Chapter 13

Network Security

- Transparent to the end users
- Blocking external attackers from accessing the network
- Permitting access to only authorized users
- Preventing attacks from sourcing internally
- Supporting different levels of user access
- Safeguarding data from tampering or misuse

Chapter 13

Reconnaissance and Port Scanning

- •NMAP
- •Superscan
- •NetStumbler
- •Kismet

- •Vulnerability
  - –Nessus
  - –SAINT
  - –MBSA

  - –CERT CC—http://www.cert.org
  - –MITRE—http://www.cve.mitre.org
  - –Microsoft—http://www.microsoft.com/technet/security/bulletin/summary.mspx
  - –Cisco Security Notices—http://www.cisco.com/en/US/products/

Chapter 13

Unauthorized Access

- **Social engineering**
- **Passwordcracking utilities**
- **Capturing network traffic**

- **Data integrity should ensure that only authorized users can change critical information and guarantee the authenticity of data.**

Chapter 13

Loss of Availability

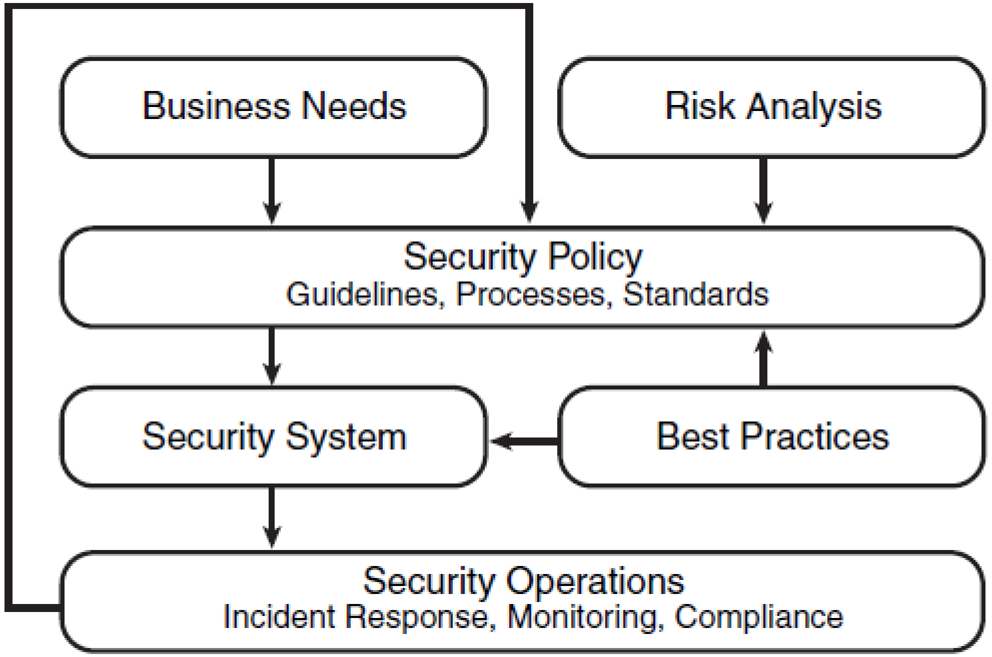
- DoS
  - process large amounts of data
  - unable to handle an unexpected condition

- Combat DoS attacks
  - DHCP snooping
  - Dynamic ARP inspection
  - Unicast RPF
  - Access control lists (ACLs)
  - Rate limiting

Chapter 13

Security Policy and Process

- **Describes the organization’s processes, procedures, guidelines, and standards**



RFC 2196 says, “A security policy is a formal statement of the rules by which people who given access to an organization’s technology and information assets must abide.”

Chapter 13

Basic Approach

- Identify what you are trying to protect.
- Determine what you are trying to protect it from.
- Determine how likely the threats are.
- Implement measures that protect your assets in a cost-effective manner.
- Review the process continuously, and make improvements each time a weakness is found.

Chapter 13

Purpose of Security Policies

- It provides the framework for the security implementation:
  - Identifies assets and how to use them
  - Defines and communicates roles and responsibilities
  - Describes tools and procedures
  - Clarifies incident handling of security events
- It creates a security baseline of the current security posture:
  - Describes permitted and nonpermitted behaviors
  - Defines consequences of asset misuse
  - Provides cost and risk analysis
  - Here are some questions you may need to ask

Chapter 13

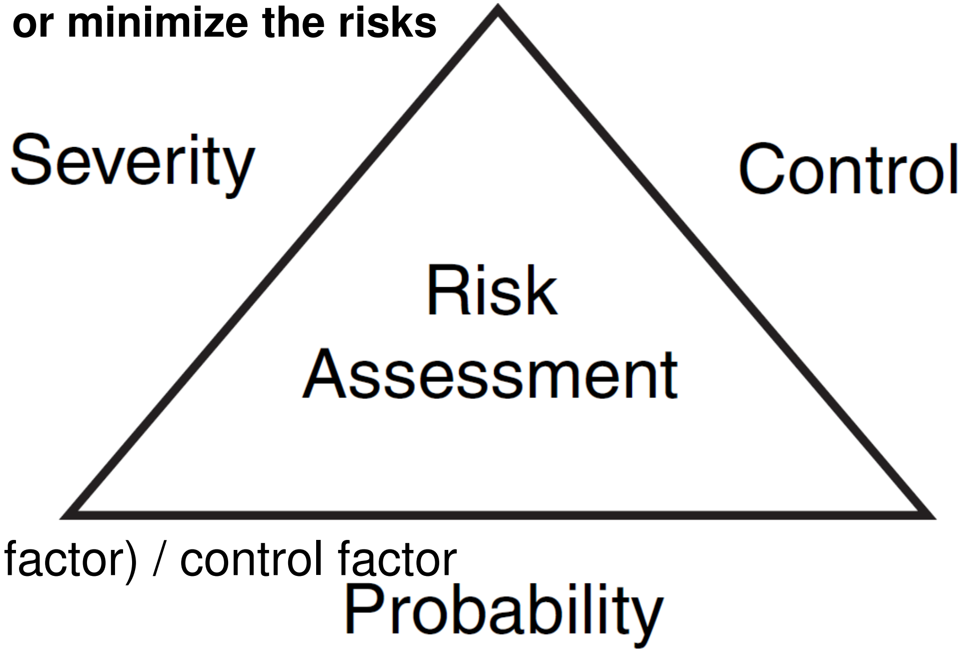
Security Policy Components

- Acceptable-use policy
- Network access control policy
- Security management policy
- Incident-handling policy

Chapter 13

Risk Assessment

- What assets to secure
- The monetary value of the assets
- The actual loss that would result from an attack
- The severity and the probability that an attack against the assets will occur
- How to use security policy to control or minimize the risks

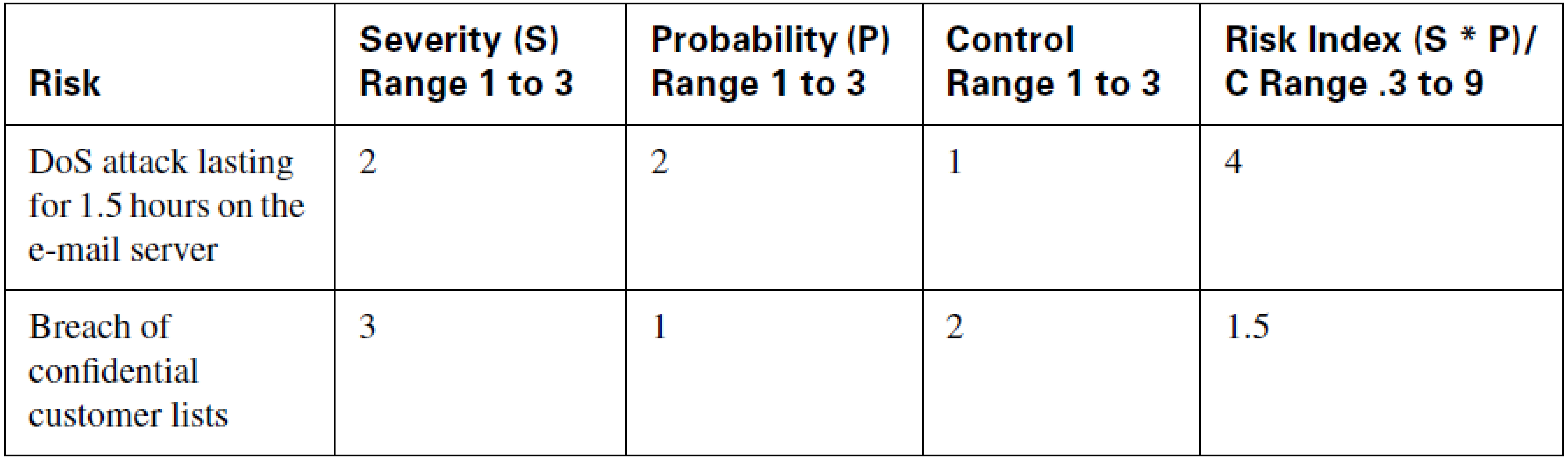


risk index = (severity factor * probability factor) / control factor

Chapter 13

Risk Index Calculation

- risk index = (severity factor * probability factor) / control factor



Risk	Severity (S) Range 1 to 3	Probability (P) Range 1 to 3	Control Range 1 to 3	Risk Index (S * P)/ C Range .3 to 9
DoS attack lasting for 1.5 hours on the e-mail server	2	2	1	4
Breach of confidential customer lists	3	1	2	1.5

Chapter 13

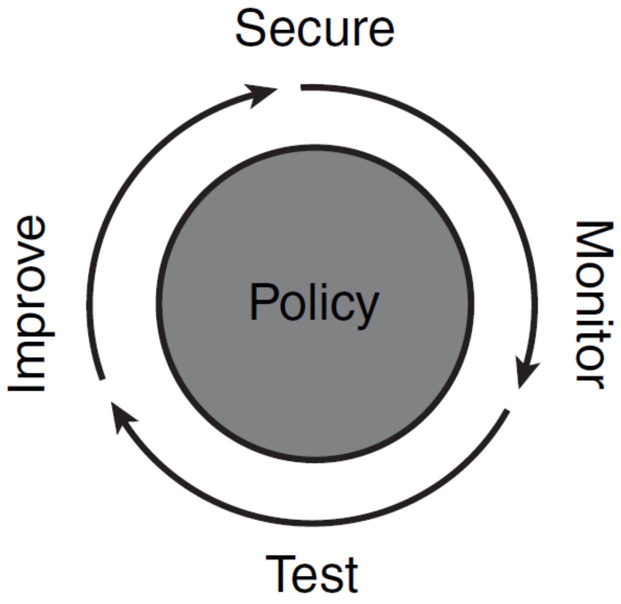
Continuous Security

Secure—Identification, authentication, ACLs, stateful packet inspection(SPI), encryption, and VPNs

Monitor—Intrusion and content-based detection and response

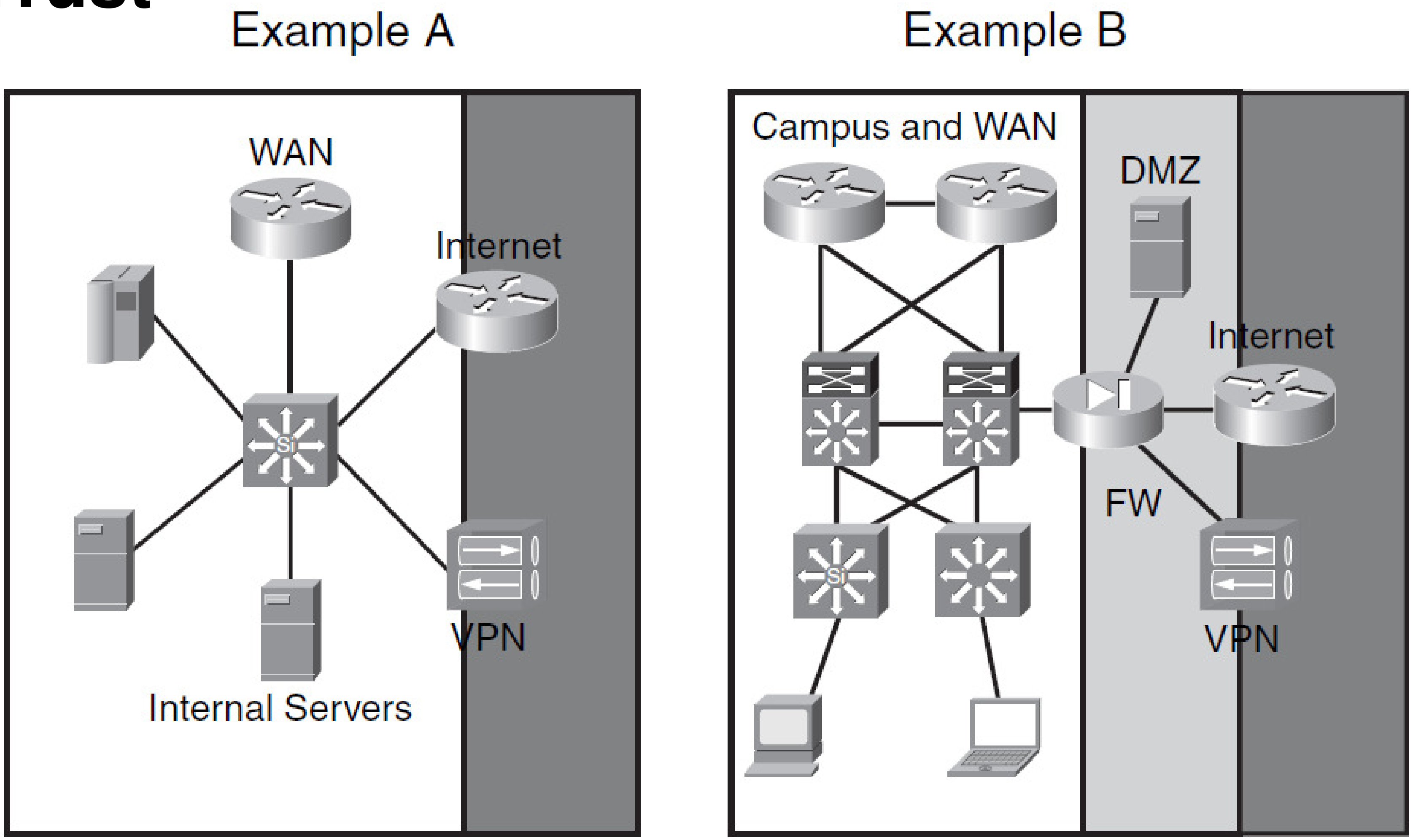
Test—Assessments, vulnerability scanning, and security auditing

Improve—Security data analysis, reporting, and intelligent network security



Chapter 13

Trust



Chapter 13

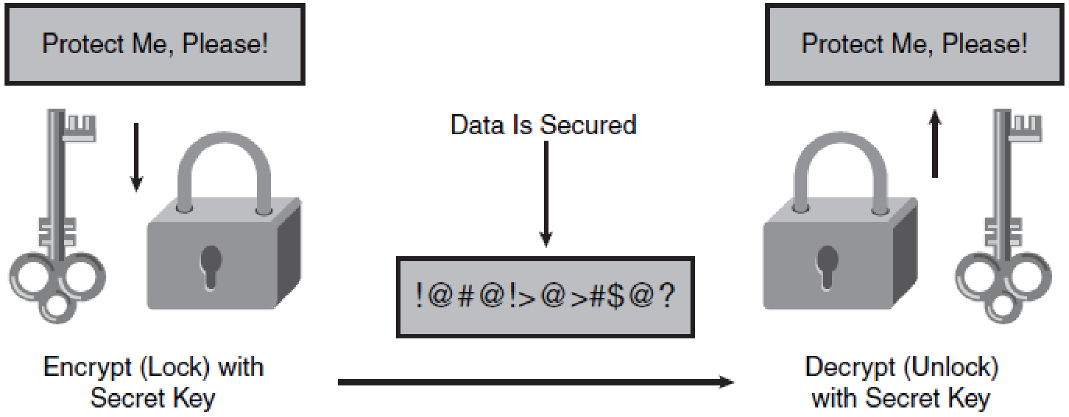
Identity

- Something the subject knows
  - Password
  - PIN
- Something the subject has
  - token card
  - Smartcard
  - hardware key
- Something the subject is
  - Fingerprint
  - retina scan
  - Voice recognition

Chapter 13

Encryption Keys

- Shared secrets
  - Both sides can use the same key or use a transform to create the decryption key.
  - The key is placed on the remote endpoint out of band.
  - This is a simple mechanism, but it has security issues because the key does not change frequently enough
- PKI
  - It relies on asymmetric cryptography, which uses two different keys for encryption.
  - Public keys are used to encrypt and private keys to decrypt.
  - PKI is used by many e-commerce sites on the Internet.



Chapter 13

Physical Security

- Use physical access controls such as locks or alarms.
- Evaluate potential security breaches.
- Assess the impact of stolen network resources and equipment.
- Use controls such as cryptography to secure traffic flowing on networks outside your control.

Chapter 13

Best practices for infrastructure protection

- Access network equipment remotely with SSH instead of Telnet.
- Use AAA for access control management.
- Enable SYSLOG collection; review the logs for further analysis.
- Use SNMPv3 for its security and privacy features.
- Disable unused network services such as tcp-small-servers and udp-small-servers.
- Use FTP or SFTP instead of TFTP to manage images.
- Use access classes to restrict access to management and the CLI.
- Enable routing protocol authentication when available (EIGRP, OSPF, IS-IS, BGP, HSRP,VTP).
- Use one-step lockdown in Security Device Manager (SDM) before connecting the router to the Internet.

Chapter 13

?