



**INTERNATIONAL INFORMATION
SECURITY CONSULTANTS PTY LTD**

ABN: 65 111 755 741

21 Castle Hill Drive South
GAVEN
QLD 4211
AUSTRALIA

Phone: +61 - 7 - 5578 2255
Mobile/Cell: +61 - 414 987 952
Fax: +61 - 7 - 5527 3255
Email: w.caelli@iisec.com.au

Mr Michael Funston
EFT Code of Conduct Review
Australian Securities and Investments Commission
GPO Box 9827,
Sydney NSW 2001

Email: eftreview@asic.gov.au

27 April 2007.

Dear Mr Funston,

I have just returned from an overseas trip and noted that submissions to your discussion paper were due on the 13th April. While late, I make the attached preliminary comments for consideration in case they may be of value and would be pleased to offer further input as the committee sees suitable.

Yours sincerely,

Professor William J Caelli, AO
Senior Consultant

Some Specific and Preliminary Comments:

Part 1. Comments on Discussion Paper - Executive Summary:

Growth in online fraud

- *While the level of internet banking fraud has grown, it remains relatively contained to date compared to other forms of fraud (such as cheque fraud and credit card fraud).*

Comment:

This discussion paper presents no concrete evidence to support this statement. Indeed, recent reports, particularly in the USA and UK appear to contradict it. Has this been independently determined by studies commissioned by ASIC or through the AHTCC?

- *Many financial institutions are looking at how user authentication can be enhanced as part of their broader anti-fraud strategy.*

Comment:

Moves overseas indicate that strong legal and regulatory influences are needed to persuade the banking and finance industry to move to better systems, e.g. in the USA/UK, etc. This also applies in the “commercial” government arena, e.g. the USA’s Federal Information Security Management Act (FISMA) of 2002.

- *Some Australian institutions have taken steps towards implementing two-factor authentication of consumer users.*

Comment:

The two factor schemes being discussed have been seen as already being OBSOLETE in regard to threats such as rootkit, “zombie”, “directed / specific Trojans” and allied attacks. The main problem, today, with extended use of “broadband” connections to the Internet is simply “session capture”, even when a token based structure is used. In this situation the actual PC being used is totally “captured” by the third party and any activity to/from that machine can be monitored and fraudulent transactions can be inserted at will, while the user is on-line to their bank, for instance.

- *Other methods used to minimise fraud include encrypting information, warning consumers of risks, monitoring activity, and imposing daily transaction limits.*

Comment:

While these all are worthwhile they do nothing to minimise the trauma and suffering experienced by those who become victims of attack. It is unsure just

what is meant by “encrypting information” in this context. Is this referring to “data in transit”, e.g. use of such schemes as the SSL subsystem, and/or “data at rest”, i.e. encryption of data stored on hard drives, backup tapes/disks, etc.?

• *Despite having concerns about online fraud, most people making transactions online appear not to take adequate steps to secure their equipment against malicious code attacks by fraudsters.*

Comment:

This comment makes the **radical and controversial assumption** that it is the responsibility of the end-user to make their systems secure and safe for use in this environment. This is simply not the case in other industries, e.g. the car and truck industry, pharmaceutical industry, etc. and it is surprising that ASIC would even suggest this via the emotive term “adequate steps”.

In any legal and contractual sense, the inexperienced end-user is at an extreme disadvantage against the resources of the banking and finance industry in terms of technological competence and risk assessment / management capability. They usually have no idea what “adequate steps” means!

Of course, it is the responsibility of the end-users to properly utilise any security and safety systems provided by the equipment manufacturer and/or service enterprise, e.g. the bank, and NOT to try and purchase, install, integrate, manage and audit such systems. That is the responsibility of any enterprise that wishes the Australian citizen or enterprise to make use of such equipment for sensitive and valued transactions over an insecure pathway, i.e. the home/business commodity PC connected to the open Internet.

It is worth repeating again and again that it is the responsibility of the banking and finance industry, just as in the car and other industries, to provide the necessary equipment and systems required to perform the services desired in a safe and secure manner. It is the responsibility of the end-user, as in the case of the car driver/passenger, to responsibly use those systems in the correct manner. Legislative and regulatory instruments must redress this balance and place responsibility on those enterprises who wish the populace to use the home/small business commodity PC and the Internet, mobile phone/PDA systems, etc. This is NOT the situation today.

Recommendation:

ASIC should investigate and report upon the situation in other industries in order to help formulate policy and regulatory requirements or similar codes of conduct in this specific area, e.g. the electric / power supply industry, etc.

Part 2. Responses to Specific Questions.

Q4

What do you see as the main challenges in relation to online fraud over the next few years? Are there trends or developments that the Review Working Group should particularly consider in reviewing the EFT Code?

The main challenge is simply based around the following facts:

1. the home PC was never built, developed or sold to perform secure transaction operations such as home banking over the Internet as clearly and constantly stated by the appropriate manufacturers and suppliers, e.g. Microsoft Inc.;
2. the level of sophistication demonstrated by such highly technical attacks as “rootkits”, “Zombie takeover”, etc. clearly indicate that the average home and small business user CANNOT RESPOND to such attack levels in any meaningful way by themselves;
3. the PC manufacturers, both hardware and software, have repeatedly claimed that their systems were not designed or sold as secure transaction systems and indeed, in one case, i.e. Microsoft Inc of the USA, that manufacturer has even proposed an URGENT REQUIREMENT for enhanced hardware and operating system changes to create such secure systems for such applications as home banking via the Internet, etc. (see Microsoft’s “NGSCB” project outline) and/or use of an external “PINPad” type device to provide a separate “trusted channel” between the PC and the bank/financial institution;
4. any form of user authentication depends totally upon there existing a “trusted channel” between the “claimant” to an identity and the “verifier” of that identity, a channel that DOES NOT EXIST in the case of the home/small business PC environment.

Summary:

Given that the manufacturers of the equipment used for Internet based banking and financial transactions have repeatedly claimed that their systems are NOT SUITABLE FOR THAT PURPOSE WITHOUT SUBSTANTIAL MODIFICATION, IN BOTH HARDWARE AND SOFTWARE BASES, then the banking and finance industry cannot claim to the contrary.

Indeed, the specifications set out in relevant EFTPOS Australian Standards (the AS 2805 series) clearly dictate the needs for high trust in the equipment used for such activities as “PIN” entry, etc.

Q5

What information can you provide to the Working Group (including on a confidential basis) about online fraud countermeasures being considered or deployed by Australian financial institutions? How does the Australian response compare with that of other comparable countries, in your view?

Q6

Is the growth in, and growing publicity given to, fraud issues having an impact on online transacting in Australia at present? (Again, you may wish to provide information on a confidential basis.)

Q7

What information can you provide to the Working Group about the online fraud mitigation skills of Australian online users?

Simply put, if a car has no seat belts then a driver cannot buckle up for driving safely!

This is the situation with the consumer level, commodity personal computer system in 2007 coupled to the Internet. Even if a home user became skilled in the configuration and operation of sophisticated “firewall”, anti-virus, anti-spyware, anti-phishing, user-access-control (UAC) and like systems, the level of change and the expertise in attack vectors can rapidly bypass those sub-systems simply because the base operating system is the attack vector of major use. The National Security Agency (NSA) in the USA clearly pointed this out in 2000 with its introduction of the “Secure LINUX” project (SELinux – see URL <http://www.nsa.gov/selinux>) when they determined that no commercially available, commodity operating system base was secure!

Moreover, the trend to so-called “web services” structures means that banking and finance systems are moving to complete use of the World Wide Web (WWW) as a means of service delivery to an extent far beyond the current situation. In these systems security is critically dependent upon the safety of the so-called “browser” system which is, itself, often the weakest link.

Microsoft in 2005 clearly proposed that a “separate channel” was needed for safe and secure transaction activity via the PC using the Internet, e.g. home/small business banking, electronic government services, etc. They proposed the use of a form of home “PINPad” similar to the trusted channel system used in Australia for EFTPOS activity. A second choice is the use of a separate phone based verification process, e.g., via voice schemes or SMS message, etc. for each and every transaction or transaction batch.

The important aspect of this discussion is simple:

1. given the manufacturer’s statements re the security of their products, and
2. the level of sophistication of attacks, expertise of attackers and sophistication of attack vectors,

it is obviously, completely unreasonable to expect an uneducated and non-expert end-user to be able to protect their on-line PC system, particularly as high speed, always-on broadband connections come into play, without the addition of industry supplied security products and systems integrated into the overall system.

It is the responsibility of the banking and finance industry, who wish their customers to make use of such unsuitable equipment, to provide the necessary ADD-ON hardware, software and/or alternate verification channel services for secure transactions to take place.

It is the responsibility of ASIC to establish the proper regulatory environment for the banking and finance industry, wishing to effectively compel its customers and the Australian people, to use acknowledged insecure systems for computer and Internet based transactions, to be required to provide the necessary systems to raise the level of security enforcement to an acceptable level against current and likely attacks for the duration of any ASIC regulatory regime. ASIC should be the mechanism for the determination of suitability for use of PC and related systems and for the assignment of necessary cost burdens between users and the banking and finance institutions.

After all, the industry provides merchants with a PINPad terminal and allied security hardware for EFTPOS transactions to be safely made, acknowledging that the simple cash register in a store is not suitable for this purpose! The same is even more important for PCs used for home/business banking and finance transactions.

As with the car, any driver expects the equipment to be safe to use and suitable for the purpose intended. The home/commodity PC and its operating system and middleware systems, such as Internet browser software, etc. DO NOT MEET THIS BASIC REQUIREMENT IN AN UNAIDED FORM. The same also applies to the next generation mobile phone/PDA systems that, in principle, can only be regarded as a highly portable PC.

WJC
070427

References:

A) Evidence that Microsoft Inc, the dominant supplier of technology relevant to ASIC concerns, clearly saw that the PC had to be substantially upgraded in all security senses for trusted transactions to be reliably done via the Internet, particularly in the banking and finance areas as well as in healthcare, government systems, etc.

1. Steeves, D

The paper by D Steeves of Microsoft Inc. and the "PINPad for a PC" Presentation is available at the 1st TIPPI Workshop 2005 website as follows:

URL = <http://crypto.stanford.edu/TIPPI/first/program.html>

1st TIPPI Workshop

Trustworthy Interfaces for Passwords and Personal Information

Speaker: Dave Steeves, Microsoft

Title: Securing Online Transactions with a Trusted Digital Identity

Abstract:

The ever increasing desire to use the web for Online Banking, Trading and E-Commerce is generally countered with a fear of technology and its inherent insecurity. By first defining the problem space that plagues "Online Transactions" and then identifying weaknesses, we can begin to find a secure solution. If the solution is designed by mitigating the threats associated with "Online Transactions", it will become more widely trusted. To solve this problem and have it accepted by users, "Online Transaction" implementations need to be both highly usable and highly secure.

The goal of this talk is to present one idea which would allow secure online transactions to take place on an untrusted computer, over an untrusted internet. This talk will conclude with some current research on creating a trusted digital identity and ask for feedback from the audience.

Bio:

David Steeves is a Security Software Engineer in Microsoft's System Protection Products Team, working to increase security protection offerings to customers. Past work includes forensics, crypto-math and strategic forecasting at the Communication Security Establishment, Ottawa. Masters of Math thesis research with Dr. Panario to break the Powerline cryptosystem at Carleton University and Masters Comp Science research/coursework at U. of Ottawa in Structural Complexity Theory.

2. Microsoft and "Palladium"/NGSCB

This project clearly indicated that the PC as currently deployed IS NOT SAFE AND SECURE for trusted transaction usage. The following is a report from <http://www.eweek.com> of 15 April 2005.

NGSCB, as Microsoft originally outlined it, was to be one of the key components of the company's overarching Trustworthy Computing Initiative.

The two foundations of NGSCB were designed to be the Trusted Platform Module on the hardware side, and the Trusted Operating Root (or "nexus") on the software side.

The nexus was to be the kernel of an isolated software stack that was designed to run inside the standard Windows environment.

The nexus was slated to provide a set of APIs that would enable sealed storage and other foundations for trusted-computing.

The goal for NGSCB was "to marry hardware and software to gain better security," said Jim Allchin, Microsoft's group vice president for platforms.

That continues to be Microsoft's ultimate goal for NGSCB, Allchin said

3. InfoWorld, USA - 30 October 2003.

NGSCB is a combination of hardware and software that creates a second operating environment within a PC that is meant to protect the system from malicious code by providing secure connections between applications, peripheral hardware, memory and storage. NGSCB will make its debut as part of Longhorn, the code name for the next version of Windows expected in 2006.

Microsoft is working with software makers, system integrators and large customers in the financial services, healthcare and government areas to create business applications that use NGSCB, Juarez said. These applications include document signing, secure instant messaging, viewing secure data and secure e-mail, he said.

In the past, Microsoft had also pitched NGSCB as an important technology for consumers. It would be part of the cure for the seemingly endless stream of viruses, worms and security bugs that also hits consumer PCs.

"We're not going to have a consumer story until version two of NGSCB," said Mario Juarez, a product manager at Microsoft's Security Business Unit. No schedule has been set for the release of version two.

4. Microsoft : Windows Platform Design Notes - Design Information for the Microsoft® Windows® Family of Operating Systems Security Model for the Next-Generation Secure Computing Base. (8 May 2003).

This paper is included in this submission as further evidence that the PC is unsuitable, without extensions, for the purposes to which the banking and finance industry wish to put it to use, and is copyright Microsoft Inc. It is publicly available on the Internet as at 27 April 2007 at URL =

http://www.microsoft.com/resources/ngscb/documents/NGSCB_Security_Model.doc

This paper is a critical document for the consideration of ASIC.

5. NewsWeek, 1 July 2002. – The “Palladium” Issue



Brian Smale for Newsweek

The Big Secret

An exclusive first look at Microsoft's ambitious-and risky-plan to remake the personal computer to ensure security, privacy and intellectual property rights. Will you buy it?

By Steven Levy
NEWSWEEK

Microsoft's hyperambitious long-range plan to literally change the architecture of PCs in order to address the concerns of security, privacy and intellectual property. The plan, revealed for the first time to NEWSWEEK, is... Palladium

.....an enticing litany of potential uses.

** Tells you who you're dealing with—and what they're doing. Palladium is all about deciding what's trustworthy. It not only lets your computer know that you're you, but also can limit what arrives (and runs on) your computer, verifying where it comes from and who created it.*

** Protects information. The system uses high-level encryption to “seal” data so that snoops and thieves are thwarted. It also can protect the integrity of documents so that they can't be altered without your knowledge.*

** Stops viruses and worms. Palladium won't run unauthorized programs, so viruses can't trash protected parts of your system.*

** Cans spam. Eventually, commercial pitches for recycled printer cartridges and barnyard porn can be stopped before they hit your inbox—while unsolicited mail that you might want to see can arrive if it has credentials that meet your standards.*

** Safeguards privacy. With Palladium, it's possible not only to seal data on your own computer, but also to send it out to “agents” who can distribute just the discreet pieces you want released to the proper people. Microsofties have nicknamed these services “My Man.” If you apply for a loan, you'd say to the lender, “Get my details from My Man,” which, upon your authorization, would then provide your bank information, etc. Best part: Da Man can't read the information himself, and neither can a hacker who breaks into his system.*

** Controls your information after you send it. Palladium is being offered to the studios and record labels as a way to distribute music and film with “digital rights management” (DRM).*

.....The first adopters will probably be in financial services, health care and government—places where security and privacy are mandated.....

END-REFERENCES