

Information Protection Issues

Professor Kenneth P. Mortensen
Digital Law
Villanova Graduate Tax



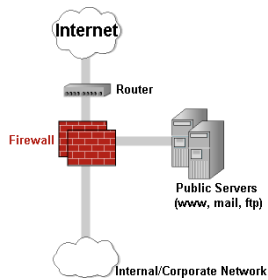
The Problem of Information Security

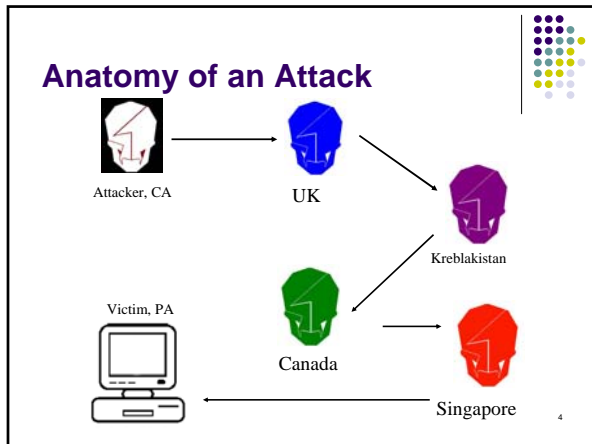
- Transparent technology
- Trust
 - Networks are built on trust
 - Only have to compromise one trust center
- Access
 - Must watch everything
 - Only have to find one weakness
- The Internet was built to be open and easily navigated



Background

- Represents a typical, permanent business connection
- The 'Public Servers' section is known as the DMZ
- Three possible breach points:
 - Router
 - Firewall
 - Servers





- ### Countermeasures
- Routers
 - Firewalls
 - Server Hardening
 - Network Intrusion Detection
 - Server Intrusion Detection
 - Anti-virus
 - Personal Firewalls
 - Policy
 - Awareness and Education
- 5

- ### Routers
- Sit between networks like traffic cops.
 - Through Access Control Lists (ACL) routers control –
 - Basic access to the network (who in, who out)
 - Advertising about what networks they know about (where are we)
 - Listening to what networks they connect to (where to go)
 - Could be subverted
- 6

Routers



- How often are the configuration files reviewed?
- What procedures are in place for log retention?
- Change management?
- Ownership?
- OS version and patches?

7

Firewalls



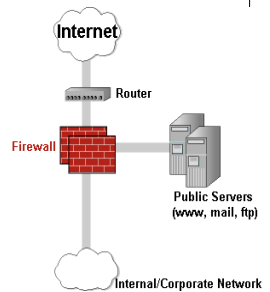
- Enforces traffic rules:
 - Allow all - expressly deny
 - Deny all - expressly allow
- Range from routers with additional code to servers to appliances.
- Good choke point, but not a silver bullet

8

Firewalls



- Controls in-bound access from the Internet
- May be used to monitor/filter outbound web content



9

Firewalls



- How closely are they monitored?
- Who has access to them?
 - Physical
 - Remote
 - Usernames and passwords
- When were the policies or logs last reviewed?

10

Firewalls



- OS, firewall versions, patches and updates.
- Default configurations
- Are they setup to protect in only one direction?
- They are not just for perimeters
 - Interior controls
 - Access vulnerabilities

11

Server Hardening



- The art of making operating systems more secure than an 'off the shelf install'.
- Extremely technical process to develop, implement and maintain.
- A hardened server today could easily be an over exposed box tomorrow.

12

Server Hardening



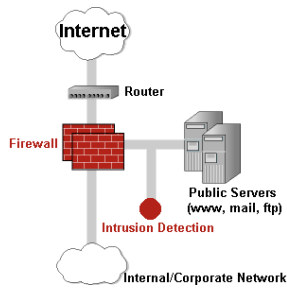
- What to look for:
 - Documented procedures
 - Time of last update
 - Update methods
 - Compliance
 - Audit – more frequently than once a year
 - Proof

13

Intrusion Detection



- The digital burglar alarms on the networks and hosts
- Several forms of commercial and freeware



14

Network IDS



- Advantages
 - A series of sensors distributed across your networks that collect traffic and compare that to well known attack signatures.
 - If the traffic and the attack signature match, you get an alert of some type.
- Disadvantages
 - Usually an add-on that loses to bandwidth
 - How do you manage them?
 - What will you do when you detect an alert?
 - Most major cyber-crimes have involved physical penetration

15

Network IDS



- Becoming more robust and cost effective
- One sensor can watch a great deal of traffic
- If well deployed, they are very effective

16

Host IDS



- Agent code that resides on critical servers and monitors in near-real time for suspicious activity such as:
 - User management
 - Critical file change
 - Permission use/abuse/change

17

Host IDS

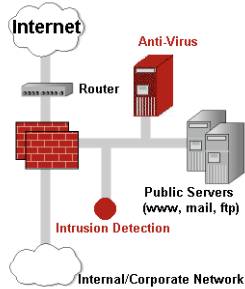


- Advantages
 - Commercially reasonable
 - Extremely powerful – can watch for a multitude of things
 - Typically very customizable
- Disadvantages
 - Who will manage them?
 - What do you do when you detect misuse/abuse?
 - Who knows where to put them?

18

Anti-virus Scanning

- Best done at the mail server
- End-users rarely update the signatures
- End-users are able to turn off at the desktop



Personal Firewalls

- Software running on the desktop that is designed to monitor for malicious network activity.
- Usually inexpensive
- Fairly effective (proof by non-incident and some warnings)

20

Policy

- The single most important piece of the puzzle.
- The one piece that most do not have
- Good policy shows management support
- Provides instructions for the disasters

21

Policy



- Law is unclear on many computer matters
- Clear policy improves success of adverse actions
- Employees must know what they may and may not do with company resources

22

Policy



- Clear and written
 - Associates should read and sign
- Enforcement procedures
 - Inspect and audit
 - Associates must
 - Understand consequences
 - Know violators will be treated accordingly
 - Must be enforced evenly across the organization

23

Awareness and Education



- Best system security is built by your own people
- Training shows an investment in human resources
 - Morale builder for your associates
 - People on board are already paid to run the system

24

Awareness and Education



- All across the enterprise must be made aware of the risks.
- This is not just for System Administrators
- It is imperative to incorporate the solution across:
 - Techies and non-techies, management, development, executive, legal, HR, marketing, etc., entire organization

25

Information security



- Is not
 - a single piece of hardware or software
 - A trained sysadmin
 - A piece of policy paper
- It is
 - All of these
 - And more

26

Information security



- Is
 - an overall methodology/business practice
 - developed
 - implemented
 - reviewed
 - updated
 - A developed and nurtured in-house skill set

27
