E. (2014). Potential Cyberattacks on Automated Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 16(2), 546-556. doi: 10.1109/TITS.2014.2342271

QUA. Traffic management systems: Report to parliament 5: 2013-2014. Technical report, Queensland Audit Office, 2013.

Schrank, D., Eisele, B., & Lomax, T. (2012). TTI's 2012 urban mobility report. *Texas A&M Transportation Institute. The Texas A&M University System,*

Sensys Networks Freeway Solutions, Melbourne. (2010). Youtube: Sensys Networks.

Traffic Signals. (2015). Retrieved from https://www.mainroads.wa.gov.au/UsingRoads/RoadTrafficInformation/Pages/trafficsignals.aspx