

# Computer Security - Part 1

**Richard E. Smith, Ph.D.**

Senior Principal Computer Scientist

**Secure Computing Corporation**

2675 Long Lake Road

Roseville, Minnesota 55033

<http://www.securecomputing.com/>

[smith@sctc.com](mailto:smith@sctc.com)

612-628-2780

**“Internet Cryptography”**

Web site at <http://www.visi.com/crypto/>

Copyright 2000 Richard E. Smith. All rights reserved.

## Outline

- » Threats and Attacks
  - Dealing with Attacks
  - Preventative Measures
- » Worked Examples
  - Isolated Workstations
  - Intranet Servers and Mainframes
  - Encryption and VPNs
  - Internet Browsing
  - Public Key Cryptography
  - Internet Servers

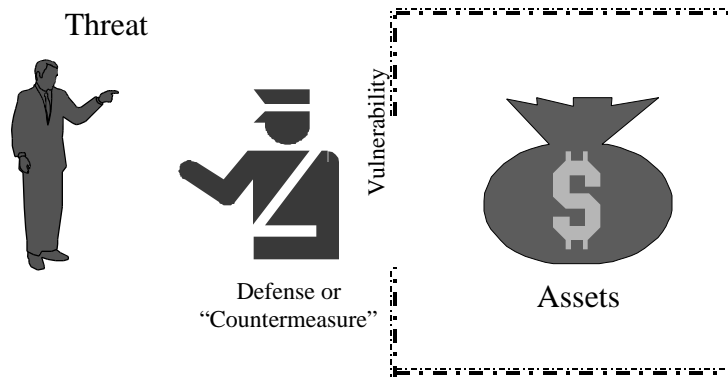
# Threats and Attacks

2/28/00

Computer Security - Richard E. Smith

3

# Threats and Defenses



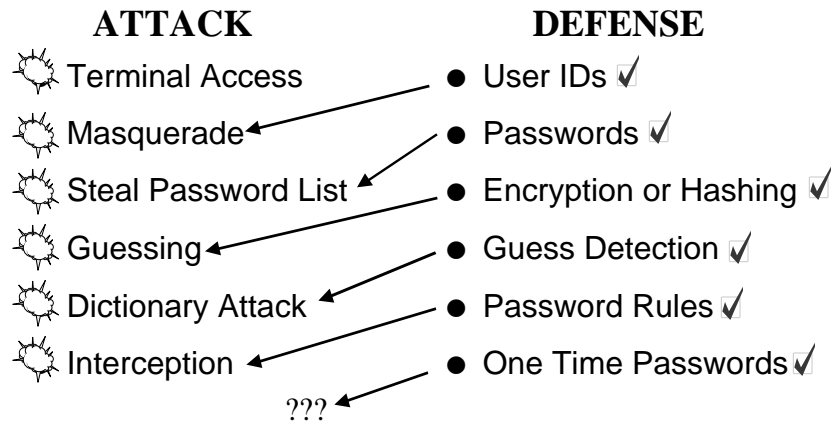
An attempt to steal or harm the assets is an **attack**

2/28/00

Computer Security - Richard E. Smith

4

# Attacks and Defenses Evolve



2/28/00

Computer Security - Richard E. Smith

5

# Dealing with Attacks

- Deterrence
- Detection Methods
- Responses
- Preventative Measures

2/28/00

Computer Security - Richard E. Smith

6

# Deterrence

- Accountability is the principal deterrent
  - » People are more likely to behave if their activities may be individually monitored
  - » Occasional monitoring is often enough
  - » Example: Web browser logs at schools, businesses
- Laws, regulations, and legal penalties
  - » Increases the risk to the perpetrator
  - » Example: Melissa virus writer was arrested

2/28/00

Computer Security - Richard E. Smith

7

# Detection Methods

- The first step in dealing with an attack
- Can be very difficult: 5% detection rates
  - » Example: Victims in military infowar games often assume it's just software "glitches"
- Keep records of attack-like behavior
  - » Invalid access attempt, login failures
  - » Remote probes: Internet port scans
- Be familiar with "normal" behavior
  - » Example: Aldrich Ames with shopping bags.

2/28/00

Computer Security - Richard E. Smith

# Responses

- Limit immediate effects of attack
  - » Break attacker's connection
  - » Shut down subverted processes
- Post-attack procedures
  - » Monitor and logs for future attacks
  - » Restore lost data, restart systems
  - » Reports to managers, outside agencies
  - » Investigations

2/28/00

Computer Security - Richard E. Smith

9

# Attack Responses in Practice

- Internet Worm (1988)
  - » Disconnect from network, abort and delete offending software, patch known holes
  - » FBI tracked down the perpetrator
- Melissa (1999)
  - » Same, with "patching" of anti-virus software
- Sniffer incidents (mid 1990s)
  - » Monitor repeated attacks, forensic analysis

2/28/00

Computer Security - Richard E. Smith

10

## Preventative Measures

- Mechanisms to block attacks
  - » Physical Protection
    - always the starting point for security
  - » Procedural Measures
    - Roles, responsibilities, operating rules
  - » Technical Measures
    - User authentication - who is trying to use it
    - Access control - give different people different capabilities

2/28/00

Computer Security - Richard E. Smith

11

## Physical Security

- Computer based security measures rely on physical protection
- Given enough time and the right hardware, attackers will succeed
- Distinguish between people **with** physical access and those **without**
- Difficult to provide security when untrusted people have physical access

2/28/00

Computer Security - Richard E. Smith

12

# Insiders versus Outsiders

## » Outsiders

- Not members of your organization, not specially committed to its success.
- Members of the general public, customers, competitors.
- Outsiders must “intrude” to access your resources

## » Insiders

- Members of your organization that are generally committed to its success.
- Have physical access to enterprise resources and assets
- Insider attacks: abuse or expand legitimately granted permissions

2/28/00

Computer Security - Richard E. Smith

13

# Users and Administrators

## » Users

- People who use computing resources to get jobs done
- Access granted to do their job: no more, no less
- Physical and technical security restricts their capabilities

## » Administrators

- People charged with maintaining the integrity of your computing systems
- In theory they can make any change to a computer within their realm of responsibility and completely cover their tracks.

2/28/00

Computer Security - Richard E. Smith

14

# The Insider Threat

- Most computer intrusions and most fraud is perpetrated by insiders
- Preventative mechanisms work best against outsiders, not insiders
- Computer systems can keep records that may deter fraud
  - » Example: bank reconciles accounts weekly; embezzler caught by deadline

2/28/00

Computer Security - Richard E. Smith

15

# Recommendations

- » Insiders have work to do - balance security measures against real threat of loss
  - Strongest measures that don't interfere
- » Put heavy restrictions on systems with a high risk of attack or embezzlement
  - Make insiders into outsiders
  - Keep logs of transactions, and audit them
- » Don't mix system administrator duties with other business responsibilities

2/28/00

Computer Security - Richard E. Smith

16

## For Further Information

- » Dorothy Denning, *Information Warfare and Security*, Addison Wesley
- » National Research Council, *Trust in Cyberspace*, National Academy Press
- » Dorothy Denning and Peter Denning, *Internet Besieged*, Addison Wesley
- » Donn Parker, *Fighting Computer Crime*, Wiley

## Worked Examples

- Isolated Workstations
- Intranet Servers and Mainframes
- Encryption and VPNs
- Internet Browsing
- Public Key Cryptography
- Internet Servers

# Isolated Workstations

2/28/00

Computer Security - Richard E. Smith

19

# Workstation Access Control

- Protection is Based Mostly on Physical Access
- “Lock screens” and authentication devices
  - » Resists unsophisticated attacks
  - » Prevent some crimes of opportunity- if the attacker doesn't steal or penetrate the physical machine
- File and Disk Encryption

2/28/00

Computer Security - Richard E. Smith

20

# File and Disk Encryption

- » Can resist refined and even innovative attacks, if built correctly
  - Transforms your data into unreadable text
  - Snooper can't read, and probably can't reliably change
- » Double Edged Sword
  - If encryption is weak, then a trained attacker can easily breach it
  - If encryption is strong and you lose your password or key, then the data is lost forever

2/28/00

Computer Security - Richard E. Smith

21

# Computer Viruses

- » Computer Virus Behavior
  - Most viruses are merely nuisances and cause no intentional damage
  - Some viruses intentionally cause damage, but this is rare because it reduces the likelihood that the virus will continue to spread and thrive
- » Virus Countermeasures
  - Careful behavior isn't practical in most environments
  - Anti-virus software finds and repairs damage
    - Updates by subscription for latest viruses

2/28/00

Computer Security - Richard E. Smith

22

## Virus Examples

- Application viruses (games),
  - » Michaelangelo “time bomb” virus
- Operating system viruses
  - » Mac window frame, boot sector
- MS Word macro viruses
  - » Melissa - word macro distributed by e-mail
- Network virus: Internet “Worm”
  - » Others: e-mail Trojan programs

2/28/00

Computer Security - Richard E. Smith

23

## Workstation Summary

- Physical Protection is essential
  - » Anti-Virus Measures are essential in most situations
  - » Systematic procedures for workstation data backup
- Other security measures
  - » “Lock” screens with password protection

2/28/00

Computer Security - Richard E. Smith

24

## For Further Information

- » Russell and Gangemi, ***Computer Security Basics***, O'Reilly
  - A classic introductory work
- » Davis and Lewis, ***Computer Security for Dummies***, IDG Books
  - Practical introduction and reams of basic advice
- » Cohen, A ***Short Course on Computer Viruses***, John Wiley
  - Technical background on viruses

2/28/00

Computer Security - Richard E. Smith

25

## Intranet Servers and Mainframes

2/28/00

Computer Security - Richard E. Smith

26

# Server Security Defenses

- » Physical Access Control
  - Server machines reside in a physically secure machine room
  - Risk of unauthorized administration (mingled machine room)
  - Terminals reside in physically safe environments
- » Identification and Authentication “I&A”
- » Computer Based Access Control
- » Auditing

2/28/00

Computer Security - Richard E. Smith

27

# Identification/Authentication

- Who are you? Can you give me evidence?
- Computer Based I&A Relies on 1 or more of these “factors”:
  - » Something You Know (a password or PIN)
  - » Something You Have (a card or token)
  - » Something You Are (a physical feature, voice, fingerprint)

2/28/00

Computer Security - Richard E. Smith

28

## I&A in Practice

- Often tied to records of what you do
  - Audit records tagged with user names
- Authentication is essential for remote access
  - War Dialer Attacks, 1980s
    - (“WarGames” movie)
- Users Generally Hate It
  - Requires something Lost, Forgotten, or Injured.

2/28/00

Computer Security - Richard E. Smith

29

## Attacks on Passwords

- » Interactive Password Guessing
  - Passwords should be easy to remember but hard to guess
  - Server should detect bad password attempts and raise an alarm
- » Password “Sniffing”
  - Shoulder Surfing, Wiretapping, Bugs, etc.
  - Example: Pennsylvania Students in 1987

2/28/00

Computer Security - Richard E. Smith

30

# More Attacks

- Stealing the Password File
  - “Ancient” trick dating back to CTSS
  - Solved by storing encrypted or “hashed” passwords
    - » 1. Collect the plaintext password
    - » 2. Encrypt or hash it in an irreversible fashion
    - » 3. Compare against hashed version in the password database
- Dictionary Attack on Encrypted Passwords
  - Computer based guessing of encrypted passwords -- extremely fast, undetectable.
  - Easy to remember passwords become easy to attack

2/28/00

Computer Security - Richard E. Smith

31

# One Time Password Systems

- » Ideal for remote access - uses a secret to generate a new password for each login
  - Eliminate the risk of password sniffing
- » Software OTP implementations
  - Examples: Windows NT, 2000
- » Hardware OTP implementation: Tokens
  - Examples: Safeword, SecurID, WatchWord
  - Eliminates intentional sharing
  - Only authorized users are issued tokens
    - Citibank example: international embezzling

2/28/00

Computer Security - Richard E. Smith

32

# Generating OTPs

- » Event or Clock Driven
  - Token generates a password for each login attempt
  - Client increments the time or a counter
  - Client encrypts it with the secret
  - Server repeats the process with same secret
- » Challenge-Response Passwords
  - Server sends a random number “challenge”
  - Client encrypts it with secret value
  - Server repeats the process

2/28/00

Computer Security - Richard E. Smith

33

# Using Multiple Factors

- » Single Factor Authentication with Passwords
  - Vastly popular, but vulnerable to Common attacks
- » Two Factor Authentication
  - usually Smart Cards or Tokens with PINs
  - used in Sophisticated environments
- » Three Factor is rarely used
  - Biometric activated Cards with PINs, or other combinations

2/28/00

Computer Security - Richard E. Smith

34

## Session Authentication

- Traditionally, I&A is applied at the beginning of an interactive session
  - » Can subvert authentication by subverting the session
- Attacks on Sessions
  - » Wiring attacks are possible but rare
  - » Attacks on dial-up connection
    - Mitnick, 1980s

2/28/00

Computer Security - Richard E. Smith

35

## Computer Based Access Control

- » Controlling what people can do on the server
  - Controlled access to computer's resources: files, printers, other Services
  - Often left fairly loose for convenience
- » Access Control is Hard to Manage
  - Sophisticated settings get "stale" as programs evolve and staff changes
  - Requires systematic maintenance to remain effective

2/28/00

Computer Security - Richard E. Smith

36

## Attacks on Access Controls

- » Access Control in Commercial Computers Rarely Stops a Trained Attacker
  - Convenience sells better -- even potentially strong computers are sold with protections disabled
- » Modern systems are very complex
- » it's extremely costly to "lock down" a sophisticated operating system completely
  - 10-15 hours of work

2/28/00

Computer Security - Richard E. Smith

37

## Activity Audit Records

- » A "Log" of security relevant events
  - Seeks to deter abuse by increasing Accountability
  - Consequences of Enforcement
    - Educational measures, Penalties, Policy changes
- » The log is often too big for casual use
  - Thousands of records for days of activity
  - Usually reviewed as a last resort
- » Intrusion Detection Systems: detect attacks by watching audit records in real time

2/28/00

Computer Security - Richard E. Smith

38

# Server Security Summary

- Essentials
  - » Rigidly restrict all outside access
  - » Authenticate all outside users
- Other measures
  - » Use stronger measures if a lot is at risk
  - » Save your audit records if trouble occurs
- For Further Information
  - » Check local computer bookstore and Internet news groups about your server