Data Theft Prevention Techniques

Prof. Zaheed Shaikh

Private Records

- Destroy paper records

Email

- Secure email
- Do not store confidential data on email

Paper Trail

- Receipts
- Credit card /ATM etc
- Not leave un attended

Credit cards/Banks/DND

- Never let them out of site
- Know the identity of the person calling
- Take name out of marketers list
- Review credit cards statements carefully

Technical Details

- **Watch out for Phishing Websites**
  - Credit card number
  - Bank account number
  - Driver's license number
  - Home address and phone number
  - Health insurance id or information
- **Use an Anti-virus/Anti-Malware Program**
- **Use OpenDNS**
  - Works as web filtering

Technical Details

- **Unique Passwords for Every Website**
  - Lastpass and Keeppass
- Secure routers/Wifi

Security Certification Levels

- Department of Defense, Trusted Computer System Evaluation Criteria (TCSEC)
- Orange book – systems; Red book – systems/networks
- Levels
  - Class D (minimal protection)
  - Class C1 (discretionary security protection)
  - Class C2 (controlled access protection)
  - Class B1 (labeled security protection)
  - Class B2 (structured protection)
  - Class B3 (security domains)
  - Class A1 (verified design)

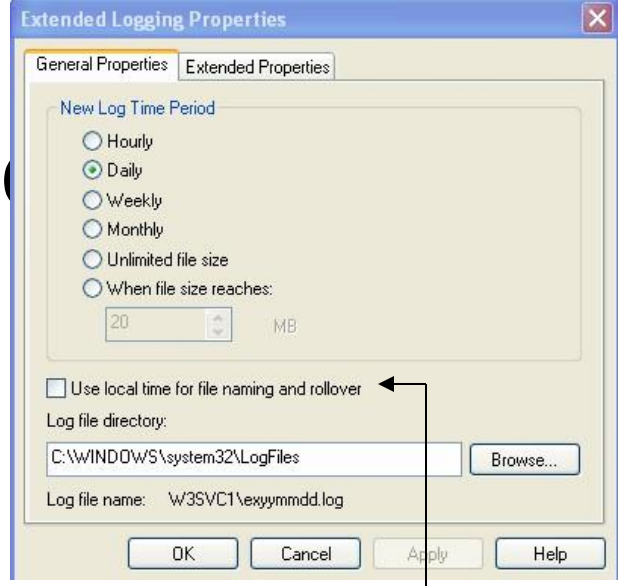
Hardening servers

- Be aware of the 5 ‘P’ s of security and compliance
  - Proper Planning Prevents Poor Performance
- Plan the installation
  - Identify
    - The purpose of the server. Example: provides easy & fast access to Internet services
    - The services provided on the server
    - Network service software (client and server)
    - The users or types of users of the server
  - Determine
    - Privileges for each category of users
    - If and how users will authenticate
    - How appropriate access rights will be enforced
    - Which OS and server applications meet the requirements
    - The security baseline(s) for installation & deployment
- Install, configure, and secure the OS according to the security baseline
- Install, configure, and secure server software according to sec. baseline
- Test the security
- Add network defenses
- Monitor and Maintain

Hardening servers (cont.)

- Choose the OS that provides the following:
  - Ability to restrict admin access (Administrator vs. Administrators)
  - Granular control of data access
  - Ability to disable services
  - Ability to control executables
  - Ability to log activities
  - Host-based firewall
  - Support for strong authentication and encryption
- Disable or remove unnecessary services or applications
  - Remove rather than disable to prevent re-enabling
  - Additional services increases the attack vector
  - More services can increase host load and decrease performance
  - Reducing services reduces logs and makes detection of intrusion easier

Hardening servers (c

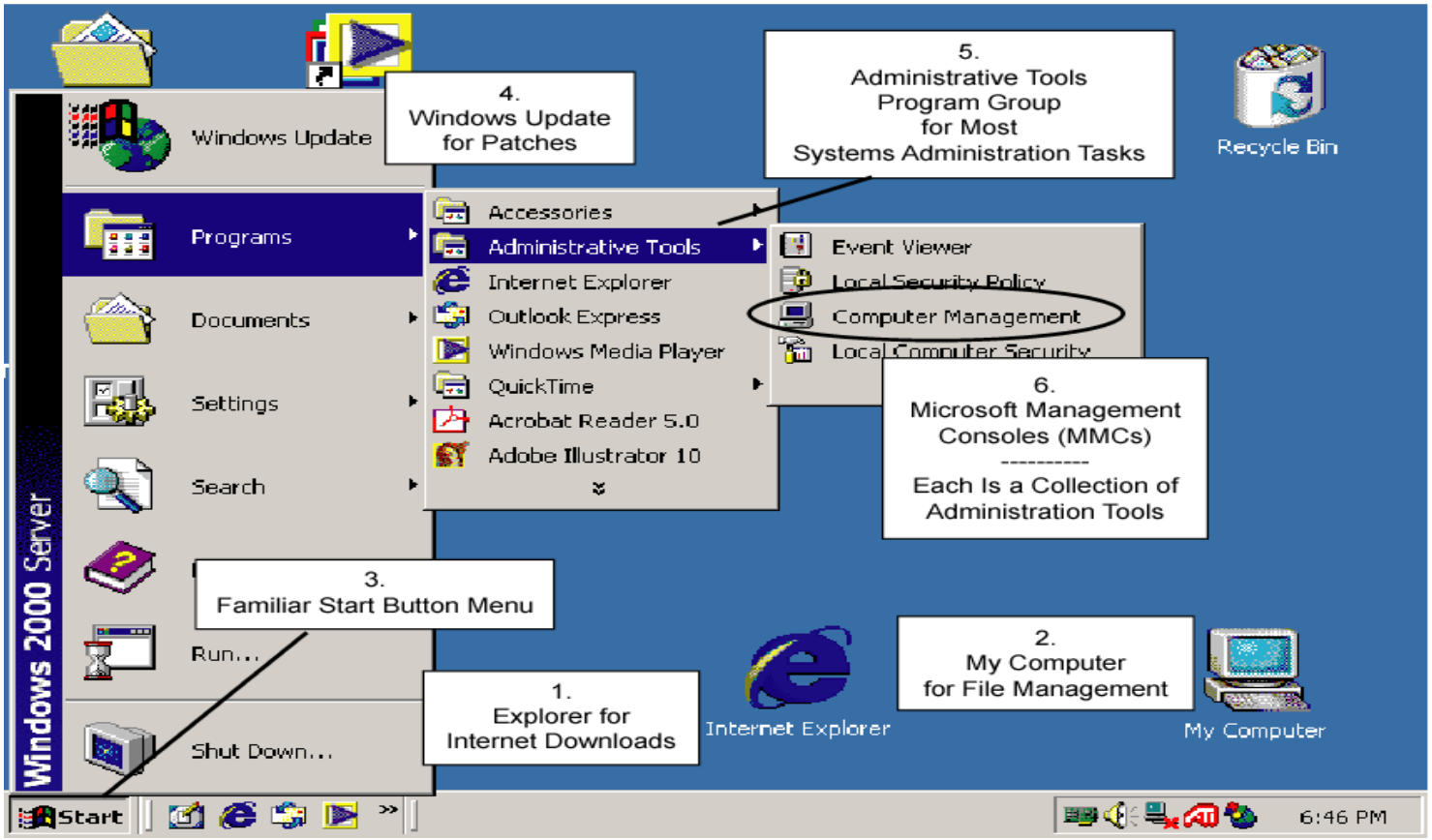


- Configure user authentication
  - Remove or disable unnecessary accounts (e.g. Guest account)
  - Change names and passwords for default accounts
  - Disable inactive accounts
  - Assign rights to groups not individual users
  - Don't permit shared accounts if possible
  - Configure time sync
  - Enforce appropriate password policy
  - Use 2-factor authentication when necessary
  - **Always use encrypted authentication**

Windows Hardening

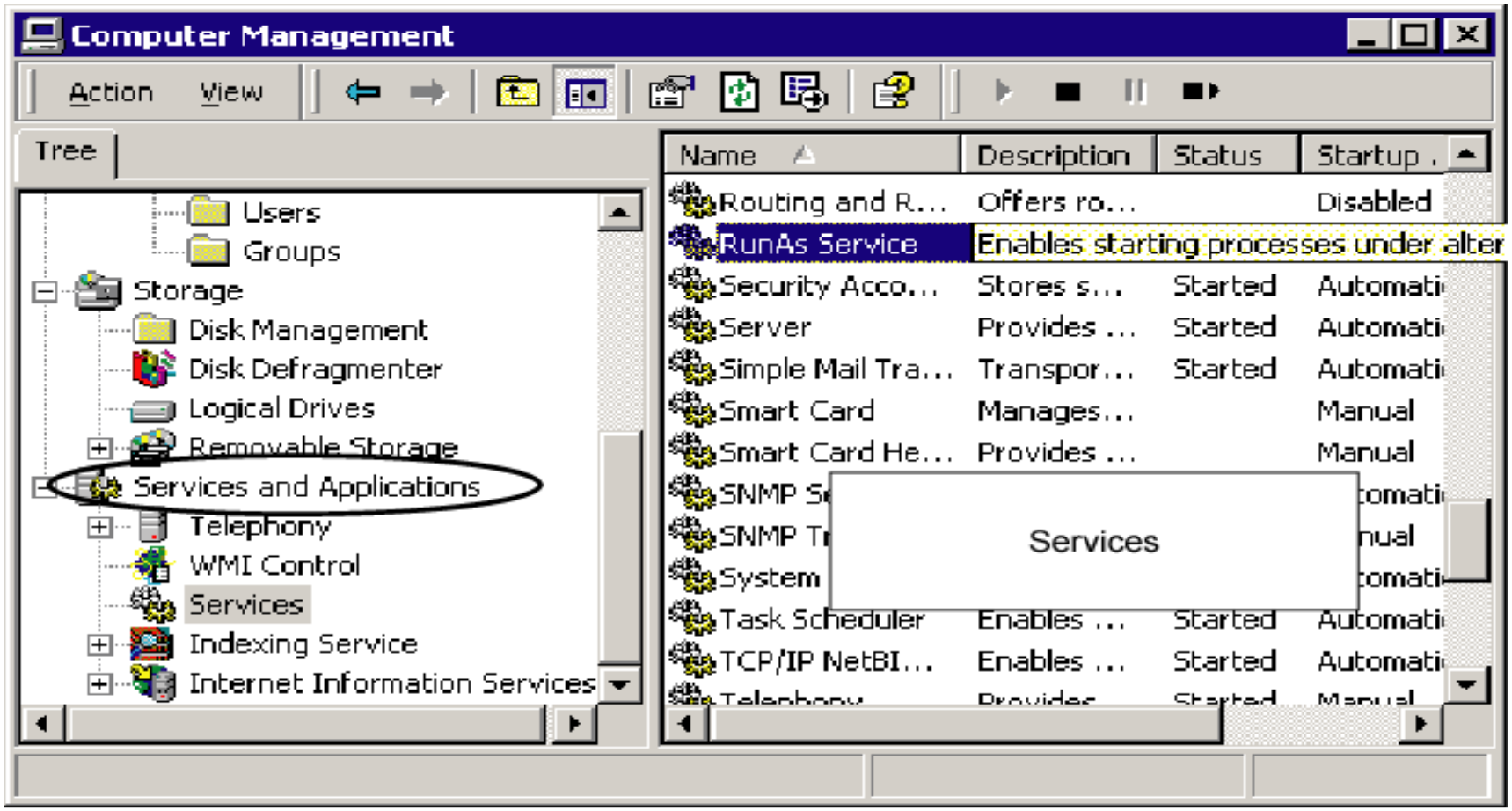
- Most Windows hardening done using Graphical User Interface

Figure 6-2: Windows 2000 Server User Interface



Windows Hardening

- Turning services and applications on/off in Windows



Q: Reducing services can increase host load and decrease performance: T F

Windows Hardening

- Domain configuration and directory service needed for central security setting
- Windows 2000 introduced hierarchical domain structure with Active Directory
    - Domain is a collection of resources
    - Domain contains one or more domain controllers, member servers, client PCs
    - Group policy objects (GPOs) on a domain controller can implement security policies throughout a domain

UNIX / Linux Hardening

- Many versions of UNIX
  - No standards guideline for hardening
- User can select the user interface
  - Graphic User Interface (GUI)
  - Command-Line Interfaces (CLIs) or shells
- CLIs are case-sensitive with commands in lowercase except for file names

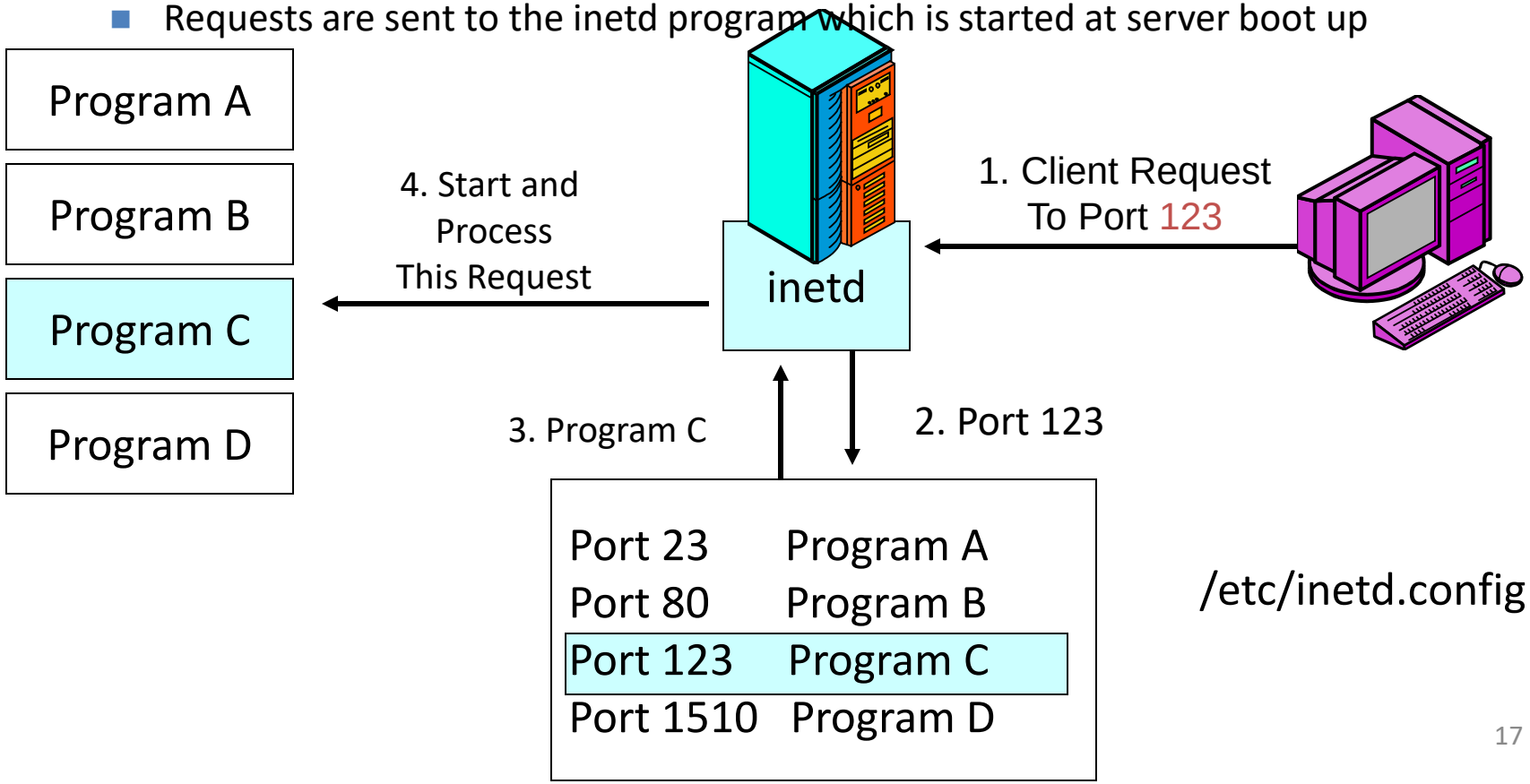
UNIX / Linux Hardening

- Three ways to start services
  - inetd program used to start services when requests come in from users
  - rc scripts to start services automatically at boot up
  - Start a service manually by typing its name or executing a batch file that does so

Inetd = Internet daemon; i.e. a computer program that runs in the background

UNIX / Linux Hardening

- Starting services upon client requests
  - Services not frequently used are dormant
  - Requests do not go directly to the service
  - Requests are sent to the inetd program which is started at server boot up



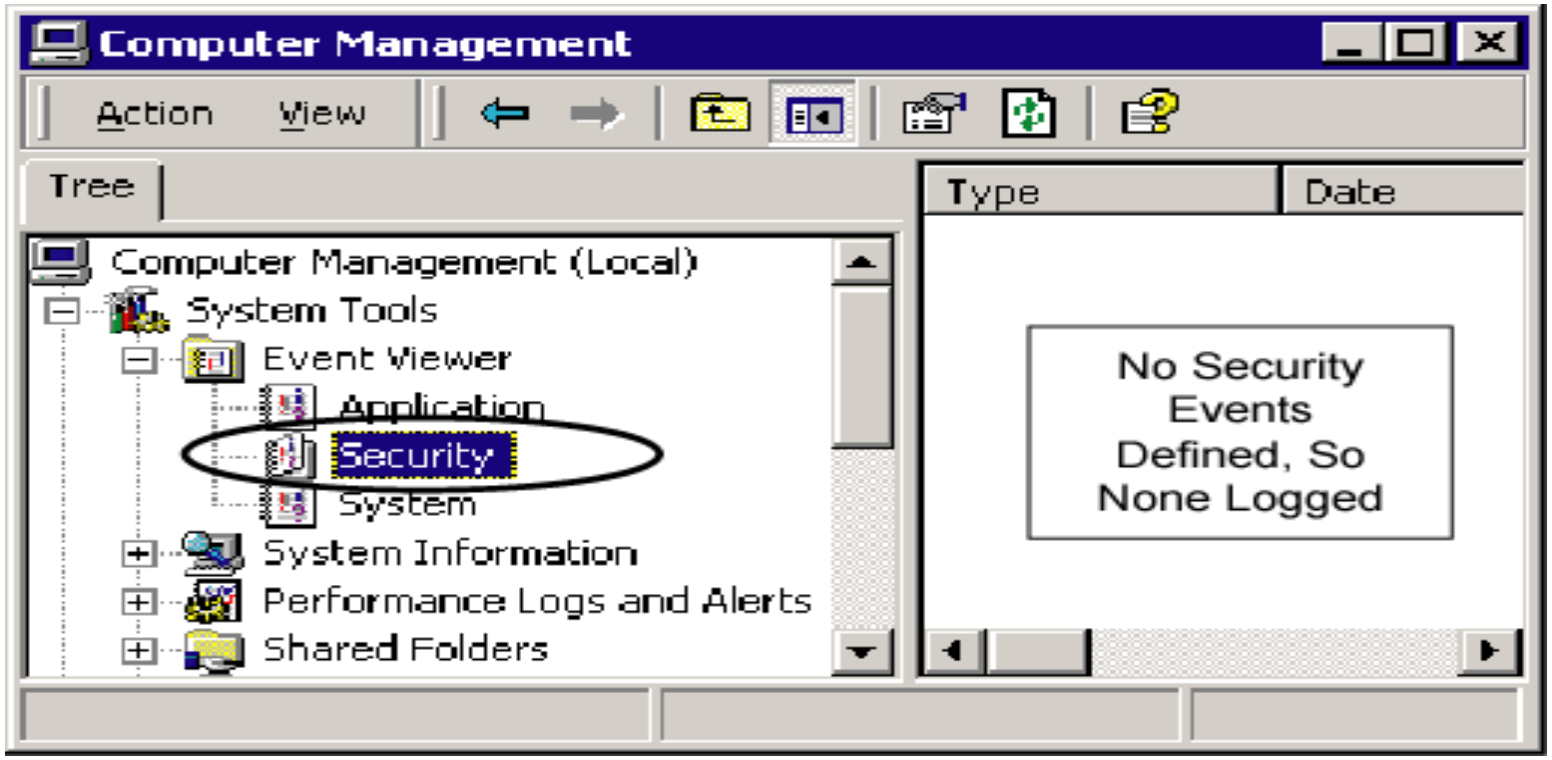
UNIX / Linux Hardening

- Turning On/Off unnecessary Services In UNIX
  - Identifying services running at any moment
    - *ps* command (processor status), usually with –aux parameters, lists running programs
      - Shows process name and process ID (PID)
    - *netstat* tells what services are running on what ports
  - Turning Off Services In UNIX
    - kill PID command is used to kill a particular process
      - » kill 47 (If PID=47)

Q: You kill some services but see that they are running again the next day. Explain why?

Advanced Server Hardening Techniques

- Need to read Event Logs to diagnose problems
  - Failed logins, changing permissions, starting programs, kernel messages, etc.



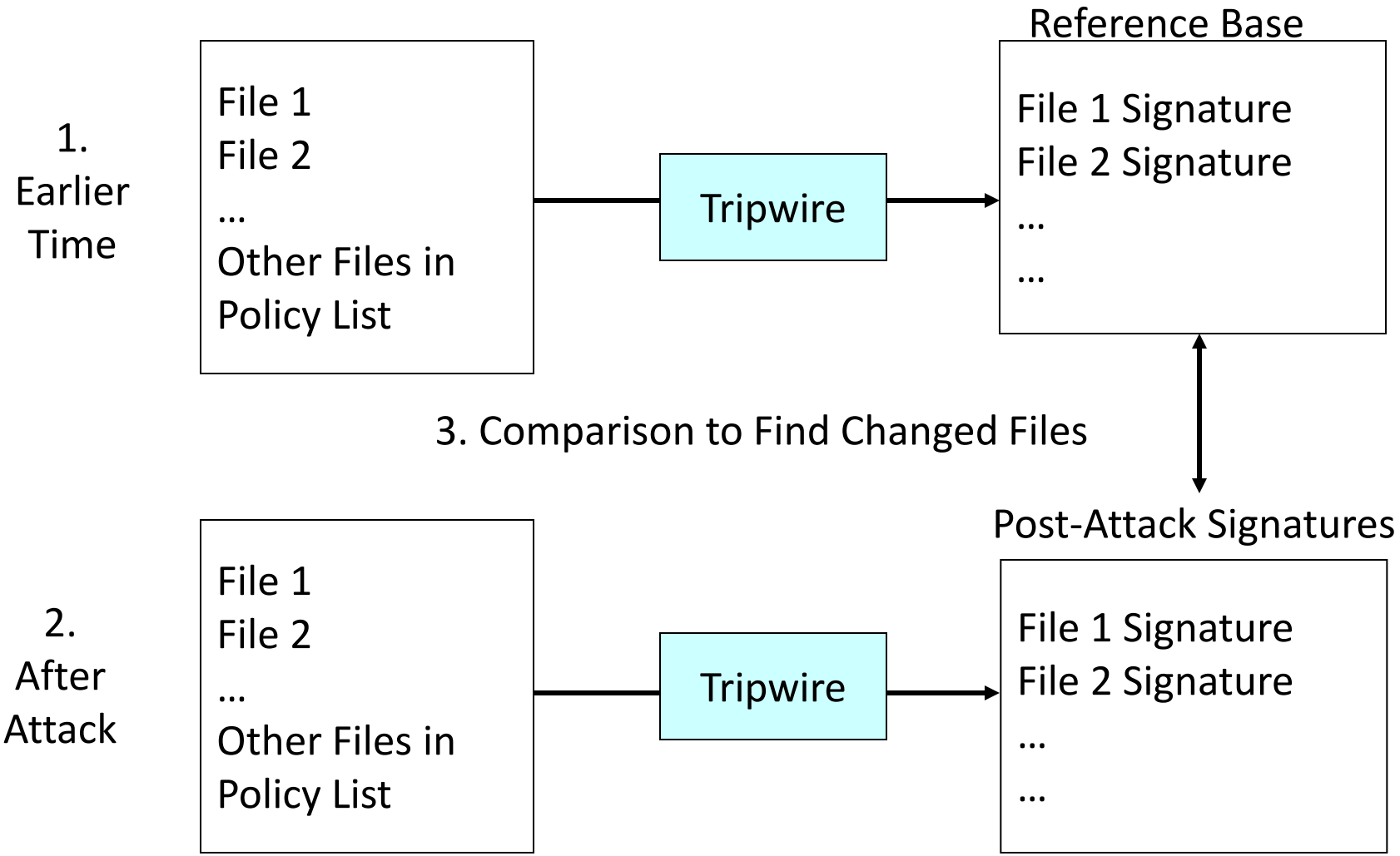
Advanced Server Hardening Techniques

- File Encryption
  - Protects files even if attacker breaks in
  - Key escrow: Copy of encryption key is kept elsewhere to protect in case of key loss
  - Windows Encrypting File System (EFS)
    - Select file in Windows Explorer, select Properties
    - Click on General tab's Advanced button
    - Click on the box Encrypt contents to secure data

Advanced Server Hardening Techniques

- File Integrity Checker
  - Creates snapshot of files: a hashed signature (message digest) for each file
  - After an attack, compares post-hack signature with snapshot
  - This allows systems administrator to determine which files were changed
  - Tripwire is a file integrity checker for Linux/UNIX, Windows, etc.: www.tripwire.com (ftp://coast.cs.purdue.edu/pub/tools/unix)

Advanced Server Hardening Techniques



File Integrity problem: many files change for legitimate reasons. So it is difficult to know which ones the attacker changed.

Other types of host that can be Hardened

- Internetwork Operating System (IOS)
  - For Cisco Routers, Some Switches, Firewalls
- Even cable modems with web-based management interfaces

How You Can Protect Yourself

- **Create a simple security plan – a checklist of what security gaps they need to fill**
  - Security rules for the home
  - Use of credit cards
  - Use of web and e-mail
  - Regular credit checking
  - Physical and document security
  - Use of security technologies
  - Care in the office

How You Can Protect Yourself

- **Create an ID theft response plan:**
  - What credit agencies to contact and how
  - All bank and credit card account details
  - Bank and credit card company contacts
  - Copy of an ID theft affidavit
  - Local police contact
  - List of all SSNs in the home
  - List of all missing or misused checks, with numbers
  - Outstanding ATM and check cards

How You Can Protect Yourself

- **Check credit reports at least every three months**
  - The more often you check, the less damage will be done
  - Understand what you're reading
  - Consumers need to be careful of the service they choose
  - Use strong passwords for credit accounts
  - Consider using a credit monitoring service

How You Can Protect Yourself

- **Don’t leave mail unattended in public places**
  - Mail theft is often the first, last and easiest step in identity theft
  - Don’t leave mail to be collected in a public place
  - Avoid making payments by mail.

    Pay online instead
  - Collect check books and ATM cards from the bank – don’t have the bank mail them
  - Have your mail collected when on vacation

How You Can Protect Yourself

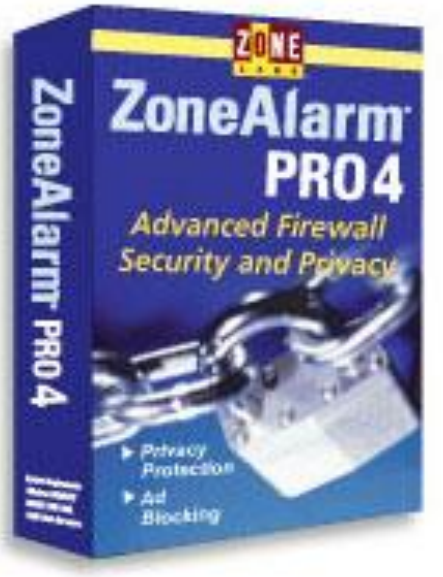
- **Protect social security numbers or other personal financial information**
  - Most ID thefts are based on combining pieces of information. The SSN is the holy grail
  - Never reveal your SSN over the phone, or send by e-mail
  - Don't give it to businesses that request it as an identifier
  - Make sure that third parties that have it, such as CPAs, protect it
  - Beware of phishing and email scams
  - Protect it from family and friends

How You Can Protect Yourself

- **Protect social security numbers or other personal financial information**
  - Most ID thefts are based on combining pieces of information. The SSN is the holy grail
  - Never reveal your SSN over the phone, or send by e-mail
  - Don't give it to businesses that request it as an identifier
  - Make sure that third parties that have it, such as CPAs, protect it
  - Beware of phishing and email scams
  - Protect it from family and friends

How You Can Protect Yourself

- **Protect every computer you use in the home**
  - Firewall
  - Virus protection
  - Spyware protection
  - Data encryption
  - Patching and updating
  - Privacy measures



What Your Organization Can Do

- **View identity theft as a brand enhancer and a brand enabler**
  - It's time to capitalize on the crime
  - Have a plan in place for prevention, response, and notification
- **Customers don't recognize data theft as the real crime**
  - The real crime is (a) what's done with the data and (b) what you failed to do
- **Educate your customers**
  - They're a captive audience
  - They want to trust you
  - They'll appreciate the help
  - Talking about security is *not* a bad thing
  - Focus on phishing

What Your Organization Can Do

- **Educate your employees**
  - Saturation awareness training
  - Policies and rules
  - Data classification and protection
  - Encryption
- **Communicate and Counsel**
  - Notify quickly, clearly, and honestly
  - Provide a hotline
  - Provide victim assistance and resolution
- **View a breach of trust as an opportunity**
  - to create better trust and a stronger relationship