

DARC  
TECHNOLOGY DIV

# IT Security

## An Introduction (DARC)

Matthew Cook  
<http://escarpment.net/>

1

---

---

---

---

---

---

---

---

DARC  
TECHNOLOGY DIV

## Agenda

- Why Bother?
- Terminology
- Physical Security
- Password Security
- Viruses
- Worms
- Trojans
- Phishing
- SPAM
- Spy/Ad Ware
- P2P Networks
- Encryption
- Operating System Patching
- Incident Response
- Not just Computers
- Windows Security
- Linux Security
- Wireless Security

2

---

---

---

---

---

---

---

---

DARC  
TECHNOLOGY DIV

## Why bother?

Why bother?

- Keeping control and service availability
- Spreading infection
- Data Integrity (DPA)
- Legal Liability
- Reactive Work Loads
- Bad Public Relations
- Personal Responsibility

3

---

---

---

---

---

---

---

---

## Why bother?

- Computing has changed...
- Ten years ago the Internet was very small, few connections, mainly dialup users.
- JANET connected UK Universities from the early 90s.
- ISDN links at 64Kb/sec for industry.
- Advent of broadband brings many, many more users on a fast connection.

4

---

---

---

---

---

---

---

---

## Why bother?

- Personal Attacks
- Information theft and modification
- Experimentation
- Bandwidth theft
- DoS Botnets
- Warez servers
- Distribute Viruses, Worms and Trojans

5

---

---

---

---

---

---

---

---

## Terminology

- Compromised – Is the technically correct term for 'hacked'. (Slang: owned)
- Cracker – Someone who breaks into computer systems for malicious reasons.
- Hacker – Someone who is creative with computers.
- Script Kiddie – Someone who runs security related scripts without much knowledge of the technology, usually teenagers.

6

---

---

---

---

---

---

---

---

## Terminology...

- Virus – Malicious code.
- Worm – Code spread automatically, usually via the Internet.
- Trojan – A piece of computer code hidden on a system to usually gain back door access.
- Bandwidth – The amount of data that can flow along a computer link.
- DoS Attack – Denial of Service attack.

---

---

---

---

---

---

---

---

## Terminology...

- IP Address – A unique address on a network specific to one machine (similar to a phone number).
- Port – A specified number between 1 and 65535 through which data can be exchanged with computer programs.
- Root – The super user account on the computer usually Root on Unix/Linux or Administrator on Windows.

---

---

---

---

---

---

---

---

## Physical Security

"The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it."

*Gene Spafford*

---

---

---

---

---

---

---

---

## Physical Security...

- Secure Location
- BIOS restrictions
- Password Protection
- Boot Devices
- Case Locks
- Case Panels

---

---

---

---

---

---

---

---

## Password Security

The object when choosing a password is to make it as difficult as possible for a cracker to make educated guesses about your chosen password. This leaves them no alternative but a brute-force search, trying every possible combination of letters, numbers, and punctuation.

---

---

---

---

---

---

---

---

## Password Security...

- Do not use your login name in any form
- Do not use your first or last name
- Do not use your spouse's or child's name
- Do not use your Car Registration etc.
- Do not use a dictionary based password
- Do not use a password shorter than 8 chars
- Do not write it on 'post-it' notes

---

---

---

---

---

---

---

---

## Password Security...

- Use a password with mixed-case characters
- Use a password with a mix of alpha- numerics and punctuation
- Use a password that is easy to type to avoid 'Shoulder Surfers'
- Use the first letters from song titles, song lyrics or film quotations

---

---

---

---

---

---

---

---

## Viruses

- Traditional viruses required human intervention.
  - Share it on floppy discs
  - Copy it
  - Email it
- Attached to programs, documents or emails.

---

---

---

---

---

---

---

---

## Worms

- One stage on from viruses
- Auto replication
  - Open shares
  - Exploits in machines
  - Outlook Address book
- Eliminating the human interaction means whole computer networks can be compromised very swiftly.

---

---

---

---

---

---

---

---

# Trojans

- Appears to be an innocent program
- Actually contains malicious code
- Quite often a backdoor to the system
- Sometimes difficult to discover

---

---

---

---

---

---

---

---

# Phishing

- The term given to the attempted theft of information by misleading information.
- Your Bank account has been compromised, please give us your account details...
- Your Email account has been suspended, please give us your password...
- Very common: Banks, eBay, PayPal etc

---

---

---

---

---

---

---

---

# Phishing...




---

---

---

---

---

---

---

---

# Phishing...



---

---

---

---

---

---

---

---

---

---

# Phishing...



---

---

---

---

---

---

---

---

---

---

# Phishing...



---

---

---

---

---

---

---

---

---

---

# Phishing...



---

---

---

---

---

---

---

---

---

---

# SPAM

- Unsolicited email or advertising messages.
- Selling pharmaceuticals, pornography, web site links, make money fast schemes, chain letters, fraud etc
- Clogs up mailboxes and wastes space and bandwidth.
- Currently filtered out on our email routers.

---

---

---

---

---

---

---

---

---

---

# Spy/Ad Ware

- Vulnerabilities with Operating Systems and browsers allow the tracking of your web browsing, information gathering and the display of advertising information.
- Check cookies.
- Use only trusted software.
- Be careful what you download or run.
- - Project to start to look at these issues.

---

---

---

---

---

---

---

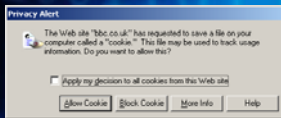
---

---

---

## Spy/Ad Ware

- Selectively accept cookies in Internet Explorer
  - Tools -> Internet Options -> Privacy -> Advanced.



---

---

---

---

---

---

---

---

---

---

## P2P Networks

- Common source of Trojan files
  - Appealing for free downloads
  - Most are illegal and copyrighted material
  - Against most ISPs Acceptable Use Policy
- Source of excessive bandwidth

---

---

---

---

---

---

---

---

---

---

## Firewalls

- Block access to malicious traffic entering the network.
- Block outgoing traffic which may have malicious affects.
- Bi-directional: Protects us from the rest of the world and protects the rest of the world from us.
- Different types of policies; default deny and default allow.

---

---

---

---

---

---

---

---

---

---

## Firewalls...

- Personal Firewalls are not recommended as the only line of defence or an excuse not to patch.
- Software Firewalls often fail open.
- Hardware Firewalls traditionally fail closed.
- Most broadband routers contain firewall features (including NAT).

---

---

---

---

---

---

---

---

## Encryption...

- In the early days of computing messages were sent in clear text across the wire.
- People using 'packet sniffers' could read these messages, including passwords and steal the identity of a user.
- Encryption methods are now used to prevent this happening.
- Examples; SSH, HTTPS, VPNs...

---

---

---

---

---

---

---

---

## Operating System Patching...

- Operating Systems do contain bugs, and patches are a common method of distributing these fixes.
- A patch or hot fix usually contains a fix for one discovered bug.
- Service packs contain multiple patches or hotfixes. There are well over 200 hot fixes in most service packs.

---

---

---

---

---

---

---

---

## Operating System Patching...

- Its not just the Operating System!
  - Software needs patching too
  - Lots of vulnerabilities are discovered in software.
  - MS Office, GDI+ JPEG Module, IIS, MS SQL, Oracle etc

---

---

---

---

---

---

---

---

## Incident Response...

- Don't Panic!
- Unplug the network
- Don't turn the computer off.
- Get a notebook
- Back-up the system and keep the Back-ups
- Look for information
- Investigate the cause
  
- Request help and assistance.

---

---

---

---

---

---

---

---

## Incident Response...

- Important to return to service swiftly
  - Do not jeopardize security
  - Always, re-build
  - Perform forensics on a backup
- Keep documentation and evidence

---

---

---

---

---

---

---

---

## Not just Computers

- Network appliances
- Printers
- Photocopiers
- CD towers
- Network switches, routers, firewalls
  
- Anything network connected...

---

---

---

---

---

---

---

---

## Windows Security

- Automatic Updates
  - My Computer > Select Properties > Select Automatic Updates tab.
  - We do NOT recommend Automatic or Turning Automatic Updates off.
  - Either; Download updates for me, but let me choose when to install them.
  - OR Notify me but don't automatically download or install them.

---

---

---

---

---

---

---

---

## Windows Security...

- Microsoft Baseline Security Analyser
- Freely available from Microsoft
- Provides advice on
  - Security best practices
  - Strong passwords
  - Security mis-configurations
  - Application configurations

---

---

---

---

---

---

---

---

## Linux Security

- Choose a sensible partitioning structure
- Install only the required packages
- Remove Unnecessary services
  - Nmap
  - Chkconfig
  - Restart
- Update via YUM

---

---

---

---

---

---

---

---

## War Driving

- Kismet
- Detects insecure wireless networks
- Provides SSID
- Can map networks with a GPS unit
- Free wireless networks available...

---

---

---

---

---

---

---

---

## Securing Wireless

- Configure the network and clients
- Use a suitable encryption method
- Use MAC address filtering/locking
- Do not broadcast SSID
- Further security
  - Offer limited or no DHCP scope
  - Check Logs

---

---

---

---

---

---

---

---

## Further Information

- Vendor Sites
- <http://escarpment.net/>
- <http://www.lboro.ac.uk/computing/security/>
  - Advice and Guidance
  - Training
  - Links

---

---

---

---

---

---

---

---

## Security Notifications

2004 - 2005	IT-Security	Windows-Security	Unix-Security	Mac-Security
September	5	1	0	0
October	2	8	1	3
November	2	5	1	2
December	4	4	3	3
January	3	5	0	2
February	12	12	18	7
March	18	4	26	3
April	11	4	45	3
Total	57	43	94	23
Grand total	217			41

---

---

---

---

---

---

---

---

## Questions and Answers

<http://escarpment.net/>

---

---

---

---

---

---

---

---