




CMT116 Cyber Security & Risk Management
Session 2



Amir Javed


1



Hacker Methodologies

Edward Snowden's leave to remain in Russia extended for three years

Former US intelligence contractor's Russian lawyer also says Snowden can apply for country's citizenship from next year



- Hackers don't usually exploit systems from the computer they are sitting in front of.
- Their system typically accesses another system under their control, known as a hop
- This has been known to include up to 10 hops
- Hops often include computers in nations that are not on good political terms
- This way, forensic investigation (and prosecution) is difficult due to political barriers. World politics provide protection to hackers!
- Hackers will often attack the lowest-hanging fruit or well known systems (Microsoft, governments etc)

2



Types of Attack

- There are two main types of attack
 - Inbound attacks
 - Technically sophisticated
 - Specific target
 - Malware
 - Social engineering
 - Broad and specific attacks

3



Inbound Attacks

- Scrambling sequence of data packets
 - Intrusion Detection Systems rely on packets coming through the network sequentially to identify patterns or “signatures”
 - Destination device reassembles packets on the “inside”
- Encoding
 - Not all IDS signature detection is normalized
 - E.g. Unicode-encoding by changing spaces to “%20”

4



Malware

- Malware (malicious software) = any software that the user or sys admin did not authorize or want on their computer
- Spyware, grayware, adware, Trojan horses, key loggers, backdoors, rootkits all examples
- Once installed, it's difficult to detect by intrusion detection/prevention systems and firewalls rarely limit egress (outbound) traffic.
- Even if firewalls do block outbound traffic, port 80 is always open for Web traffic
- Malware uses this port to “phone home” to command and control systems, and to transmit captured sensitive information (e.g. login credentials, key strokes)

5



Malware

- Once “inside” the system, malware can scan for vulnerabilities and exploit them
- Internal systems are often the last to be patched (behind Internet facing machines)
- Portable devices are acceptably used more on the “inside”

6



Malware

- How does malware get onto systems?
 - Phishing (Social Engineering) – emails sent to people who are then
 - lured to download the software
 - visit a website that infects the system
 - give up passwords (in tests, this works 75% of the time!)
 - Pharming – redirecting a website's traffic to another site
 - DNS poisoning - modifying a router's DNS address
 - Modifying OS local resolution *hosts* file

7



Backdoors and Logic Bombs

- Backdoors (a.k.a trapdoors) are secret entry points into a program that bypasses normal security checks.
- Maintenance hooks are an example of a legitimate form of backdoor, to debug and test programs
- Logic Bombs are embedded in programs and are set to “explode” when certain conditions are met (e.g. Mondays at 06:00, or when user X logs on)
- Once triggered, a bomb may alter files or delete data

8



Viruses

- Viruses (self-propagating)
 - Attach to programs or files enabling it spread
 - Almost always an executable file
 - Cannot spread without human action
 - Rising since 80's, helped by Internet
 - ILOVEYOU email attachment (10% of computers in 1 day...50 million in 9 days)
- Comprise three parts:
 - Infection mechanism = means by which it spreads
 - Trigger = event or condition that enacts the virus
 - Payload = what the virus does

9



Types of Virus

- Encrypted Virus
 - A portion of the virus creates a random encryption key and encrypts the remainder of the virus
 - When the virus is invoked, the key is used to decrypt the virus
 - When the virus replicates, a different key is used
 - Difficult to monitor bit patterns of the virus
- Stealth Virus
 - Explicitly designed to hide itself from detection e.g. compressing itself to be the same size as the program it has infected, or detecting virus scans and presenting the original version of the program

10



Types of Virus

- Polymorphic Virus
 - Mutates with every infection making signature detection impossible
 - Functionally the same but bit patterns are different
- Metamorphic Virus
 - As with polymorphic but the alteration of bit pattern is even more complex
 - Routines may also change so behavior as well as bit pattern may change

11



Worms

- Worms
 - Unlike a virus, worms can travel without human action
 - Uses vulnerabilities of the system to travel unaided
 - Can replicate many times, consuming system memory and/or network bandwidth
 - Code Red worm (359k MS IIS Web servers in 1 day (July 2001))...patch made available >1year earlier. Costed at \$2.62 billion.
 - SQL Slammer worm (2003) infected 75k victims within 10 minutes...patch released 6 months earlier

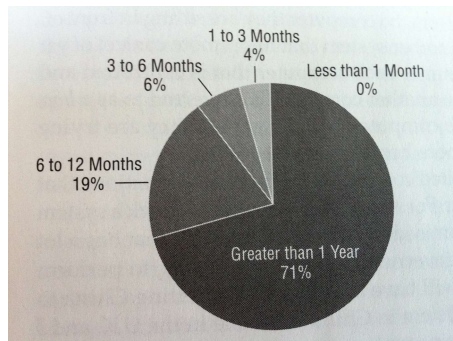
12

Trojan Horses

- “Hides itself” as useful software but actually does damage once installed
- Can delete files, corrupt information
- Also create “backdoors”, giving malicious users access to your system
- Do not reproduce, unlike viruses and worms
- The software may continue to perform the task you installed it for, but behind the scenes it is attacking the system
- Alternatively, it may be acting maliciously while operating as expected e.g. collecting passwords and form data

13

Patching



Who causes more damage? Hackers or IT system administrators?

- Chart indicates length of time between when a vulnerability was exploited and when a patch was made available 90% of vulnerabilities had patches available for more than 6 months
- Remaining 10% between 1 and 6 months
- No zero-day exploits (where patches don't exist) Verizon study of >500 breaches (2008)

14



Patching

- Many believe that firewalls gave organisations a false sense of security and led to poor execution of patches
- Patches update systems to repair/remove vulnerabilities
- A vulnerability = a million keys being made available by accident for the lock on your front door
- A firewall = building a fence around your house to stop people getting in
- A patch = getting a new lock with a unique key

15



Legacy code

- Billions of lines of code are currently being used and re-used
- Security has only recently been highlighted to the masses as significant
- We will be finding vulnerabilities for many years to come
- According to the Open Source Vulnerability DB, there are 20 new vulnerabilities found each day (average)
- Current DB of exploits is > 40k
- Maybe fixing everything is just too difficult, what about going after the hackers?

16



Automated Attacks

- Attacks are increasingly systematic and automated
- System by system, IP address by IP address, scanning for vulnerabilities
- Find – Exploit – Spread
- Can be done using freely available tools with GUIs
- Recent Uni. Maryland study – automated attack every 38 seconds
- So frequent that it quickly becomes “background noise”
- Lock your doors and only worry when the attackers get in!

17



Hacker Motivation

- End of the 90s – defaced websites, political statements, competitions to see who could deface the most over the weekend
- Hackers soon realised there was money to be made!
- A zero day exploit can sell for tens of thousand of pounds
- *Modern worms are stealthier and they are professionally written. The criminals have gone upmarket, and they're organized and international because there is real money to be made.* – Bruce Schneier (2008)
- International? Only official copies of Windows receive patched updates – pirate software all over the world – millions of machines open to hackers

A zero-day virus (also known as zero-day malware or next-generation malware) is a previously unknown computer virus or other malware for which specific antivirus software signatures are not yet available. Traditionally, antivirus software relies upon signatures to identify malware.

18



Botnets

- *Zombie* = when a system gets infected with malware and falls under external control
- *Botnet (roBOT NETwork)* = collection of zombies under command and control of a hacker
- Vint Cerf (2007) – Up to 25% of PCs part of a botnet
- Today there are c.1.2 billion computers on the Internet
- Feb 2000 – schoolboy brings down Dell, CNN, Amazon, eBay and Yahoo website using 200 university networks in the US to launch distributed denial of service (DDoS) attacks
- DDoS = hundreds of systems requesting a new session with a website – servers cannot handle the requests and crash

19



Hacking Web Services

- Web services act as middleware to connect distributed systems and share data
- Vulnerable to attacks:
 - Cross-site scripting (XSS)
 - Attackers “inject” malicious scripts into web pages (e.g. posting a message on a social network that includes a script to collect session cookies, hidden inside <script> elements...readers of the message have their cookie stolen)
 - Cross-site request forgery
 - Attackers uses user cookies (e.g. while logged into bank) to authorize attacks (e.g. transfer money to account X) without user’s knowledge
 - Browser flaws
 - A form of malicious code that takes advantage of a flaw or vulnerability in an operating system or piece of software with the intent to breach browser security to alter a user’s browser settings without their knowledge. Malicious code may exploit ActiveX, HTML, images, Java, JavaScript, and other Web technologies and cause the browser to run arbitrary code.

20



Search Engine Manipulation

- Search engines are also manipulated to:
 - Present false results that link to malicious sites
 - Rank malicious sites at the top of the results
 - Manipulate adverts to direct to malicious sites
- Search engines use (secret) page ranking algorithms but word count, result click-thru, and the number of sites linking to a result often supersedes these
- Botnets are used to:
 - add references to hacked sites to boost search engine rankings of malicious sites
 - add keywords to pages, relating to current events, celeb, political, natural disasters – links to malicious page

21



Virtualization and the Cloud

- Virtual machines now allow hundreds of instances of an operating system to run on a single server.
- What happens if the virtualization software is compromised?
- Happened in 2009 when over 100,000 websites hosted in a virtual environment were destroyed by a hacker, using a zero day exploit to gain root access.
- Less than half the customers had a full backup

22

Virtualization and the Cloud



Image: Shutterstock

Hackers have stolen over 60 million account details for online cloud storage platform Dropbox. Although the accounts were stolen during a previously disclosed breach, and Dropbox says it has already forced password resets, it was not known how many users had been affected, and only now is the true extent of the hack coming to light.

Motherboard obtained a selection of files containing email addresses and hashed passwords for the Dropbox users through sources in the database trading community. In all, the four files total in at around 5GB, and contain details on 68,680,741 accounts. The data is legitimate, according to a senior Dropbox employee.

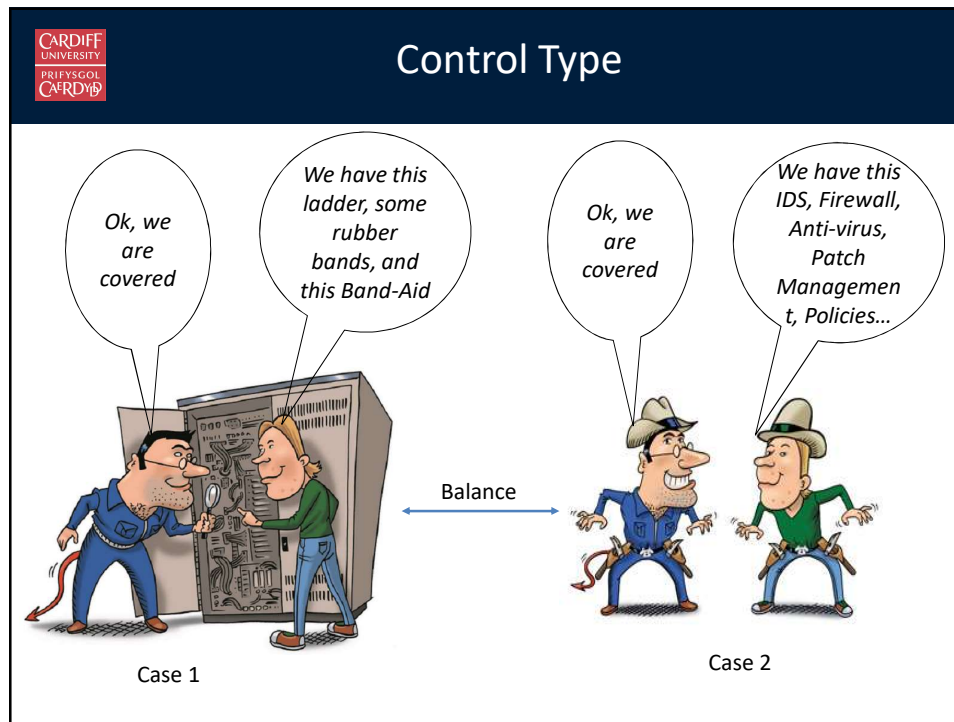
Source: <https://qz.com/771196/stolen-dropbox-passwords-are-circulating-online-heres-how-to-check-if-your-accounts-compromised/>

23

The Challenges

- Social engineering, Automated attacks, Malware, Worm and Virus replication, Undetectable code, Search engine indexing...The list goes on and there is no single solution
- *"The difference between an inexperienced chess player and a pro is the ability to use the pieces on the board in combinations and look several moves ahead..."*
- *The inexperienced player is always responding defensively with individual pieces and moves...until they run out of moves"*
- See the bigger picture...be proactive...patch, monitor, think ahead and educate. Don't be the low-hanging fruit.
- Fear causes human reaction. The human mind forgets fear, and this applies to security risks. We need to modify our cultural DNA to be more security conscious!

24



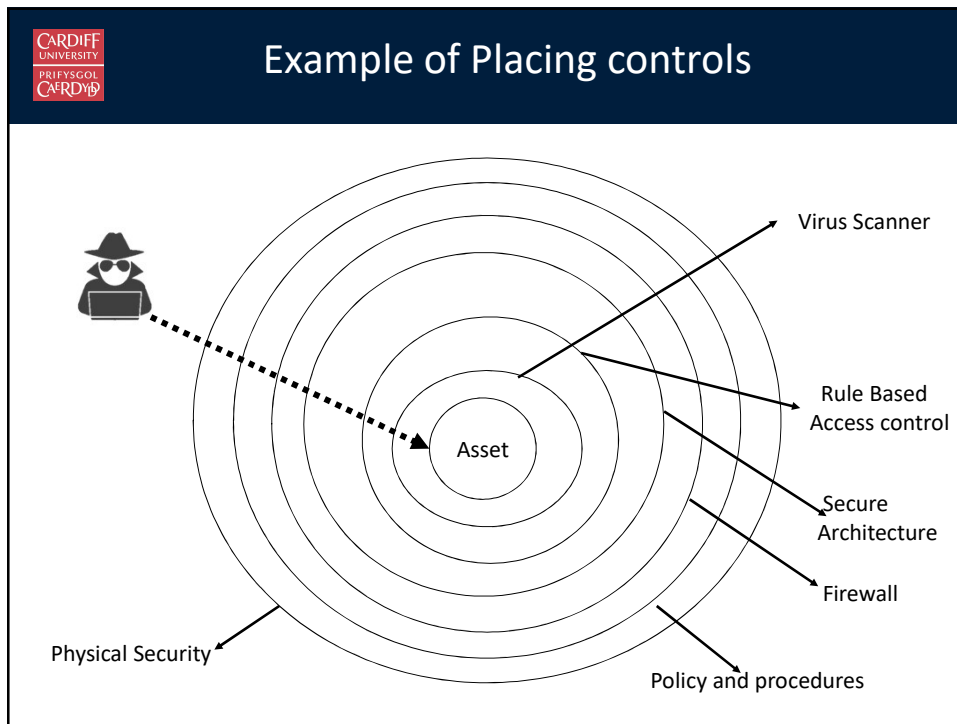
25

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

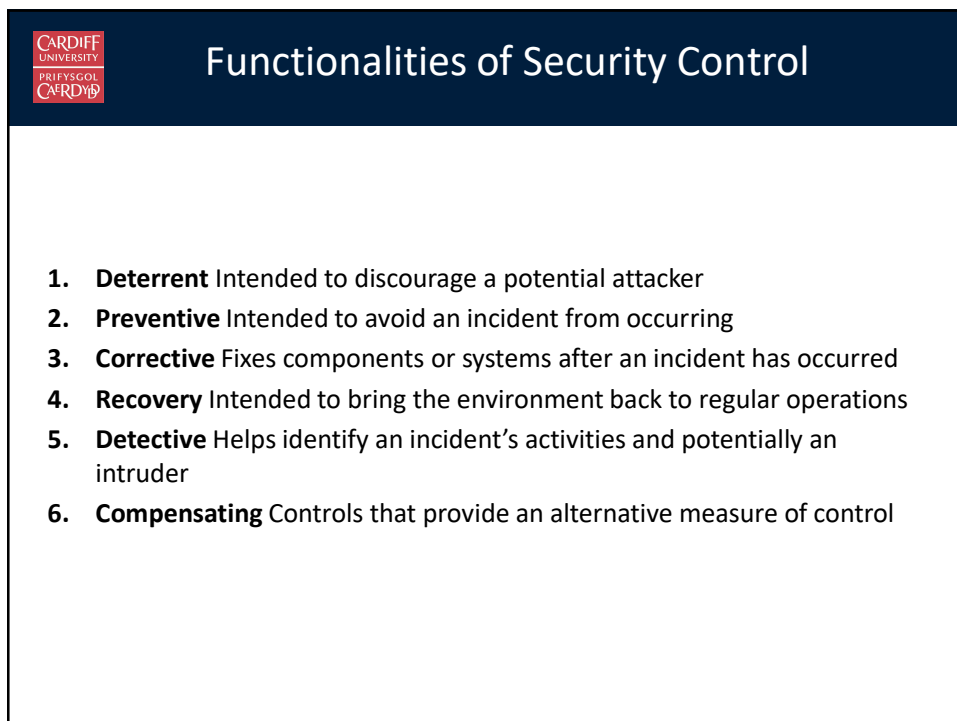
Control Types

- **Administrative:**
 - are commonly referred to as “soft controls” because they are more management-oriented.
 - Examples of administrative controls are security documentation, risk management, personnel security, and training.
- **Technical**
 - Are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms
- **Physical**
 - are items put into place to protect facility, personnel, and resources.
 - Examples of physical controls are security guards, locks, fencing, and lighting.

26



27



28



External Influences on Security

- World events
 - Pandemic health issues (e.g. H1N1 flu virus), rising oil prices = people working from home
 - sensitive data outside the corporate network
 - home PCs not monitored by corporate IT sys admin
 - spread of computer virus from home PC network
 - attackers using compromised home PC network as bridge to corporate networks
- Government policies
 - Do governments really understand IT security?
 - Cyber-czars for top-down strategic approach
 - Good idea but will they be empowered?

29



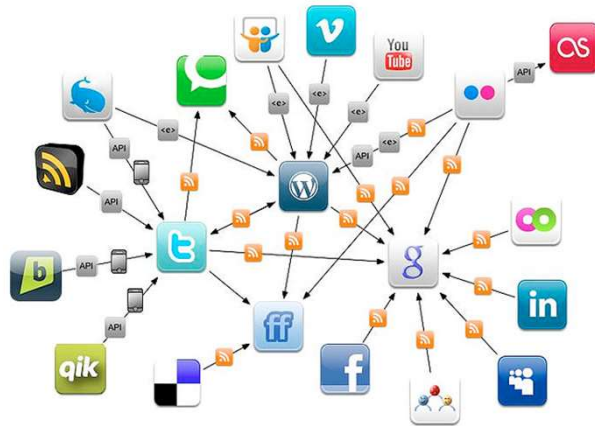
The Social Network

- Social networks allow social engineering attacks on a whole new level
- The aggregation of data published to these sites can offer new information security risks
 - Say the London-based “Big Corp” CEO becomes connected to the New York-based “Mega Corp” CEO on LinkedIn
 - Then the “Big Corp” CEO publishes that he’ll be in New York next week on Facebook
 - Then “retweets” something about economic survival on Twitter
 - Maybe the stock from one or both companies fluctuate
 - A merger on the cards? In public...
- The next generation of leaders will have grown up with timeline within social networks. Social engineering jackpot?

30

Social Data

- Ethics
- Persistence
- Citizen-control
- Inference



31

“Big Data”

- AOL released an “anonymised” database of search queries in 2006 – many claim to have identified people using it
- Netflix ran a competition to identify new ways to recommend movies to customers. It released viewing habits and is being sued by individuals who claim it released personal information
- Google uses email content to present ads to users

32

Security Metrics

One consultant said this threat could cost us \$150,000, another consultant said it was red, and the audit team assigned it a four. Should we be concerned or not?



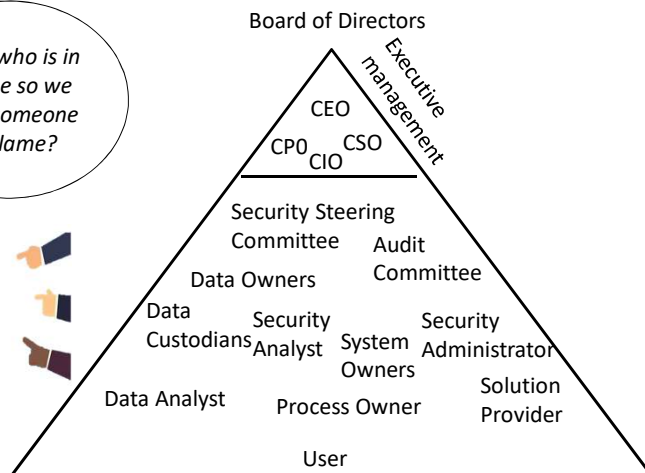
Risk can be measured by two ways

1. *Quantitative risk analysis* is used to assign monetary and numeric values to all elements of the risk analysis process.
2. *Qualitative risk analysis* uses a "softer" approach to the data elements of a risk analysis. It does not quantify that data, which means that it does not assign numeric values to the data so that they can be used in equations.

33

Roles of people in Cyber Security

Okay, who is in charge so we have someone to blame?



34



How do we cope?

- Educate, educate, educate...
- Do not underestimate the importance of information security and cybersecurity awareness
- The biggest risk is people. Employees in particular
- Everyone needs to understand the impact of their actions