University of Otago
Te Whare Wananga o Otago
Dunedin, New Zealand

Electronic Security

H B Wolfe

The Information Science Discussion Paper Series

Number 98/02
March 1998
ISSN 1177-455X

University of Otago

Department of Information Science

The Department of Information Science is one of six departments that make up the Division of Commerce at the University of Otago. The department offers courses of study leading to a major in Information Science within the BCom, BA and BSc degrees. In addition to undergraduate teaching, the department is also strongly involved in postgraduate research programmes leading to MCom, MA, MSc and PhD degrees. Research projects in software engineering and software development, information engineering and database, software metrics, knowledge-based systems, natural language processing, spatial information systems, and information systems security are particularly well supported.

Correspondence

This paper represents work to date and may not necessarily form the basis for the authors' final conclusions relating to this topic. It is likely, however, that the paper will appear in some form in a journal or in conference proceedings in the near future. The authors would be pleased to receive correspondence in connection with any of the issues raised in this paper, or for subsequent publication details. Please write directly to the authors at the address provided below. (Details of final journal/conference publication venues for these papers are also provided on the Department's publications web pages: `http://divcom.otago.ac.nz:800/COM/INFOSCI/Publctns/home.htm`). Any other correspondence concerning the Series should be sent to the DPS Coordinator.

Department of Information Science
University of Otago
P O Box 56
Dunedin
NEW ZEALAND
Fax: +64 3 479 8311
email: dps@infoscience.otago.ac.nz
www: `http://divcom.otago.ac.nz:800/com/infosci/`

Electronic Security

by Dr. H.B. Wolfe

Introduction:

Electronic security in this day and age covers a wide variety of techniques. One of the most important areas that must be addressed is that of commerce on the Internet. The Internet is an insecure medium to say the least. Every message sent must pass through many computers that are most likely controlled by unrelated and untrusted organizations before it ultimately reaches the final destination. At any one of these relays the information within the message can be scrutinized, analyzed and/or copied for later reference. There are documented and suspected instances of surveillance of Internet traffic. It has been suggested that several of the major communication switches (through which 90% or more of Internet traffic must pass) have permanent surveillance in place.

Another insidious but less obvious fact about Internet use is that messages once sent, are not discarded nor do they disappear forever. Usually, at one or more relays, copies of messages are archived and kept for differing time periods. Most ordinary users are not aware that messages sent six months ago may be able to be retrieved. That fact could have serious legal ramifications for the sender.

At this time cryptography is really the only effective method that can be used to protect Internet transactions and communications from unauthorized interception. Unauthorized means **anyone** who you have not expressly given permission to read your private communications. Cryptography is the art or science of hidden writing. Plain text (your message in readable form) is modified using an algorithm (like a mathematical equation) that requires at least one special variable (your special private key that no one else knows) to create ciphered text (your message in unreadable form). At the destination the person who the message is meant for must have the "special key" in order to be able to unlock the ciphered message.

All encryption is not created equal nor does it necessarily provide equivalent security. It would be wrong to intimate that merely using "encryption" to protect your communication is enough. There are other factors at work here as well and they have to do with the politics of privacy. I have often heard it said in New Zealand that "if you have nothing to hide then it shouldn't matter who reads your communications". Of course, that opinion is naïve and does not represent reality in any meaningful way.

A Short Primer in Cryptography:

For the average user, cryptographic products come in two flavors: *Symmetric* (meaning that you use the same key to encrypt as you use to decrypt) and *Asymmetric* also know as "public" key (meaning that you have two keys - one for encrypting and a different related key for decrypting).

Symmetric systems are the older of the two and vendors often use the key size (in bits - an example: the Data Encryption Standard - DES uses 56 bit keys) to describe the strength of the algorithm. This is but one dimension that describes that strength and should not be misinterpreted to be the only attribute that measures its security. The Data Encryption Standard (commonly used in the banking industry) when it was adopted as the US standard in the mid-1970's was thought to be extremely secure. Its defeat is described a bit later in the paper.

Asymmetric systems provide the very important advantage of not requiring the secure exchange of keys in order to communicate securely. Each user's "public" key can be kept by a trusted third party that certifies its authenticity or exchanged much more easily than the symmetric system. The RSA public key crypto-system was introduced in 1978 (created by Ron **R**ivest, Adi **S**hamir & Ken **A**dleman). At the time it was thought that it would take "40 quadrillion years to factor" - this system's security is based on the difficulty associated with factoring large prime numbers. The creators issued a challenge in 1977 to defeat a key pair consisting of a 129-digit number. On the 27th of April 1994, after 100 quadrillion calculations coordinated using the CPU's of some 600 participants, the RSA-129 was defeated.

The important lesson to be learned from the material described above is that there is really no 100% solution. With larger keys, either system can approach a level of computational security that would be acceptable in today's business community. However, these two examples have addressed brute force attacks only (brute force attacks try every possible key or attempt to factor every combination of prime numbers within the key range). The field of cryptanalysis is prolific and there are other attack strategies that can be successful with various encryption algorithms (some examples: linear cryptanalysis, differential cryptanalysis, plain text attacks, and differential fault analysis). To use this tool effectively, the user needs to consult an expert or spend the time necessary to achieve a reasonable depth of understanding of the discipline. *Note: "strong" cryptography refers to the way encrypted messages are attacked. An algorithm is said to be "strong" if using all of the computing power in the world to attack it would not produce a decrypted result within a time frame to make that result useful.*

Cryptographic Products:

There are a number of cryptographic products available in New Zealand, however, cryptographic products created in the US cannot legally be exported unless they have in some way been significantly weakened in their level of security. Coincidentally, we have a community of interest here in New Zealand and there are several products that have been created here. There is a firm in Christchurch that produces hardware cryptographic devices (SignalGuard by CES). This system is useful for secure communications between branches of organizations and does not require any computing resources (for the encryption/decryption process) for its use. Two crypto systems have been developed independently in Auckland. The first by Peter Smith and is called LUC and is a public key system. The second is produced by William Raike and is called RPK and is also a public key system. Internationally, the most commonly used crypto system used in the world is called PGP (Pretty Good Privacy – a public key system) and was initially produced by Phil Zimmermann, however, there have been several others who have assisted with this project and Peter Gutmann of Auckland has been involved in this effort. PGP can easily be obtained from the Internet (free) as long as you don't try to download it from the US.

There are a couple of products from Finland that hold a great deal of promise due to their very user friendly interface and the choice offered to users of a range of strong encryption algorithms. The first is TeamWare Crypto (a symmetric key system) and that's available from Fujitzu (NZ). The second is F-Secure Desktop produced by DataFellows. These products are a sample of what can be acquired here easily and at a reasonable expense; however, the list should not be misconstrued as complete nor as an endorsement of any product. Each, however, can provide strong encryption to users.

Internet Protocols:

The discussion of cryptography thus far presupposes that the user will control their use of such products. For most users this is yet another activity that can go wrong and/or impede their activities and further complicates their use of the tool. Resistance is bound to occur. Virtual Private Networks (VPN) have been designed and created to give control of the cryptographic function to the VPN owner and provide a secure environment within an organization for communications - some using public networks. The network administrator gets to choose the specific crypto algorithm to be implemented. In so far as the user is concerned, they operate as usual without any need to be concerned with cryptography. These systems are private as indicated and as such do not solve the problem of communication outside of the VPN.

There are, however, a number of protocols for communicating over the Internet that offer various levels of cryptographic security. For the most part these are designed to provide for secure transactions so that business can be transacted safely. Some of the more common examples are Secure Multipurpose Internet Mail Extensions (**S/MIME**), Secure HyperText Markup Language (**S-HTTP**), Secure Sockets Layer (**SSL**), Secure Electronic Transactions (**SET**), Point to Point Tunneling Protocol (**PPTP**), and there several others.

It is important to note that of the five protocols listed, three have been successfully attacked either because their cryptographic algorithm was weak or because the implementation of an otherwise strong algorithm was flawed (S/MIME, SSL, PPTP). One successful attack has been implemented in the form of a screen saver program that quite happily performs a brute force attack on the 40-bit RC2 keys (RC2 for Ron's Code or Rivest's Cipher is the name of the variable key-size crypto algorithm). Of course, that program is readily available from the Internet. It is also worth mentioning that even though a protocol may have been successfully attacked, that does not mean that it cannot be improved such that the flaw or weakness no longer exists.

All cryptographic products purchased from the US are intentionally hobbled as a result of US legislation which limits the strength of cryptographic products exported. Currently, it's okay for Americans to have strong encryption but it's definitely not okay for non-Americans to have strong encryption. The rationale for taking this position is the topic of heated debate around the world. However, the fact remains that we cannot buy strong encryption products from the US and therefore should look elsewhere for products that do offer that kind of protection.

Cell Phones:

Another important method of communication is the use of cell phones. When writing last year's paper, I included the following excerpt about cell phone technology:

> Over the course of the past several years new products have emerged amongst fanfares touting their absolute security. One such product is the digital cell phone. Claims surrounding it were, and continue to be, that the scanners used in the past to monitor analog cell phone conversations would not be able to decode the new technological wonder. It is a fact that signal content is very different and that the old scanner technology will not translate intercepted conversations. Additionally, they claimed that no one would be able to decrypt the "smart cards" that are the principle piece of the technology used to actually encode and decode transmissions within the cell system (cell phones are nothing more than radio transmitters and receivers). The current state of this

technology is very different from the claims made, however, and as recently as 20 March 1997, these algorithms have been decrypted and it is thought that producing a digital scanner capable of interception and translation would now be a trivial electronic exercise. As a result, secure communications via digital cell phone can no longer be assured. One should never consider a cell phone of any type to be a secure medium of communication ("loose lips sink ships").

Computers have played a huge role in the privacy arena. They are used day by day, minute by minute to infringe our privacy. Recently, a friend in the US, with the cooperation of a local news caster, attempted to obtain as much information about the newsman as was reasonably possible from the various databases, both public and private, which track people. He used a private investigator and a computer type (hacker) in parallel. The result after expending less than $1,000 was seventeen pounds of documents containing information about the subject with regard to his medical history, financial activity including a history of all banking and credit card transactions, history of his telephone activity, arrest records, motor vehicle records, use and location history for his cell phone, and many other things as well. The exercise served to prove that information about anyone can be obtained for a price and that a significant part of that information is sensitive and potentially damaging to the individual. Safeguards offered in legislation cannot cope with the greed which surrounds the profitable provision of these "services" much of which comes from someone on the "inside".

One of the interesting issues raised was the fact that organizations who provide cell phone services record the history of the location of every cell phone that is active within a cell. In other words, if you have a cell phone and it is turned on, your every movement is not only being tracked at regular intervals but those movements are being recorded and a history of those movements can be made available to whoever is willing to pay for that information as well as to law enforcement. Some basic questions need to be asked: Why is this information recorded? Who has access to the information and for what purpose? Under what conditions do they have that access? Finally, does this happen in New Zealand and if so, what safeguards are in place to protect the privacy of our movements?

Please notice that no where in the preceding material have I accused anyone or any organization within New Zealand of selling cell phone location history. Also you will note that I have not specifically mentioned GSM or DAMPS or any other specific scheme of digital

service. I didn't have an axe to grind then nor do I at this time. *I believe that digital cell phones are an innovative, reliable and convenient form of communication that contributes to business efficiencies, personal safety and general improved quality of life for those who use them.* My comments were and continue to be focused on security and privacy issues only.

However, the week after *Privacy Forum '97*, I received a letter from an unnamed organization accusing me of making "serious allegations about the way New Zealand cell phone operators conduct their business and about the security of their systems". I had **spoken for less than two minutes about the topic** during my entire presentation and what you have read above is all that I had written. The letter was a bit aggressive, intimidating and designed to put me on the defensive making me feel that if I did not comply with their demands (for a public retraction) that there would be legal repercussions. You tend to pay attention when an organization with multi-billion dollars in assets takes a shot at you.

It could reasonably be argued that the phrase:

> "those movements are being recorded and a history of those movements can be made available to whoever is willing to pay for that information as well as to law enforcement."

gives the reader the impression that this material is for sale to anyone willing to pay for it. That assumption is incorrect and it was not the intention of the writer to infer that the information was freely available for sale here in New Zealand. While that statement may have lacked clarity, I have made no allegations whatsoever about any New Zealand organization or business selling cell phone tracking data. All of the information above and in the presentation were and continue to be supportable facts.

Since that time, however, there have been some developments in the field of cell phone technology. The GSM system, which has claimed in the past to be totally secure and impossible to breach, has had a few interesting developments. In the first instance the Subscriber Identification Module (SIM) - a small smart card, which holds the identity of the cell phone, has been breached. This was accomplished by the Smartcard Developer Association and two Berkeley researchers (13 April 1998). One of the primary advantages for the digital service is that the phone cannot be cloned by virtue of the use of this smart card. Cloned phones can be used illegally to sell international calls.

On the surface that doesn't appear to damage the security of GSM in any meaningful way and it probably doesn't, however, the research process required to accomplish the breach made it possible to discover the nature of the encryption algorithms used to encrypt communications over the GSM System. The folks at GSM had made use of the common approach to security

called *security by obscurity*. While this approach may have merits in some specialized circumstances, those who use it are usually disadvantaged at some point as a result. **Note: Security by obscurity means keeping all aspects of security secret. At first blush this sounds like a good idea, however, this technique precludes any peer assessment that might identify weakness in the approach taken or devices and procedures used. Where weaknesses do exist they are usually identified by successful attack as opposed to reasoned assessment.**

The interesting fact that has emerged as a result of investigating the algorithms used is that the sixty-four (64) bit algorithm used by GSM has been deliberately and substantially weakened - a thousand fold. This is accomplished by **presetting ten (10) of the sixty-four bits to zero**. The question has to be asked: Why would anyone do that? It serves no purpose other than to make GSM based communications more vulnerable to successful cryptanalytic attacks.

In the past it has been argued that a brute force attack on the Data Encryption Standard would take as much as 2,300 years to decrypt and that a sixty-four bit algorithm would take as much as 584,542 years (*GSM Security and Encryption* by David Margrave, George Mason University - 1994). In the example, one would be encouraged to conclude that the sixty-four-bit GSM algorithm is not breakable - in our lifetime.

The DES was publicly defeated in 1997 for the first time using 78,000 computers working in concert for 96 days. It was defeated in 1998 for the second time using 52,000 computers working in concert for 39 days. On the 17th of July 1998 a **single**, purpose built, machine (known as *DES Crack*) working for fifty-six **(56) HOURS** defeated the DES for the third time. Using the *DES Crack* machine (assuming that it could be used for this purpose) the GSM effective fifty-four (54) bit algorithm would take less than one-fourth the time or sixteen (16) hours. The *DES Crack* machine was not especially designed for speed and only runs at 40 MHz. That could probably be increased ten fold without serious modification. Without any other modification to enhance its power that puts GSM decryption at about an hour and a half. *DES Crack* is the first publicized attempt at building such a machine and has a good deal of room for improved efficiencies - and these will undoubtedly be made.

The notion that one system or another is unassailable is a fiction and judging by the facts of history unsupportable. It is not a question of **whether it can** be done but rather of **when it will** be done. In GSM's own documentation (*UMTS- Security Objectives*, Version 3.0.0, 1st October 1997), and I quote "Lawful **interception of telecommunications transactions shall be supported** in accordance with national regulations". The facility for the surveillance of private digital cell phone communications is already built into the system. Moreover, there are GSM intercept devices currently being marketed. For example the **GSTA-1400** manufactured by G-COM Technologies Ltd. claims that the "system can randomly screen GSM Mobile

communication, with the ability to monitor and record traffic" and that "conversations can be monitored and logged simultaneously to a high capacity digital voice and data logger for storage and retrieval".
The FBI has asked Congress to explore possible changes in existing law to allow law enforcement access to physical location data of cell phone users, without court order, under certain "emergency" conditions. Mandated 911 requirements are leading toward the ability of cell phone carriers to track, and potentially record, the movements of all powered-on cell phones, regardless of whether or not calls are in progress. It is inevitable that this data will be desired by various parties for other purposes, in realtime and perhaps retrospectively as well, in criminal, civil, and perhaps even commercial contexts. The US model is likely to be followed here in New Zealand as well.

It is neither prudent nor reasonable to conclude that **ONLY** law enforcement has access to digital intercept equipment. Therefore, and with these facts in mind, I repeat my previous admonishment: One should never consider a cell phone of any type to be a secure medium of communication ("loose lips sink ships").