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

Privacy Enhancing Technology

Henry B. Wolfe

The Information Science
Discussion Paper Series

Number 97/09
July 1997
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/`

Privacy Enhancing Technology

by Dr. H.B. Wolfe

Introduction: Privacy is one of the most fundamental of human rights. It is not a privilege granted by some authority or state. It is, in fact, necessary for each human being's normal development and survival [Bok]. Those nations who have, in the past, and currently follow the notion that they have the authority and/or moral high ground to grant or deny privacy to their citizens are notable for their other human rights violations. This paper is centered around the above premise and will offer the reader some good news and some bad news. But most important, it will put the reader on notice that our privacy is constantly under attack from one vested interest or another and that each and every one of us must be vigilant in the protection of our private matters.

It is common in New Zealand to assume that anything secret is bad. This is an extremely naive position to take for any intelligent individual. The old phrase "if you haven't got anything to hide, then you shouldn't mind....." is often used to intimidate, manipulate or coerce an individual to "confess" or share information that he/she initially believes to be confidential, private or otherwise not for sharing with others. Secrecy is not bad nor good in and of itself. It is merely a factual description of the condition of some information.

Now for some good news. There are a number of technological devices and procedures that can be used to enhance one's privacy. The bad news is that most, if not all, can be easily defeated with other technological advances.

Privacy Enhancing 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?

Computers are an important part of society today and many people use them as routinely as phones were used in the past. The computer is, after all, just another tool. The Industrial Age brought us the opportunity to significantly expand our abilities to produce. Those things formerly produced by hand are now produced, in quantity, by machine. This net effect can be equated to an extension and enhancement of our body's physical capabilities to be able to manipulate more, faster and with greater precision.

The Computer Age has brought with it the ability to extend and expand our information storage and manipulative capacity. This can be equated to an extension of our individual intellect, memory and evaluation processes – our mind. What you think, can be kept private by not exposing it to anyone – controlled by the individual. What you type into your computer, however, cannot be kept private in the same way. Moreover, a Court of Law does not view information stored on a computer to be private and can and will explore, assess and evaluate information found there. Very few people consider that the information which they store on their computer is public and can be demanded by a Court of Law or confiscated and obtained by Law Enforcement – without your cooperation or permission.

Private conversations between two individuals over the Internet are not and should not be considered private either. These are routinely monitored by NSA (the American National Security Agency) at the fifteen, or so, key switches through which the vast majority of Internet traffic passes. These folks are monitoring conversations (by computer) for key words that fit their particular agenda and they act upon information gathered via this method. The issue here is not about guilt or innocence but about privacy. One cannot and should not expect that private conversations carried out over the Internet will remain private under any normal conditions.

There are many emerging surveillance techniques that further invade our privacy. Video surveillance is a good example. Currently, a video surveillance camera can be purchased for less than $200. That price brings the technique to just about anyone who wants to use it. Moreover, the size and capabilities of these cameras are such that it is all but impossible to detect them. These cameras are now beginning to show up in public places monitoring the activities of everyone who enters the surveillance area. Each of us are being photographed without our permission and usually without our knowledge. Justification of these measures usually make use of one of the principle techniques of propaganda: Special Appeals – FEAR. We are told that the cameras are in place to "protect" us.

Useful Techniques: So far most of my comments have been negative and offer little hope for privacy of any kind. However, there are some techniques that we can employ that will offer higher degrees of privacy. In the first instance; where sensitive, confidential or private information is stored on computer; we can make use of data encryption to encode that information and thus deny its usefulness to anyone other than who we choose. There are some additional utilities that can be used to ensure that private information is not inadvertently stored in a usable form (for an intruder of whatever description). In-so-far-as the Internet is concerned, we can also make use of data encryption to protect our private communications from prying eyes.

MS/DOS based personal computers (and Windows too) have some peculiar attributes and operating processes. There are three specific areas where information is stored that most users are not aware of. First, when you delete a file, the file is not removed from your storage space. It is only tagged as no longer active and that specific space is available to DOS for storing new information. If the contents of the file that was deleted was confidential then anyone who might have access to the PC can gain access to that information. Most PC's use Windows today. Windows has a work area of variable size from 4 megabytes to 20 or more megabytes. Information that Windows chooses to place there (for example passwords in plain text) will remain there until it is overwritten. Another little quirk is something called "slack space". This refers to the fact that (in MS/DOS) the smallest physical piece of data that can be read and written to disk is a cluster. Cluster sizes vary depending on the size of the specific hard disk.

If you create a document that has as little as one character the system still writes a single cluster to store that single byte. The important issue here is that the remaining space in the cluster is not cleared and will contain whatever was there before. In other words, that cluster will contain 1 character from the document just written and 3,999 to 15,999 or more characters of previously written material. Once again, someone who was able to gain access to the specific PC could easily view and/or make copies of that old information. This little known risk can be eliminated by the use of a set of utilities which is freely available on the Internet (see the *Wipe Utilities* entry in the *Internet Sites of Interest* found at the end of this paper).

For the reader that does not know what data encryption means, I will attempt to explain. Cryptography is the science of secret writing. The technique is used to encode private messages, changing them into a collection of meaningless apparently random characters that cannot easily be translated back into the original form without knowing the exact key and the exact algorithm used (an algorithm is sort of like an equation). This key and the appropriate algorithm are used to process the message and translate it from one form to the other. The two forms are plain text (the message or data in readable form) and cipher text (the message or data in unreadable or secret form).

Cryptography has been with us in various incarnations since Caesar's time. It has been said that cryptography played a decisive part in the outcome of World War II. Up until recent times, this technique has been the exclusive domain of the intelligence, military and diplomatic corps around the world. With the advent of personal computing and the ever increasing capabilities of these machines, cryptographic techniques have become available to everyone. Some nations have taken the view that the common man should not have access to "strong" cryptography and further, that because of its strategic importance in history, that cryptography should be considered to be of national strategic importance. *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 it useful.*

To that end, the US has legislated that cryptographic devices and software are classified as a munition subject to the same regulatory law as hand grenades and rocket launchers. Their apparent agenda is to prevent people around the world from having the ability to communicate in a secure manner and also to prevent them from having the ability to store information in a form that the US cannot retrieve and reconstruct in plain text form. They have most recently attempted to hijack the proceedings of the OECD (Organization for Economic Cooperation and Development) committee responsible for defining cryptographic policy for the member states (New Zealand is a member). The thrust was to obtain agreement of member states to their agenda - a policy for weak cryptography initially called Key Escrow

and now called Key Recovery or Trusted Third-Party encryption. Fortunately for the rest of the world, the majority of the members of this committee have not acceded to their demands. On the 27th of March the OECD committee put forward their recommendations concerning the guidelines for cryptographic policy. In part it states "Users should have access to cryptography that meets their needs, so that they can trust in the security of information and communications systems, and the confidentiality and integrity of data on those systems.". Purposely weakened encryption algorithms certainly cannot be trusted. For now, at least, we are not bound by the notion that governments, intelligence and law enforcement should have the authority to decrypt ANY and ALL encrypted information from whatever source.

For the reader that says that they violate no laws and have nothing to hide, I would like you to consider that this is not about guilt or innocence. This is purely about privacy. One of the basic techniques of propaganda (Word Games: Glittering Generalities) is making use of emotional issues to accomplish the objectives. The emotive issues here are child pornography, drug dealing and terrorism and the likely use of cryptographic technology by these groups. No one wants to help these groups to flourish, however, the bridge between being a "bad guy" and being stupid has definitely not been made. The fiction that preventing honest law abiding citizens from having control of their privacy is going to somehow prevent the "bad guys" from carrying out their activities is just that - a fiction. A classic propaganda technique. The only thing that outlawing "strong" encryption for the masses will achieve is the denial of privacy to the masses.

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. The current crop of word processors, for example, offers document encryption as an optional way to store a document. If you use Microsoft Word or Word Perfect, there are cracker (attack) programs freely available on the Internet that will derive the key from an encrypted document file. Neither product is secure and neither should be trusted in-so-far-as data encryption is concerned.

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 is another product (from Finland) that holds a great deal of promise due to its very user friendly interface and the choice offered to users of encryption algorithms – TeamWare Crypto (a symmetric key system) and that's available from Fujitzu (NZ). 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. *NOTE: Mentioned above is "public key" encryption (asymmetric – using two different keys – one is public and the other is private) . There are actually two general types of encryption that are currently popular. The other one is symmetric or single key encryption Both types of encryption can be computationally secure. The weakest part of otherwise strong encryption algorithms is key management (how users exchange keys without those keys being compromised). Public key encryption makes key exchange practical without the risk of key compromise.*

Conclusions: The use of cryptography offers the opportunity to have real privacy of information and communications. It can be used to protect stored information (ideal for notebook computers and for files stored on any computer) as well as live or Internet communications. It can be used to protect business transactions that are communicated over the Internet (including the protection of credit card information). But only if it is available and only if it is "strong encryption". There are other technological tools that can be used to improve and enhance privacy (such as the utilities mentioned previously).

The important issue to remember is that there is a continuous assault on our privacy and that new techniques are being developed all the time. While you are using your computer you should be aware of and consider that whatever you can see on your VDU can be seen by anyone with the proper equipment up to 1,000 meters away (which can be created by a home hobbyist for less than $1,000). Moreover, it is virtually impossible to detect certain sophisticated bugging devices. Anyone can be bugged. It does happen here in New Zealand. Another example is a microwave device that "sees" through clothing and can be used to create a holographic view of an individual (naked) showing anything not made of cloth that they are carrying on their person – soon to be tested in selected airports in the U.S. Yet another example is an iris recognition unit that can be used to positively identify individuals – from distance – initially one meter but experiments are being carried out to extend the distance. Soon to be tested in the banking community in the U.S. for positively identifying clients. The important issue here is that this device works just as in the previous examples – without the individual's knowledge.

Take note – govern yourself accordingly.

Additional Sources of Useful Information:

Cryptography:

Schneier, Bruce, *Applied Cryptography*, 2nd Edition, New York, John Wiley & Sons, Inc., 1996, ISBN 0-471-11709-9.

Schneier, Bruce, *E-MAIL SECURITY: How to Keep Your Electronic Messages Private*, New York, John Wiley & Sons, Inc., 1995, ISBN 0-471-05318-X.

Stallings, William, *PROTECT YOUR PRIVACY: A Guide for PGP Users*, Englewood Cliffs, New Jersey, Prentice Hall PTR, 1995, ISBN 0-13-185596-4.

Bamford, James, *The Puzzle Palace*, Harmondworth, England, Penguin Books, Ltd., 1983, ISBN 0-14-006748-5.

Kahn, David, *THE CODE-BREAKERS: The Story of Secret Writing*, New York, MacMillan Publishing Company, 1967, ISBN 0-02-560460-0.

Periodicals:

Cryptologia, Terre Haute, Indiana, Rose-Hulman Institute of Technology, 4 issues per year, ISSN 0161-1194.

Computers & Security, Oxford, England, Elsevier Advanced Technology, 8 issues per year, ISSN 0167-4048.

General:

Bok, Sissela, *SECRETS: Concealment & Revelation*, Oxford, England, Oxford University Press, 1986, ISBN 0-19-286072-0.

Internet Sites of Interest

http://www.ifi.uio.no/pgp/download.shtml
A place from which to download PGP 2.6.3I

http://www.aegisrc.com:80/Products/index.htm
AEgis Products – A Windows front end for PGP to make it more user friendly

http://www.ifi.uio.no/pgp/PGPfone.shtml
Where to get PGPFone

http://www.cs.auckland.ac.nz/~pgut001/links.html
Peter Gutman – Cryptographic reference – closer to home

http://www.cs.hut.fi/ssh/crypto/
International Cryptographic Software Pages for Encryption, Decryption, Cryptanalysis, Steganography, and Related Methods

http://www.netsurf.com/nsf/v01/03/nsf.01.03.html
Netsurfer Focus on Cryptography and Privacy – More crypto reference information

http://www.sky.net/~voyageur/wipeutil.htm
Wipe Utilities Home Page – where to get free software to clear slack bytes, etc.

http://www.tscm.com/
Counterintelligence and CounterTerrorism Home Page – reference material

http://www.thecodex.com/
The Codex – A place to view surveillance reference material

http://www.isecure.com/newslet.htm
SECURE NEWS – the latest in security issues (monthly)

http://ciac.llnl.gov/
CIAC Security Web Site (U.S. Department of Energy)

http://www.sei.cmu.edu/technology/cert.cc.html
CERT Coordination Center (Lawrence Livermore Laboratory)

http://www.first.org/
Forum of Incident Response and Security Teams

NOTE: The Internet is a fluid living thing. What is valid today may not be valid tomorrow. One or more of these addresses may no longer be active but give them a try.