



Cyber Security

Enabling Transformation

Dr Malcolm Shore
Head of Security, Telecom NZ
Senior Fellow, Canterbury University

Cyber Threats



The Landscape

Malicious software

- Confiker October 2008..... Still effective
- Increasingly sophisticated variants – Confiker F

Botnets

- Increasingly sophisticated
- Fast flux networks
- Botnet-to-rent
- Recent DDoS measured at 40Gb/s on a target

Cybercrime

- Is it bigger than drug dealing?
- Highly motivated adversaries
- Safe havens exist

Information Warfare

- Moonlight Maze
- Titan Rain
- Estonia
- Every country.....

System Resilience

- Continues to be a challenge.....

Cyber security research strategy



Maintain a secure environment

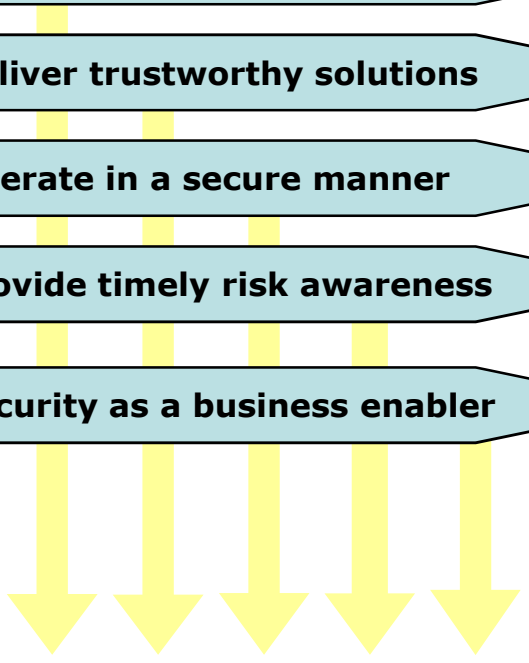
Deliver trustworthy solutions

Operate in a secure manner

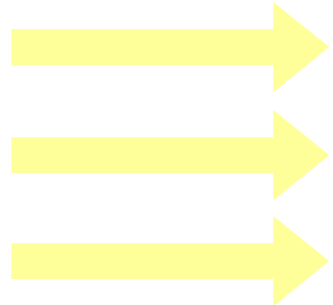
Provide timely risk awareness

Security as a business enabler

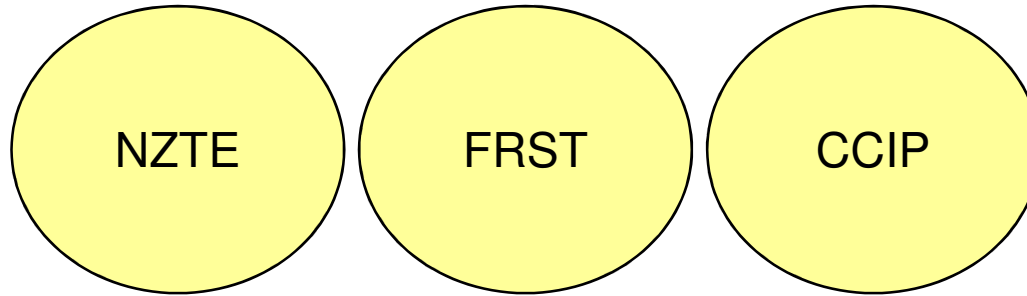
Ensure the protection of Telecom and its customers from security breaches



Cyber security research through partnerships



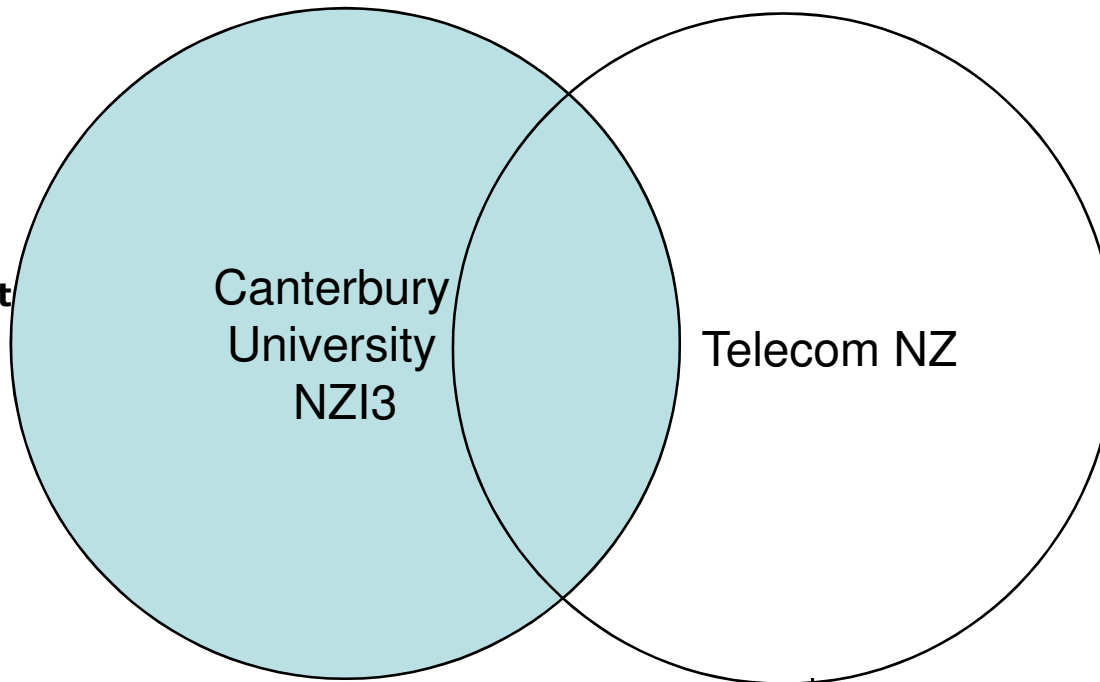
Cyber security research relationships



**Post Graduate
Security Course**

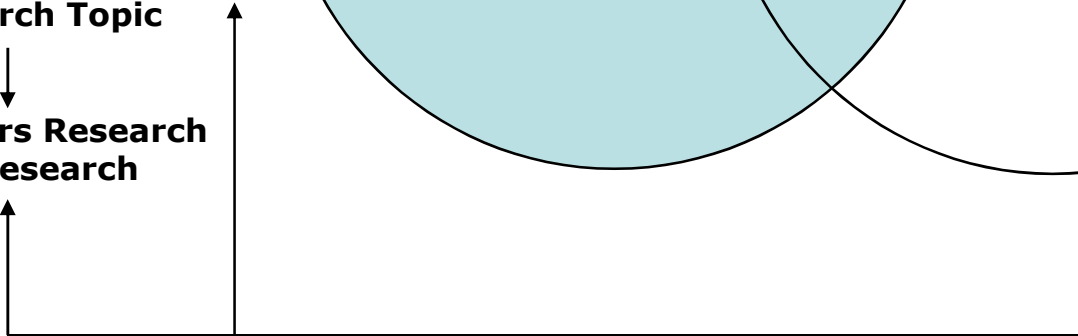
**Security Management
Network Security
Secure Software
Forensics
Identity & Access
Information Warfare
Research Topic**

**Masters Research
PhD Research**



**Lines
Wholesale**

**Mobile
Broadband
ICT services
Security Services**



Cyber security research strategy



Challenges for Telecom

Telecom is an important part of the national critical infrastructure, but thinking around critical infrastructure, especially security and survivability of networks, is still in its infancy. Telecom is instrumental in driving this forward in the NZ telecommunications industry.

- Security investment is per-project and focused on engineering
- No collaborative support from strategic partners
- Limited resource priority for cybersecurity research
- Academic research is a short-term focused activity
- No clear focus or direction on critical infrastructure protection

Challenges for Canterbury University

Canterbury University has an advanced security teaching programme and collaborative ties to the equivalent programme in the University of South Australia. A recent review by the University has indicated a need to increase resourcing for this programme.

- No national programme of information assurance teaching and research
- Focus on academic achievement

Cyber security research -past

Maintain a secure environment



Evaluation Techniques for IDS (Ting-Yi Chu)



The IDS evaluation project involved surveying the IDS field to determine a taxonomy of IDS functionality, developing a methodology for evaluating IDS equipment, to ascertain its relative effectiveness. The project also delivered an attack

generator which could be used for testing devices. The attack generator was shown to be able to mimic the kind of attacks seen through malware using port scans and SYN style attacks, as well as more specific techniques used in the Blaster, Smurf, SQL Slammer attacks. The Esphion SP5000 IDS was used to validate the methodology and generation capability.

Ms Chu now works in the Security Operations Centre, Telecom NZ

Cyber security research - present

Maintain a secure environment



Juniper Netscreen SIEM integration (M Pearce)



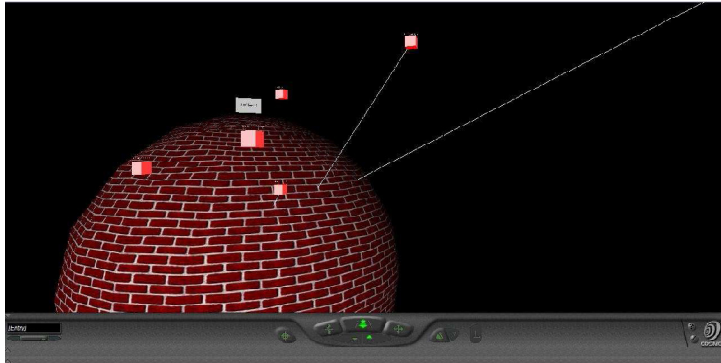
This research focuses on trialling the effectiveness of a range of SIEM tools to deliver event correlation from the Juniper Netscreen firewalls. Of particular interest will be the ability to link the source of external scans and probes to identified traffic inside the firewall, to detect a successful intrusion. This is based on the likely multi-stage nature of cyber attacks.

Cyber security research -past

Maintain a secure environment

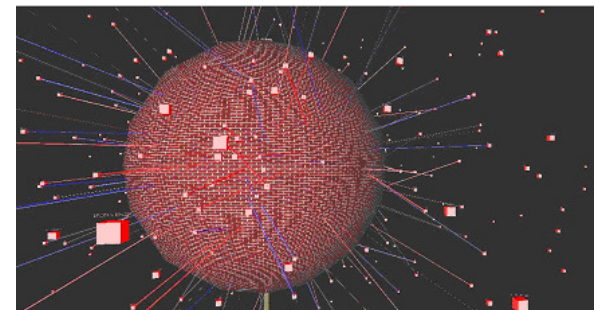


Network Security 3D Visualisation (Tri Minh Pham)



The purpose of this project was to look at a technical solution for 3D visualisation of networks, providing a 'fly-through' view of external, DMZ and internal networks. The original concept was to use a 3D world such as Second Life or Exit

Reality, but the research demonstrated that the most effective approach was to use VRML. One of the interesting challenges was creating an effective algorithm for spatial representation of the nodes based on their network address. Getting data into the VRML session in real time also proved difficult, requiring a re-read of a configuration file rather than having any event driven capability. Nevertheless, the work demonstrated the dynamic 3D power of VRML.



Cyber security research - future

Maintain a secure environment



Firewall Rule 3D Visualisation (tba)

The screenshot shows a Juniper Netscreen firewall rule configuration window. The main table lists several rules with columns for Name, Source, Application, Dest, Type, Operator, Admins, System, and Action. A context menu is open over rule 12, showing options like 'Add Rule', 'Delete Rule', 'Copy Rule', 'Move Up', 'Move Down', 'Support', and 'Export'.

Name	Source	Application	Dest	Type	Operator	Admins	System	Action
1	Block P-IP		Any	Any	Deny	AF Admin	Any	Deny
2	Block P-IP over P-IP		Any	Any	Deny	AF Admin	Any	Deny
3	Block P-IP over P-IP		Any	Any	Deny	AF Admin	Any	Deny
4	Allow-HTTP		Any	Any	Allow	AF Admin	Any	Allow
5	Allow-HTTPS		Any	Any	Allow	AF Admin	Any	Allow
6	Allow-SSH		Any	Any	Allow	AF Admin	Any	Allow
7	Allow-FTP		Any	Any	Allow	AF Admin	Any	Allow
8	Allow-TELNET		Any	Any	Allow	AF Admin	Any	Allow
9	Block local file sharing		Any	Any	Deny	AF Admin	Any	Deny
10	Block Windows updates		Any	Any	Deny	AF Admin	Any	Deny
11	Allow-HTTP		Any	Any	Allow	AF Admin	Any	Allow
12	Allow-HTTPS		Any	Any	Allow	AF Admin	Any	Allow
13	Allow-SSH		Any	Any	Allow	AF Admin	Any	Allow
14	Allow-FTP		Any	Any	Allow	AF Admin	Any	Allow
15	Allow-TELNET		Any	Any	Allow	AF Admin	Any	Allow

This project will follow on from the 3D network visualisation with a specific visualisation of Juniper Netscreen firewall rules. The objective will be to demonstrate that visualisation can more easily highlight discrepancies than manual rule review.

The intention is to deliver a product which can be commercialised and become an ongoing production capability for the Security Operations Centre.

Cyber security research - past

Deliver trustworthy solutions



Advanced Protocol to Defeat SIP Flooding (Xianglin Deng)



Use of the Jain Slee Rhino development system to develop a new protocol for combating advanced SIP flooding. Penetration of commercial SIP servers was demonstrated using a variable load flooding tool. The Jain Slee SIP server was modified to

become a security-enhanced SIP server using a known address synchronisation protocol. This successfully combated the attack across a range of flooding techniques based on malicious INVITE, CANCEL, OK requests.

Ms Xianglin Deng is now working at Alcatel-Lucent and continuing to collaborate in research work with Telecom NZ.

Cyber security research - past

Deliver trustworthy solutions



Secure Short Transaction Architecture (Andrew Gin)



A significant factor underpinning pervasive deployment of EFT-POS was development and deployment of the specifically-architected "Telecom Transaction Service" (TTS) network capability. TTS was based on the best legacy protocols of the period – HDLC(NRM) on the terminal side, X.25 on the bank switch delivery side – and a simple "connectionless" datagram transport layer protocol known as AS2805.1(1985) using PSTN dial-up access. With the transition to next generation networks, EFT-POS must become an IP application over shared IP networking infrastructure, rather than a dedicated network solution. This research trialled and compared an Internet and a private IP network solution for building secure short transactions, again using the Jain Slee environment.

Cyber security research - present

Deliver trustworthy solutions



Critical Infrastructure Survivability (M Shore/X Deng)



The increasing awareness of governments of the vulnerability of and threats to national critical infrastructures is bringing into focus the need for survivable telecommunications networks. This research is focused on delivering a means of assessing the level of survivability of a network, and defining the correct security policy architecture to support both government and provider business drivers. This research will deliver a survivability overlay for the SABSA end-to-end security framework.

Cyber security research - future

Security as a business enabler

Web Notification Service (tba)



This project involves trials on the deployment of an automated internet security draft web notification service, through integration with IDS sensors. This enables a sensor placed on the Internet with visibility across Telecom's address space to automatically notify Telecom customers via their web browser of malicious activity. The trials will be based on the ICAP protocol (RFC3507) and the research will determine the extent to which real time notification can usefully be deployed as an early warning system.

Cyber security research - future

Security as a business enabler



DDoS Mitigation



This project involves trials on various DDoS mitigation technologies, to determine an effective technology to underpin a future service for businesses. Existing vendor technologies provide a part of this solution, and advanced work on squid farms and other traffic sink technologies will be trialled to determine their ability to provide additional capability for the emerging types of attacks and in both fixed and wireless critical broadband environments.

Cybersecurity going forward



Cybersecurity research as we do it today....

...but with a vision of

A Strategy for Information Assurance

Information Assurance Education

- Leveraging existing academic programmes

Cybersecurity National Lead

- Responsible for setting policy and standards
- Built on a public/private partnership
- Accountable for delivering a protected infrastructure

Centre of Cybersecurity Excellence

- Leverage existing innovation capability, eg NZI3
- Encouragement for industry collaboration
- Encouragement for international collaboration

Conclusions



The cyber security research programme has leveraged Telecom's relationships with the academic community to focus talented individuals on specific problems. This has been relatively successful. The level of investment in cybersecurity research has fluctuated as the economic imperatives for Telecom and the government approach to research funding have changed.

There would be benefits in moving into more collaborative research around the business-application security and security infrastructure, with clear national leadership.

Threat detection, advanced visualisation and reporting, more protection in customer services and, in extremis, critical infrastructure survivability are major areas which can benefit from further research.