2016

An analysis of chosen alarm code pin numbers & their weakness against a modified brute force attack

Alastair Nisbet
Security & Forensic Research Group, Auckland University of Technology

Maria Kim

DOI: 10.4225/75/58a69fd2a8b03
Nisbet, A., & Kim, M. (2016). An analysis of chosen alarm code pin numbers & their weakness against a modified brute force attack. In Johnstone, M. (Ed.). (2016). *The Proceedings of 14th Australian Information Security Management Conference, 5-6 December, 2016, Edith Cowan University, Perth, Western Australia.* (pp.21-29).

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.

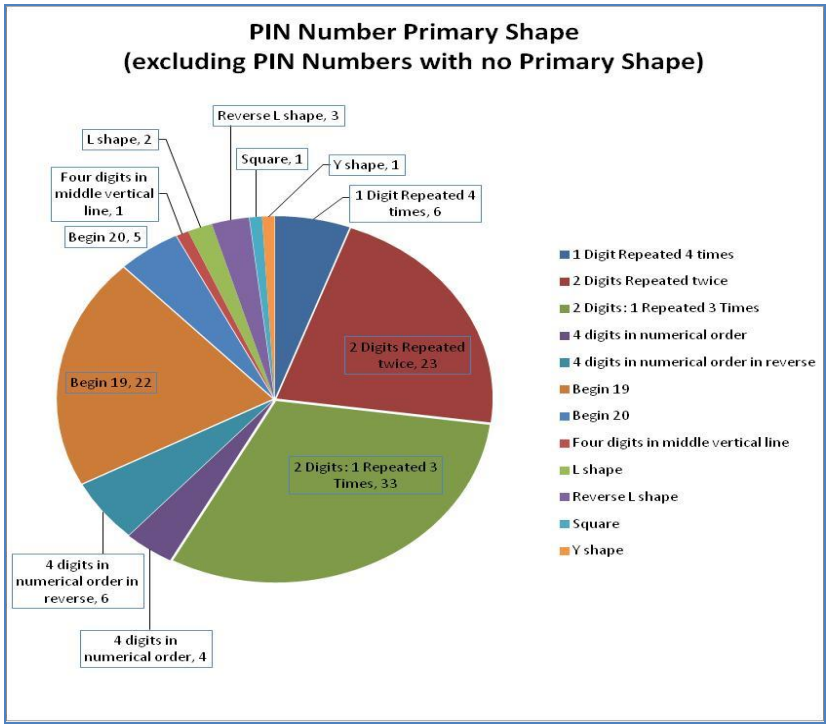

Figure 2: Most commonly chosen PIN numbers

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