Relearning "Trusted Systems" in an Age of NIIP:
Lessons from the Past for the Future.

Professor William J Caelli
Head - School of Software Engineering and Data Communications
Member and Foundation Director - Information Security Research Centre (ISRC)
Faculty of Information Technology
Queensland University of Technology
Brisbane. Qld. 4000
AUSTRALIA

Abstract:
Current Intel-based computer architecture, at least from the iAPX-286 CPU onwards, owes its security structure in large part to the earlier MULTICS program. This developed from the 1960s to late 1970s to create a secure, time-shared computing environment. However, in current commodity operating systems of today the major security principles of that architecture are largely ignored.

This paper discusses this failure of systems and supporting software systems to use well established security hardware features in computers as a failure in education related to IT security, and even software engineering, over at least the last twenty year period. At the same time, IT systems managers are being asked to consider enhanced security in relation to *National Information Infrastructure Protection (NIIP)* as a cooperative effort between Government and the private sector, against growing international standards. This means that system managers must be able to assess the security "rating" of computer and network hardware, operating systems, "middleware" and applications against requirements of emerging world *"Information Security Management (ISM)"* standards such as ISO 17799. The paper discusses the work at the Queensland University of Technology (QUT) to redevelop an education program in this area, originally commenced in 1988, that is suitable to the needs of its student cohort, which includes a strong representation of Asian / South-East Asian and Scandinavian students. It is aimed at both students who will be involved in security assessment of installed systems as well as more specialised occupations of system design and evaluation, both formal and informal.

Presenter : Prof William J (Bill) Caelli
Contact Details:
Professor William J Caelli
Head – School of Data Communications
Queensland University of Technology (Gardens Point Campus)
GPO Box 2434
Brisbane. Qld. 4001
AUSTRALIA

Phone: +61 – 7 3864 2752 Fax: +61 – 7 – 3221 2384
Email: w.caelli@qut.edu.au

Relearning "Trusted Systems" in an Age of NIIP:
Lessons from the Past for the Future.

Abstract:
Current Intel-based computer architecture, at least from the iAPX-286 CPU onwards, owes its security structure in large part to the earlier MULTICS program. This developed from the 1960s to late 1970s to create a secure, time-shared computing environment. However, in current commodity operating systems of today the major security principles of that architecture are largely ignored.

This paper discusses this failure of systems and supporting software systems to use well established security hardware features in computers as a failure in education related to IT security, and even software engineering, over at least the last twenty year period. At the same time, IT systems managers are being asked to consider enhanced security in relation to *National Information Infrastructure Protection (NIIP)* as a cooperative effort between Government and the private sector, against growing international standards. This means that system managers must be able to assess the security "rating" of computer and network hardware, operating systems, "middleware" and applications against requirements of emerging world *"Information Security Management (ISM)"* standards such as ISO 17799. The paper discusses the work at the Queensland University of Technology (QUT) to redevelop an education program in this area, originally commenced in 1989, that is suitable to the needs of its student cohort, which includes a strong representation of Asian / South-East Asian and Scandinavian students. It is aimed at both students who will be involved in security assessment of installed systems as well as more specialised occupations of system design and evaluation, both formal and informal.

1. Introduction : Trusted Systems and Computer System Architecture : The MULTICS Project to Intel x86 Architecture, via the DEC/VAX.

> *"... Can somebody please tell me why a fault in my sound card driver has to crash my system? I mean, **really**. Think about it."* (VISC-01)

> From: "Herb Lin" <HLin@nas.edu>
> Date: Wed, 9 Jan 2002 22:50:35 -0500
> Subject: announcing a new CSTB report on cybersecurity
>
> ***Cybersecurity Today and Tomorrow: Pay Now or Pay Later***
> *A narrative describing the findings of prior CSTB reports relevant to cybersecurity. Though the most recent of the reports was issued 2 years ago and the oldest 10 years ago, not much has changed with respect to security as it is practiced. The unfortunate reality is that relative to the magnitude of the threat, our ability and willingness to deal with threats has, on balance, changed for the worse, making many of the analyses, findings, and recommendations of these reports all the more relevant, timely, and applicable today.*
> http://www.cstb.org/web/pub_cybersecurity
>
> Herb Lin, Senior Scientist, Computer Science and Telecommunications Board
> National Research Council.
>
> (PRIVATE COMMUNICATION)

The first of the above statements comes from a small magazine published by a New Hampshire, USA, company dedicated to the person who was known in the past as the "system programmer", a position within IT departments now almost totally forgotten in most corporations and the public sector alike. The concern is expressed simply as a question as to why a simple buffer overflow problem can cause a device driver to inherit full system kernel privileges. The answer, of course, is as old as the MULTICS project and the "Ware" report and is clearly provided in all the Intel x86 architecture books. Device and like drivers, particularly where such drivers may originate from a multiple of uncontrolled sources and which need to be integrated into a total operating system environment from another vendor, belong in a separate, controlled "protection ring" (Ring 1) with the "trusted computing base (TCB)" firmly set at highest privilege (Ring 0). The second statement is really a message of despair that the IT industry itself, as well as its users, have really gone backwards in terms of system security over the last ten years. In an Australian and Asian / South-East Asian context this is not surprising given that reports have continuously emphasized that IT investment is still regarded by corporate and public sector management alike as a cost centre that must be contained and minimised. IT security simply becomes a "cost on a cost" in this line of thinking.

The call for more “draconian” legislative measures by Government is the obvious follow-up. That reaction is expected and follows precedents in the car, pharmaceuticals, health-care, airline and like industries. The IT industry has no claim for exemption. Given its importance in National Information Infrastructure Protection (NIIP) and Critical Infrastructure Protection (CIP) there can be no doubt that the question of stronger legislation should be considered and urgently.

These concerns raise the key question as to just how much knowledge and training IT professionals have received and continue to receive in the vital area of operating systems security, "trusted systems" principles and technologies and related topics in computer architecture. In this regard, such professionals need the competence to be able to assess risk in IT systems against defined standards. The evidence is that in most education courses developed over the last twenty years, as the “commoditisation” of the IT industry occurred through the “PC revolution” between the years of 1980 and 2000, fundamentals and practice in basic hardware and operating system security were slowly removed or downgraded.

This paper examines the evidence for this statement and suggests that a reconsideration of computer science courses is needed to provide an emphasis on basic secure computer and operating system principles and structures. Without this, it is submitted, any management group trying to make meaningful statements in relation to information security management, particularly related to new international and national standards and legislation, such as ISO/IEC 17799, privacy legislation, etc., will be unable to check the veracity of statements made to management by IT vendors. In addition, those IT professionals charged with the creation of the next generation of basic operating systems and network interfaces will be left with little appreciation of the underlying principles and history of the area and, in particular, the requirements for equal attention to security evaluation and functionality.

The Queensland University of Technology will again offer in late 2002 a subject of study, viz. “Trusted Systems and Networks”, relevant to the professional appreciation of trusted functionality and evaluation in network oriented workstations and servers. This subject was first envisaged and preparation commenced in the late 1980s but lack of student interest in the subject meant that it did not progress at that time.

2. Segments, pages and rings in the decade of the "Rainbow" series.

At the same time, around 1981, that the "Trusted Computer System Evaluation Criteria (TCSEC)" were being created and promulgated in the USA , Intel Corporation was developing a vital microprocessor that was to become the CPU for the IBM PC/AT system, the iAPX-286. (At the same time, however, it should be noted that Intel was also marketing its iAPX-432, "object-oriented" CPU for larger scale information processing systems.) The 286 was unusual in that it recognised that security had to be a fundamental part of the basic CPU architecture, including all aspects of memory management, I/O control, privilege enforcement, etc. It has been recognised that the earlier Intel 8086 / 8089 / 8087 chip set did not provide any security enforcing features at all and that, even for such systems as Microsoft's

Xenix'86 operating system, an "add-in" memory management hardware facility was needed. (Essentially, such a hardware "add-on" simply provided a "dual-memory" facility to enable separation of application and system memory.) The 286 took the unusual step of incorporating the concepts of "protection rings" and memory segmentation much along the lines of the MULTICS effort of the previous 15 years and the 4 “levels” of protection in the DEC VAX design. This fact as clearly acknowledged by two Intel designers in their 1986 book "The 80286 Architecture" by Morse and Albert (MORS-86), in the following words:

"The 286 protection mechanism was inspired by protection in the MULTICS operating system." (Pg. 190).

Use of this ring structure was suggested in the appropriate Intel reference manuals and the basic structure has not changed to the present, even under the Intel Pentium 4 processor group. It was placed in good use in the "GEMSOS", high-trust operating system developed by Roger Schell in the mid-1980s. It became clearly useful in the development of a high trust kernel structure upon which further trusted functionality could be based.

The reality is that such a structure was ignored when it came to the development and marketing of next generation operating systems, e.g. those based upon or inspired by UNIX, DEC’s VMS, etc.

3. Reality of the Microprocessor Revolution.

3.1 "Freedom" from the corporate data centre - *"Charlie Chaplin"*

The overriding marketing "push" for the IBM PC had moved during the first three years of its life from the "personal" nature of the machine to the business potential arena. “End-user” computing became a theme of the early 1980s as the PC was seen as enabling enterprise managers to bypass the traditional delays in software and systems development apparently associated with the mainframe and corporate data centre arrangement. Speed of system development became the “catchcry” of the period as demand for new information services outstripped programming and systems analysis staff resources. Minimal training and end-user resources became the method of development, coupled with an intense development of “user friendly” systems and software development tools.

An IBM advertisement of the mid-1980s (Fig. 1) demonstrates this philosophy as the *“Charlie Chaplin”* figure, personifying the inexpert, end-user of the system, admires a printed result from the PC. However, the inherent security processes and procedures involved in the corporate data centre structure was simply not mirrored in the new environment. At the same time this spirit of “liberation” from the controls of the mainframe / minicomputer based data centre meant that the operating systems for PCs were created with no security features at all since they were seen as “stand alone”, “personal assistant” devices under the complete control of their owner or user. The complete openness of the early CP/M-80 microcomputer "monitor"

program, moved into the "QDOS" then "MS-DOS" systems and highlighted this open progression with no attention at all by computer professionals developing such systems to IT security. This "openness" quickly spread into the IT education sector.

Figure 1

IBM Advertisement, BYTE Magazine :Dec. 1985.

Programming classes were created around the use of early programming languages on PCs, e.g. Turbo PASCAL, GWBASIC, etc. In the corporate environment, information systems were created and set to work with little to no testing regime and even integration into overall corporate data systems was limited. For Universities, the time-shared minicomputer / mainframe terminal laboratory was replaced by rooms of PCs, not even LAN-networked until the mid-1980s at the best.

3.2 The "Windows'NT" Route.

"At the outset of the NT project, Cutler treated security as an afterthought, another item on a long list of features. Gary Kimura initially handled it, but he also ran file systems, which kept him too busy to pay attention to security…. About a year into the project…Cutler asked Jim Kelly.. to take charge…'Security was a Johnny-come-lately to NT' he realized. Given the late start, he thought it best to roughly duplicate the security offered by Microsoft's Lan Man networking program." (ZACH-94, Pg. 144.)

A close examination of the open literature in relation to the development of the Windows'NT operating system seems to indicate that at no time was basic operating system security foremost in the minds of developers. Moreover, there appears to be no indication that any developer had the specialised education and training in this area needed to create a next generation of secure operating systems. Essentially, security is seen as a network management operation with the basic structure of the workstation left largely intact and relatively "open". At the same time, the earlier research and education into trusted, security kernel structures appears to go largely unnoticed. Of particular note is the decision to not use any of the advanced security features of the Intel x86 architecture, such as segmentation and the four protection ring structure since essentially a "flat memory model" and dual state only protection structure seemed to enable porting of the NT system to then popular RISC architectures, such as MIPS, Intel 860 and the DEC Alpha. Strangely, even Intel's clear statement, in its processor manual for the 386 CPU, stated *"Segmentation provides the basis for protection."* (INTE-91, Pg 5-321) but this was also ignored. Likewise, the lack of interest in the vital ring protection scheme is confirmed by Solomon and Russinovich (SOLO-00), in relation to Microsoft's "Windows 2000" system, the follow-on product to Windows'NT, when they state :

"The architecture of the Intel x86 processor defines four privilege levels, or rings, to protect system code and data from being overwritten either inadvertently or maliciously by code of lesser privilege. Windows 2000 uses level 0 (or ring 0) for kernel mode and privilege level 3 (or ring 3) for user mode. The reason Windows 2000 uses only two levels is that some of the hardware architectures that were supported in the past (such as Compaq Alpha and Silicon Graphics MIPS) implement only two privilege levels.

Although each Win32 process has its own private memory space, kernel-mode operating system and device driver code share a single virtual address space…Windows 2000 doesn't provide any protection to private read/write system memory being used by components running in kernel mode. In other words, once in kernel mode, operating system and ***device driver code*** *has complete access to system space memory and* ***can bypass Windows 2000 security*** *to access objects."* (Pg. 10)

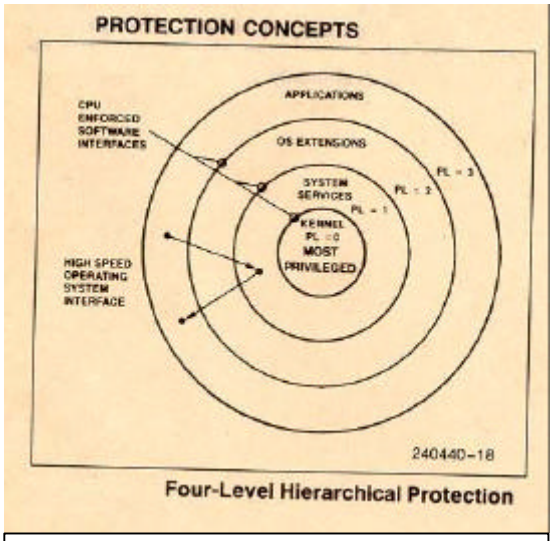


Figure 2 : Intel 386 Ring Usage

They go on to offer the only way around this critical problem, given that many different groups may provide device drivers over time, is to carefully design and test such drivers "to ensure that they don't violate system security." Is there any wonder that the 2001 plug-and-play (PnP) driver buffer overflow problem was of such concern ?

It has to be remembered, in this regard, that all cryptographic sub-systems incorporated likewise as some form of driver set into the system kernel, thus become vulnerable to any device driver in such a system. Device drivers were meant to be isolated in ring 1, not incorporated into ring 0 kernel privileges as illustrated in Fig 2.. The question is one of just what security education was given to system designers in this case. Just what had been learned from engineering experience ? Any attacker only has to simply persuade a user to install a new driver, e.g. for some advanced graphics, sound processing or the like, and that rogue driver could simply take over complete control of the system. Even early Intel manuals demonstrate the need for separation of kernel and device driver structures using the protection ring architecture. In a "*.NET*" environment this takes on new and urgent importance. For example, the "just-in-Time (JIT)" compiler for CIL "assemblies" must itself NOT assume system privileges at Ring 0 or attacks on the compiler become possible. the question is one of just what security education developers in this regime have had or need and just how is that education need being addressed.

The important aspect of these early decisions, from an education and training viewpoint, is that computer security is largely delegated to data network access control and management as well as some form of user surveillance. It is common, at least in Australia, for the banking and finance industry to explain their security parameters to customers in terms of 128-bit cipher, SSL implementation without any discussion at all of the system security at each end of the "line".

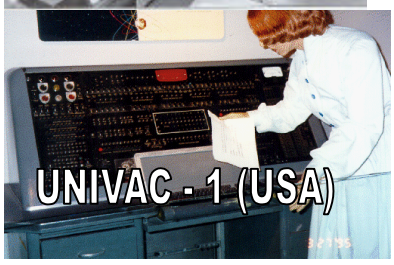
This trend has unfortunately been enhanced over the last five years as cryptography, in the form of digital signatures, public key certificates, and the like have become the "security architecture" for network based systems of the future. This trend totally ignores the fundamental fact that such encryption will only be as secure as the operating system structure in which it sits. The emphasis must then move back to the "TCSEC/Common Criteria" environment and reasonable proof that software and hardware based encryption structures are fully protected. Contrary to accepted ideas, then, the use of cryptography actually enhances the need to reconsider security functionality and evaluation at the operating system and hardware levels in line with the "Common Criteria" (ISO standard 15408).

The question is now one of how universities and colleges respond to the new challenge of providing such a trusted environment through the education of the "fourth generation" of system developers and IT professionals. In turn these professionals need to become concerned about NIIP and the related problem of Critical Infrastructure Protection (CIP) through the systems they create and deploy.

4. Computer Science / Software Engineering Curricula and Education

4.1 The 4 Generations of IT Professionals.

In considering overall education programs in IT security it is valuable to attempt to understand the nature and background to IT education and training itself over the last 60 years. It could be argued that in IT education we have now entered a 4th generation of students and professionals. This is based upon the supposition that the history of IT education and the IT "professional" can be divided into four distinct 20 year periods. These periods may be seen as "generations" that encompass those who started or developed their careers in IT during that period. The four distinct periods may be summarised as shown in Table 1.

Generation	Period (Approx)	Characteristics	System
1 Engineer / Scientists	1940 to 1960	No large separation between hardware and software systems professionals Learn on the job Some specialist subjects offered at Universities Age of the engineer / scientist	 

2 **Elites**	1960 to 1980	The age of the specialist professional Commands and gets due acknowledgement from management First full IT university level courses (not as EE) and acceptance of the “computer science” discipline Industry training programs Separate systems and application programmers Maintenance engineers	  
3 **Professionals vs Hobbyists Hackers and Amateurs**	1980 to 2000	The “diverse” IT manager The “network” and “database” manager “End-user” application developer Diversification of the “profession”	 
4 **Everyone**	2000 - On	Clear separation between “amateur” and “professional” Software development for "K12" “Black-box” systems Legal and societal obligations Commodity appliances	

		vs special systems Programming for a networked environment		

5. The Future - Towards "4th Generation" Professionals

5.1 Beyond cryptography, "code signing", SSL and "know the developer"

There is a disturbing trend in the IT industry to leave security matters to network oriented structures and cryptography. The developing philosophy appears to be one of minimising or even ignoring security at the computer systems level and depending upon networked connection to be carefully monitored and secured. One likely explanation for this is the perception that cryptographic systems may be readily added-in to an already designed, developed and delivered computer systems, be it workstation or server. However, without trusted functionality and evaluation of the underlying operating systems and hardware structures, e.g. FIPS 140-2 evaluation for cryptographic sub-systems, etc., such a philosophy can easily produce a false sense of security. For example, the use of public key certificates may depend upon the actual presence in the systems of a "root" level public key to enable verification of the signature affixed to a user's public key in a certificate. the overall structure then becomes only as secure as the trust in the storage and processing of that "root" key and its association with a trusted entity.

Such cryptographic schemes also make no claim at all as to the veracity and trustworthiness of any program code so signed. Moreover, in a developing trend towards network based software structures as a normal mode of operation of computer programs, it may be practically impossible to make a trust assessment for every program that is required to be run on a users workstation based solely upon some form of knowledge of the originator.

This all points to some new paradigm closely associated with the earlier "B"-Level or "Mandatory Access Control" structures of the USA's TCSEC series. A user or manager needs to be able to carefully and completely define the mandatory security requirements of all subjects and objects that are allowed to operate or exist with a network connected workstation or server. These structures will then need to be enforced to a high level of reliability (EAL-5 ?) by an underlying hardware / system software structure.

The challenge to education is thus obvious. there is an urgent need to re-visit the concepts of trusted systems and to relate them to the emerging needs of a connected network environment.

6. Conclusion - Education and "Trusted Systems" in the 21st Century.

6.1 Teaching "Trusted Systems" again.

The QUT unit of study ("unit"), labelled ITN531, runs for a 13 week period and commences in the second half of 2002. It is aimed at postgraduate (4th year) students or advanced, high achieving undergraduate students. Typically students will be completing a "Masters Degree by Coursework". This follows an early attempt to introduce such a subject of study in the early 1990s for which there was little demand. This has changed as such requirements as the Australian federal Government's "amendments to the 1988 "Privacy Act" came into operation from December 2001. These amendments place new information security obligations on the private sector as well as the Federal public sector, as originally covered.

The metric for due diligence in this one area is determined by the Federal Government "Privacy Commissioner" and is influenced by appropriate standards in the area, such as the Australian / New Zealand Standard SA/NZS ISO/IEC 17799 for "Information Security Management". This standard requires risk analysis and assessment with associated management processes to be clearly identified by management where personally identifiable data are collected and stored. In turn, it can be argued that the metric for that assessment must include appropriate technical standards, such as ISO 15408 for Security Evaluation, as well as normal personal and allied practices and procedures.

The unit is aimed at IT professionals who may be responsible for such analysis and assessment. In particular, the unit aims to equip such students with the ability to create relevant and necessary questions and check lists for computer and data network systems vendors. At the same time, the principles involved will become useful and pertinent to the creation of high-trust applications in the government, health-care, e-commerce and related areas. Already, such evaluation parameters have been set by the Australian Government in relation to public key infrastructure (PKI) under the "Gatekeeper" scheme.

The unit also aims at motivating research oriented students to take up doctoral or masters level research programs in the area within the Information Security Research Centre (ISRC) within the Faculty of Information technology at QUT.

The unit of study consists of 13 weeks of study with the following major formal components each week:

- formal lecture - 1 hour,
- tutorial / discussion session - 1 hour
- laboratory practice - minimum 1 hour.

Students are expected to dedicate a further 8 hours or so to personal study and/or laboratory work.

The laboratory session consists of familiarisation, analysis, testing, management and problem solving with a mandatory access control operating system. The choices at present are:

- LINUX with NSA SeLINUX adaptations,

- QUT *"SESAME"* structures for LINUX (smart card oriented, role-based access control), and
- SUN Trusted Solaris (SPARC base).

Assessment consists of:

- final "open-book" examination of 2 hour duration, based around relevant scenario consideration, (70%)
- a set of 3 related assignments performed throughout the period of study requiring the production of a group of related reports on the topics given, (30%).

Each member of the class receives an individual and unique assignment topic, potentially related to an employment associated activity, if relevant to them particularly if they are part-time students. This has proven to be most welcome by students from the military, government, health-care, banking/finance/insurance and like industries. However, some emphasis is placed on the relevance of the topics to the small to medium enterprise sector, i.e. enterprises with up to 20 employees and annual revenue figures in the less than $20 million (Aust) per year. Each class member is required to create and deliver a twenty minute summary of their assignment topic towards the end of the semester.

Pre-requisite Study

Students will be expected to have studied a number of undergraduate level topics equivalent to the following information security related subjects/units at QUT:

- Data Security
- Network Security and E-Commerce.

In addition basic studies in data networks, operating systems and programming languages are required.

From previous experience, a class cohort of around 35 is expected for 2002.

Course Unit Outline

The course unit outline at QUT consists of a plan of study for the 13 weeks of the semester. The tentative structure for the new unit of study is as follows.

Week Number	Study Topics / Activities
1	History and Background to "Trusted Systems" From the "Ware" report to the "Common Criteria"
2	Market, societal and legal demand for trusted systems
3	The "Common Criteria" - 1
4	The "Common Criteria" - 2
5	The "Common Criteria" - 3 Special Case : The role and place of cryptography
6	Evaluation Methodology - Who, What, Why. The Evaluated Products List (EPL) - Interpreting and understanding

	evaluation reports
7	Creating a "Target of Evaluation (TOE)" - 1
8	Creating a "Target of Evaluation (TOE)" - 2
9	Protection Profiles
10	Specialised needs Network vs server/workstation Embedded systems / consumer products Sub-system evaluation
11	Alternative "evaluation" schemes International, national, IT industry and end-user industry based
12	Current Vendor offerings - Overview and analysis Preparing vendor checklists Determining the "level of trust" in commercial and governmental systems
13	The future

Texts.

There appears to be no single modern textbook, i.e. published after January 2001, yet available to meet the needs of this unit of study. It is planned to use readings from various older texts and relevant published papers, vendor web-sites, EPL reports and publications as well as like materials.

Summary

The new unit sits at the "top" of a number of specific information security subjects which have been offered at QUT for over 12 years. Other undergraduate and postgraduate units of study include:

Undergraduate

ITB523	Data Security	(Initial unit of study)
ITB566	Introduction to Cryptology	(Basic cryptology unit)
ITB569	Network Security and E-Commerce	

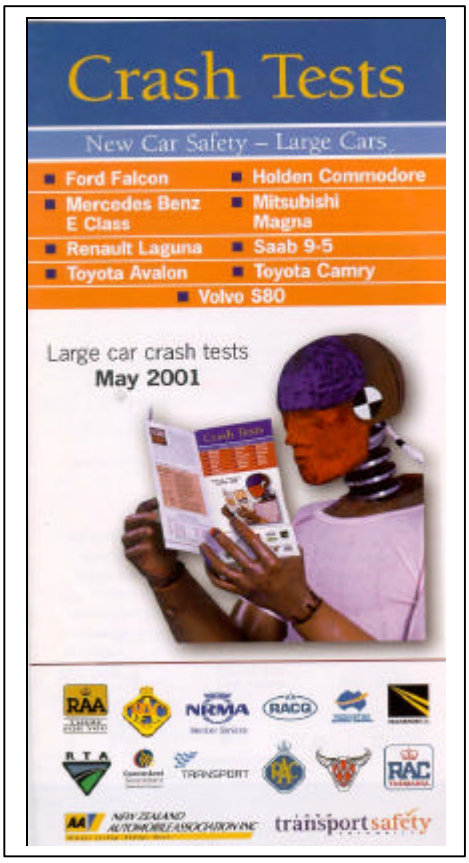
Postgraduate

ITN567	Access Control
ITN536	Topics in Security
ITN556	Advanced Topics in Cryptology

The undergraduate units of study are also offered in a post-graduate format for those undertaking the “Graduate Certificate” or “Graduate Diploma” in information security or the “Masters by Coursework” degree. Information security also enters other units of study as appropriate, including such units as those concerned with “wireless networks”, “network management”, “network administration”, etc.

Conclusion.

The new unit of study at QUT is aimed at resurrecting professional interest in basic system security at the computer level. Only by having educated professionals in this area will it be possible to promote the necessity for enhanced security in information



systems to enterprise management. It is only through new purchasing requirements from user management that IT vendors will themselves take on new responsibility for a next generation of secure computers and operating systems. The only other way is for government to follow what has been done for the car, pharmaceutical and like industries and that means strong and determined safety and security related legislation for the IT industry.

Unfortunately, the willingness of governments to act in this regard has almost disappeared over the last 20 years. Perhaps it needs a new *"Ralph Nader"* to target the IT industry for that direction to succeed. After all, in the car industry we do have mandatory safety and security standards that are legally binding on that industry.

Moreover, we consider it essential to relentlessly smash new cars to determine weaknesses, with full governmental encouragement and support. What about the computer industry ?

7. References:

INTE-83 Intel Corporation
"iAPX 286 Hardware Reference Manual",
Intel Corporation, USA, Order No. 210760-001, 1983

INTE-91 Intel Corporation
"Microprocessors, Volume II",
Intel Corporation, USA, 1991. ISBN 1-55512-115-2

LIPN-2001 Lipner, S
"IT Security Requirements"
Presentation to the NIAP Government-Industry IT Security Forum
"Strategies for the Development of Security Requirements and Specifications for Computing and Real-Time Control Systems"
7 March 2001
Available on the NIST / NIAP web site as at 14 Jan 2001 as :
http://niap.nist.gov/niap/events/govind-forum/proceedings/

MORS-86 Morse, S and Albert D.
"The 80286 Architecture",
John Wiley & Sons, New York, USA, 1986. ISBN 0-471-83185-9

ORGA-72 Organick, Elliott, I
“The Multics System: an examination of its structure”,
MIT Press, USA. 1972, ISBN 0262150123

SCHE-01 Schell, R
“Security Requirements for Operating Systems : A View from 30 Years Experience”
Presentation to the NIAP Government-Industry IT Security Forum
“Strategies for the Development of Security Requirements and Specifications for Computing and Real-Time Control Systems”
7 March 2001
Available on the NIST / NIAP web site at 14 Jan 2001 as:
http://niap.nist.gov/niap/events/govind-forum/proceedings/

SOLO-00 Solomon, D and Russinovich, M
"Inside Microsoft Windows 2000" - Third Edition
Microsoft Press, Redmond, Washington. USA., 2000.
ISBN 0-7356-1021-5

VISC-01 Viscarola, P
“Peter Pontificates : I Dream of ... A New Version of Windows.”
The NT Insider, OSR Open Systems Resources, Inc., Vol. 8, Issue 4, July-August 2001.

ZACH-94 Zachary, G Pascal
"Show-Stopper ! The Breakneck Race to Create Windows NT and the Next Generation at Microsoft",
The Free Press, New York, 1994, ISBN 0-02-935671-7