12-4-2013

# Security Analysis And Forensic Investigation Of Home & Commercial Alarm Systemsin New Zealand: Current Research Findings

Alastair Nisbet
*Auckland University of Technology*

Maria Kim
*Auckland University of Technology*



DOI: 10.4225/75/57b3d66bfb872
11th Australian Digital Forensics Conference. Held on the 2nd-4th December, 2013 at Edith Cowan University, Perth, Western Australia

# SECURITY ANALYSIS AND FORENSIC INVESTIGATION OF HOME& COMMERCIAL ALARM SYSTEMSIN NEW ZEALAND: CURRENT RESEARCH FINDINGS

Alastair Nisbet, Maria Kim
Auckland University of Technology, Digital Forensic Research Laboratories
Auckland, New Zealand
anisbet@aut.ac.nz, mkim@aut.ac.nz

**Abstract**
*Alarm systems with keypads, sensors and sirens protect our homes and commercial premises from intruders. The reliability of these systems has improved over the past years but the technology has remained largely as it was 3 decades ago. With simple keypads and generally 4 digit PIN codes used for setting and unsetting the alarms, the main protection against a determined intruder is the necessity to choose robust PIN codes. However, with PIN codes chosen that are generally easy to remember and therefore relatively easy to guess, or numbers chosen to follow a pattern on the keypad, the main protection from these systems lies in the ability to detect an intruder as they approach the keypad. This gives the intruder very little time to try multiple codes meaning the systems are secure because the intruder is detected quickly. This research looks at the choices of PIN codes and the patterns that they often follow, and sets out the forthcoming research that will look at circumventing the safeguards by performing computer-driven attacks against the codes when access to the device is possible and when remote access to the device can be made over the telephone system. Additionally, the forensic evidence left behind by an attacker is discussed and how simple enhancements to systems can have significant advantages in enhancing the amount of evidence that can be found. This paper describes the preliminary findings from analysing 700 alarm codes used in alarm systems throughout New Zealand and describes the planned research into alarm system security and forensic evidence remaining after a successful attack by an intruder.*

**Keywords**
Security, digital forensics, alarm systems

## INTRODUCTION

Home alarm systems are installed in a large number of homes in New Zealand and other countries. With almost 60 000 burglaries reported in New Zealand in 2012(New Zealand Police 2013), and a Rutgers University research study finding that alarm systems do reduce the occurrence of burglaries to residences with alarms fitted, alarm systems are currently viewed as a fairly simple and available technology to reduce the chances of burglaries(Clarke, Felson et al. 2007). In 2006 a study in Salt Lake City, Utah, found that 44% of residents had a burglar alarm but that 80% of the residents were not aware of a city law requiring police to respond to alarms only if someone at the scene could verify that a crime was being committed. Once informed of this law, 65% of people disapproved and wanted the law changed(Bisconti Research Inc 2006). This unique survey indicates that people trust their burglar alarms to protect their homes and businesses but want a law enforcement response if the alarm is activated.

Commercial alarm systems are similar to their home use counterparts but often incorporate additional features or more sophisticated detection sensors. The systems themselves however, are similar in operation. They consist of an alarm box containing the motherboard and memory chip, wiring to the sensors, wiring to an external alarm siren and often internal alarm squealers and wiring to a keypad or multiple keypads. Many systems for both domestic and commercial use are also wired into the telephone system so that remote access is possible as well as remote monitoring. Additionally, many systems in commercial premises also have wiring to swipe card readers which unlock doors and raise and lower roller doors giving access to the building.

The general practice for installers is to place sensors in locations that overlook keypads, so that a user's presence will be sensed setting the alarm to counting down to activation as they approach the keypad. The countdown can be set to various lengths but is generally around 30 – 60 seconds, time to retry a code if it is accidentally entered incorrectly but not time to have any serious attempt at guessing a correct code. The security of the system then generally relies on 2 factors, the unlikelihood that a few guesses of a code will be correct, and the placing of keypads in range of sensors so that approximately 3-4 attempts only can be made before the alarm is activated. This seems to have worked well for many decades as most deactivations of alarm systems by intruders tends to be either from maliciously obtained alarm codes or disabling an alarm at the motherboard without getting in range of a sensor. For this reason, the technology used in alarms has changed little of the past few decades, with more sophisticated sensors and lcd displays on keypads, but with the same basic operations at the motherboard.

This Masters research is currently investigating the security of these systems and highlights several security deficiencies already found in many systems. Section 2 looks at the published literature on alarm systems and highlights the lack of academic and practical research into their security. Section 3 discusses the current state of this research and the plans for further research to be undertaken later in the year, and finally the conclusions make preliminary recommendations that can assist with ensuring more robust security in these vulnerable systems.

**STATE OF THE ART**

Alarm systems generally have 3 types of codes. In New Zealand a common alarm is the Paradox system. As an example, this system has firstly has the installer code which is the code giving complete control over the system. This can be likened to gaining root on a computer system. By entering this code the installer can tell the system what sensors are present and which ones to make active or ignore. They can set or delete other codes, set doors to open or lights to turn on or off when certain codes are entered, set notifications to telephones by dialling on the public phone system or if installed, calling a cell phone and have control every other feature that the system is equipped with. The second code is the Master code. This is similar to the installer code but with more limited control. This code allows for user codes to added or deleted but little else. Finally is the standard user code, generally used by employees in an organisation who are often given their own unique code. It is most desirable to have one code per user so that if an alarm is turned off, the forensic evidence on the system will identify the code entered and therefore the person who knows that code(Paradox Security Systems 2012). However, in reality often one code may be shared by many users. Most systems permit at least 50 user codes with some systems allowing for up to 11000 codes. A single user may be part of a user group where the codes within that group can set or unset particular areas within the system such as one floor of a building. This allows users to only enter areas that they are authorised to enter. The users cannot alter, delete or add codes but can only set or unset an alarm.

The alarms are generally set and unset by entering a code on the keypad. On most systems, by default this code can be from 4 to 10 digits but is generally chosen by users to be 4 numeric characters ranging from 0 to 9, giving 10 000 possible codes, called the keyspace. A feature of most alarms is the lockout feature. This locks the system for a preset time if too many unsuccessful attempts are made. While available, it is rare for this feature to be implemented and most users seem unaware that it exists. If this feature is not set, then on average, an intruder with access to the keypad and who could work without entering the sensor zone, would need to try 5000 codes before stumbling across the correct code. However, this assumes that there is 1 code for the alarm. In practice in commercial buildings, often users have their own unique code and there may be many users. If for example there were 10 users, then on average an intruder would need to try 500 codes before stumbling across one. This is still a lot of codes to try by pushing numbers on a keypad and on some systems also having to press the enter key after entering a code. An intruder could likely attempt one code every 5 seconds meaning 500 codes would take 2500 seconds or approximately 42

minutes. If there was only one code and 5000 attempts were required, then it would take approximately 7 hours. The worst case of being successful on the final attempt of 10 000 codes would require approximately 14 hours, still achievable for a very determined intruder.

It is common for users of electronic devices to enter a code, such as pin numbers for ATM machines and 4 digit user codes for cell phones. Much research has been undertaken looking at the numbers that users most often choose. Rasmussen and Rudmin (2010) point out the problem of people's difficulty with memorising number codes which can cause further problems(Rasmussen and Rudmin 2010). Although it is a well-known that longer and randomised PIN codes are more difficult to guess or crack, the lack of users' ability to memorise more complex passcodes means many people use simple and easy to guess number combinations, including using patterns on keypads that are easier to recall than the numbers themselves(Chou, Lee et al. 2013). Whilst choosing more complex codes is ideal, this can be a problem for the elderly or patients with Alzheimer or other brain diseases.

Pritchard (2012) admits that having multiple different PIN numbers may provide better security but can be difficult to remember(Pritchard 2012). Therefore he gives methods how PIN numbers can be constructed by methods such as words converted to numbers, dates or calculation of a single code from numbers with personal meaning. The advantage of this is that although one PIN Number is discovered, only the account which uses that particular PIN number would be affected and other accounts would remain safe therefore the loss can be minimised. However one downside of this is that the users would be forced to remember many different sets of numbers which people would struggle to remember (Carstens and McCauley-Bell 2004). This may force people write down and record the numbers and this can be especially dangerous, if the user negligently loses the information. It means anyone can access effortlessly to the system without brute forcing.

One overseas study of 3.4 million PIN number in several databases listed the top 10 chosen PIN numbers(Berry 2013). The purpose of these numbers was not stated but appears not to be alarm codes. Table 1 shows these PIN numbers and their frequency.

*Table 1. Top 10 Database PIN Numbers*

| Rank | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| PIN | 1234 | 1111 | 0000 | 1212 | 7777 | 1004 | 2000 | 4444 | 2222 | 6969 |
| Frequency | 11% | 6% | 1.9% | 1.2% | 0.7% | 0.6% | 0.6% | 0.5% | 0.5% | 0.5% |

For an intruder guessing PIN numbers in these databases, quickly trying the top 5 choices will give them approximately a 20% chance of finding the number. It is human nature to select numbers that are easy to remember, either because they have some meaning to us or because they form a pattern on the keypad. The top 10 in this study all appear easy to remember except the 6$^{th}$ most common. If a brute force attack were attempted there is almost a 2% chance of finding the code on the first attempt. It is not stated in the study what these PIN numbers are for but they appear not to be related to alarm codes.

**RESEARCH PLAN & INITIAL RESULTS**

An examination of a database of 700 alarm code numbers in New Zealand found that codes were often chosen by pattern more than easy to remember codes, except for the years beginning with 19..which account for over 3% of codes. For example, the PIN 1234 occurs almost 11% of the time in the non-alarm database example but was found to represent only 0.3% of codes for alarms. Table 2 shows the most common pattern ranges with 1000 codes in each range.

| Rank | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| Code | 4000-4999 | 1000-1999 | 3000-3999 | 6000-6999 | 7000-7999 | 9000-9999 | 5000-5999 | 2000-2999 | 8000-8999 | 0000-0999 |
| Frequency | 16% | 16% | 12% | 12% | 11% | 11% | 10% | 7% | 3% | 2% |

*Table 2. Top 10 NZ Alarm Code numbers*

The alarm code analysis indicates that some ranges are far more common than others. Even this small amount of information makes an attacker's task simpler by indicating which ranges should be attempted first in a brute force attack. If an attacker begins at 0000 then 1000 attempts will result in only a 2% chance of success, yet trying the range of 1000-1999 will result in a 16% chance of success. An attacker can therefore improve their chances of success when trying less that the entire keyspace or on average significantly reduce the time required by trying ranges out of numerical order. By trying 1000-1999 followed by 4000-4999, the attacker will have tried 1/5 of the codes with a 1/3 chance of success. More information about the users' preferred choices of codes can further speed up the brute force attack. It is common for patterns on the keypad to be used to aid in remembering the code. Figure 1 shows a typical keypad layout. The keys are arranged in a top down manner with 1 at the top left. This is the opposite of a computer keypad where 1 is at the bottom left. The patterns made generally follow straight lines or 'L' shapes such as 2580, 1236, 3214 etc. These numbers appear to be random at first glance but plotting their location on a keypad will often show the numbers to be a pattern that is easier to remember than numbers.


*Figure 1. Typical keypad layout*

A deeper analysis of the codes finds that users will commonly repeat numbers. In this manner a number that is repeated will make patterns simpler, such as a straight line made with 1123 or 1233. Most often the repeated numbers are in pairs at the start of the code. Table 3 shows the frequency of choices. The '?' represents a wildcard which can be any number.

| Rank | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** |
|---|---|---|---|---|---|---|---|---|---|
| Code | 77?? | 11?? | 99?? | 22?? | 55?? | 33?? | 66?? | 88?? | 44?? |
| Frequency | 1.8% | 1.7% | 2.3% | 0.8% | 0.6% | 0.4% | 0.4% | 0.1% | 0% |

*Table 3. Repeated numbers*

This information also assists in indicating those ranges to attempt first and those to leave until last. In the case of 4000-4999, there is a 16% chance that the code will lie within this range, yet the 100 code range of 44?? results in almost no chance and can therefore be avoided or left to last. It is interesting to note that 44?? is avoided by users yet overall ??** accounts for 2.1% of codes.

The security of alarm systems partially relies on a potential attacker having to attempt so many alarm codes in order to stumble across a correct one so that the attack may not be feasible in the time available. However, if the attack can be automated so that a computer or similar device performs a brute force attack, then the task may become much more feasible. If the sequence of

codes attempted can be performed in an informed manner, so that the most likely numbers are attempted first, then the attack becomes highly feasible and in some cases may be trivial. This leads to the set of research questions:

Hypothesis 1: The numbers chosen by users as alarm codes can be categorised into 2 main categories. Those that are more likely and those that are less likely to be chosen.
Hypothesis 2: By identifying the most likely codes, the time for a successful attack can, on average, be significantly reduced.

A feature that most systems have, although often unknown to the users and owners of the system, is the ability to remotely connect to the alarm control box by the telephone network. To do so, the proprietary software must be started on a computer and a dial-up modem is connected. The appropriate page on the software with telephone number and alarm code is located and the system is then contacted by the modem. When the system answers, the passcode is sent and if correct the user on the computer has control over the system. On many systems this passcode must be from 8 – 10 digits long. The purpose of dialling into the system is generally for one of two reasons. Either the system settings need modification such as a new user has joined the company or one has left and the code must be deleted, or the system has been activated and must be reset. For either reason the remote management facility allows an installer or manager to control the alarm system without having to visit the site, something which can be very convenient. However, if the installer code was entered then the user has complete control over the system, even if they are remotely located in a different city or country. Whilst this can be convenient for the installer, the ability to completely control the system remotely means security must be robust to ensure this feature is not available to a potential intruder. The software is designed such that when the modem is answered by the system, one alarm code only can be tried and if incorrect the system hangs up. This means that even a few attempts at different codes is very time consuming and not practical for a brute force attack on the code. The planned research will modify the modem software so that unlimited attempts at the codes can be performed over the telephone line. This leads to the third hypothesis.

Hypothesis 3: A brute force attack can be made over the telephone line and performed in a similar manner to the attack at the keypad.

The systems also have a logging feature on the software side and the alarm side. On many systems, the memory is sufficient as standard to record the last 50 logins to the system which can be increased by 1000 logins by purchasing an expansion memory module. In practice, expanded memory is rare and the record of an access to the system will likely drop off the system within a few weeks or months. This gives an attacker the opportunity to remotely access the system, enter the installer code, switch off a zone or multiple zones and wait until the access drops off the system. Then a physical burglary can take place in the areas where the zones were switched off with no evidence on the alarm motherboard of the malicious dial-in to the system in the months previously.

For this reason, and commercial sensitivity, the installer codes tend to be closely guarded secrets. Installers often will install alarms and may not use the code again for years or will go out of business and the code is forgotten. A new contract to maintain the alarm will require the new installer to obtain the installer code so that modifications to the setup can be made. However, if the installer code is forgotten or cannot be obtained the system cannot be modified. Most systems have a reset function but this is often locked for security reasons. In practice, this means that many good systems are discarded because the installer code is not known. Additionally, most systems have the functionality of a lockout where multiple attempts with incorrect codes will render the system locked so that only the installer code will unlock the system. This feature is very seldom implemented on the system, meaning that a forgotten installer code is not needed if a forgetful user makes many attempts and that intruders who can get unhindered access to the keypad can systematically try every code.

The research to this stage has looked at the alarm codes used in a sample of 700 users in a number of different systems. The next stage of the research is to perform a brute force attack on a test device where all programmed codes can be found. These will be logged in a file so that the three types of programmed codes and all user codes can be simply read. This will involve writing custom software and utilising a device such as a Raspberry Pi, Arduino or rubber ducky, to try every possible code in turn and noting the response which will be; not a code, installer code, master code or standard user code. This will show that a brute force attack by a computer against an alarm utilising intelligence on the more commonly chosen numbers is possible and can be performed more quickly than a systematic attack trying each number incrementally. This will also have a practical use for installers where the custom software will be useful to discover an installer code from devices where the code cannot be found with any other method. This will have the benefit that devices where the installer code could not be located can now be useful again to installers.

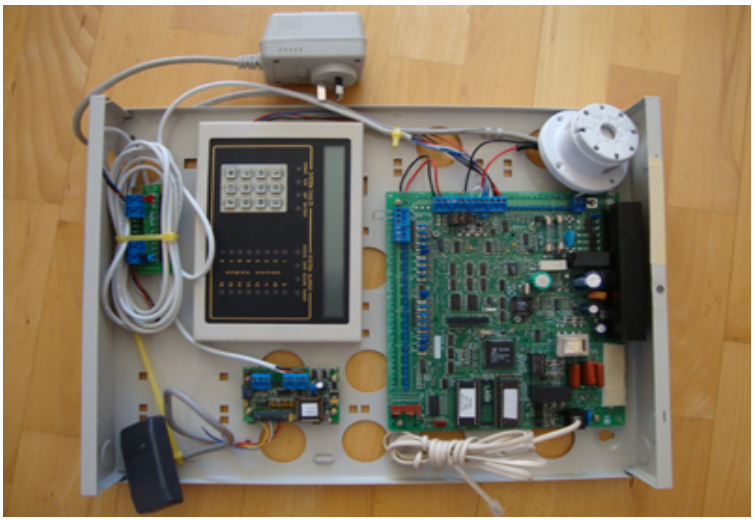

*Figure 2. Alarm Test Unit*

Figure 2 shows the test unit that will be used for the experiments. Once this attack is shown to be successful, the next step will be to remotely contact a test device over the public telephone system. Currently, with the correct proprietary software and a 2400 baud dial-up modem, a single code can be entered which is matched in the device once a connection is made. If the code is not correct, the device will hang up and the connection is lost. The goal of this phase will be to perform a brute force attack over the telephone system where codes can systematically be attempted. This will involve writing custom software to systematically work through the codes and the test device will be forced to maintain a connection and will not hang up until the tester terminates the connection at the completion of the simulated attack. Additionally, settings for alarms could be modified so a brute force attack against the system could trigger an alert to the owner or installer so that monitoring of the attack and recording of forensic evidence could be done while the system is under attack.

Once this attack is proven to be feasible the next stage will be to design a forensic framework to ensure permanent logging of these types of attempts. This will ensure that attacks against alarm systems can not be acted on months later with the record of the attack having been deleted. It is clear that activity should be logged for the lifetime of the device if possible and a method for doing this will be investigated. The final stage of the research will be to construct a guideline for installers and users that will highlight the areas where particular attention to setup of the systems needs to be taken. This will provide a framework that can be followed so that the security of these systems can be enhanced so that these types of attacks will be considerably more difficult to mount in the future.

## CONCLUSION

This initial research has highlighted the security issues and possible attacks against home and commercial alarm systems. If an attack does occur, forensic evidence can often be found on the system but may be deleted after time. The preliminary findings indicate that as with many other devices requiring PIN codes, alarm code numbers are chosen by users that are easy to remember and easy for an attacker to guess. Additionally, with a keyspace of 10 000 codes, an unhindered brute force attack against these systems is feasible in just a few hours. This research is designed to show what attacks are possible at present and to provide a basis for mitigation of these attacks by describing how they work and how in some cases they can be prevented. Additionally, a framework to act as a guide for the installers and users of the system is to be developed so that alarm systems in the future can be better safeguarded against malicious attack and intrusion. Currently little research into home and commercial alarm systems has been done, but with older technology still used in these systems, and with the inherent problems of PIN code choice for users, this research is an important step in securing systems against malicious attack.

## REFERENCES


Berry, N. (2013). "PIN analysis." from http://www.datagenetics.com/blog/september32012/.

Bisconti Research Inc (2006). Public Opinion Survey of Salt Lake City Registered Voters Regarding Crime and Police Response to Burglar Alarms. Salt Lake City, Utah, Alarm Industry Research & Educational Foundation.

Carstens, D. and P. McCauley-Bell (2004). "Evaluation of the Human Impact of Password Authentication Practices on Information Security." Informing Science Journal 7.

Chou, H., H. Lee, H. Yu, F. Lai, K. Huang and C. Hseueh (2013). "Password Cracking Based on Learned Patterns From Disclosed Passwords." International Journal of Innovative Computing Information and Control 9(2): 821-839.

Clarke, R., M. Felson, G. Kelling and R. McCrie (2007). The Impact of Home Burglar Alarm Systems on Residential Burglaries.

New Zealand Police. (2013, 18th August 2013). "Crime Statistics for calendar year ending 31 December 2012." from http://www.police.govt.nz/about-us/publication/crime-statistics-calendar-year-ending-31-december-2012.

Paradox Security Systems (2012) "System Manager's Manual."

Pritchard, J. (2012). "PIN - Personal Identifcation Numbers - PIN Number Tips." Retrieved 6th August 2013, 2013, from http://banking.about.com/od/securityandsafety/p/pinnumber.htm.

Rasmussen, M. and F. Rudmin (2010). "The coming PIN code epidemic: A survey study of memory of numeric security codes." Electronic Journal of Applied Psychology 6(2): 5-9.