Successful Ageing Seminar

Cyber Communication

The perils of the online environment and how to keep safe

23 September 2011

UniSA

Dr Norton Jackson AM

Master of Ceremonies

Cybercrime: how to keep safe online

Professor Jill Slay AM
Professor of Forensic Computing
Dean: Research
Division of IT, Engineering and the Environment
University of South Australia

Overview

- Motivation
- Collaboration
- Forensic Computing
- The Challenge
- How to keep safe online

Motivation for research in cybercrime, security and forensics

- A personal response to War on Terrorism
- “Failure of complex socio-technical systems”
- Advice to teach people to secure their systems
- Implies that all our research acknowledges the human dimension in security, forensics and cybercrime
- Have background in engineering, IT and social science.

Collaboration with SAPOL

- Since 2003 Slay and Blundell (plus students and colleagues) have researched
  - Harddisk forensics
  - Network forensics
  - Mobile phone forensics
  - Development of national standards for software validation
  - Wii, Ipod, VoIP (SKYPE), Google Desktop
  - Culture and Forensics
  - E-discovery and Forensics
  - Drug crime and the Internet
  - Process control and forensics

5 PhDs, 20 odd honours grads, > 50 papers complete.

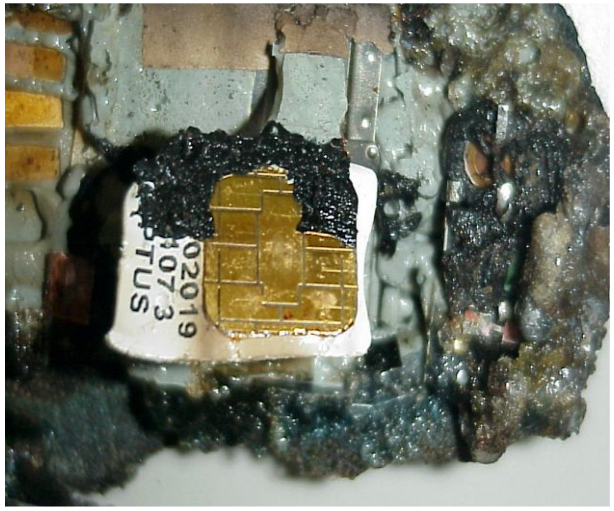
8 PhDs in progress

Definitions

- Forensic Computing is:
  - the application of computer science to the process of collecting digital evidence from electronic storage mediums in such a way as to preserve the state of the original item.
  - done according to the established rules of gathering evidence that is to be presented to a court of law.
  - broken down into the four key areas of **identification**, **preservation**, **analysis** and **presentation**

Rules of Forensic Computing

1. Minimal Handling of the Original – must not change the evidence (and this is hard)
2. Account for any change – because sometimes we can't help this
3. Comply with the rules of evidence
4. Don't exceed your knowledge



The Challenge

- ‘Everyone has the right to life, liberty and security of person’. (Declaration of Human Rights)
- Challenges to the security of person have changed dramatically.
- Inter-connectivity via the Internet has seen the growth of crime and even ‘weaponisation’ of computer and communication networks and the complex control systems of major national utilities.
- How can security of person may be provided in such an environment?

How to keep safe online?

- Don’t give family and friends your password, and don’t write them down.
- Use different passwords for different accounts.
- Don’t put personal details on your social media pages
- Frequently check your security settings on Facebook
- Never reply to an email or click on any links in an email offering you money or asking you to verify your bank account details.
- Don’t put anything in an email that you wouldn’t write on a postcard.
- If you are regularly using a credit card for online purchases, get a card with a small limit, such as $1000.

Being more systematic

- http://www.staysmartonline.gov.au/
- Has help on many issues
- Many other similar sites

Being more systematic

- **Use only supported operating systems**
- **Enable automatic updates of your operating system**
  - Factsheet 23, Setting up automatic updates for Windows 7;
- **Install and update security software which provides functionality for anti-virus, anti-spyware and a personal firewall.**
  - See Factsheet 18, Free security software for non-commercial use.
- **If using broadband, turn your computer off when not in use.**
  - See Factsheet 16, Securely configuring your broadband modem/router.
- **Secure your email software**
- **Secure your web browser**
- **Don’t click on links or open attachments in spam email, or email that is otherwise suspicious.**

Target selection - phishing

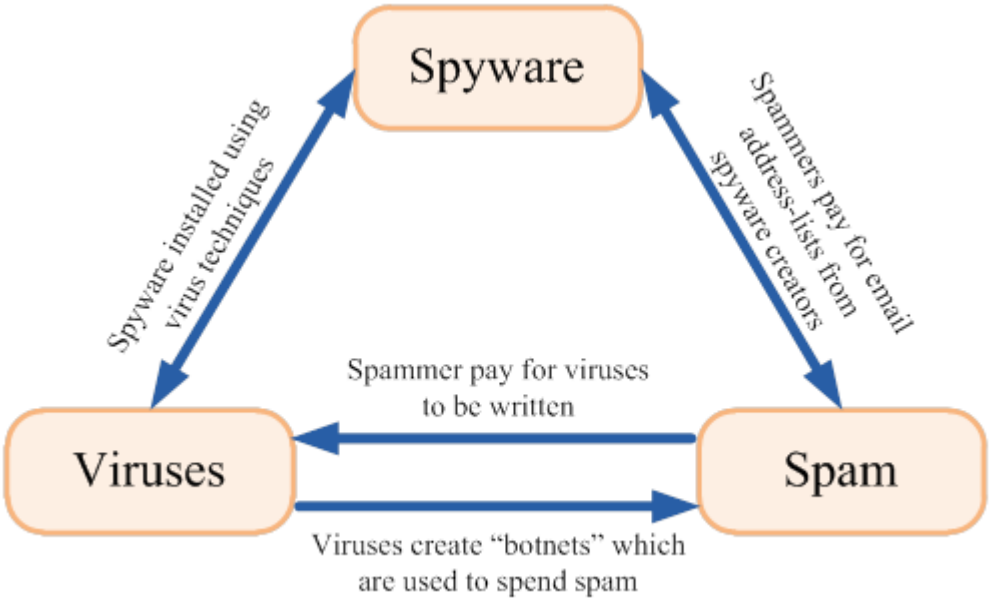
http://www.microsoft.com/en-au/security/online-privacy/phishing-symptoms.aspx

Phishing email messages take a number of forms:

- They might appear to come from your bank or financial institution, a company you regularly do business with, such as Microsoft, or from your social networking site.
- They might appear to be from someone you in your email address book.
- They might ask you to make a phone call.
- They might include official-looking logos They might include links to spoofed websites where you are asked to enter personal information.

Botnets

- If you get phished you will possibly become part of a botnet

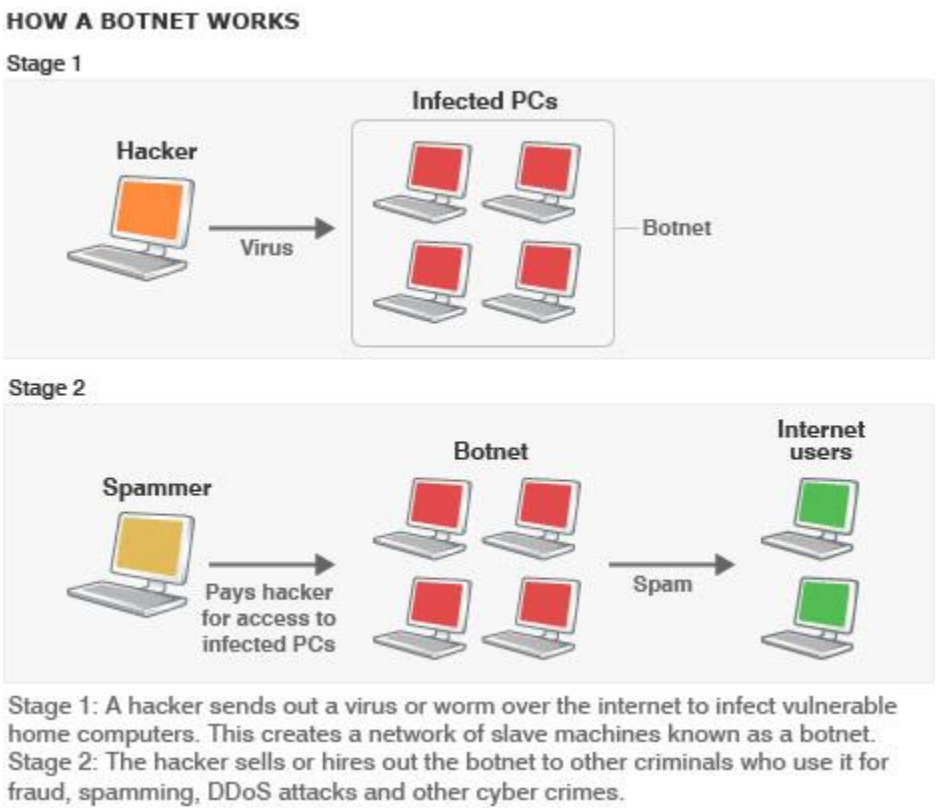


Bots & Botnets

- A (ro)bot (also called webcrawler) is a software agent which interacts with other network services intended for people as if it were a real person.
- A botnet is a collection of software robots or bots, which run autonomously. Botnets are frequently a collection of compromised machines running worms, trojans, spam, SMTP mail relays bots (Spambot), DOS (denial of service) and other vulnerabilities.
- Several botnets have been found and removed from the Internet.
- In July 2010 the Dutch police found a 1.5 million node botnet and the Norwegian ISP Telenor disbanded a 10,000-node botnet.
- It has been estimated that up to one quarter of all personal computers connected to the Internet may be part of a botnet.
- Examples of botnets over the last two years include BredoLab (November 2010), Mariposa (December 2009), Conficker (January 2009) and Zeus (June 2009) and in each case the number of compromised machines ranged from 10 million to 30 million.

Botnets

- http://hothardware.com/News/Microsoft-Granted-Permission-To-Kill-Botnet-Domains-Spam-Galore/



Stage 1: A hacker sends out a virus or worm over the internet to infect vulnerable home computers. This creates a network of slave machines known as a botnet.
Stage 2: The hacker sells or hires out the botnet to other criminals who use it for fraud, spamming, DDoS attacks and other cyber crimes.

Target selection – social engineering

- A consultant hired to see if a company would be vulnerable
- The CEO informed him that "hacking him would be next to impossible" because he "guarded his secrets with his life."
- "He was thinking someone would probably call and ask for his password and he was ready for an approach like that."
- After some information gathering, he found the locations of servers, IP addresses, email addresses, phone numbers, physical addresses, mail servers, employee names and titles, and much more.
- But the real prize of knowledge came when he managed to learn the CEO had a family member that had battled cancer, and lived.
- As a result, he was interested and involved in cancer fundraising and research. Through Facebook, he was also able to get other personal details about the CEO, such as his favorite restaurant and sports team.

Target selection – social engineering

- Armed with the information, he was ready to strike.
- He called the CEO and posed as a fundraiser from a cancer charity the CEO had dealt with in the past. He informed him they were offering a prize drawing in exchange for donations—and the prizes included tickets to a game played by his favorite sports team, as well as gift certificates to several restaurants, including his favorite spot.
- The CEO bit, and agreed to let himsend him a PDF with more information on the fund drive. He even managed to get the CEO to tell him which version of Adobe reader he was running because, he told the CEO "I want to make sure I'm sending you a PDF you can read." Soon after he sent the PDF, the CEO opened it, installing a virus that allowed himto access his machine.

What motivates hackers?

Release Information

- *Some hackers see a need for freedom of information and thus attack in order to "liberate" the information*

Release Software

- *Some make copies of software that can be installed on multiple computers –they crack the licensing code for "ethical" or financial reasons*

Consume Unused Resources

- *Try to access any resource – telephone line, bandwidth, disk space – which is not being used*

What do Hackers do?

Find Vulnerabilities

- *Find and exploit vulnerabilities – "security researchers"*

Find fame

- *Just another way of seeking attention*

How do hackers do this?

Produce Malicious code (software) and PUT IT ON YOUR COMPUTER WITHOUT ASKING!!!

- Logic Bomb
  - *Dormant until activated*
- Parasite
  - *Code added to existing program and draws information which hacker does not have privileges to access. Covert and non-destructive*
- Trojan horse
  - *Useful program with an alternative agenda*
- Virus
  - *Infects another program by replicating itself in to the host.*
  - *Mostly destructive, perhaps with logic bomb*
- Worm
  - *Transport mechanism for another program, utilising network*

How do hackers do this?

Exploit network protocols

- *Use the internet daemon,* inetd*, which listens to each port and passes control of it to the associated program*
- *Hacker can then get control of root*

E-mail Spoofing

- *Use software to pretend to send an email from someone you know*

IP Spoofing

- *Pretend to be a website that you trust*

Keylogging

How do hackers do this?

Network flooding and SYN flooding

- *Use patches*

Exploit Vulnerabilities

- Scanners and Profilers
  - *Preliminary evaluation of software*
  - *Determine hardware*
  - *Identify versions and patches*
- Sniffers and snoopers
  - *Might watch network or disk traffic or be planted inside to watch print spooler or logins*
  - *Must monitor own system – SNORT*
- File permissions
- Password Crackers

How do they start?
Target selection – information gathering web

- Whois
  - http://www.networksolutions.com/cgi-bin/whois/whois – Network Solutions whois query tool (.com, .net, .org)

```
BBN Planet (NET-SATNET)
   150 Cambridge Park Dr.
   Cambridge, MA 02138
   US

   Netname: SATNET
   Netblock: 4.0.0.0 - 4.255.255.255
   Maintainer: BBNP

   Coordinator:
      Soulia, Cindy  (CS15-ARIN)  csoulia@BBNPLANET.COM
      781 262 3395

   Domain System inverse mapping provided by:

   NIC.NEAR.NET                  192.52.71.4
   VIENNA1-DNS-AUTH1.BBNPLANET.COM 4.1.16.4
   NIC3.BARRNET.NET              131.119.245.6

   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

   Record last updated on 17-Feb-1999.
   Database last updated on 12-May-2000 17:51:31 EDT.
```

Target selection - Passive methods

- Facebook
- Other media
- Forums

Hackers software

- http://metasploit.com/
- Choosing and configuring an *exploit* (code that enters a target system by taking advantage of one of its bugs; about 300 different exploits for Windows, Unix/Linux and Mac OS X systems are included);
- Checking whether the intended target system is susceptible to the chosen exploit (optional);
- Choosing and configuring a *payload* (code that will be executed on the target system upon successful entry, for instance a remote shell or a VNC server);
- Choosing the encoding technique to encode the payload so that the intrusion-prevention system (IPS) will not catch the encoded payload;
- Executing the exploit.

Free security software

- Avira
  - http://www.avira.com/en/avira-free-antivirus
- Malwarebytes
  - http://www.malwarebytes.org/products/malwarebytes_free
- Turn on firewall
  - http://windows.microsoft.com/en-us/windows7/Understanding-Windows-Firewall-settings
- Turn on updates
  - Start, Control Panel, Windows updates

Successful Ageing Seminar

Cyber Communication

The perils of the online environment and how to keep safe

23 September 2011