December 1997

Information Security in electronic Commerce

W. Caelli
Queensland University of Technology

Information Security in Electronic Commerce

W.J. Caelli
Information Security Research Centre, School of Data Communications
Queensland University of Technology

Abstract:
Electronic commerce over the Internet on a global basis presents major security architecture challenges for guaranteed and end-to-end security services. The scalability problem alone presents major concerns, i.e. availability, one of the acknowledged three main aspects of information security along with confidentiality and integrity. Additionally, national, social and legal issues impinge on any technical decisions made, including the operation of national and international public key infrastructures in an environment emphasizing control of cryptographic keying systems.

The question is one of achieving such security with a straight-forward and implementable design which, in turn, is easily understood by users of such e-commerce schemes. For the disciplines of information and enterprise analysis, the incorporation of security requirements into overall information systems is a challenge for education and research into the 21st century. Security design impinges not only on data network security architectures but also on aspects of trust in host operating systems and database management systems. Indeed, national and international legal regimes may soon form a basic system protection requirement for all information systems, needing to be assessed and implemented by information system professionals.

1. Introduction and Business / Personal Risk.

"It would be nice to have encryption software and I wish I had it right now, but I don't think it has cost me much business. We are still unsecured and it really doesn't seem to make any difference." [1]

Mr Barry Michaels
Stitching Horse, Melbourne, Victoria, Australia.

"Further down the track when we want to talk to our suppliers and ask them for stock information which we are thinking of doing, then we will probably implement encryption software because of course they won't want people to get in and look at their information." [2]

Mr Geoff Paine,
IS Manager, Lowes, Sydney. NSW. Australia.

The above quotations appeared in the *ComputerWorld (Australia)* newspaper of 21 February, 1997 along with a report that Swedish hackers had successfully demonstrated the use of Microsoft's *"ActiveX"* language to bypass password and allied controls in PC based banking software. They allegedly were able to illicitly transfer funds from the user's bank account when connection to the bank was made using the popular Microsoft *"Money"* package was used [3]. This followed media publicity relating to the "Chaos Computer Club" in Germany who had, allegedly, demonstrated a earlier version of this procedure using another popular browser, JAVA program "applets" and the Intuit Inc. *"Quicken"* financial management package[4].

In relation to the Active-X situation above, the response from a representative of Microsoft Inc. of the USA, the originator and manufacturer of the "Active-X" programming / scripting systems, has been interesting. Essentially the whole problem is to be solved by simply checking and verifying the origin of programs that are down-loaded from the Internet onto a PC.

A global infrastructure of so-called "certificate authorities" will supposedly enable users to verify code "applets" or indeed any other executable content loaded to their machines, through the originator of the down-loadable program / script digitally signing their product. The signature, in turn, can be checked by the users through access to these "certificates" issued to the program originator.

This paper submits that this is only a very small part of the problem. The main concern is a requirement to move to a new generation of computer systems, particularly operating systems, that, in the era of global inter-connectivity, permit information system managers to implement

MANDATORY security policies for their installations and global information systems operations. This proposal has been outlined by the author in a recent paper[5]

In simple terms, global inter-connectivity means that a new generation of operating systems is urgently needed, at a minimum of the earlier USA's "**B1**" level of security certification, preferably "**B2**", (ITSEC "F-B1, E2" and "F-B2, E2") to enable reliable connection to the global information infrastructure (GII) for trustworthy national and international electronic commerce. Information technology professionals worldwide must now consider their professional responsibility in relation to the creation of international electronic commerce systems on untrusted and non-evaluated systems. There is now at least 15 years experience in the creation and assessment of trusted systems under schemes like the USA's Trusted Computer System Evaluation Criteria (TCSEC). It is time for these considerations to enter the "mainstream" of information systems analysis, design and development[6].

Web bank robbers poised to pounce.

German hackers have found a way to commit the perfect bank robbery. By exploiting security loopholes in Microsoft's Internet software and a popular financial management program called Quicken, the Chaos Computer Club claims it can make someone transfer money to another bank account without knowing they are doing so. The first a victim would know about the crime is seeing the transaction on their bank statement.'

New Scientist, 22 February 1997. Pg. 4.

ACTIVE HACK. *The security surrounding Microsoft's ActiveX component architecture came under fire again last week when Swedish hackers demonstrated to their government how an ActiveX control could bypass any password protection and transfer funds from a user's bank site by controlling a copy of Microsoft Money.*

ComputerWorld (Australia) 21 February 1997.

2. Bases for Secure Electronic Commerce on the Global Internet

The bases for secure electronic commerce on a global scale can be summarised as follows :

- willingness for consumers, merchants and banks / financial institutions to enter into integrated schemes,
- global, open standardisation of underlying formats, protocols and processes,
- national and international standards for security, technology and management, and
- national and international agreements on the social, economic and legal aspects of the systems.

Electronic commerce, by its nature, encompasses a number of sub-systems, including earlier electronic data interchange schemes (EDI), electronic mail and messaging (E-mail), electronic banking and file transfer.

All of these have coalesced into the world-wide-web and associated browser paradigm of the late 1990s and electronic commerce schemes have now been seen as being inextricably linked into this environment. In turn this means that underlying computer hardware, operating systems, middleware and applications all need to operate in an environment in which users can be confident and in which enterprise management personnel may place trust.

The hierarchy chain of electronic commerce has now been clearly identified in information technology terms. Essentially, from the point of view of the consumer "looking out" to the global information infrastructure, he or she sees :

- a personal computer, network computer or workstation, including consumer information appliances such as TV sets, etc.,
- connection to a telecommunications carrier, wired, radio or satellite,
- connection to an Internet service either directly or through an Internet service Provider (ISP),
- connection to a national and international switching network
- access to host nodes on the Internet offering products and/or services, including merchants, banks, etc.
- access to payment facilities.

All of these must operate in a secure way enabling the consumer to have full confidence in the confidentiality, integrity and availability of information flows, processing and storage. Cryptography and allied access control technologies form the basic tools for the creation of secure environments in both the computer systems and data networks that form the global information infrastructure or GII.

However, cryptography is still a highly controversial technology with most countries deeming it to be a "dual-use" technology, of significance in national security and defence terms. (Perhaps airplanes had the same status before and during the first world war but no-one would regard that as so today ! In the "infotronics" age, new schemes for assessment of this technology are urgently needed.)

This paper concentrates on the security aspects of electronic commerce and, thus, on cryptography. However, firstly, there is a need to place the overall security assessment methodology on a firm footing and into the mainstream of information systems analysis and development.

3. Role of IT Professionals - Risk / Security Assessment and Information / Enterprise Analysis.

Whether it is called data, systems, information, relational, object-oriented, enterprise or any other form of analysis, there has been little evidence to suggest that over the last twenty years the needs of information systems security have been fully incorporated into the education processes for information systems professionals, let alone the analysis tools used. Early relational database schemes, for example, started to assess what became known as "constraint" analysis but even this was very little, very late. The opening of data and program collections to national and international networks that accelerated in the 1990s has meant that information analysis techniques must consider not just the data structures themselves (the "objects") but the environment in which those objects "live". There is little doubt that national and global legal obligations in this area, such as for confidentiality in transborder data flows, integrity of medical records data, etc. will impinge on the information systems professional.

Recent work (e.g. Kwok[7]) has demonstrated the need for the rapid incorporation of risk analysis and assessment techniques into the mainstream of information / enterprise analysis methodologies and resulting security service and mechanisms determination into information systems development. Such concepts and systems as the "Risk Data Repository (RDR)", integrated into "data dictionaries", for example, mean that IS professionals will have a first set of tools to move into the new requirements of information analysis in a global electronic commerce and information network environment[7].

4. Cryptography and Related Public Policy.

Cryptography is the single, most vital tool for the protection of electronic commerce on a global scale but it is bedeviled by national political and legal regimes. The underlying techniques are needed to provide the necessary :

- confidentiality (the most controversial aspect),
- integrity, and
- authenticity

aspect of overall system security. While the OECD has worked over the last 18 months or so (as at March 1997) on an international set of guidelines for the use and development of cryptography these guidelines will not be sufficient to allow for immediate action by IT professionals worldwide, i.e. they will not "spell out" in detail policies for incorporation of cryptographic systems into international electronic commerce schemes at a level needed by IT professionals charged with the creation of the necessary hardware, software and telecommunications structures.

Cryptography and its efficient and, itself secure, usage comprises a numbers of aspects:

- correct identification of necessary cryptographic algorithms and pertinent mathematical structures
- associated cryptographic key management schemes
- necessary data network and systems protocols, message formats and associated structures to support the cryptographic system and key management schemes
- integration of the cryptographic sub-systems into computer systems and data network structures.

Of all of these the last one is the most difficult. Unless the cryptographic system is reliably integrated into, for example, an operating systems or middle-ware structure, then it can be compromised and/or bypassed rendering the whole scheme "worse than useless". It could produce a totally false sense of security. However, as for the political (export controls, usage) limitations on cryptography, there are also limitation on the integration aspects of the technology.

Cryptographic Service Providers (CSP) are software and hardware sub-systems that provide such services in an operating system environment. However, the very incorporation of the technology into the system is itself politically sensitive, e.g. for Microsoft products it is a requirement that any CSP be integrated into the system in the United States by Microsoft itself. The whole scheme then becomes subject to US export restrictions. This places non-USA cryptographic systems companies and providers at a distinct disadvantage. They need, in principle, to expose their products to a potential competitor in a foreign nation and then to have their own technology subject to the export rules of another nation !

For global electronic commerce to progress on a "level playing field" base, a solution to this problem has to be found given that such companies as Microsoft dominate the world IT industry in the operating systems and middleware area. Unfortunately it appears improbable that any competitor to this situation will arise in the short or even medium term and the world IT industry will be almost totally controlled through one set of system software from one nation. Not even the car industry has achieved this state of affairs in 100 years ! Nations may need to incorporate cryptographic sub-systems of their own choice into the basic software of computer and data network nodes.

5. Public Key Infrastructure with or without Key Recovery Infrastructure

This leads to the need for national and international agreement on the infrastructure needed to support the underlying cryptographic key management schemes used for electronic commerce. A global public key infrastructure (PKI) of appropriate "certificate authorities (CA)" is slowly being defined but its introduction is slow at both national and international levels. It is possible that, given the slow pace of governments worldwide, industry ad-hoc solutions may arise in 1997 that will difficult if not impossible to "rewind" in the future. The Internet itself is an example of this problem.

However, a far more difficult problem is the resolution of the debate between privacy advocates and law enforcement over the national and international usage of cryptography for confidentiality purposes. It can now be fairly safely assumed that the use of cryptography for integrity and authenticity purposes is less controversial and could, in 1997, become widespread globally. It is in the confidentiality area that the problems have arisen and they have been around for may years.

Law enforcement insists on maintaining its ability to have access to traditional "line-tapping" facilities to perform its legitimate and government mandated functions. Cryptography can rob law enforcement of that investigatory tool. However, the growth of electronic commerce mandates the need for confidentiality of transactions and associated messages. One solution seems to be some form of internationally accepted "key recovery" or "key escrow" scheme whereby law enforcement may gain access to "plaintext" forms of transmitted messages and/or associated confidentiality encryption keys, under necessary legal regimes. In turn, this means that keys themselves need to be clearly identified and tagged as to their proper or approved usage. Misuse of the key needs to be prevented.

For most nations involved in this debate their is a political absurdity. Each nation (with some notable exceptions) attests that there is a clear need for its citizens to have access to any form of encryption needed to protect their business. No restriction is placed on the ownership, usage, development or research into cryptographic systems in any form (again with some exceptions). Indeed, politicians have argued that both public and private enterprises need to adopt strong cryptographic solutions to minimise risks to overall information systems. However, they do not extend the same courtesy or policy to people of other nations. What is "sauce for the goose" is NOT "sauce for the gander". Export restrictions for cryptographic systems exist in many forms, including in the case of the USA, in the form of expert assistance to foreign nations to develop and integrate cryptographic systems into IT products.

These restrictions have to be over-ridden to enable full international interoperability of electronic commerce schemes. Schemes, such as key recovery, are a way forward.

6. Conclusions

The above clearly raises the question as to just when the professional responsibility of information technology professionals , along with the associated ethical behaviour principles of their associated professional organisations, come to play in advice offered to owners and users of information systems. Just when does that IT professional advise management that an electronic commerce

system is *"unsafe to use"* or does not incorporate *reasonable* security technologies and management procedures ?

The stage for just these types of dilemnas has been reached now in the late 1990s as feverish interconnection of enterprise information systems into the global Internet occurs and at accelerating rate.

There is no doubt that at last we need to look carefully at the incorporation of risk analysis and assessment methodologies into the professional "toolkits" of information and enterprise analysis techniques now widely used, and taught at Universities worldwide. Whether we call this constraint analysis, access control parameterisation, confidentiality requirements assessment, trusted systems parameter assessment, or whatever, the IT professional of the 21st century, the groups we are educating today, need to be familiar with these tools and to incorporate them into daily professional practice.

At the technology end of the spectrum, we must now admit that untrusted and unevaluated computer systems linked to the global information infrastructure is equivalent to allowing unroadworthy cars onto modern high speed freeways. Downloadable, executable content, such as Microsoft Active-X controls, Java language applets, Word Processing / Spreadsheet macros, etc. have all changed the risk assessment for global electronic commerce. The problem is one of whether or not consumers of IT products and systems, through IT professionals worldwide, will insist on much higher levels of "safety" in computer systems and data networks.

Experience, unfortunately, does not indicate that this will happen and that legislation will be needed to force compliance with even the most rudimentary of security controls. Seat belts in cars just did not happen through consumer demand !

7. References

1. Sim and A Prodromou
   "Oyster opens up e-comm for all"
   ComputerWorld (Australia), Vol. 19, No.28, 21 Feb. 1997, Pg. 4.
2. As for 1.
3. *"Active Hack"* in "This Week" Column
   ComputerWorld (Australia), Vol. 19, No.28, 21 Feb 1997, Pg. 4.
4. Ward, M
   "Web bank robbers poised to pounce."
   New Scientist, 22 February 1997, Page 4.
5. AS/NZS 4444:1996
   "Information security management"
   Standards Australia / Standards New Zealand, August 1996.
   ISBN 0 7337 0739 4
6. Caelli, W.
   "B means Business"
   Proceedings of the NISSC'19 Conference, Baltimore, MD, USA., October 1996.
7. Kwok, L. F.
   Ph.D. thesis, submitted to the Queensland University of Technology, Brisbane, Queensland, Australia, March 1996.
8. Longley, D
   Private communication - discussion of the work of Anderson, A., Information Security Research Centre (ISRC), Queensland University of Technology, Brisbane, Queensland, Australia.
9. Wood, C.
   "How to Handle Internet Electronic Commerce Security : Risks, Controls & Product Guide"
   Baseline Software, Inc., Sausalito, California. USA., 1996.
   ISBN 1-881585-03-4
10. Kalakota, R and Whinston, A
    "Frontiers of Electronic Commerce"
    Addison-Wesley Publishing Co., USA. 1996
    ISBN 0-201-84520-2
11. Dam, K and Lin, H (Editors)
    "Cryptography's Role in Securing the Information Society"
    National Academy Press, USA, 1996. ISBN 0-309-05475-3