SWINBURNE UNIVERSITY OF TECHNOLOGY

Network Security and Resilience/ Advanced Security

Threats – Notable exploits

Lecture six

Introduction

- Examine some recent network related exploits and see what can be learnt from them
- NOT an encyclopaedic list of recent exploits
  - An attempt to identify common themes, ideas, problems...
- Will look at some network infrastructure oriented exploits that I think are interesting and tell us something useful
  - Stuxnet, Conficker, Athens phone tapping scandal, BGP vulnerabilities, Gemalto Superfish, DROWN, Heart Bleed
- Want to see what is new but also what is unchanged

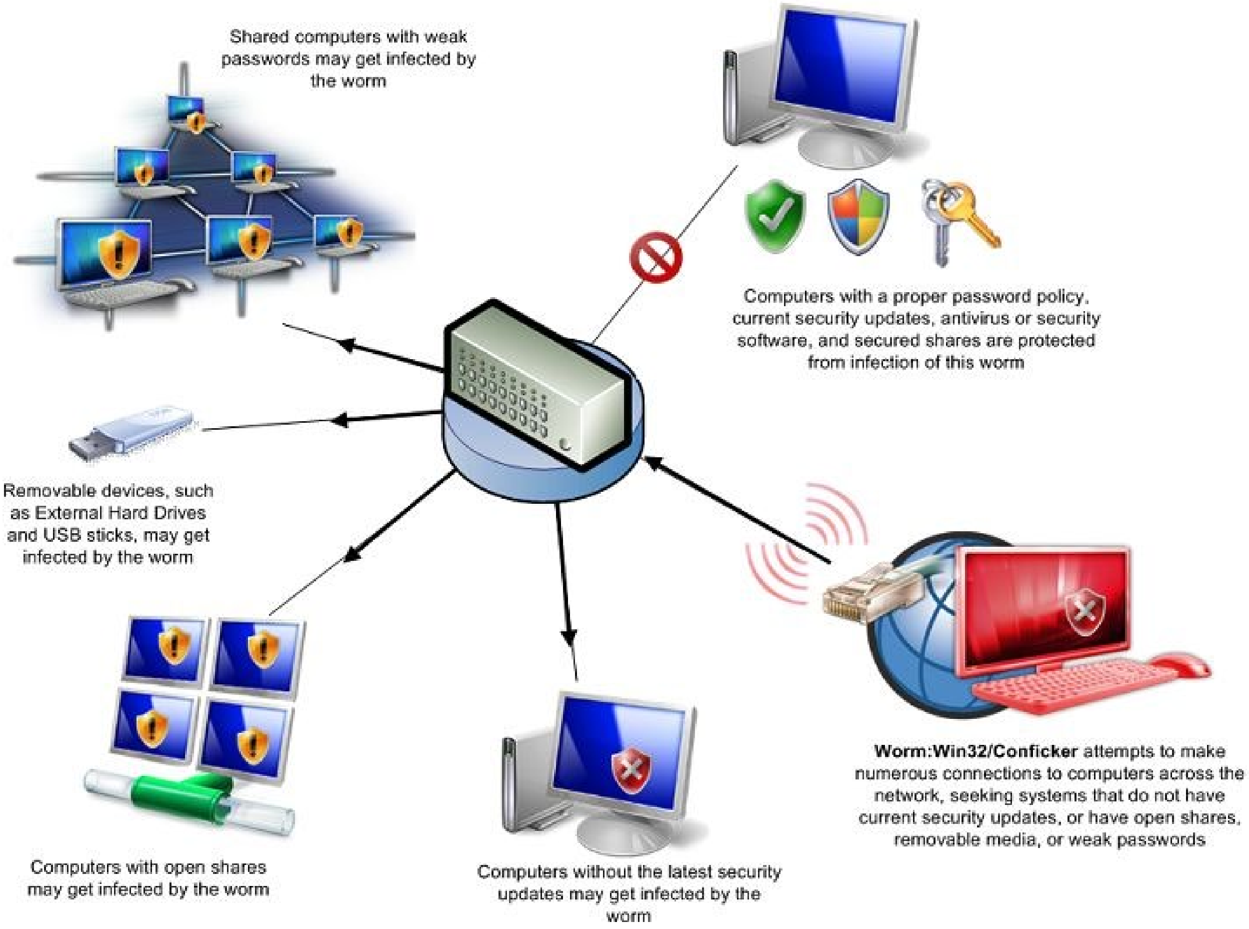
Some interesting exploits and events

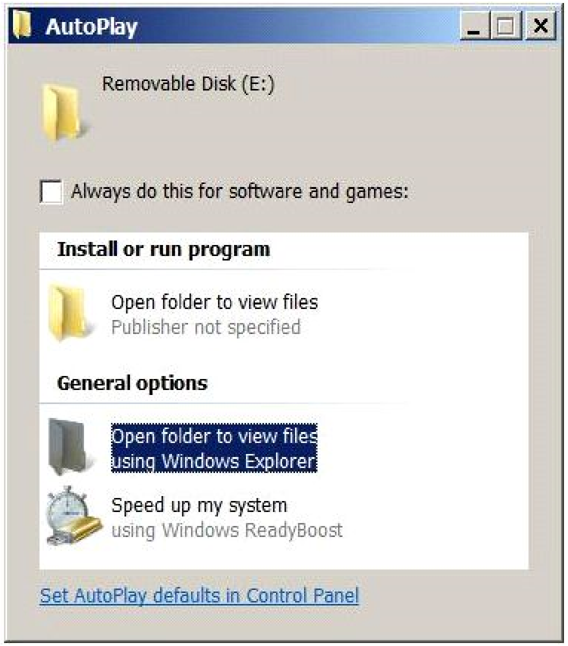
- Conficker
- Stuxnet
- Athens phone tapping scandal
- BGP outages
- Estonian cyber attacks

Conficker

- A computer worm that spreads itself to other computers across a network or via USB without human interaction (from Microsoft.com)
  - □ Five versions – A, B, C, D, E
- Consumes resources, disables accounts, blocks DNS lookups, may load a more recent version of itself
  - □ Version E loads spam software
- Attempts to spread itself in many different ways
  - □ Unpatched systems (exploits a buffer overflow vulnerability)
  - □ Weak passwords (uses a dictionary attack on password files)
  - □ Infects removable devices (USB memory sticks)

Conficker


Shared computers with weak passwords may get infected by the worm
Computers with a proper password policy, current security updates, antivirus or security software, and secured shares are protected from infection of this worm
Removable devices, such as External Hard Drives and USB sticks, may get infected by the worm
Computers with open shares may get infected by the worm
Computers without the latest security updates may get infected by the worm
Worm:Win32/Conficker attempts to make numerous connections to computers across the network, seeking systems that do not have current security updates, or have open shares, removable media, or weak passwords



AutoPlay

Removable Disk (E:)

☐ Always do this for software and games:

Install or run program

Open folder to view files
Publisher not specified

General options

Open folder to view files using Windows Explorer

Speed up my system using Windows ReadyBoost

Set AutoPlay defaults in Control Panel

From microsoft.com/security/worms/conficker.aspx

Why is it notable?

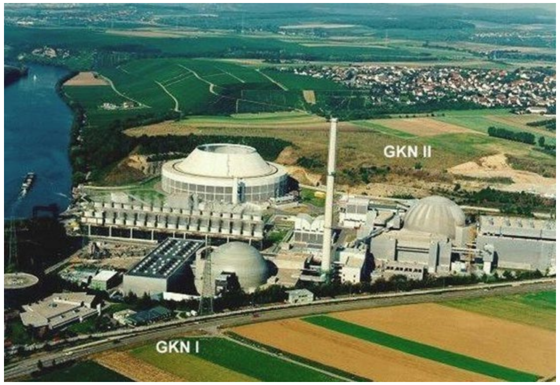
- Exploits weaknesses that have been known of for a long time
  - Buffer overflow
  - Trusted hosts
  - Moveable media
- Can be difficult to eradicate because new versions have been released as patches become available
  - So far five versions found
- If system is unpatched it patches it to prevent other malware from exploiting it

Lessons to be learnt?

- Keep patches up to date
- Implement a strong password policy
- Avoid use of trusted hosts
- Control moveable media

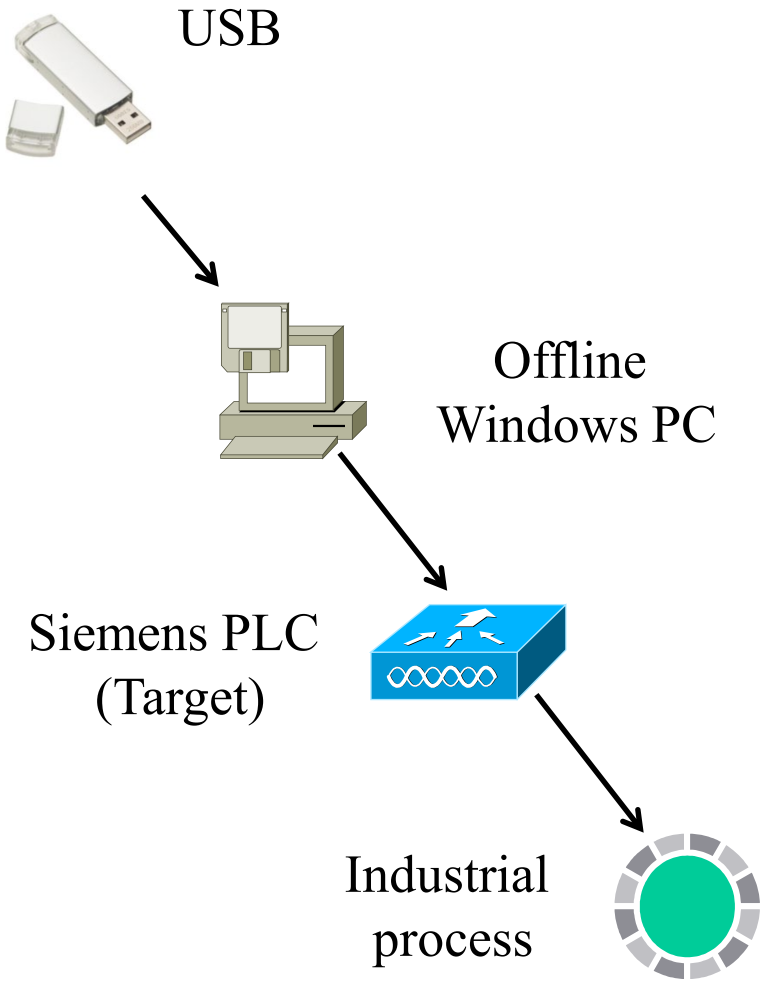
The Stuxnet Worm

- Windows worm that attacks industrial systems
- Transmitted via USB keys
  - □ Targets were Siemens Programmable Logic Controllers (PLCs) controlled by offline Windows machines
- Used to target the Bushehar nuclear power station in Iran
- Motivation was sabotage
- Believed to be joint US/Israeli cyberwarfare venture



How did it happen?

- Target was the Siemens Programmeable Logic Controller
- PLC reached via infected USB in unpatched Windows software
    - □ Same vulnerability exploited by Conficker
- Worm used default Siemens password on controller



USB

Offline Windows PC

Siemens PLC (Target)

Industrial process

Why is this notable?

- So many things make this a fascinating exploit
  - The software itself
  - Its sophistication, its origin, the breadth of expertise it manifests...
- A demonstration of how offline hosts can be targetted
- Questionable practices in some industrial plants
  - Contaminated USB keys used to transfer software in nuclear power plants
  - Well known vulnerabilities (exploited by Conficker) not patched
  - Siemen's default passwords not changed

Why is this notable?

- Very complex and sophisticated software
  - Estimated to have taken eight to ten people six months to write
  - Required a knowledge of industrial processes
  - Used four zero day exploits
    - Unusually extravagant
- People behind Stuxnet stole two legitimate digital certificates
  - An impressive attention to detail as well as technical breadth and depth
- Software was written to be difficult to detect
- An example of electronic warfare?
  - Despite denials by Iranian officials, appears to have succeeded

Lessons to be learnt

- Control malware infection vectors
- Keep patches up to date even with offline machines
- Implement a strong password policy (or at the very least change the default passwords)

The Athens wiretapping scandal

- The mobile phones of over a hundred Greek public figures were illegally tapped from August 2004 to March 2005
  - Figures included the Prime minister, Mayor of Athens, senior public servants in the Departments of Defence, Public Order, the Navy and even the American embassy
- No one knows what the motivation was or who the perpetrators were
  - Investigation botched
  - Foreign power?
  - Internal power struggle?

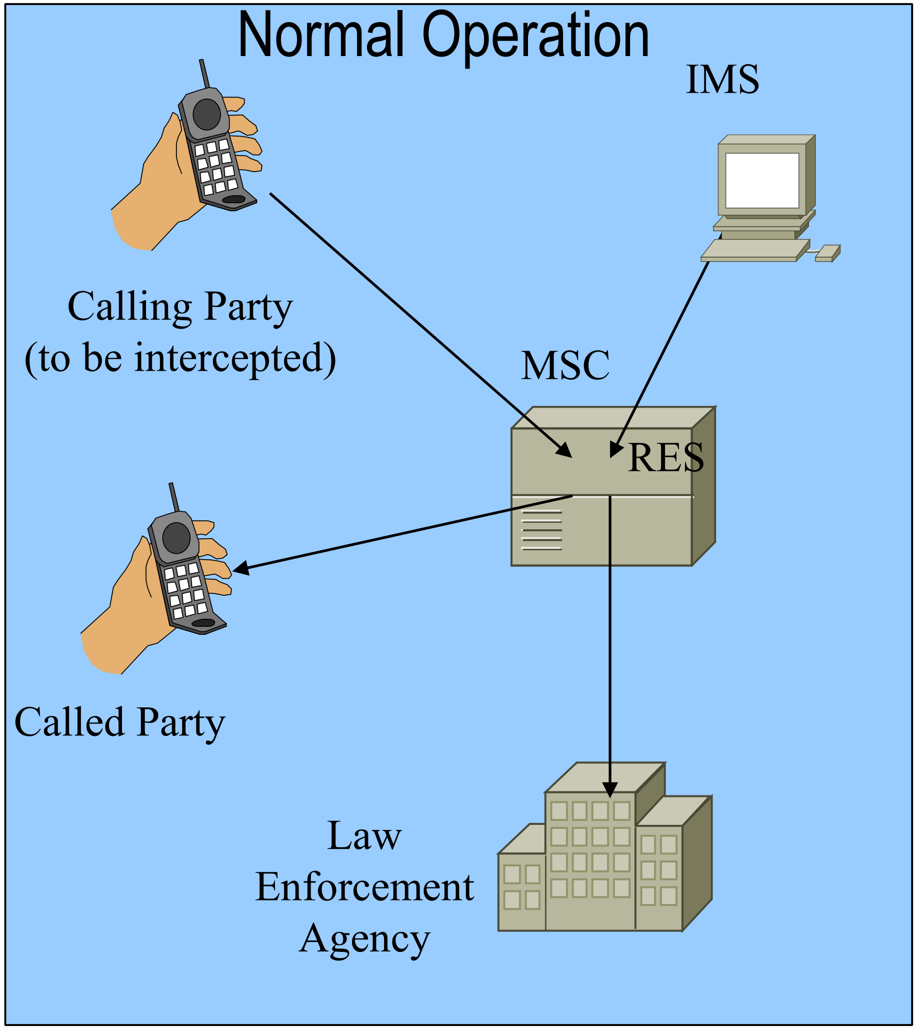
How did it happen?

- Telecommunications companies usually have the ability to wiretap communications if instructed to do so by law enforcement authorities
- Ericsson's interception capability is based on software built into the switch (MSC) called the remote-control equipment subsystem (RES)
- RES is usually activated within Ericsson switches by an external system called the Interception Management System
- When configured for wiretapping RES causes a copy of the call to be transmitted to the appropriate Law Enforcement Agency

How did it happen?

- Vodafone were not using Ericsson's RES or IMS
  - Using 3rd party LI system
- During an upgrade of the switch software RES was either accidentally or deliberately installed
- Although RES is usually managed via IMS it does not need to be
  - Instructions can be entered directly on the switch if the arcane instructions are understood
  - Most likely had physical access to the switch
- The perpetrators directed the intercepted calls to prepaid (anonymous) mobile phones

How did it happen?



Normal Operation

IMS

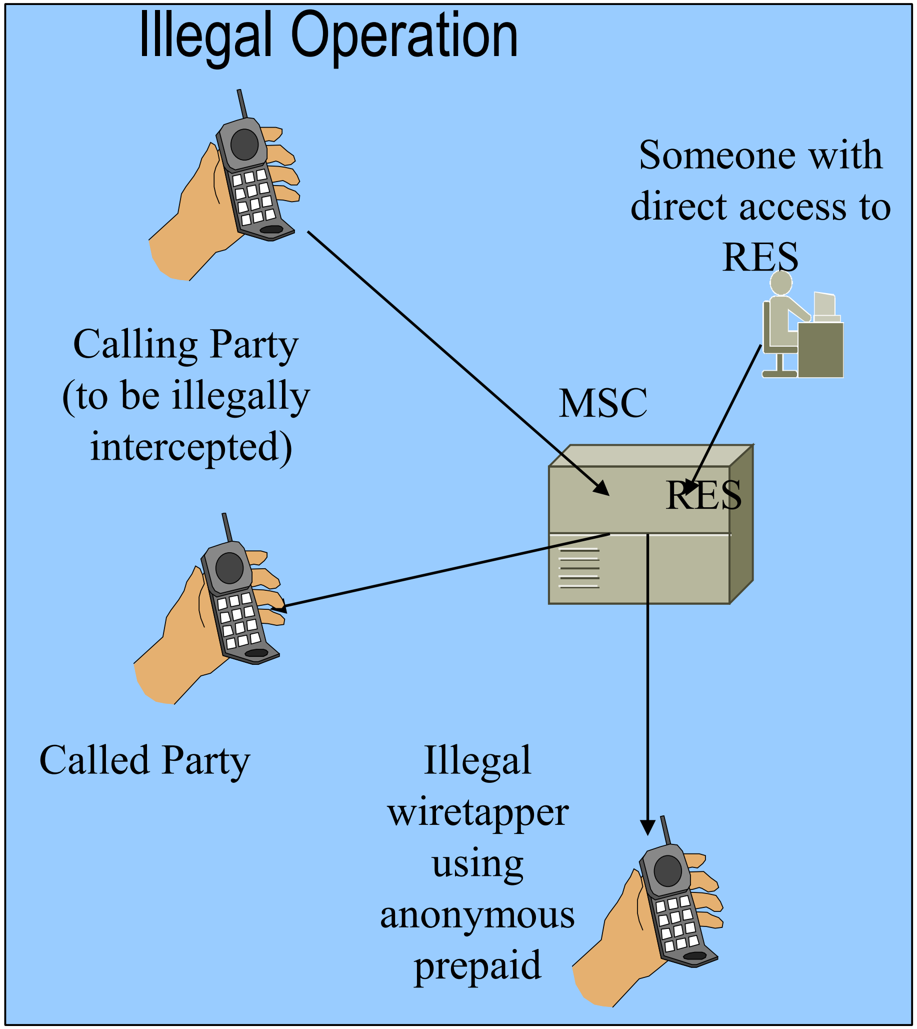
Calling Party
(to be intercepted)

MSC

RES

Called Party

Law
Enforcement
Agency



Illegal Operation

Someone with
direct access to
RES

Calling Party
(to be illegally
intercepted)

MSC

RES

Called Party

Illegal
wiretapper
using
anonymous
prepaid

Why is this notable?

- An unusual hack of a telephone system
  - □ An example of hacking being used for political purposes?
- Vodafone and Ericsson are among the largest telecommunications companies in the world
  - □ It is disturbing that they had difficulty with security of such an important and sensitive area
- Lawful Interception is a contentious area. Whether the Internet should include LI capabilities was a source of much heated debate in the late 90s
  - □ Ultimately the IETF (Internet Engineering Task Force) decided that it should not
  - □ Some see the Athens event as vindicating that decision

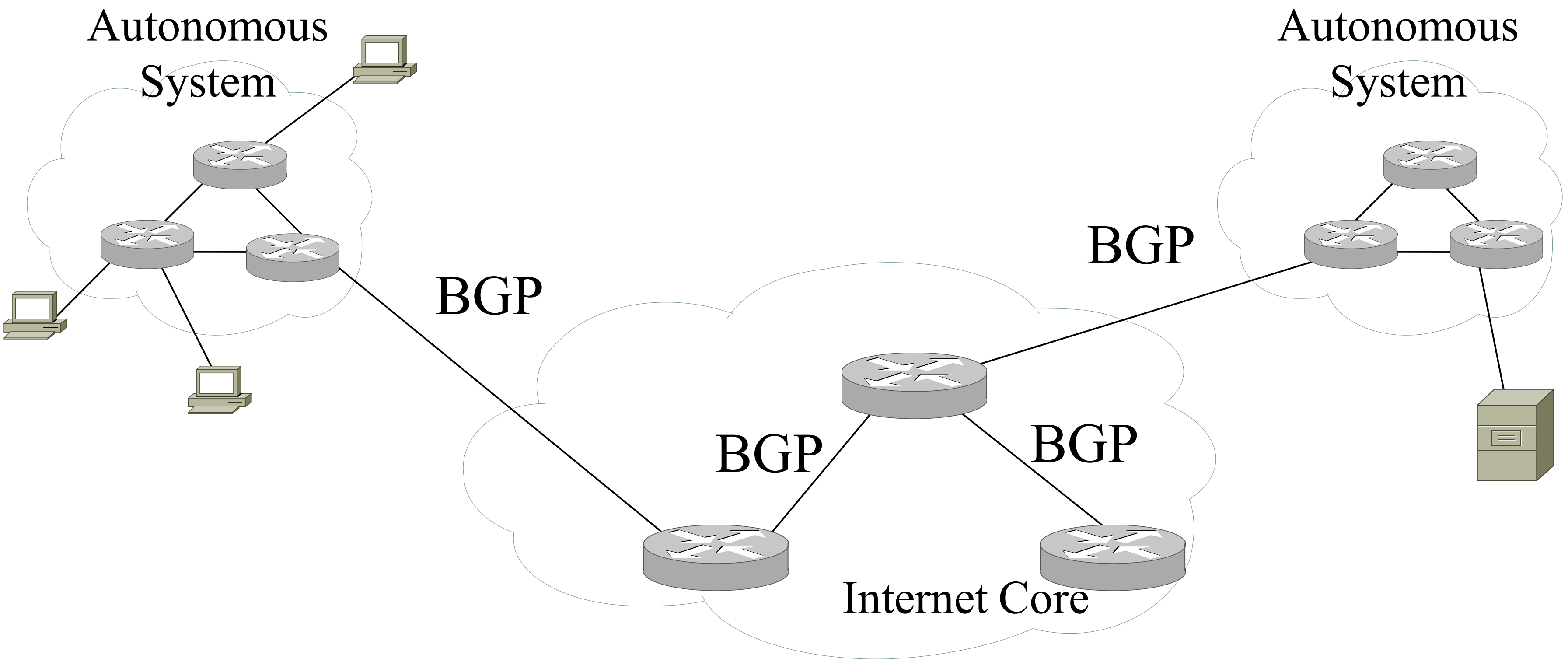
Lessons to be learnt?

- Physical access matters
- Disable unwanted services
- Carry out regular audits of what services are actually running on your equipment
- Avoid designing systems in such a way that they can be 'half-installed'

BGP vulnerabilities

- Not an attack but a demonstration of the fragility of key Internet infrastructure
- On 27th August 2010 a research group at Duke University and RIPE NCC conducted an experiment using BGP
- The experiment used a variation on the format of BGP messages that although in the specification, had not been used
- Cisco routers at the core of the Internet did not recognise the different format but passed on the corrupted messages
- Recipients of the corrupted messages dropped the connection
- Caused approximately 1.4% of address prefixes on the Internet to be unstable

BGP vulnerabilities



BGP vulnerabilities

- A few lessons...
- Even high end routers operating in some of the most critical locations in the Internet can have inadequate input checking
- Critical software should be written defensively
  - □ If a format is not recognised it should be dropped
  - □ Buffer overflow?

BGP misconfiguration

- In 2008 Pakistan Telecom was ordered by the Pakistan government to block YouTube.
- Pakistan Telecom implemented this by changing the BGP entry for YouTube to a local IP address that pointed to a server that would return a ‘blocked’ message
- Regrettably, it announced the new route to its upstream provider which then announced it to everyone else
- The result was that
  - YouTube was unreachable for over two hours
  - Pakistan Telecom was deluged with YouTube requests
- Lessons
  - Core Internet infrastructure is surprisingly fragile
  - One misguided engineer in a Pakistan ISP can accidentally take down one of the worlds most popular sites

BGP misconfiguration

- DoDo misconfiguration
  - In 2012 ISP DoDo caused Telstra to be taken offline for about 30 minutes
  - DoDo used both Telstra and Optus to provide transit routes (for redundancy)
  - DoDo mistakenly announced its Optus routes to Telstra
  - Telstra BGP policy was to prefer direct customer routes over its own transit provider (Telstra International)
  - All Telstra traffic then went via DoDo which was overwhelmed
- Lessons
  - Similar to Pakistan Youtube event
  - Core internet surprisingly fragile

Chinese cyberwarfare

- Chinese government see cyberwarfare as a new theatre of war
- Lot of denial and ambiguity as to whether or not the attacks emanating from China are state sponsored
- Regardless, there have been some interesting attacks from China the past few years
  - Australia on the end of one of them in 2013 when plans for new ASIO headquarters hacked
- Lesson learned
  - Network infrastructure vulnerable and a target during international conflict

Cloud Computing

- Two issues
  - Use the resources of the cloud to attack someone
  - Attack someone in the cloud
- Amazon’s Elastic Cloud Computing used to do a brute force attack on Wireless LAN 63 character passphrases (WPA-PSK)
  - Use the cloud to run through 400,000 passphrases / second
- Security in some cloud providers has not been very strong
  - PlayStationNetwork user details hacked by LulzSec
- Quite a bit more later in the unit

Lenovo Superfish

- Lenovo pre-installed "Superfish" adware on its laptops with the aim of introducing advertisements into Google search results
- "Superfish" installation includes a self-signed Certiticate Authority with a common private key
  - The software acts as a man-in-the-middle that decrypts what should be secure communications
  - Implication is that others can install their own certificate verified by this self-signed certificate
  - This certificate may perhaps be used to validate a malicious site
- Lessons
  - Even large organisations like Lenovo who should understand security sometimes make mistakes

Gemalto security breach

- Gemalto is a manufacturer of smart cards, used as SIMs in mobile handsets
- Each SIM card contains keys used for authentication and encryption
- According to leaked documents (via Edward Snowden) NSA and GCHQ infiltrated Gemalto and stole keys used for SIM cards
  - Some question as to whether they stole keys used to generate SIM card keys, or just keys used for a limited number of cards
  - Gemalto claim only some keys transmitted between Gemalto and some carriers were captured
- Lessons
  - Reach of the NSA?
- Worth reading Gemalto's response at http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx

Heart Bleed

- A buffer overread exploit
  - Faulty implementation of a protocol
- Periodic exchange between a server running OpenSSL and a client
  - "Heart beat" to ensure server still connected
- The exchange of messages consists of a message being echoed back to the client
  - The message and message length are both specified.
  - If the actual message length does not match the claimed message length, then buffer over-read occurs, potentially releasing confidential information
- Excellent explanation by xkcd
  - https://xkcd.com/1354/

DROWN

- Decrypting RSA with Obsolete and Weakened eNcryption
- Potentially affects a third of all https websites (any that support sslv2) but quite a lot of work to compromise a server
  - Medium risk
- Built around weakness in PKCS#1 standard which specifies padding of short messages
  - Attempt multiple keys until a valid padding is achieved
    - Tells attacker that some parts of the key are correct
    - Successively try key values until full key found
  - DROWN
    - Use TLS key values and apply them using SSLv2
    - Needs server to be using same key for TLS and SSLv2

Conclusion

- Hacking has become much more sophisticated… But it is still built on the same psychological bedrock as it has always been
  - □ Password practices usually poor
  - □ Patches often not applied
  - □ Software not written defensively
- Technical solutions important but even more important is what we have known for at least a decade to be good practice
  - □ Update patches
  - □ Have a strong password policy (particularly if using cloud computing or social networking sites)
  - □ Educate users about hacking
  - □ Write software defensively