A Secure Electronic Commerce Environment : Only with "Smart Cards"

Professor William (Bill) J Caelli FACS, FTICA, MIEEE

Head - School of Data Communications
Faculty of Information Technology, Queensland University of Technology

Key words: Smart cards, electronic commerce

Abstract: There is growing move to rely upon penetration detection / analysis schemes and add-on software processes and network security products to combat attacks on information systems used for the operation of global electronic business / commerce systems. These sub-systems and management procedures have taken the place of the development and deployment of solid information systems security and assurance technologies, particular at the computer security levels, both hardware and software. This is most notable at the small, commodity systems level; those system largely used by small to medium size enterprises, both private and public, and by divisions of larger corporate and government and even defence units, as well as by individuals.

This paper presents the proposition that current commodity level systems do not present the level of information assurance needed to create the necessary trust required for rapid and reliable uptake of electronic commerce systems, against a reliable, legal framework. Indeed, it appears impossible to raise the level of security of these systems, both at client and server levels, without the addition of supplementary hardware and software systems that provide appropriate security services and mechanisms in a trusted systems environment capable of being independently assessed as being effective. Smart cards, coupled with associated trustworthy reader/writer/terminal facilities, appear to be the most suitable method to create such necessary trust in electronic commerce facilities, providing a "trusted path" between the user and the electronic commerce infrastructure. However, it would appear that their usage may need to be legislated by Governments since without such "force of law" it appears unlikely that end-users or PC/server manufacturers

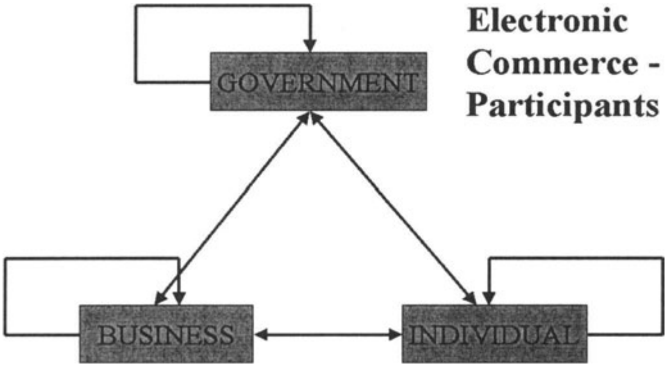
The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35575-7_19

J. H. P. Eloff et al. (eds.), *Information Security Management & Small Systems Security*

will voluntarily meet the cost, albeit small. At the same time, however, the sound and secure integration of such sub-systems into commodity, commercial-off-the-shelf (COTS) systems is a subject of active research.

1. INTRODUCTION - GROWING THREATS TO "TRUST" IN ELECTRONIC COMMERCE SYSTEMS, PARTICULARLY AT THE RETAIL LEVEL.

Global electronic business has been the "catch-cry" of the last half of the 1990s. The dimensions of the situation are best illustrated in terms of a triangle that incorporates the major entities involved, government, business and the individual. In order for the systems to widely adopted, however, there has to be trust in the overall operation of such schemes and such trust could be fragile. Indeed, there are signs already in the USA that early adoption of electronic business is being tempered, particularly at the retail transactions level, because of :



- concerns about privacy, including the protection of confidentiality of personal information at both the client and server ends of the systems;
- information assurance concerns, in that confidence must exist in the ability of the systems to fulfill the electronic business transaction in

a safe, reliable and efficient manner, on a total "end-to-end" basis; and

- lack of confidence by both merchants and consumers in the overall financial sub-systems that support the "electronic shopping" experience.

Indeed, there have been a number of concerns of late in the USA in relation to :

- "charge-backs" by consumers against web merchants in relation to credit card purchases;
- unwillingness of web "surfers" to commit to purchase and to then finalize a transaction after preliminary perusal of a merchant's web site; and
- overall performance of the Internet causing severe limitations to overall transaction performance.

All of this "micro-level" concern may be combined with a related "macro-level" concern related to "information warfare" and overall national "information assurance". Once the base economy of a nation becomes dependent upon electronic business activity, the risk assessment and management task takes on new dimensions. These new dimensions go beyond individuals using home / business PCs as electronic commerce terminals connected to an open and unprotected Internet as well as merchants and Government groups providing information servers, to the question of the overall protection of such nationally significant and critical information infrastructures. Once these infrastructures are in place and society becomes totally reliant upon them, then those very systems become targets in an information warfare scenario. Questions then arise as to just who is responsible for the protection of such nationally significant structures against internal and external "cyber-attack". Newsweek magazine of the USA highlighted this concern on the front cover of its 31 May 1999 edition, under the main banner (NEWS-99) :

"EXCLUSIVE: PLOTTING A CYBERWAR AGAINST MILOSEVIC"

This article (VIST-99) went on to explain that under a secret proposal to President Clinton of the USA use of cyberwarfare tactics could be beneficial through the use of *"government hackers to tap into foreign banks"* and thus possibly gain access to Mr Milesovic's banking accounts. *". The National Security Agency's hackers would ... try to overcome today's sophisticated* *encryption software and firewalls. If they gained access, the hackers could do almost anything they liked with Milesovic's cash....* " The article goes on, however, to point out that such a plan could really "backfire" if "*..confidence in the world banking system were undermined..*"

However, such plans, even if somewhat ad-hoc and not fully considered, highlight the concerns that people feel in approaching the new worlds of electronic business, commerce and banking. Altogether, they point to a need to carefully consider the bases upon which such national and international networks are created. And not just the network components but also the actual computer systems at each end and within the network itself. Together they caste doubt on the integrity of system software and allied sub-systems operating on computers attached to the Internet as clients and servers, a vital concern for global secure electronic commerce.

2. THE CURRENT ELECTRONIC BUSINESS ENVIRONMENT AT THE USER AND MERCHANT COMPUTER SYSTEM LEVEL.

Recently the "banking roundtable" in the USA set up a group to carefully examine again the security of the basic technology used for the provision of home and corporate banking services, particularly where these services are made available over the Internet. Particular attention was seen to be urgently needed, not just on the network technologies involved, but more urgently on the connected commodity level computers used to provide the information services themselves at all points in the service. It must considered that even the larger server systems may themselves be based upon PC hardware technology, in terms of PC "motherboards", disk drives, etc.

Essentially, this USA financial group recognised that there are legitimate concerns as to whether or not commodity level computer systems based upon PC hardware and software, never really developed for such purposes, can be made suitable for such important societal activity. Essentially, there are doubts in the minds of the USA's banking industry that such systems, without substantial modification, are suitable at all for these purposes.

The absolute requirement, then, to augment the commodity computer system with higher trust and security technologies has also been acknowledged in the Congress of the USA. For example, Senate Bill "S.1059" (SENA-99) in the current 106th congress (the military appropriations Bill) has a section (Section 346) that is clearly entitled *"Use of Smart Card Technology in the Department of Defense".* Essentially the whole project is seen as a means of ".. enhancing readiness and improving business processes throughout the military departments...". Section 347 of the same Bill goes on to support a *"Study on Use of Smart Card as PKI Authentication Device Carrier for the Department of Defense."* This all supports the contention that even at the Governmental and military level there is growing awareness that "trust" in overall information systems and associated data networks must be enhanced well above current commodity product levels. As below, this comes at a time when actual shipments of commodity level PCs, selling at retail levels in the USA at well below $,1000 , seem set to increase yet again.

The important point is that, as Bill Gates pointed out in that same Newsweek edition of 31 May 1999 (GATE-99) *".. for most people at home and at work, the PC will remain the primary computing tool.... When the PC is at the center of a home network (probably connected to a broader network that will constantly monitor performance, update software and download device drivers and the like), it will be incredibly easy to administer, automatic in operation and maintenance-free."* Indeed, a side box in the article predicts even further rises in PC shipments well into 2000 and beyond with growth to 150 million units per annum predicted. This article makes absolutely no mention at all of any form of system integrity, information assurance, privacy or indeed any other form of security at all.

This dependency upon unaltered PCs to perform critical electronic commerce functions, with only software add-ins, including cryptographic sub-systems, that are downloaded from Internet web sites is a major concern but one that has been tacitly supported by recent advertisements. For example, an advertisement in the 7 June 1999 edition of Time magazine (Australian edition) presents the unadorned Intel Pentium processor as a solution to electronic commerce security. The advertisement states (INTE-99):

> *" Is your e-business walking a tightrope ?*
> *The power of the Pentium III processor.*
> *Your safety net in the Internet economy.*
>
> *It's a fact. Doing business through the Internet exposes your company to viruses, unauthorised access, and potentially overwhelming network traffic loads. Your safety net ? The Intel Pentium III processor. It has the power to run sophisticated compression, encryption and anti-virus software behind the scenes, without compromising performance. So you work faster and safer. And to add an even higher level of protection, each processor has a unique serial number to help protect your vital assets.... "*

Interestingly, the advertisement makes no mention at all of the most powerful feature of the Intel architecture; its "MULTICS" inspired segmentation and "ring" structures. These provide the necessary hardware architectures needed to create highly secure operating systems, even those up to the highest "A1" trusted systems class in the USA TCSEC category. However, their full power is simply turned off by current PC operating systems.

At present, particularly in the USA, Australia and elsewhere, but less so in Europe, the trend is to allow critical transactions to be initiated on home/business PCs, and even simple touch-pad telephones, using just specialised application software sub-systems, including software based encryption schemes and link-level encryption through the Secure Sockets Layer (SSL) for confidential transport of information across the Internet between client and server. In most cases such software sub-systems are themselves even further sub-systems to commodity product Internet "Web browsers" that provide no security services at all within themselves, beyond possible integrity checks on down-loaded "byte-code applets" of Java language origin. (This fact is based on the consideration of the SSL scheme as being a separate "layer" in an OSI sense that is utilised by a higher "application layer" in the form of the browser.)

3. STRONG LEGISLATION AT THE TRANSACTION AUTHORISATION TIME - NOT JUST AT ITS ACCEPTANCE.

In considering the levels of security and assurance needed to create trustworthy electronic business operations, information technology professionals need to be guided by appropriate legal obligations and, moreover, must take a prominent role in the formulation of those same legislative instruments. At present there is worldwide trend to weaken the security requirements for the operation of electronic commerce systems. Australia's "Electronic transactions" Bill, before the federal Government at June 1999, exemplifies this weakening of overall information security requirements when it comes to electronic commerce. Essentially the Bill aims at making electronic transactions have the same status as those conducted in the more traditional paper-based way but, when it comes to the provision of security requirements, the Bill offers only vague and almost meaningless appeals to security that is considered pertinent and relevant given the situation. Surprisingly this is the complete reverse to the paper world where hundreds of years of law have arisen covering all aspects of the use of paper for transactions, even to the level of the type and colour of ink used to affix signatures, the use of notaries to verify affixation of signatures, and the like.

In other national jurisdictions, total emphasis is placed on the server's verification of a "digital signature", even down to the level of creating requirements for so-called "public key certificates" while absolutely no statements are made about the process of affixing such "digital signatures" to transactions. Once again, this is a reversal of common legal practice and legislation where a body of law and regulations exists covering the affixation of signatures to documents and very little law exists in relation to the verification of those signatures in a "court-room" environment, e.g. the use of witnesses, hand-writing experts, etc.

The USA's State of Illinois in its "Electronic Commerce Security Act" of 24 August 1998 illustrates this vagueness in legislative instruments, contrasting markedly, for example with similar legislation in the car safety arena. It states, in relation to digital signatures (ILLI-98), that a "qualified security procedure" is used where this procedure is ;

> *"1. Commercially reasonable under the circumstances,*
> *2. applied by the relying party in a trustworthy manner, and*

3. reasonably and in good faith relied upon by the relying party."

Essentially such a digital signature, according to the Illinois Act must be such that the digital signature ".. can be used to objectively identify the person signing the electronic record...". Simply, an unmodified PC cannot do this in any way at all.

Similar problems to this occur at national, regional and international levels.

4. THE PC - NOT A SUITABLE VEHICLE FOR "SIGNING" A TRANSACTION ?.

The hardware and software base of a consumer PC is totally unsuitable for use in trustworthy electronic business operations. There is simply no other way of expressing a fundamental point. The PC's hardware and software, essentially developed in the early 1980s for a completely different purpose, was never seen as a trustworthy business transaction terminal. This includes all PC hardware available at retail outlets as well as systems and generic software such as PC operating systems commonly used for home and small business purposes, such as Microsoft's Windows'95/98, Apple's MacOS, IBM's OS/2 as well as generic sub-systems often used to "host" electronic business operations, including WWW browsers. These systems were not designed with computer security in mind but have been pressed into operation into application systems where individual privacy as well as transaction integrity and authenticity are vital aspects of business and governmental operations. In Australia, for example, the EFTPOS standards (SA-2805 series) have clearly mandated a secure device (PINPad) for the entry of identifying and authorizing data (the user's PIN - Personal Identification Number) for credit and debit transactions at retail and other outlets. These units have become mandatory "add-ons" to all "cash register" operations and such point-of-sale devices are themselves mostly based upon PC technology.

The problem is that, to management, information security is still a cost centre and as such, is an area that must be minimised. It is not seen as a basic requirement as much as the information technology systems needed to provide corporate and government services.

5. SMART CARD BASED SUB-SYSTEMS - KEY TO TOKEN BASED SECURITY IN ELECTRONIC COMMERCE.

Current legislation and draft legislation, particularly in Europe, has set some initial requirements for the provision of a safe environment for consumers to use in pursuing electronic business activities. However, as would be expected, these legislative instruments are generalized and provide no real technical guidance as to appropriate security services and associated mechanisms to be employed. There is general agreement emerging, based upon actual experience, that the use of a smart card as a "signing instrument" offers the best method for provision of a safe and secure digital signing or signature affixation environment. However, while actual smart cards exist that are capable of performing digital signature and allied cryptographic and key management functions, it is their secure and reliable integration into the untrusted environment of the commodity PC that requires major attention and may still be the subject of further research activity. It is assumed that users will be issued with an appropriate smart card alone, rather than any "super-smart" token, or other device that incorporates a complete computing environment incorporating display and data entry facilities.

The following table summarises the risks associated with each form of product used to provide such enhanced security services in a PC.

Technology	**Risk Assessment**
Smart card reader/writer in simple form attached to PC keyboard port or serial/parallel port	Card activation, e.g. via PIN/password requires entry of security critical data on untrusted PC keyboard. "Trojan horse" software sub-system may capture PIN/password. Untrusted device driver.
Smart card reader/writer integrated into keyboard.	As above
Smart card reader/writer integrated into separate keyboard component with isolation hardware.	Some risk is alleviated IF separate component creates an encrypted/trusted "channel" between the PC and the separate keyboard component.

	Risk of “Trojan horse” device driver still exists (e.g. capture PIN/password, insert fraudulent transactions for processing by smart card, etc.) BUT such driver needs to possess channel crypto key.
Smart card reader/writer integrated into full “PINPad” device with separate display and keyboard connected via keyboard/serial/parallel port.	Less risk and best solution at present. Capture of activating PIN/password avoided BUT unprotected PC hardware/software could permit insertion of fraudulent transactions for processing.
Fully integrated smart card sub-system as above plus trusted system driver set for PC.	Better solution and Minimizes insertion of “Trojan horse” software sub-systems capable of creating or passing on fraudulent transactions.

6. CONCLUSIONS.

Smart card, and allied token, technologies present the best possibility for meeting the trust requirements for national, regional and global electronic commerce assurance. However, the is a great need for urgent research and development on the creation of “trusted pathways” between the user, the smart card token activation process and the electronic commerce terminal, usually a PC. Without that trust being created, test and demonstrated, then the potential for massive litigation exists given the vague and indecisive state of legislation in this area.

7. REFERENCES.

GATE-99Gates, Bill
"Why the PC Will Not Die."
Newsweek, 31 May 1999. Pg. 64

ILLI-98 The State of Illinois, USA.
“Illinois Electronic Commerce Security Act”
24 August 1998
1997 Illinois House Bill 3180, Illinois 90th General Assembly
1997-98 Regular Session

NEWS-99 Front Cover, Newsweek, 31 May 1999

SENA-99 Senate of the United States of America
Senate Bill S.1059, Sections 346-347.

VIST-99 Vistica, G. L.
"Cyberwar and Sabotage"
Newsweek, 31 May 1999, Pg. 38.