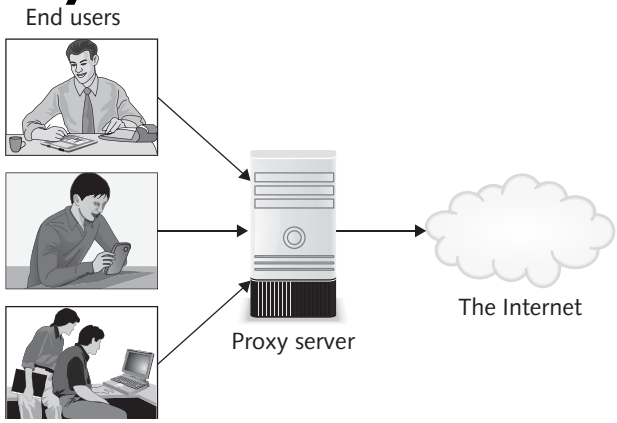
5. Proxy Servers and Virtual Private Networks

- An intermediary between a web browser and another server on the Internet that makes requests to websites, servers, and services on the Internet for you
- A proxy server can hide your IP address and block cookies from being sent to your device.



What is network-layer confidentiality ?

Between two network entities:

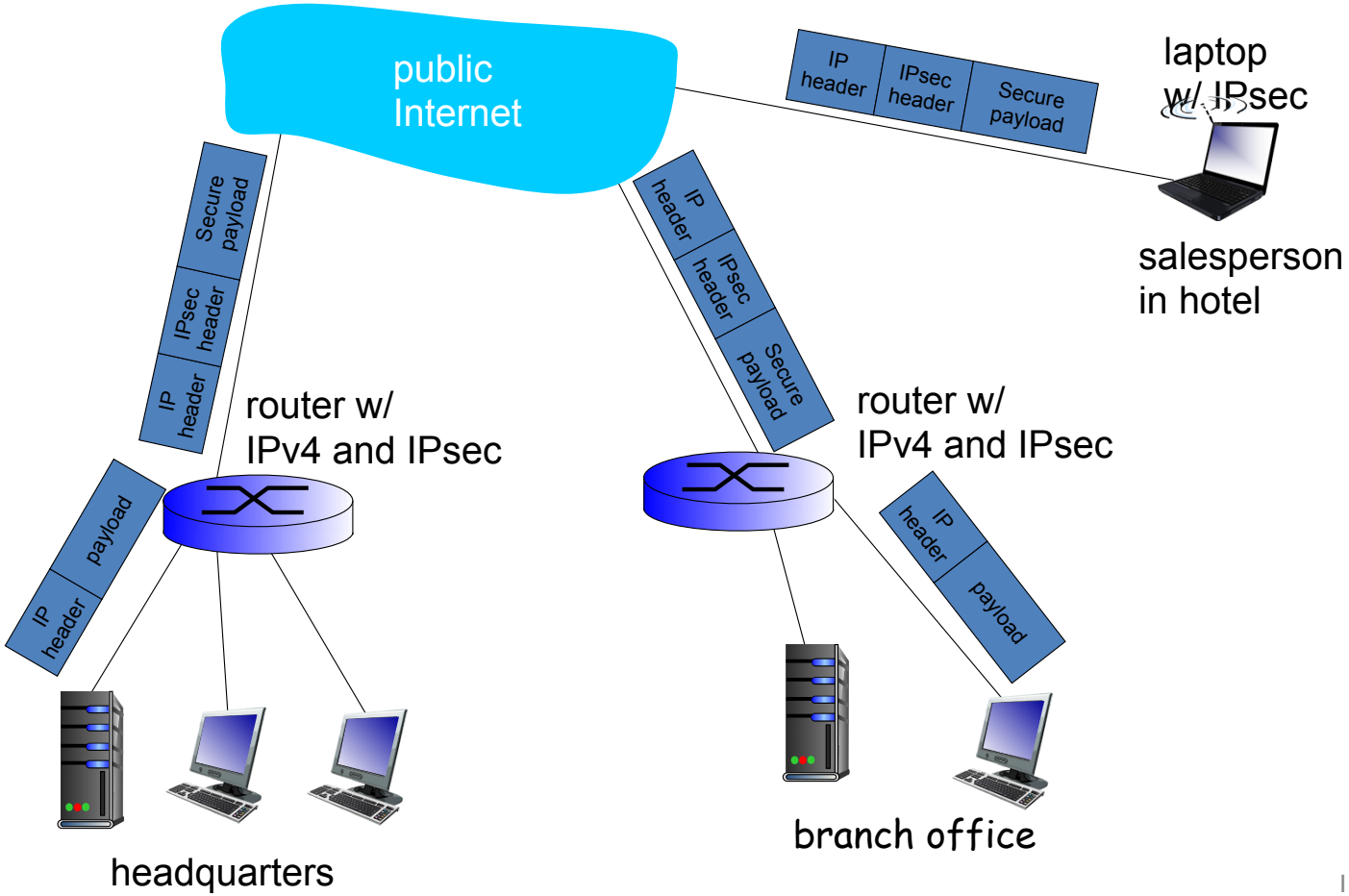
- Sending entity encrypts datagram payload, payload could be:
  - TCP or UDP segment, ICMP message, OSPF message ….
- All data sent from one entity to other would be hidden:
  - web pages, e-mail, P2P file transfers, TCP SYN packets …
- "blanket coverage"

Virtual Private Networks (VPNs)

Motivation:

- Institutions often want private networks for security.
  - costly: separate routers, links, DNS infrastructure.
- VPN: institution's inter-office traffic is sent over public Internet instead
  - encrypted before entering public Internet
  - logically separate from other traffic

Virtual Private Networks (VPNs)



IPsec services

- data integrity
- origin authentication
- replay attack prevention
- confidentiality

- Two protocols providing different service models:
  - AH (Authentication Header)
  - ESP (Encapsulation Security Payload)

Two IPsec protocols

- Authentication Header (AH) protocol
  - provides source authentication & data integrity but *not* confidentiality
- Encapsulation Security Protocol (ESP)
  - provides source authentication, data integrity, *and confidentiality*
  - more widely used than AH

Four combinations are possible!

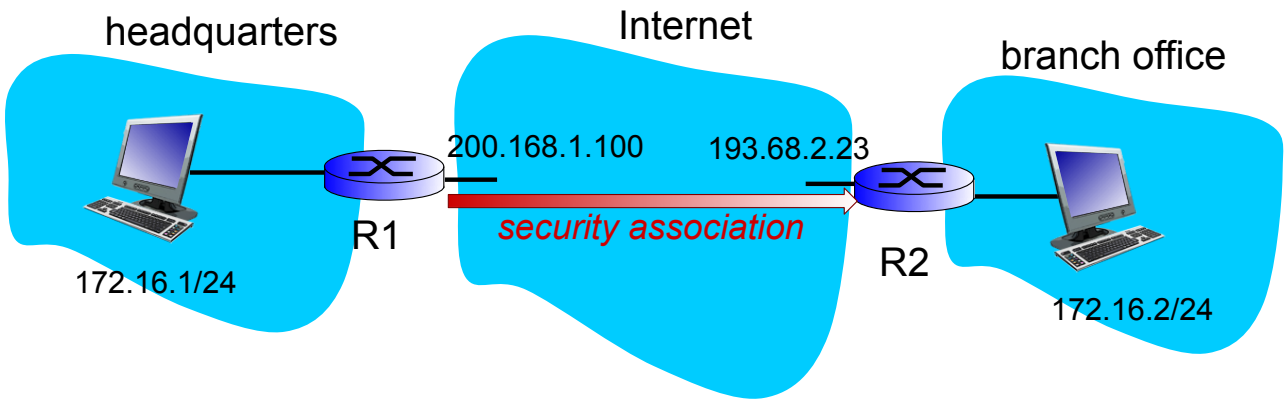
Host mode with AH	Host mode with ESP
Tunnel mode with AH	Tunnel mode with ESP

most common and most important

Security Associations (SAs)

- before sending data, "security association (SA)" established from sending to receiving entity
  - SAs are simplex: for only one direction
- ending, receiving entitles maintain *state information* about SA
  - recall: TCP endpoints also maintain state info
  - IP is connectionless; IPsec is connection-oriented!
- how many SAs in VPN w/ headquarters, branch office, and n traveling salespeople?

Example SA from R1 to R2



R1 stores for SA:

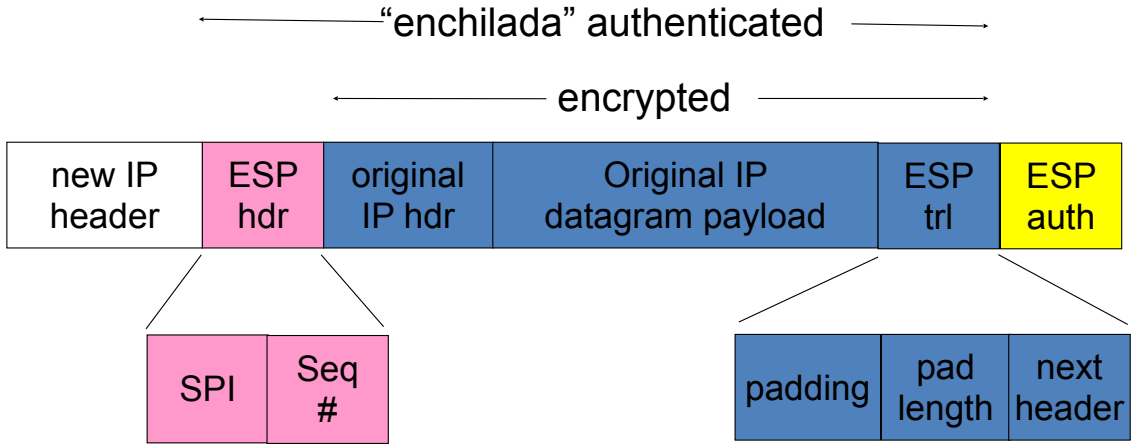
- 32-bit SA identifier: *Security Parameter Index (SPI)*
- origin SA interface (200.168.1.100)
- destination SA interface (193.68.2.23)
- type of encryption used (e.g., 3DES with CBC)
- encryption key
- type of integrity check used (e.g., HMAC with MD5)
- authentication key

Security Association Database (SAD)

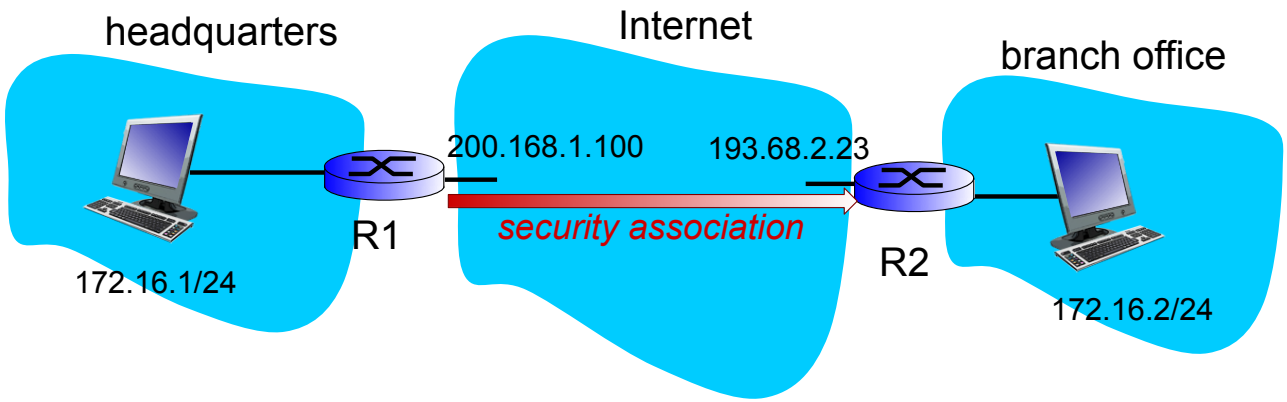
- endpoint holds SA state in *security association database (SAD)*, where it can locate them during processing.
- with n salespersons, 2 + 2n SAs in R1's SAD
- when sending IPsec datagram, R1 accesses SAD to determine how to process datagram.
- when IPsec datagram arrives to R2, R2 examines SPI in IPsec datagram, indexes SAD with SPI, and processes datagram accordingly.

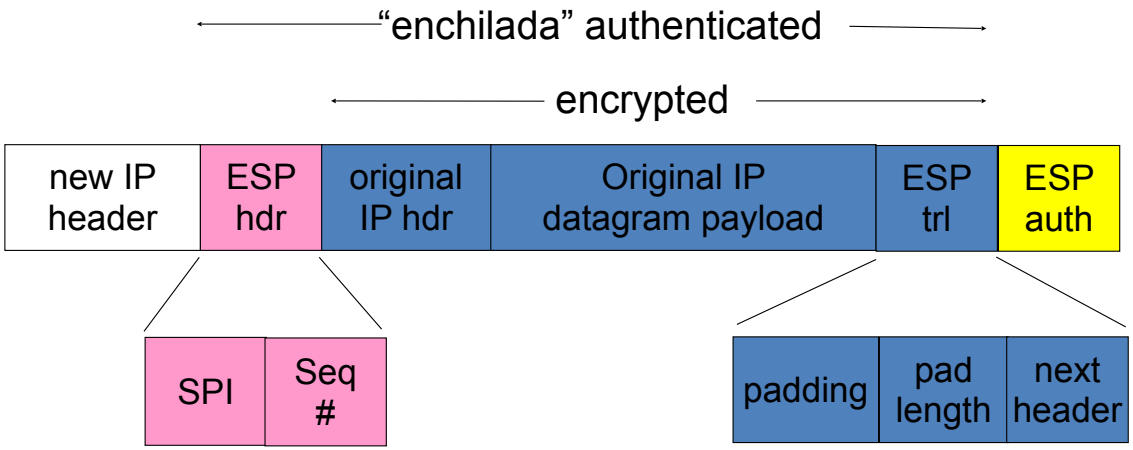
IPsec datagram

focus for now on tunnel mode with ESP



What happens?

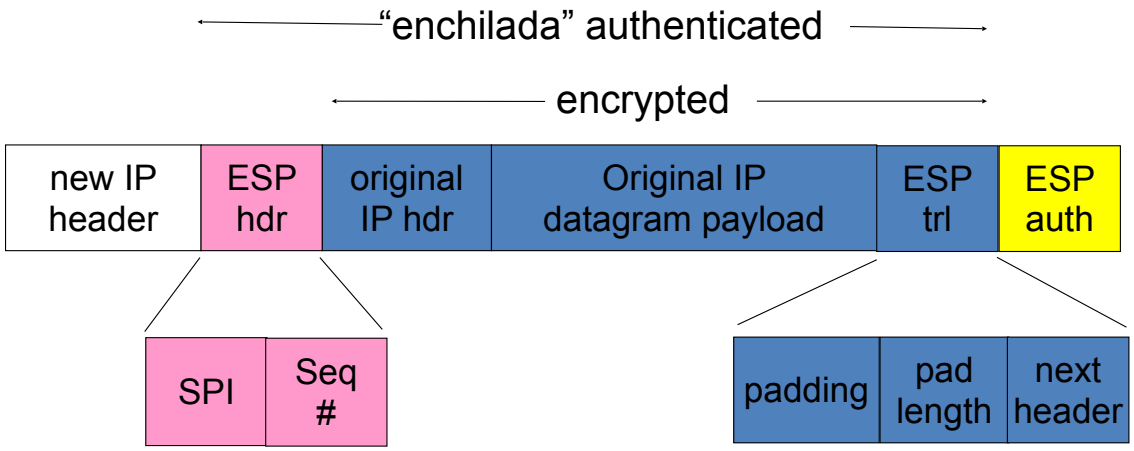




R1: convert original datagram to IPsec datagram

- appends to back of original datagram (which includes original header fields!) an "ESP trailer" field.
- encrypts result using algorithm & key specified by SA.
- appends to front of this encrypted quantity the "ESP header, creating "enchilada".
- creates authentication MAC over the *whole enchilada*, using algorithm and key specified in SA;
- appends MAC to back of enchilada, forming *payload*;
- creates brand new IP header, with all the classic IPv4 header fields, which it appends before payload.

Inside the enchilada:



- ESP trailer: Padding for block ciphers
- ESP header:
  - SPI, so receiving entity knows what to do
  - Sequence number, to thwart replay attacks
- MAC in ESP auth field is created with shared secret key

IPsec sequence numbers

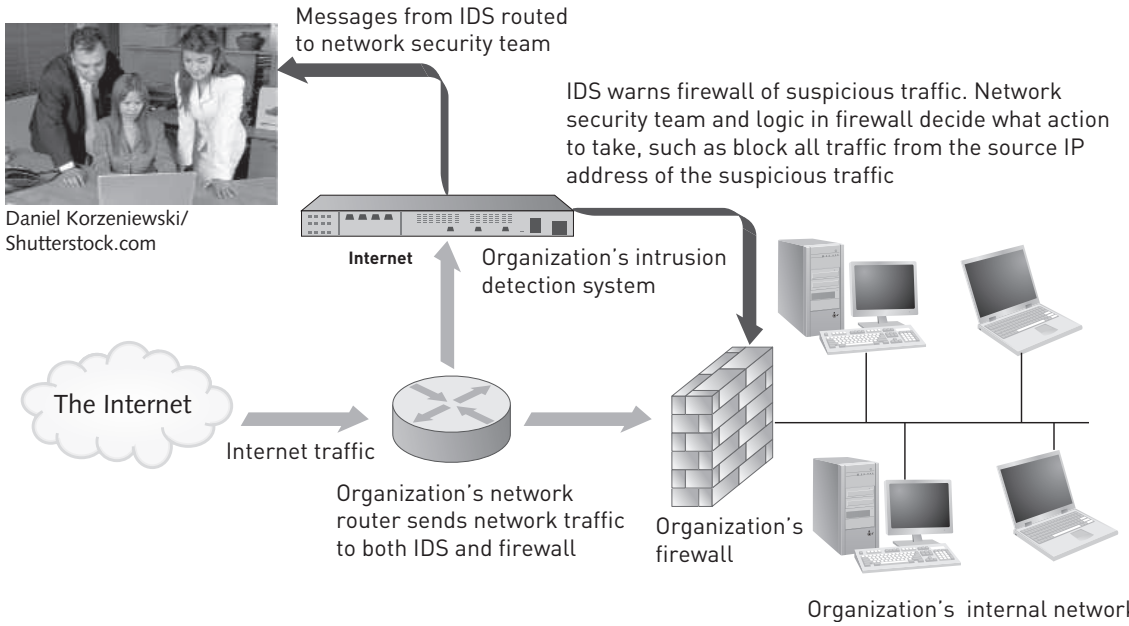
- for new SA, sender initializes seq. # to 0
- each time datagram is sent on SA:
  - sender increments seq # counter
  - places value in seq # field
- **goal:**
  - prevent attacker from sniffing and replaying a packet
  - receipt of duplicate, authenticated IP packets may disrupt service
- **method:**
  - destination checks for duplicates
  - doesn't keep track of *all* received packets; instead uses a window

Security Policy Database (SPD)

- policy: For a given datagram, sending entity needs to know if it should use IPsec
- needs also to know which SA to use
  - may use: source and destination IP address; protocol number
- info in SPD indicates **"what"** to do with arriving datagram
- info in SAD indicates **"how"** to do it

6. Intrusion detection system (IDS)

- Software and/or hardware that monitors system and network resources and activities and notifies network security personnel when it detects network traffic that attempts to circumvent the security measures of a networked computer environment

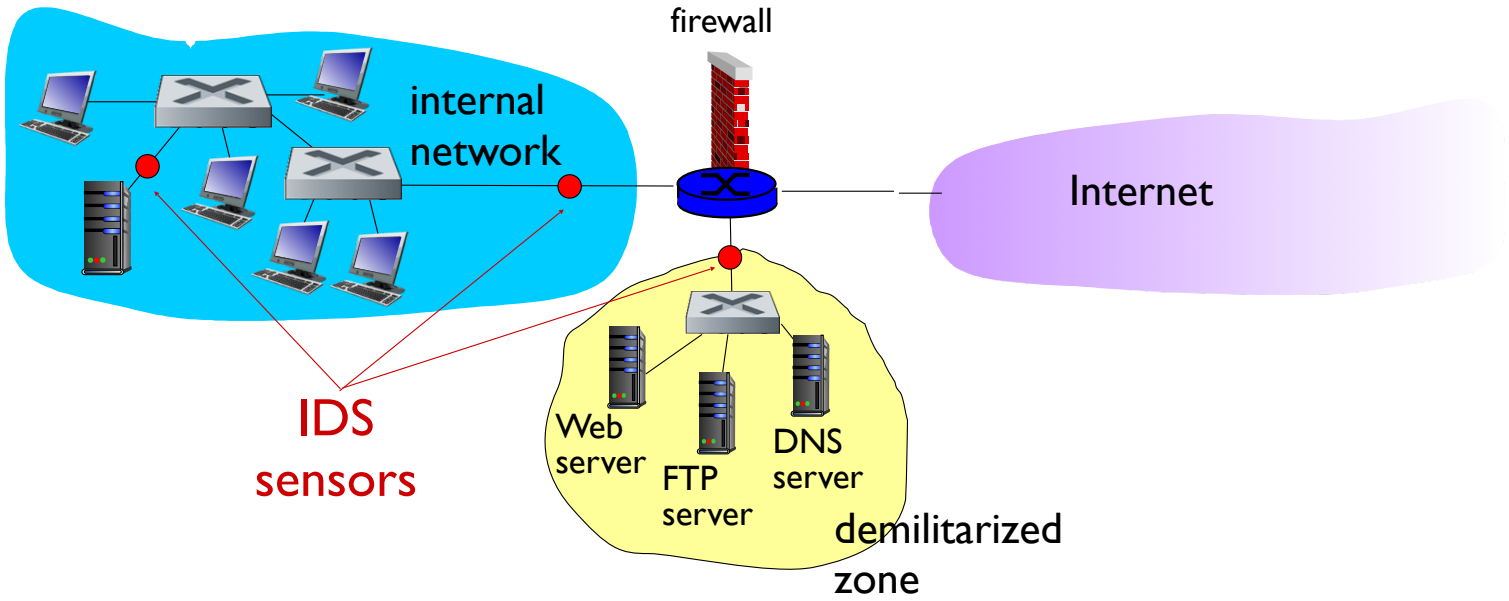


Intrusion detection systems

- Packet filtering:
  - operates on TCP/IP headers only
  - no correlation check among sessions
- ***IDS: intrusion detection system***
  - ***deep packet inspection:*** **look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)**
  - Examine correlation among multiple packets
    - Port scanning
    - Network mapping
    - DoS attack

Intrusion detection systems

- Multiple IDSs: different types of checking at different locations



IDS Types:

- **Knowledge-based:** Contain information about specific attacks and system vulnerabilities and watch for attempts to exploit these vulnerabilities:
  - Repeated failed login attempts or recurring attempts to download a program to a server
- **A behavior-based:** IDS models normal behavior of a system and its users from reference information collected by various means. The IDS compares current activity to this model and generates an alarm if it finds a deviation.
  - Unusual traffic at odd hours or a user in the human resources department who accesses an accounting program that he or she has never before used.

Contents

- ➢ Implementing Trustworthy Computing
  - ◇ CIA Security Triad
  - ◇ Implementing CIA at the Organization Level
    - ✦ Risk Assessment, Disaster Recovery, Security Policy, Security Audit, Regulatory Standards Compliance, Security Dashboard
  - ◇ Implementing CIA at the Network Level
    - ✦ Authentication Methods, Firewall, Routers, Encryption, VPN, IDS
  - ◇ Implementing CIA at the Application Level
    - ✦ User Roles and Accounts, Data Encryption
  - ◇ Implementing CIA at the End-User Level
    - ✦ Security Education, Authentication Methods, Antivirus Software
  - ◇ Response to CyberAttack

CIA at Application Level:

1. Authentication methods
   - Two factor authentication (Something you know/have/are to make a login)
2. User roles and accounts
   - Creation of roles and user accounts with responsibilities
3. Data encryption
   - Encryption in ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), and PLM (Product Lifecycle Management)

Contents

- ➢ Implementing Trustworthy Computing
  - ◇ CIA Security Triad
  - ◇ Implementing CIA at the Organization Level
    - ✦ Risk Assessment, Disaster Recovery, Security Policy, Security Audit, Regulatory Standards Compliance, Security Dashboard
  - ◇ Implementing CIA at the Network Level
    - ✦ Authentication Methods, Firewall, Routers, Encryption, VPN, IDS
  - ◇ Implementing CIA at the Application Level
    - ✦ User Roles and Accounts, Data Encryption
  - ◇ Implementing CIA at the End-User Level
    - ✦ Security Education, Authentication Methods, Antivirus Software
  - ◇ Response to CyberAttack

Educating Employees, Contractors, and Part-Time Workers

- **Educate users** about the importance of security
  – Motivate them to understand and follow security policy
- **Discuss recent security incidents** that affected the organization
- **Help protect information systems by:**
  1. Guarding passwords
  2. Not allowing others to use passwords
  3. Applying strict access controls to protect data
  4. Reporting all unusual activity
  5. Taking care of portable computing and data storage devices

Self Assessment Security Test

Security assessment question
Do you have the most current version of your computer's operating system installed?
Do you have the most current version of firewall, antivirus, and malware software installed?
Do you install updates to all your software when you receive notice that a new update is available?
Do you use different, strong passwords for each of your accounts and applications—a minimum of 10 characters, with a mix of capital and lowercase letters, numbers, and special characters?
Are you familiar with and do you follow your organization's policies in regard to accessing corporate websites and applications from your home or remote locations (for example, access via a VPN)?
Have you set the encryption method to WPA2 and changed the default name and password on your home wireless router?
When using a free, public wireless network, do you avoid checking your email or accessing websites requiring a username and password?
Do you refrain from clicking on a URL in an email from someone you do not know?
Do you back up critical files to a separate device at least once a week?
Are you familiar with and do you follow your organization's policies regarding the storage of personal or confidential data on your device?
Does your device have a security passcode that must be entered before it accepts further input?
Have you installed Locate My Device or similar software in case your device is lost or stolen?
Do you make sure not to leave your device unattended in a public place where it can be easily stolen?
Have you reviewed and do you understand the privacy settings that control who can see or read what you do on Facebook and other social media sites?

Contents

- ➢ Implementing Trustworthy Computing
  - ◇ CIA Security Triad
  - ◇ Implementing CIA at the Organization Level
    - ✦ Risk Assessment, Disaster Recovery, Security Policy, Security Audit, Regulatory Standards Compliance, Security Dashboard
  - ◇ Implementing CIA at the Network Level
    - ✦ Authentication Methods, Firewall, Routers, Encryption, VPN, IDS
  - ◇ Implementing CIA at the Application Level
    - ✦ User Roles and Accounts, Data Encryption
  - ◇ Implementing CIA at the End-User Level
    - ✦ Security Education, Authentication Methods, Antivirus Software
  - ◇ Response to CyberAttack

Response to CyberAttack

- **Response plan**
  - Develop well in advance of any incident
  - Approved by
    - Legal department
    - Senior management
- **Primary goals**
  - Regain control
  - Limit damage

1. Incident Notification

- **Incident notification defines**
  - Who to notify
  - Who *not* to notify
- Security experts recommend **against** releasing specific information about a security compromise in public forums
- **Ethical Decision:** what to tell customers and others whose personal data may have been compromised by a computer incident?

2. Protect of Evidence and Activity Logs

- **Document** all details of a security incident
  - All system events
  - Specific actions taken
  - All external conversations

3. Incident Containment and Eradication

- Act **quickly** to contain an attack
- **Eradication effort**
  - Collect and log all possible criminal evidence from the system
  - Verify necessary backups are current and complete
  - Create new backups

4. Incident Follow-Up

- Determine how security was compromised
  - Prevent it from happening again
  - Write a formal incident report:
    - IP address and name of host computer(s) involved
    - The date and time when the incident was discovered
    - How the incident was discovered
    - The method used to gain access to the host computer
    - A detailed discussion of vulnerabilities that were exploited
    - A determination of whether or not the host was compromised as a result of the attack
    - The nature of the data stored on the computer (customer, employee, financial, etc.)
    - A determination of whether the accessed data are considered personal, private, or confidential
    - The number of hours the system was down
    - The overall impact on the business
    - An estimate of total monetary damage from the incident
    - A detailed chronology of all events associated with the incident

5. Review

- Determine exactly what happened
- Evaluate how the organization responded
  - Capture the perpetrator
    - Consider the potential for negative publicity

6. Using an MSSP

- Outsource network security operations to a **managed security service provider (MSSP)**:
  - A company that monitors, manages, and maintains computer and network security for other organizations.
  - MSSPs include such companies as AT&T, Computer Sciences Corporation, Dell SecureWorks, IBM, Symantec, and Verizon.
  - MSSPs provide a valuable service for IT departments drowning in reams of alerts and false alarms coming from VPNs; antivirus, firewall, and IDSs; and other security-monitoring systems.
  - Some MSSPs provide vulnerability scanning and web blocking and filtering capabilities.

7. Computer Forensics

Discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law.

Summation and Forensic Toolkit by Grant Thornton

Grant Thornton has deployed forensic software:

1. Summation (a web-based legal document, electronic data, and transcript review platform that supports litigation teams)
2. Forensic Toolkit (used to scan a hard drive to find a variety of information, including deleted emails and text strings, to crack encryption)

Manager's checklist for assessing an organization's readiness to prevent and respond to a cyberattack

Question
Has a risk assessment been performed to identify investments in time and resources that can protect the organization from its most likely and most serious threats?
Have senior management and employees involved in implementing security measures been educated about the concept of reasonable assurance?
Has a security policy been formulated and broadly shared throughout the organization?
Have automated systems policies been implemented that mirror written policies?
Does the security policy address the following? • Email with executable file attachments • Wireless networks and devices • Use of smartphones deployed as part of corporate rollouts as well as those purchased by end users
Is there an effective security education program for employees and contract workers?
Has a multi-layered CIA security strategy been implemented?
Has a firewall been installed?
Is antivirus software installed on all personal computers?
Is the antivirus software frequently updated?
Have precautions been taken to limit the impact of malicious insiders?
Are the accounts, passwords, and login IDs of former employees promptly deleted?
Are employee responsibilities adequately defined and separated?
Are individual roles defined so that users have authority to perform their responsibilities and nothing more?
Is it a requirement to review at least quarterly the most critical Internet security threats and implement safeguards against them?
Has it been verified that backup processes for critical software and databases work correctly?
Has an intrusion detection system been implemented to catch intruders in the act—both in the network and on critical computers on the network?
Are periodic IT security audits conducted?
Has a comprehensive incident response plan been developed?
Has the security plan been reviewed and approved by legal and senior management?
Does the plan address all of the following areas? • Incident notification • Protection of evidence and activity logs • Incident containment • Eradication • Incident follow-up