

## Trends and Challenges in the Security of Information Systems and Networks

Prof. William J (Bill) Caelli, AO  
Queensland University of Technology  
Brisbane, Queensland.  
Australia  
Email: w.caelli@qut.edu.au

Presentation to the Information Security Workshop  
OECD and APEC  
Seoul, Republic of Korea  
September 5-6, 2005

5 Sept 2005

W. Caelli (QUT)

1

### THEMES – 2005:

- **Government** reaction and public policy in a situation of market failure.
- **Challenges:**
  - ICT Industry – regulation ?
  - Application systems – requirements ?
  - Users – expectations !
- **R&D & Education/Training/Certification:**
  - Challenges
  - National competencies

5 Sept 2005

W. Caelli (QUT)

2

## THEMES – 2005:

- **Government** reaction and public policy in a situation of **market failure**.
- **Challenges:**
  - ICT Industry – regulation ?
  - Application systems – requirements ?
  - Users – expectations !
- **R&D and Education/Training/Certification:**
  - Challenges
  - National competencies

5 Sept 2005

W. Caelli (QUT)

3

## **Government** reaction and public policy in a situation of **market failure**.

### Accepted:

- ICT industry supplies against market demand and/or regulation-legislation
- Application customers buy ICT security against perceived needs and/or regulation-legislation (usually latter)
- End-users are **NOT** IT experts – getting frustrated!

5 Sept 2005

W. Caelli (QUT)




4

## POLICY FOR PARTICIPANTS

Manufacturer / Vendor

Vertical industry application

User

↓

**CAR**

**TAXI**

**DRIVER**


5 Sept 2005
W. Caelli (QUT)
5

## SUMMARY PROPOSITION - 2005

The personal computer (PC), and server systems based around it, are not suitable for safe and secure business transaction usage without substantial security enhancement, including add-in hardware bases.

This includes:

- e-government
- e-health
- banking/finance



5 Sept 2005
W. Caelli (QUT)
6

## SUMMARY PROPOSITION - 2005

***IT'S NOT THE 'NET,  
IT'S THE NODES !***



5 Sept 2005

W. Caelli (QUT)

7

## THEMES – 2005:

- **Government** reaction and public policy in a situation of market failure.
- **Challenges:**
  - ICT Industry – regulation ?
  - Application systems – requirements?
  - Users – expectations !
- **R&D and Education/Training/Certification:**
  - Challenges
  - National competencies


5 Sept 2005

W. Caelli (QUT)

8

## ICT INDUSTRY


- Regulation
- Patching = software quality - NOT security
- Secure by design/implementation
  - Allow for software problems – **“fail-soft”**
- Generic systems
  - SELinux – gaining market momentum BUT CIO understanding?
  - TPM / VMs – enough ? (NGSCB - ??)
  - Threat from “web services”, middleware & software “component” / driver libraries



5 Sept 2005 W. Caelli (QUT) 9

## ICT INDUSTRY

- Role and function of the ISP
  - Gatekeeper?
- Making the “Common Criteria” better and more industry relevant today & enforcing Government purchasing policy for security evaluated systems
  - Create the necessary lead!



5 Sept 2005 W. Caelli (QUT) 10

## APPLICATION SYSTEMS



- External security enforcement
  - “PINPad”
  - WYSIWYS
    - “What-You-See-Is-What-You-Sign”
- Responsibility of vendor/supplier, e.g. bank, Health Department, etc.

5 Sept 2005

W. Caelli (QUT)

11

## USERS

**STOP** blaming the user –  
**START** blaming the vendors !

Patching  
Firewall  
Anti-virus  
Anti-spyware  
Anti-spam

e.g.  
**Virus =**  
**failure of OS integrity**  
**/ access control**

5 Sept 2005

W. Caelli (QUT)

12

"Your Money and Your Life" – Four Corners**QUENTIN McDERMOTT:**

This advice is standard, and there's no shortage of it from banks and credit card companies. In fact, there's a great deal of advice, much of it complex and difficult to master.

**ALAN PALLER:**

Their line is, "You users are to blame." They don't say it in those words. They say, "You users should follow our 16-step process." There isn't a grandmother in the world who can follow those, and there aren't many sons and daughters and even smart school kids who can follow that advice. Most of it was written by people who've never actually done it. If they'd done it, they wouldn't have written it that way. So the problem is that the people who sell the software, sell the hardware and sell the services have decided to blame the user.

5 Sept 2005

W. Caelli (QUT)

13

**THEMES – 2005:**

- **Government** reaction and public policy in a situation of market failure.
- **Challenges:**
  - ICT Industry – regulation ?
  - Application systems – requirements ?
  - Users – expectations !
- **R&D & Education/Training/Certification:**
  - Challenges
  - National competencies

5 Sept 2005

W. Caelli (QUT)

14

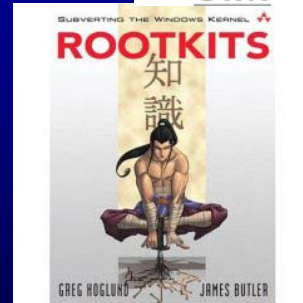
## CHALLENGES

### Research and Development

- CRA / USA – 4 challenges in R&D
- Enhancing OS/Middleware
- MAC/RBAC

### Threats

- Expertise (on the other side)
- Broadband
  - “Zero-day” virus/worm/Trojan
- Web services / moving the perimeter



5 Sept 2005

W. Caelli (QUT)

15

## EDUCATION / TRAINING /CERTIFICATION

- Expertise at tertiary college / uni level?
  - USA – PITAC Report 2005
- Small/medium enterprises?
- Certification of IT security professionals

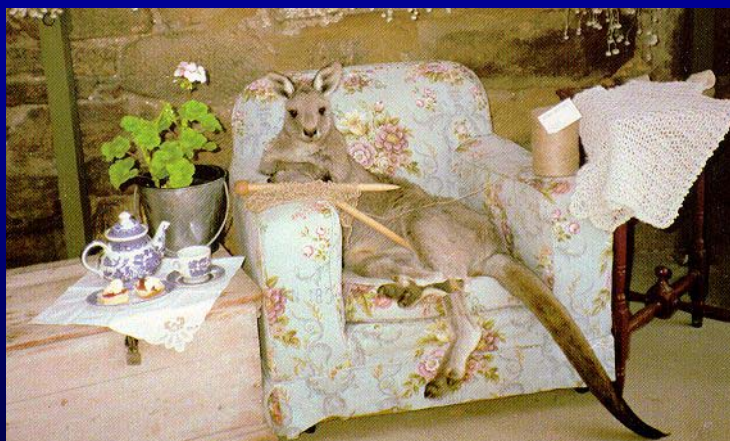


5 Sept 2005

W. Caelli (QUT)

16

**THANK YOU**



**QUESTIONS ?**

5 Sept 2005

W. Caelli (QUT)

17