Recent Advances on Securing Wireless Transactions

Abstract

With the increasing use of wireless technologies, particularly in mobile (m-) commerce, comes the increasing threat of hacking. Since wireless knows no architectural confines, it is straightforward for a hacker to gain access to confidential data. The security of the data is dependent upon the strength of the security scheme. In this paper we look at common security concepts, investigate the problems of wireless security and then focus on a new type of encryption scheme called chaotic encryption. The Logistic map chaotic encryption has had deficiencies but those have now been corrected. The beauty of this encryption is that it is fast due to its low computational overheads. Finally, we look at a way of placing this security into devices with embedded microcontrollers like PDAs, phones and other tiny computing systems.

Authors

Dr. Terry Rowlands
UQ Business School
University of Queensland
Ipswich, Australia, 4305.
Phone: +61-7-3381 1218
Fax: +61-7-3381 1227
E-mail: T.Rowlands@mailbox.uq.edu.au

Dr. David Rowlands
School of Microelectronic Engineering
Griffith University
Nathan, Brisbane, Australia, 4111
Phone: +61-7-3875 5383
Fax: +61-7-3875 5384
E-mail: D.Rowlands@mailbox.gu.edu.au.

Recent Advances on Securing Wireless Transactions

1.0 Introduction

Normal business practices cover a wide range of activities from product manufacture to stock control to point of sale. The electronics industry in the last couple of decades has revolutionised considerably the way that business is performed. There is an increasing reliance upon technology to improve the efficiency and improve the profitability of small and large businesses. Possibly the greatest effect has been through the use of computers. Computers have changed the way the core business principles are carried out. There has been a trend to reduce the size of these computers and place increased computing power in the hands of the ordinary users. One way of achieving this aim has been through the use of mobile/wireless technology. Wireless technology allows any data entry device to be moved to any location within a mobile cell. This operation is achieved by dispensing with cables and using radio communications to transmit data.

Wireless technologies are attempting to become ubiquitous and the diffusion of these technologies is expected to increase throughout the business and home user populations (Jones, 2002). The number of non-mobile phone handsets (e.g. Personal Digital Assistants, laptops etc) that have wireless capability is expected to exceed 1.5 Billion worldwide by the end of 2005 (Jones, 2002). These projections indicate that wireless technologies must be part of the strategic aim for any business that utilises communications technology. It is projected that at least 40% of Business to Employee (B2E) applications for Global 2000 companies will be partially converted for wireless by 2005 (Jones, 2002). B2E over wireless enables roaming employees to have access to applications and information on demand irrespective of their location. An indication of the current state of the wireless market is that it experienced a 3% growth in the fourth quarter of 2002 and had revenues totalling US $419 million (DellOro, 2003).

Wireless can allow a more streamlined business process, by allowing agents to have mobility without the restriction of cabling systems. This scheme allows a more flexible customer – salesperson relationship and provides the basis of m-commerce. M-Commerce can be defined as "any transaction with a monetary value either direct or indirect that is conducted over a wireless telecommunications network" (Barnes, 2002, p.92) The sales personnel can serve customers at any location throughout the store by connecting via wireless to the central server that processes the order (du Preez and Pistorius, 2003). This arrangement provides a more accurate and immediate solution than the paper based information systems that previously existed. The stocktaking function performed by staff of large grocery stores that walk around to the shelves, scan the barcode of the item and update the inventory lists is also more streamlined with wireless connections. There are many more examples of such efficiencies. For a very large list of the different facilities that can be available over mobile systems see Table 1 of du Preez and Pistorius (2003) and also section 3 of Sabat (2002).

Another exciting development is the way Wireless can provide for the capturing of nomadic customers. For example, a customer may walk within a wireless cell that encompasses a restaurant. The customer's PDA could (with suitable client programmes and protocols) receive a message stating that today's special is Greek (Crisler et al., 2003). Cinemas could utilise similar technology to advertise movie times, special deals etc.

Wireless technologies are becoming more pervasive (Sabat, 2002; Tsalgatidou and Pitoura, 2001). The cost of adopting wireless technologies is dropping rapidly due to demand, ease of deployment and reliability. In fact, the costs have reached such a level where some Small to Medium Enterprises (SMEs) are beginning to consider incorporating the wireless technologies into their business strategies. They even have representative membership in the Wireless World Research Forum based in the European Union (Mohr, 2003).

Some of the data sent over the airwaves is public property and may even be "pushed" at a customer. Other wireless data may be intended for a specific recipient within an office environment. The mobility provided to those within the office by means of not being hampered by cabling may be advantageous to the productivity of those workers. Since there are no restrictions about who can physically enter a wireless cell the information is easily available to any person with wireless capability. If the information is not protected from the eavesdropper by a scrambling scheme (encryption) then it is inherently readable and therefore security can be breached. It is worth noting that wireless cells may extend beyond the confines of a building and this provides an entry point for hackers.

Encryption methodologies are the agreed schemes used by two parties for the transfer of information that ensures privacy by making the data look incomprehensible to an eavesdropper. These schemes entail two main components, an agreed scrambling/descrambling algorithm (cipher) and the keys that allow only the permitted parties to encrypt/decrypt the message.

The encryption schemes that are used on wireless technologies need to be tight. These schemes must provide no exploitation opportunities for hackers and yet still be fast enough on low processing power handsets to be practical. Both the Bluetooth and the Wi-Fi standards of wireless networking have been shown to have security problems that allow them to be compromised. In this paper it is argued that a fast, simple and strong cipher based on the "apparent randomness" of a chaotic sequence is required. Major problems with previous chaotic schemes are corrected and an efficient, fast, and very strong chaotic cipher is presented. The applicability of this cipher to secure sockets is also discussed. Finally we present a general methodology for chaotic ciphers to be implemented at the chip level without major calculation overhead. This method increases the speed of the cipher by removing the costs of non-integer calculations and thereby making it even more eminently suitable for low processing power mobile devices. The chaotic ciphers that we propose will make mobile wireless devices more secure without the penalty of loss of speed.

This paper is in five parts. The first part presents a commonly encountered encryption scheme. The second part deals with wireless connections and their main security deficiencies. The third part provides an introduction to chaos theory and chaotic encryption. The final part describes cutting edge research on chaotic security schemes.

2.0 A Commonly Encountered Security Protocol: SSL

Instead of having an application (e.g Pretty Good Privacy PGP) do the encryption for us, it would be expedient to have the communication system (i.e. protocol stack) do the encryption. By virtue of being a protocol, it could also negotiate things like the cipher algorithm that is used. The Secure Sockets Layer (SSL) provides this aspect and more. It was originally developed by Netscape and is currently at version 3 (Claessens et al., 2002).

In communications theory, the presentation layer that does the message formatting sits above the transport layer that lays a logical "pipe" between two machines. SSL is a presentation layer protocol so it will encrypt any data leaving an application before it is sent down the pipe and decrypt any data arriving at an application. In the Transmission Control Protocol (TCP) the pipe is a socket between two client/server applications e.g. web browser and web server. SSL comprises three main parts: public key cryptography, symmetric key cryptography and digital certificates.

2.1 Symmetric Key Cryptography (SKC)

Symmetric key encryption is also called session key encryption. It is where both parties have the same single key for encryption/decryption. The main advantage of single key encryption is that it is fast and relatively efficient. Its vulnerability is that the once an eavesdropper has attained the key, it allows the deciphering of the messages going in both directions.

2.2 Public Key Cryptography (PKC)

PKC is a technology where there are two sets of keys (Lancaster et al., 2003; Kinsella, 2002). One key is publicly available and the other set held privately by an individual. These keys are linked in such a way that encryption with one of the keys

can *only* be decrypted by the other key. This methodology is an improvement over SKC as it requires the "cracker" to determine two unknowns.

PKC and SKC assume that the other party with whom you are having a secure transaction (e.g. a Bank) is who they claim they are. In other words, either scheme does not guarantee that a single key or key pair cannot be used fraudulently. It boils down to an element of trust.

2.3 Digital Certificates

A scheme that distributes public keys and provides key management is called a Public Key Infrastructure (PKI). The most common PKI in use today employs digital certificates. A digital certificate is a trusted binding of a public key to an identity. A Certificate Authority (CA) is a commercial organisation that issues these certificates. A digital certificate from a CA is a data structure that encases the public key and contains fields that indicate the CA, a certificate serial number, the PKC encryption algorithm used and the certificate expiry date. For commercial and other reasons, the CA retains the right to revoke certificates.

In this scheme, a valid digital certificate must be loaded into an application that can read certificates so that we can assert our authenticated identity when we digitally sign our data stream. Since the expiry date is built into the certificate, the application can issue warnings that the certificate is out of date and is therefore invalid.

2.3.1 Certificate Authorities

The CA charter is to create trust in relation to the issuance of digital certificates. The level of trust is directly proportional to the market perception of the CA. The most frequently recognised CA is Verisign. Others include Entrust, Baltimore and Certicom (Guel, 2002). A more comprehensive list can be obtained from your web browser e.g. with Microsoft's Internet Explorer through the Content - Certificates tab of Internet options.

The digital certificates are from a trusted authority (CA) but a breakdown of the system occurs when the CA is duped. For example, Verisign has been duped into

issuing fraudulent certificates. The duper "... signed on as a Microsoft employee ... and provided enough correlatable information" (Palmer, 2001, p.1).

2.3.2 SSL and Digital Certificates

SSL is based principally on symmetric key encryption for high efficiency. The symmetric key must be agreed by both the client and the server. This scheme implies that a secure method of exchange for the symmetric key must be used otherwise it will be a trivial exercise for an eavesdropper to obtain the key. PKC is used for the symmetric key exchange and digital certificates are used to authenticate the public keys.

When a connection is initially made from the client to the server through SSL, a request is made for a digital certificate to be passed from the server to the client. The request and the certificate pass unencrypted over the link. The client extracts the server's public key from the digital certificate. The client then generates a private key which it encrypts using the server's public key so that it can be transmitted to the server. The server receives the encrypted key and decrypts it to get the symmetric key. This scheme means that both the client and server have the same symmetric key so SKC can proceed. Note that the use of encryption in the private key exchange scheme ensures that the symmetric key is not easily able to be determined by eavesdroppers. Negotiations for which symmetric key encryption cipher will be used during this session occur in the initial SSL "handshaking" between the client and the server (Shoriak, 2000; Claessens et al., 2002).

2.4 Common Ciphers

The most commonly encountered public key cipher in eCommerce (Batina et al., 2003) is the RSA (Rivest-Shamir-Alderman) cipher. The problem with RSA is that the increasing key sizes cause increasing computational overhead that then leads to lower performance. The overhead comes from the time consuming number crunching that is based on very large primes.

DES (Data Encryption Standard) is a symmetric key encryption cipher that has been used in many financial institutions in the past (Shepherd, 1995). It is one of the

SSL ciphers. DES is "crackable" (Biham, 2002) in a finite number (268,435,456) of steps.

Triple DES is a three key version of DES, thus providing more security. It is also an SSL cipher. It has been shown (Biham, 2002) that a single 168 bit key of Triple DES is "crackable" with (19,342,813,113,834,066,795,298,816) steps. This number appears large but it is eminently achievable.

For wireless systems (not including Bluetooth), a symmetric key is used and is included in the Wired Equivalent Protocol (WEP) standard. We will discuss this in the next section.

3.0 Wireless Technologies and Security.

3.1 Wireless technologies

The two major competing wireless standards at this point in time are Wi-Fi (IEEE802.11b) and Bluetooth (IEEE802.15). The technologies of Wi-Fi and Bluetooth are pitched at different market segments (Sabat, 2002). Wi-Fi has a range of up to 150m and a high speed of up to 11Mbps (Dennis, 2002). It is suitable for intra-office wireless networking. Bluetooth has a range of only 10m with a data rate of 1Mbps (Dennis, 2002) and it is therefore only suitable for close proximity networking often called Personal Area Networking. Wi-Fi is expected to take market share (Sabat, 2002).

As mentioned earlier, wireless security is of utmost importance due to the fact that it is unguided and therefore can leak past architectural boundaries. Both Bluetooth and Wi-Fi have their own methodologies for secure communications.

Any two Bluetooth devices can connect with each other when they are within range. This scheme is insecure since it is possible to interface with any Bluetooth device and collect packets. The risk can be lessened due to Bluetooth's short transmission range. This problem needs to be "seriously addressed ... [because] there appear to be no applications that will monitor and defend a network from Bluetooth-based attacks" (Barber, 2001, p.378).

Wi-Fi uses a technology called Wired Equivalent Privacy as its basis for security. This scheme is a symmetric key system that can be cracked by collecting enough data i.e. between 4 and 6 million packets for a 128 bit WEP key (Stubblefield et al., 2001). It should be noted that even though WEP is based on RC4 (a fast symmetric key streaming cipher) it is implemented incorrectly and this "bug" is the root cause of the insecurity. SSL which can also use RC4 is not susceptible to the WEP style of attack (Stubblefield et al., 2001) . Improvements to WEP are being discussed by Karygiannis et al (Karygiannis and Owens, 2002).

Since most wireless systems are mobile they require a cipher that is not computationally heavy and that does not lead to vulnerabilities. A cipher that is not computationally heavy but is very robust (Medium Level Security) is the chaotic cipher (Rowlands and Rowlands, 2002) which will be discussed in section 4.

3.2 Other Wireless Security Problems

According to Lancaster et al (2003), Corporate espionage, E-Commerce fraud and IP theft have spurred the development of Digital Security. An increasing threat to digital security is the unauthorised access of airspace. "Drive by Hacking" (Hinde, 2001) is where a person with a wireless device sits within range of an organisation's wireless cell, collects information and hacks "invisibly". This arrangement is an increasingly common phenomenon and is being proliferated by "Warchalking". Warchalking (Hinde, 2002) is where these sites are marked by chalk symbols placed on the pavement by previous hackers to alert the hacker community that there is an unprotected Wireless LAN entry point at this location. The solution is to tighten up security at the Wireless Access Point and possibly implementing a firewall.

4.0 Chaotic Encryption

At the heart of all ciphers is a generated sequence of numbers that when combined with a message results in a stream of characters that appears unintelligible to the casual observer. There are a number of such ciphers available. The theory of chaos provides the basis of a good cipher since chaotic time-series are extraordinarily unpredictable. Baptista (1998) was the first to suggest using the logistic map (a

specific type of chaos) as a symmetric key encryption scheme. Other efforts followed that analysed and extended the cipher (Jakimoski and Kocarev, 2001; Kocarev and Jakimoski, 2001; Schmitz, 2001; Yang et al., 1998; Rowlands and Rowlands, 2002, 2003).

In order to understand how chaos is useful to cryptography, we need a gentle introduction to the basics of chaos theory.

4.1 Deterministic Chaos

A system is visibly chaotic to an observer if it appears to act in a very unpredictable manner. A deterministic chaotic system is where there are simple laws governing the system but it still appears to behave unpredictably. A chaotic time-series is shown in Figure 1 and demonstrates the unpredictable nature of the generated sequence. The chaotic function (deterministic system) used to create this sequence is the logistic map. It is called a map since each point predicts the next point i.e. it is an iterative function.

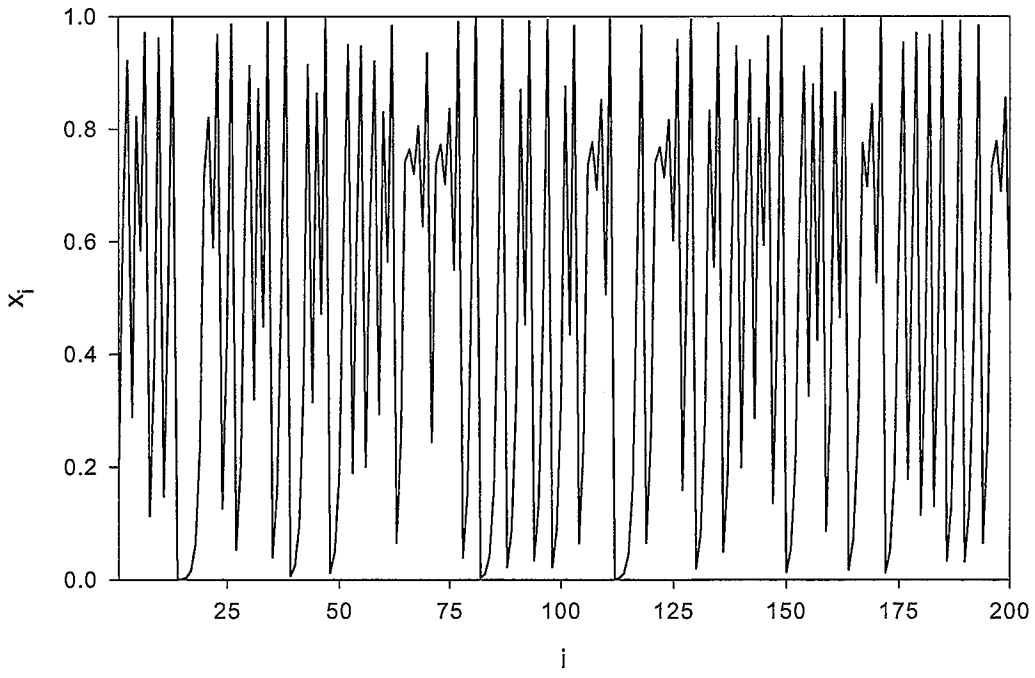

FIGURE 1: A CHAOTIC MAP TIME-SERIES

There are two main requirements for a system to behave chaotically (Banks et al., 1992). These characteristics are the sensitivity to the initial conditions and the density of states.

4.1.1 Sensitivity to Initial Conditions.

The sensitivity to initial conditions can be determined by feeding an initial value (seed) into the system and then allowing the system to evolve for a number of iterations. The resultant sequence is then compared to other sequences with a slightly altered seed from the original that has also been allowed to evolve. The difference between the new sequences and the original will indicate the sensitivity.

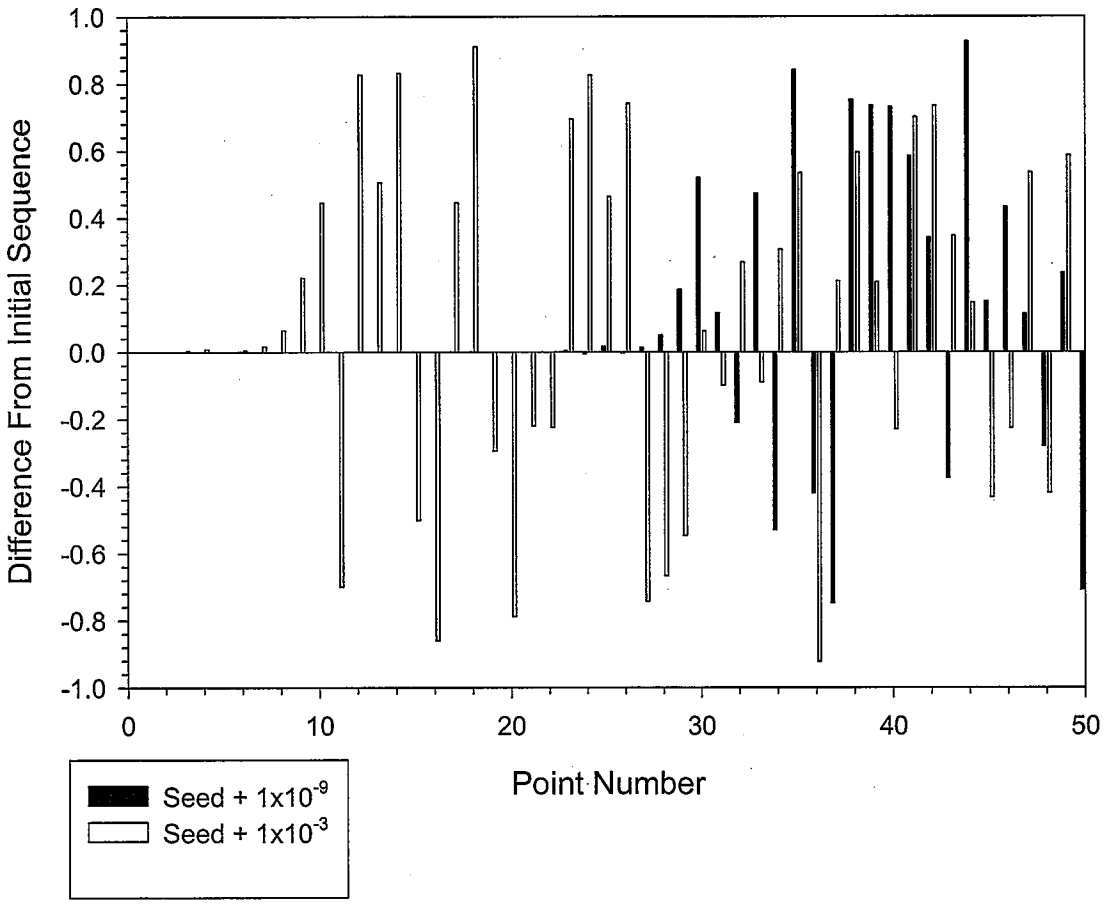

FIGURE 2: SENSITIVITY TO INITIAL CONDITIONS (ROWLANDS AND ROWLANDS, 2002)

Figure 2 shows a chaotic system (logistic map) that was given three initial values. The first value we will call the original seed. The other initial values (adjusted seeds) are related to the original seed by tiny offsets. The adjusted seeds were adjusted by an offset of 1 thousandth from the original seed and 1 billionth from the original seed. The three sequences were generated and the normalised difference between the adjusted seed sequences and the original seed sequence were plotted. This plot clearly demonstrates the sensitivity to initial conditions of the system.

4.1.2 Density of States.

The density of states is an indicator of the utilisation of the possible points within a given range. The greater the density of states the less predictable the sequence is going to be.

Assume that a system is chaotic and varies over the range 0 to 1. That is, its minimum value is 0 and its maximum value is 1. Dense states imply that every point on this interval is used ignoring the limited set of fixed point gaps (Rowlands and Rowlands, 2003; Scarf, 1967; Chow et al., 1978; Devaney, 1989; Sprott, 2000). This aspect can be also be viewed from another equivalent perspective. Choose at random two very small but separate regions within the interval [0,1]. Pick a point from one of those regions and use it as a seed. Evolve the system and eventually it will end up on a point in the second region. This property is called topological transitivity (Devaney, 1989) and is equivalent to dense points (Banks et al., 1992).

4.2 Vulnerabilities in Logistic Map Chaotic Encryption

As mentioned earlier in the paper, the logistic map is an excellent candidate for chaotic encryption. This section covers the concept of the logistic map and indicates some of the possible vulnerabilities in the logistic map method of encryption.

Figure 1 and Figure 2 are both based on a time-series chaotic sequence calculated from the logistic map. It is well known (Devaney, 1989; Cogswell, 2002; Bolt, 2002; Mingarelli, 2003; Hilborn, 1994; Frame, 2002; Elert, 2003; Davies, 2002; Cvitanovic, 2002; Sprott, 2000) that the logistic map obeys all the criteria required for a chaotic system. The logistic map is a specific iterative quadratic equation that is multiplied by

a constant parameter α and has as its initial value x_0. There is only a small range of values for which the control parameter α will result in a chaotic system. The particular numerical sequence within this chaotic system is selected by the seed x_0.

5.0 Logistic Map Chaotic Encryption

In order to reverse engineer (hack) a chaotic sequence you would need to know which chaotic map is being used and also the values of the two state variables (α, x_0). Therefore there are three unknowns that the hacker has to determine. This characteristic makes it very hard to crack the scheme since a slight error in guessing the initial seed leads to a totally incorrect sequence being generated due to the sensitivity to the original seed as shown in figure 2.

The type of chaotic map used and the value of the control parameter α can be calculated (with a lot of data) by using return maps. A return map recovers the shape of the chaotic function but gives no clue as to the seed (starting point). Figure 3 shows the return map of the logistic map.

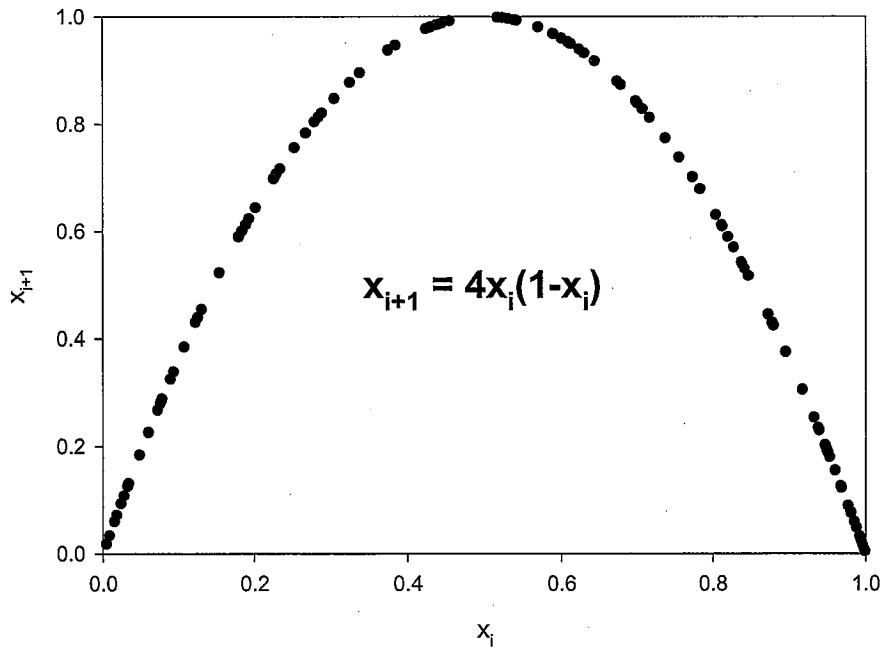

FIGURE 3: THE LOGISTIC RETURN MAP

The quadratic nature of the return map shown would indicate to a knowledgeable hacker that it is likely to be the logistic map. By applying a polynomial regression to the return map a value for the control parameter (α) can be determined which in the case of figure 3 would be $\alpha = 4$.

Unfortunately, this ability now removes two of the three unknowns. If enough of the ciphered message stream is collected then it becomes possible via brute force methods to obtain the initial seed (Jakimoski and Kocarev, 2001).

5.1 Improvements to Logistic Map Chaotic Encryption

A solution to the problems plaguing earlier attempts at logistic map chaotic ciphers has been previously published (Rowlands and Rowlands, 2002, 2003). The heart of the problem with previous logistic map ciphers is that the collection of long data streams can allow hackers to determine the state variables and therefore decode the encrypted messages. The solution is to have many short sequences rather than one long sequence.

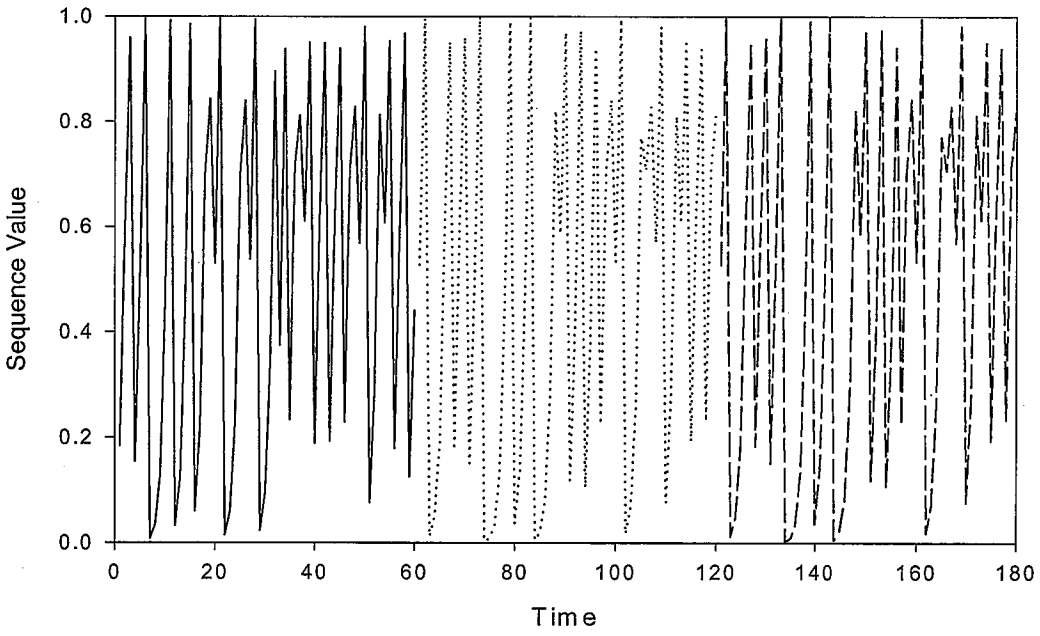

FIGURE 4: A MORE ROBUST METHODOLOGY

This task is done by generating a sequence starting with an initial seed for a small number of iterations (the "run length") and then create a new seed by an adjustment to the initial seed. The new seed will create a new subsequence that is also only run for the run length and so the process continues. Figure 4 shows this method graphically.

In figure 4, the run length is 60 iterations before the seed is adjusted by a small constant. Each subsequence is represented by a different line style. As can be seen the total sequence is still chaotic but is clearly made up of smaller chaotic sub-sequences.

Since it is easy to determine the type of chaotic map used, then it can be assumed that the hacker knows the type of map and hence the value of the control parameter. Here we have set the parameter to $\alpha = 4$ to guarantee chaos as well as for simplicity and speed of computation. Thus the set of unknowns are the initial seed, the run length, and the algorithm used for seed adjustment including its associated constants.

It is known that any chaotic sequences take a certain number of iterations before the sequence settles down into a chaotic state (Rowlands and Rowlands, 2002, 2003; Hilborn, 1994). This settling period needs to be specified beforehand and is also an unknown. Thus we now have 4 unknowns (more if the seed adjustment method involves multiple constants). The increase in the number of unknowns increases significantly the security of the encryption method. It also implies a symmetric key in that both the client and server need to know these parameters to encode/decode the message.

5.2 Possible Applications of the Improved Logistic Map Chaotic Cipher

The work by previous authors has focused primarily on the encryption algorithm and its resilience. We have addressed these problems (Rowlands and Rowlands, 2002, 2003) and now propose that the improved chaotic logistic map cipher will rectify the weaknesses of WEP due to its low computational cost and encryption strength. We are currently working on the verification of the schemes strengths and weaknesses through the incorporation our chaotic routine within WEP.

Since SSL is fundamentally based on a choice of using different symmetric key encryption ciphers, our improved logistic map cipher will provide an excellent

addition to the armoury, especially since DES and Triple DES have deciphering problems.

5.3 Logistic Map Encryption for less powerful mobile devices.

Ubiquitous computing requires the two features of mobility and portability. A good example of this requirement is the pervasiveness of PDAs and laptops. However the trend extends a lot further than just mobile computing. The use of small purpose-built computing systems is becoming more prevalent. Typically these devices are based around an embedded system (Hennesey and Patterson, 2003). An embedded system typically consists of a low-power (for long battery life), low-speed microprocessor/microcontroller typically between 10MHz to 40MHz, a small amount of memory typically a few bytes to kilobytes in size, a dedicated purpose-written real-time operating system, and some control circuitry. The advantage of these systems is that they are tailor made for the application as opposed to a typical PC type system that is very general in nature and thus can be more powerful than required. The other major advantage of these systems is that the computing hardware is very much cheaper than a PC system. For example the bottom end "PIC" microcontroller (Microchip Corp., 2003; RS-components, 2003) is typically in the order of tens of dollars and the Pentium (Intel, 2003) series is typically of the order of hundreds of dollars. Hence an embedded system is cost effective and this drives the diffusion of the technology into many different types of business. For example, restaurants can use embedded systems in small mobile ordering terminals.

Although there are many applications for embedded systems, it should be noted that there are limitations when using them. The microcontroller speed and the memory size are important considerations that must be taken into account in the software written for these systems. The number of calculations performed and the type of calculations must be taken into account. As it takes a finite amount of time to perform a calculation, then more calculations performed will slow the program. Also the type of calculation is important since the microcontroller is integer-based and performs all its operations as integers. This characteristic means that if floating point

(real) numbers are used then special software routines to perform the basic arithmetic must be used. These software routines cost calculation speed due to the calculation overheads and the result is a slowing down of the program. If these overheads become too large they may negate the benefits of using these floating point routines.

Many encryption methods rely upon integer operations to increase the speed of calculation so that they can be used efficiently. However some of these are quite calculation intensive and therefore are not suitable for microcontroller operation. It has been shown earlier that the chaotic encryption is a medium level encryption method that is not calculation intensive. However, the chaotic encryption schemes presented earlier are based upon floating point numbers. The necessary floating point routines will thus incur overheads on any embedded system. There is therefore a need for an integer-based chaotic encryption that takes into account the limitations of microcontroller systems. This requirement can be achieved by generating a chaotic sequence from the logistic map, converting the sequence to integer values and loading them into a limited sized lookup table. The table can appear to be longer than its actual size through the use of multiple entry points. For example, one entry point into the table will generate a list that is as long as the table itself before repetition occurs. Two entry points into the table allow the generation of a list that has a length given by the square of the table size. In future work we will determine the optimum size for the table and the optimal number of entry points.

6.0 Discussion & Conclusion

Data security is a matter of care, trust and technology. With wireless technologies, there are more constraints than with the conventional cabled network solution. The devices are smaller, slower and the bandwidth is not high. This situation means that any overheads are going to affect data throughput rates and efficiency. Thus, a strong encryption that caters for the decreased resources available is essential to allow m-commerce to gain the confidence of consumers.

The improved logistic map chaotic encryption scheme is an ideal resolution to these constraints. It is also perfect as a symmetric key cipher within the common SSL

scheme. An integer version has been developed that is eminently suitable to the extremely limited resources of an embedded microprocessor. Embedded microprocessors appear in all small intelligent devices from the PDA and mobile phone to smart household appliances so finding robust efficient encryption algorithms for these devices is becoming increasingly important.

The improved logistic map encryption scheme is not just applicable to transmission encryption. Due to its speed it is also suitable for disk and file system encryption.

Further work would be the inclusion of the logistic map chaotic cipher within an SSL implementation and then gather statistics demonstrating the magnitude of the speed increase over the other symmetric ciphers e.g. RC4. These statistics would also indicate the performance increase over WEP since WEP is based on a faulty implementation of RC4. Further work will also include investigating the applicability of other chaotic maps as a cipher.

References

Banks, J., Brooks, J., Cairns, G., Davis, G. and Stacey, P. (1992) *American Mathematical Society,* **99,** 332-334.

Baptista, M. S. (1998) *Physics Letters A,* **240,** 50-54.

Barber, R. (2001) *Computers & Security,* **20,** 374-379.

Barnes, S. J. (2002) *International Journal of Information Management,* **22,** 91-108

Batina, L., Berna Ors, S., Preneel, B. and Vandewalle, J. (2003) *Integration, the VLSI Journal,* **34,** 1-64.

Biham, E. (2002) *Information Processing Letters,* **84,** 117-124.

Bolt, E., What is Chaos anyway?, http://mathweb.mathsci.usna.edu/faculty/bolltem/AboutChaos/DefiningChaos/DefiningChaos.html

Chow, S.-N., Mallet-Paret, J. and Yorke, J. A. (1978) *American Mathematical Society,* **32,** 887-899.

Claessens, J., Dem, V., De Cock, D., Preneel, B. and Vandewalle, J. (2002) *Computers & Security,* **21,** 253-265.

Cogswell, K., Chaos in the Logistic map, http://learn.sdstate.edu/cogswelk/ChaosFractals/CHAPTER_6_MORE_CHAOS/htmlstuff6/CHAOS_IN_THE_LOGISTIC_MAP/CHAOS_IN_THE_LOGISTIC_MAP.htm

Crisler, K., Anneroth, M., Aftelak, A. and Pulil, P. (2003) *Computer Communications,* **26,** 11-18.

Cvitanovic, P., Classical and Quantum Chaos, http://nbi.dk/ChaosBook/

Davies, B., Lectures in Non-linear modelling and chaotic behaviour, http://www.maths.anu.edu.au/~briand/MATH2062.html

DellOro (2003) Dell'Oro Group, http://www.delloro.com/PRESS/PressRelease/2003/WiL021803.shtml.

Dennis, A. (2002) *Networking in the Internet Age,* John Wiley & Sons.

Devaney, R. L. (1989) *An Introduction to Chaotic Dynamical Systems,* Addison-Wesley, Redwood, CA.

du Preez, G. T. and Pistorius, C. W. I. (2003) *Technological Forecasting and Social Change,* **70,** 1-20.

Elert, G., The Chaos Hypertextbook, http://hypertextbook.com/chaos/42.shtml

Frame, M., Fractal geometry - Deterministic Chaos, http://classes.yale.edu/math190a/Fractals/Chaos/welcome.html

Guel, M. D. (2002) *Information Security Technical Report,* **7,** 63-78.

Hennesey, J. L. and Patterson, D. A. (2003) *Computer Architecture a quantitative approach,* Morgan-Kaufmann.

Hilborn, R. C. (1994) *Chaos and Nonlinear Dynamics,* Oxford University Press, New York.

Hinde, S. (2001) *Computers & Security,* **20,** 295-301.

Hinde, S. (2002) *Computers & Security,* **21,** 689-693.

Intel, Intel Products - Processors, http://www.intel.com/products/server/processors/index.htm?iid=ipp_home+server_proc&

Jakimoski, G. and Kocarev, L. (2001) *Physics Letters A,* **291,** 381-384.

Jones, N. (2002) In *Gartner Symposium ITxpo*Gartner, Walt Disney World, Orlando, Florida, pp. 18,

Karygiannis, T. and Owens, L. (2002) National Institute of Standards and Technology, pp. 119,
Kinsella, R. (2002) *Network Security,* **2002,** 12-13.
Kocarev, L. and Jakimoski, G. (2001) *Physics Letters A,* **289,** 199-206.
Lancaster, S., Yen, D. C. and Huang, S.-M. (2003) *Computer Standards & Interfaces,* **In Press, Corrected Proof.**
Microchip Corp., PICmicro Microcontrollers, http://www.microchip.com/1010/pline/picmicro/index.htm
Mingarelli, A. B., The Logistic Equation and its associated map, http://mathstat.math.carleton.ca/~amingare/chaosday/node1.html
Mohr, W. (2003) *Computer Communications,* **26,** 2-10.
Palmer, C. (2001) *Network Security,* **2001,** 1-2.
Rowlands, T. and Rowlands, D. (2002) In *International Conference On Information Technology & Applications (ICITA)*, Vol. TBA (Ed, Tien D.) Bathurst,
Rowlands, T. and Rowlands, D. (2003) In *5th Operations Research Conference on Operations Research into the 21st Century*Noosaville, Australia,
RS-components, PIC12C/CE5XX Microcontroller Prices, http://au.rs-c.dk/servlet/dk.stibo.module.ShowModuleServlet?moduleId=5176266
Sabat, H. K. (2002) *Telecommunications Policy,* **26,** 505-535.
Scarf, H. (1967) *SIAM Journal on Applied Mathematics,* **15,** 1328-1343.
Schmitz, R. (2001) *Journal of the Franklin Institute,* **338,** 429-441.
Shepherd, S. J. (1995) *Computers & Security,* **14,** 349-357.
Shoriak, T. G. (2000) *Computers & Security,* **19,** 100-104.
Sprott, J. C., Chaos And Time-Series Analysis Lectures, http://sprott.physics.wisc.edu/phys505/
Stubblefield, A., Ioannidis, J. and Rubin, A. D. (2001) AT&T Labs Technical Report TD-4ZCPZZ Revison 2,
Tsalgatidou, A. and Pitoura, E. (2001) *Computer Networks,* **37,** 221-236.
Yang, T., Yang, L.-B. and Yang, C.-M. (1998) *Physics Letters A,* **245,** 495-510.