Knowledge Transfer Network
ICT

Technology Strategy Board
Driving Innovation

Cyber Security:
The Changing Nature of the Threat

A Presentation to IUA, 19th October 2011

Tony Dyhouse

ICT Knowledge Transfer Network

QinetiQ

A rampage through history and horror…

The First?

- **~1957 - blind 8 year old Joe Engressia ('Whistler' pre 1991/ 'Joybubbles' 1991 until his death 8/8/07) rang answerphone messages**
  - **He whistled to himself while he did this, and found that sometimes the call would stop dead - as he had perfect pitch, he realised E above middle C (2600hz) made this happen**
  - **He had stumbled on the tone for in-band reset of the telephone trunk**

- **Free long-distance calls = connect to telephone exchange; dial a free (800) via trunk; send 2600hz to reset trunk but not hang up; dial wherever you like**

- **1971 - John Draper ('Cap'n Crunch'), running a pirate radio station, was contacted by phone phreaks, who explained the whistle in cereal was 2600hz**
  - **He agreed to create an electronic version (blue box)**
    - Jailed in 1972 and 1976
  - **Also made+sold by 13yo Steve Wozniak ('Berkeley Blue') and Steve Jobs ('Oak Toebark')**
    - Draper claims Apple I was made from blue box profits

Pre 1990

- “Band of Brothers”. Egos and underground. ID theft for mainframe account access only. Carding to fund online costs only (anything else bad form)
- Altos Chat (like IRC, Altos Computer Systems in Hamburg). Realtime X.25. Pad and Gandalf “met” on Altos Chat
- Electron (Richard Jones) and Phoenix (Nahshon Even-Chaim) and NOM (David Woodcock) from Melbourne chatted at The Realm. All later prosecuted by the AFP.
- Suelette Dreyfus (1997). Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier. Mandarin. ISBN 1-86330-595-5. (Free electronic edition)
- 1982 CIA, Reagan and Siberian Pipeline. Largest non-nuclear explosion seen from space. Disclosed in 2004.
- 1985-1989: Cuckoo’s Egg. Clifford Stoll noticed 75c accounting error Lawrence Berkley Labs. Hagbard Celine, Hess, Peter Kahl, Pengo passed info to KGB. Hagbard dead in wood burned with petrol. Suicide.
- 1989 Worms Against Nuclear Killers worm. Brought down NASA systems days before launch of Galileo spacecraft which had Plutonium-based PSUs. Melbourne hackers Electron and Phoenix suspected.
- 1998: Cult of The Dead Cow’s Back Orifice – Landmark RAT

1990's – 2000

- Carding for goods (jet skis)
- Identity theft for fraud (fake financial accounts)
- No honour amongst thieves (Secret Service driven)
- 1998 "Solar Sunrise" attack on US DoD by Israeli Ehud Tenenbaum (The Analyzer). Arrested. Freed. CTO of company. Jailed in 2008 ATM fraud in Canada.
- 1999 Moonlight Maze. Co-ordinated attacks on US Federal & Subcontractors.
- 2000: 16 yr old Canadian Michael Calce "MafiaBoy" DDoS against Yahoo, Amazon, Dell, eBay, CNN. Project Rivolta (riot in Italian). $1.2bn damage.
- SQL Injection and cross-site scripting. Revival in progess.
- 8LGM (8-Legged Groove Machine) by Pad & Gandalf. Later joined by Wandii. Compromised FTSE, NASA, MoD, Oracle, and FO. Released "Advisories". Gandalf & Pad served time. Wandii "addicted to computers".

2000 - 2007

- 9/11 drives underground “If guns are outlawed only outlaws have guns”.
- Carding goes mainstream. Online fraud profits out-strip drug dealing
- Phishing, Spear-phishing, Whale-phishing
- Rise of DDoS blackmail (Insurable?)
- 2003 Titan Rain against US Feds & UK FCO. Shawn Carpenter from Sandia tracked to Guangdong, PRC. Fired for going outside of US Law to gather evidence. Sued for wrongful termination and defamation won $4.7M in 2007.
- 2004 German Sven Jaschan virus disabled Delta Airlines - $500M damage.
- 2005 Sumito bank key-loggers in attempt to steal £220M. Cleaners inserted the key-loggers. Video tapes blank.
- 2006 U3 USB sticks by SanDisk – autorun
- 2007 Zeus botnet for sale and Estonia attacks (moved Bronze statue of Tallinn)
- 2007 TJX dept store lost 45 million cc’s estimated cost $250M
- 2007-8 Hannaford Bros Grocers. 4.2M cc’s estimated cost $252M

2008 - today

- 2008 Heartland Payment Systems lost $140M in stolen cc's
- 2009 Ghostnet infiltration of 1,295 computers in 103 countries
- 2010 Bredolab - 143 C&C at LeaseWeb seized by Dutch. Countered with 220,000 DDoS.
- 2010 Aurora attacks against Google and Yahoo. Also Adobe, Northrop Grumman, Rackspace, Dow Chemical, Symantec.
- 2010 Stuxnet. 4 Zero days.Iranian nuclear programme. Siemens centrifuge controllers.
- 2011 Night Dragon attacks against 5 (unnamed) Petrochemical giants discovered. Started 2009.
- 2011 Shady RAT (72 targets across 14 countries) Mitsubishi, International Olympic Committee, UN, several Security firms, Steel Industry, 13 Defence firms, Oil, Gas & Energy, CIA, FBI, Sony, SOCA, Citigroup, Govts of Canada, Vietnam, Taiwan. Began 2006.
- Hacktivism impacts commerce (Anonymous, LulzSec)
- 2011 Lurid attacks. 47 victims across 61 countries but mostly Russia, Vietnam and Kazakhstan… by UK and US?

The Present?

Knowledge Transfer Network
ICT

Technology Strategy Board
Driving Innovation

Digital Society – The Good, The Bad and The Ugly

More static hardware

More mobile devices

More connectivity

More e-Business

More online services

More hackers

More targets

More vulnerabilities

More online fraud

1. Script Kiddies

Who?

- Bored teenagers
- Live in online social world where they build their hacking skills
- Don’t know where or how to use these skills

Why?

- Ego
- Practice skills
- Impress peers

2. Hacking groups

Who?

- Loosely connected online groups of script kiddies

Why?

- Ego
- Impress friend, outdo each other

Knowledge Transfer Network
ICT

Technology Strategy Board
Driving Innovation

Zone-h.org

Total notifications: 2,187 of which 532 single ip and 1,655 mass defacements

Legend:
H Homepage defacement
M Mass defacement (click to view all defacements of this IP)
R Re-defacement (click to view all defacements of this site)

Time	Notifier	H	M	R	Domain	OS	View
15:37	TR0xiT	H	M		cafesaffron.com.au	Linux	mirror
15:37	ali ahmady	H	M		enochmukiibi.net	Linux	mirror
15:37	SnA!pEr.7rB		M		www.hmsalriyadh.com/vb/	Linux	mirror
15:37	SnA!pEr.7rB		M		www.hosudan.com/vb/	Linux	mirror
15:37	Hmei7				blog.weststu.com/indonesia.htm	Win 2003	mirror
15:37	TeAm Dr.HaCkEr	H		R	oroquietacity.gov.ph	Linux	mirror

3. (H)Activists

Who?

- Groups of hackers connected by a cause, eg Anonymous, Lulzsec
- Use hacking skills to attack organisations they dislike
- Frequently find new causes… sometimes ask!

Why?

- Disagree with something your company does – pollution, business practices, employee treatment
- Dislike of business in general (anti-capitalist)
- Targets may not be rational, or have a clear motive
- Stated aim to cause mayhem and disruption

4. Organised crime

Who?

- Highly organised and skilled groups
- Have vast botnets at their control which monitor for sensitive information and infect other computers
- Money making spam
- Use data to steel identities
- Sell data to fraudsters and blackmailers

Why?

- Make vast amounts money

Whilst not DDoSing…

Pay per Install

Get that herd installing! 20p per install
Small herd of 10,000 yields £2,000
Medium herd of 150,000 yields £30,000

Website of advertisements (eg Google AdSense)

Get that herd clicking!
Implement website full of “pay per click” advertisements
Instruct your herd to all visit and automatically click all the adverts

Manipulate polls and votes

Get that herd voting!
Every IP address has a vote
Change the odds in that online game

Grow the herd!

Get that herd stealing other herds!

5. Nation states

Who?

- Arms of national governments
- Steel huge amounts of data and filter for something useful

Why?

- Steal data of value to their country
- Intellectual property, research, corporate deals, military plans
- Detail of critical infrastructure, including economics

Tan Dailan (Wicked or Withered Rose)

- Network Crack Program Hacker 2004
- Recruited by Chinese military 2005. Trained
- In DoD systems 2006
- Speciality Microsoft Office trojans
- Not State protected? Arrested 2010?

What can you do about it?

Simple precautions to minimise the risk of compromise

1. Good Practice

Risk Management

- Define (critical) Assets
- Define Threats and vulnerabilities
- Assess Impact
- Document
- Spend Budget
- Measure!

2. Good Practice

People.

Process.

Technology.

3. Good Practice. People.

Your staff are your weakest link.

- Ensure staff have basic security training, eg, what constitutes a suspicious email
- Develop basic security policies, eg, password protect phones and laptops - AUP
- Staff of 3rd party providers become yours
- Background checks

4. Good Practice. Process.

When you're up to your neck in alligators, it's easy to forget that the initial objective was to drain the swamp.

- Starter and leaver process
- Near miss incident reporting
- REGULAR awareness briefings with examples
- Code of Connection for 3rd parties (ISO27001)
- If you don't need it don't keep it. Thinning process
- Backup. Restore!
- Secure disposal
- Incident response and recovery (DR, BCP)

5. Good Practice. Technology.

Don’t bin the firewall yet!

- Layered defences - AV
- If you don’t need it disable it
- Not just for compliance – Information (lots of it)
- Ensure required level of competence available
- Update and patch
- Pentest!

Knowledge Transfer Network
ICT

Technology Strategy Board
Driving Innovation

Thank You

Tony Dyhouse

tony.dyhouse@ictktn.org.uk