Network Penetration

Lesson 1: Introduction + System Fundamentals + Cryptography + Footprinting

Program

- Introduction to ethical hacking
  - Evolution of hacking
  - Attack types
  - Planning
- System Fundamentals
  - Network topologies
  - OSI
  - TCP/IP
  - OS
  - Backup
- Cryptography
  - Applications of cryptography
  - Symmetric and asymmetric cryptography
  - Working with hashing
- Footprinting
  - IP address ranges
  - Namespaces
  - Employee information
  - Phone numbers
  - Facility information
  - Job information
- Exercises

Evolution of hacking

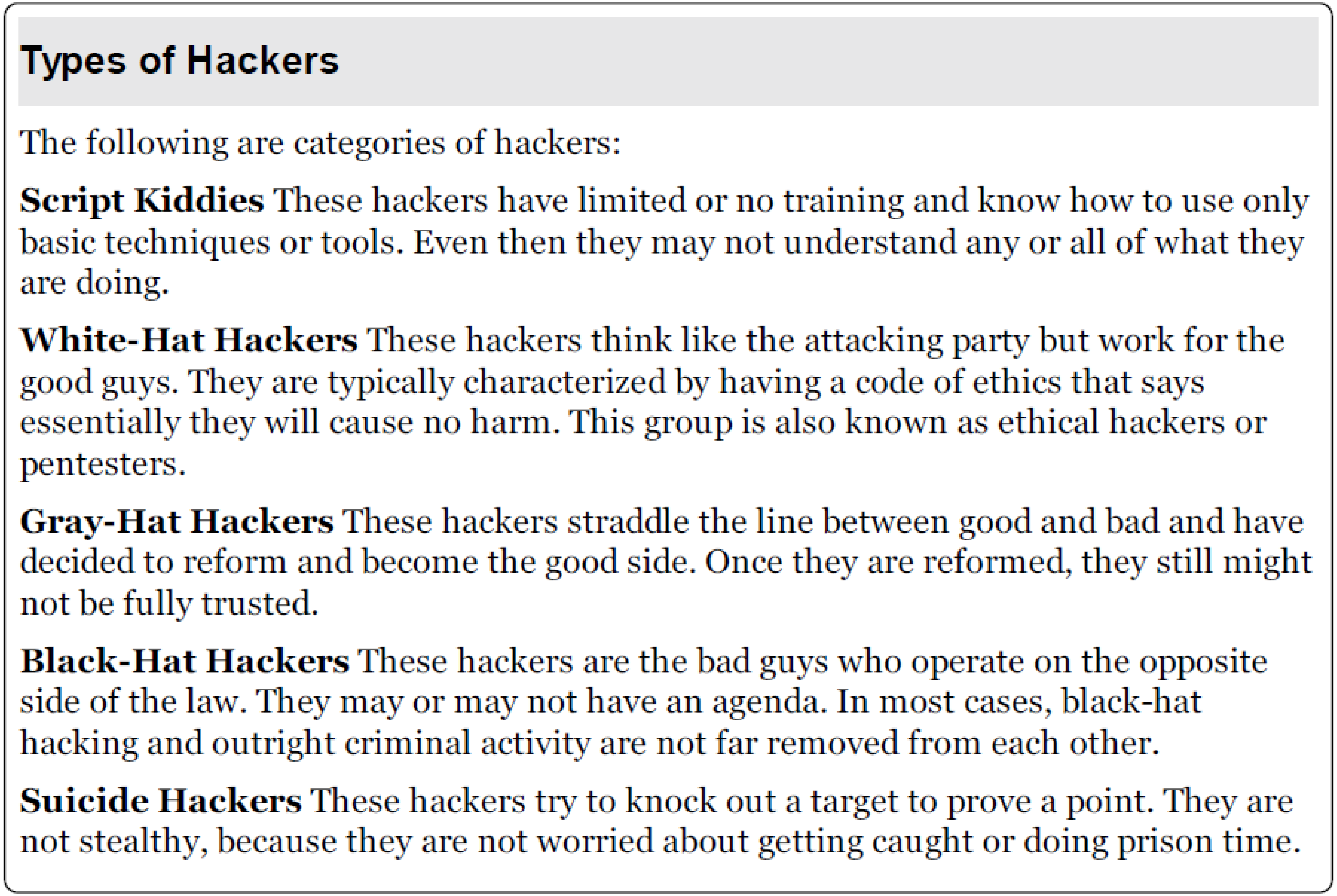
- Pre- 1970 – taking things apart
  - Mostly due to curiosity
- 80’s – Attacking PC’s
  - Via software, distributed using e.g. floppy disks
- 90 – Distributed attacks via the Internet
  - Browsers were targeted, defacing pages, pranking
- 2000 – Attacking devices
  - More malicious attacks

Current attack types

- Denial-of-service attacks
- Manipulation of stock prices
- Identity theft
- Vandalism
- Credit card theft
- Piracy
- Theft of service

Cyber crime types

- Stealing passwords and user names
- Network intrusion
- Social engineering
- Fraud
- Malicious code – virus, worms, spyware…
- Embezzlement
- Denial of service
- Ransomware



Types of Hackers

The following are categories of hackers:

Script Kiddies These hackers have limited or no training and know how to use only basic techniques or tools. Even then they may not understand any or all of what they are doing.

White-Hat Hackers These hackers think like the attacking party but work for the good guys. They are typically characterized by having a code of ethics that says essentially they will cause no harm. This group is also known as ethical hackers or pentesters.

Gray-Hat Hackers These hackers straddle the line between good and bad and have decided to reform and become the good side. Once they are reformed, they still might not be fully trusted.

Black-Hat Hackers These hackers are the bad guys who operate on the opposite side of the law. They may or may not have an agenda. In most cases, black-hat hacking and outright criminal activity are not far removed from each other.

Suicide Hackers These hackers try to knock out a target to prove a point. They are not stealthy, because they are not worried about getting caught or doing prison time.

The ethical hacker

- Testing the security of an organization
- Same skills as a hacker
- Having ***permission*** to carry out attacks
- Does not report found weaknesses to anyone but the system owner
- Work under contract
  - What is off – limit
  - What is expected
  - Keep contract up to date at all times
    - Might get into troubles otherwise

Penetration testing

- Penetration testing
  - Structured and methodical means of
    - Investigating
    - Uncovering
    - Attacking
    - Reporting
      - Strengths and weaknesses of the system
  - Owner can then adjust plans and defenses

Lingo in ethical hacking

- Hack Value – target with above-average level of interest
- Target of Evaluation – system/resource which is being evaluated
- Attack – targeting/engaging a target of evaluation
- Exploit – clearly defined way to breach security of a system
- Zero Day – threat/vulnerability unknown to developers
- Security – state of well-being, only defined actions are allowed
- Threat – potential violation of security
- Vulnerability – weakness in the system, entry point to the system
- Daisy Chaining – several attacks, each building on previous

Testing types

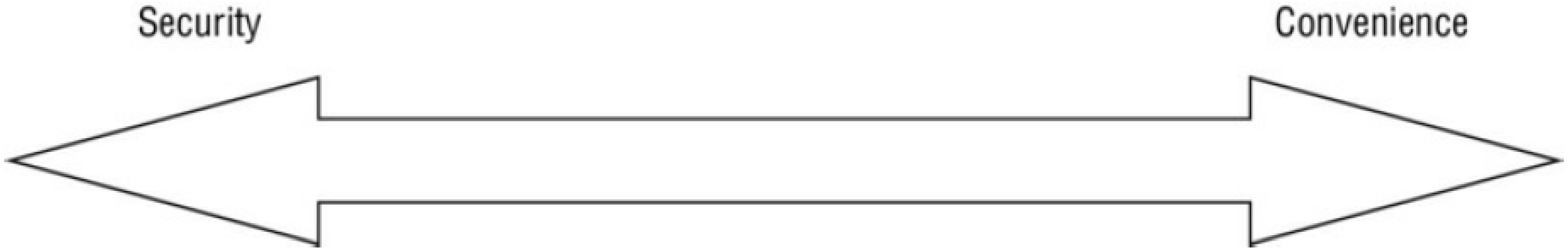
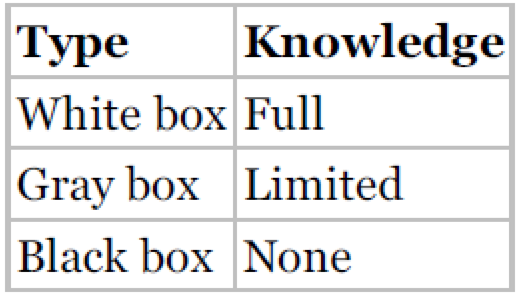


Figure 1.1 Security versus convenience analysis

Table 1.1 Available types of pen tests

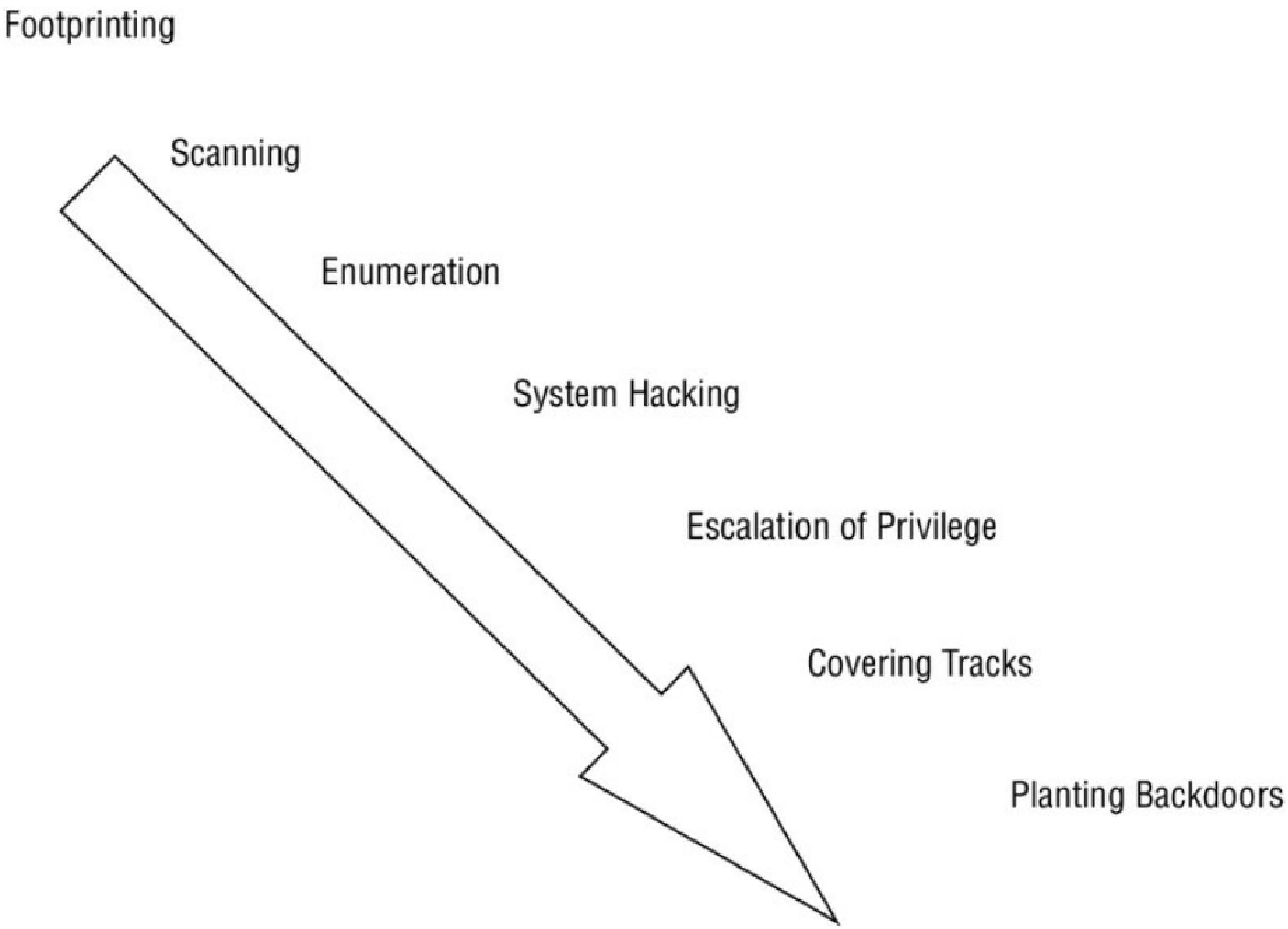


Type	Knowledge
White box	Full
Gray box	Limited
Black box	None

The CIA triad

- When testing, the ethical hacker must preserve the CIA triad:
    - Confidentiality
        - Safeguarding information and keeping it away from unauthorized access
            - Examples: Permission and encryption
    - Integrity
        - The data received is the data that was sent
            - Example: Checksum
    - Availability
        - Keep information and resources available for those who need them
            - Data is useless if it is not available
- Supporting concepts: Non-repudiation and Authenticity
    - Actions cannot be denied, check if source is legitimate and identifiable

Hacking methodologies



Footprinting

Scanning

Enumeration

System Hacking

Escalation of Privilege

Covering Tracks

Planting Backdoors

Figure 1.2 The hacking process

Hacking methodologies

- Footprinting – passively gaining information
- Scanning – actively gaining information
- Enumeration – gaining more precise information
- System hacking – actual attack based on newly acquired information
- Escalating privileges – use information to gain higher privileges
- Covering tracks – remove information of the attack process
- Planting backdoors – ensure access in the future

Plans and policies

- Incident response
  - what to do in case of a security breach
- Incident response policies (IRP)
  - specification on course of action
  - This includes different phases; response, triage, investigation, containment, analysis and tracking, recovery, repair and finally debriefing and feedback
- Incident response plan
  - check IRP, may need update; follow it
- Business continuity plan
  - how to continue the business
- Disaster and recovery plan
  - how to recover in the event of an incident or a disaster

Evidence

- Evidence must be collected
- Various evidence types
- Chain of custody
  - Documents the whereabouts of the evidence at all times
  - Documents who handles evidence at all times
- Evidence can only be used in court if rules are followed:
  - Reliable
  - Preserved
  - Relevant
  - Properly identified
  - Legally permissible

System Fundamentals

Network topologies

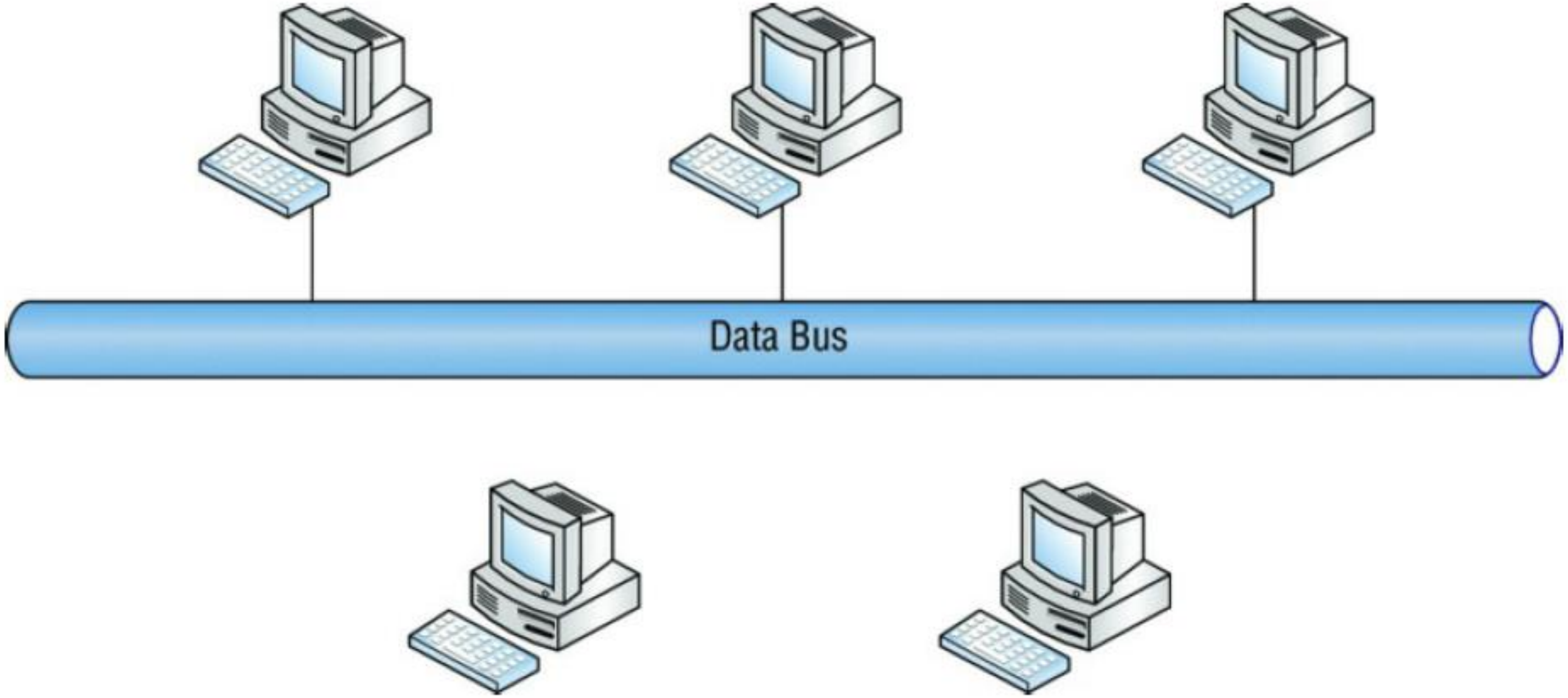


Figure 2.1 Bus topology

Network topologies

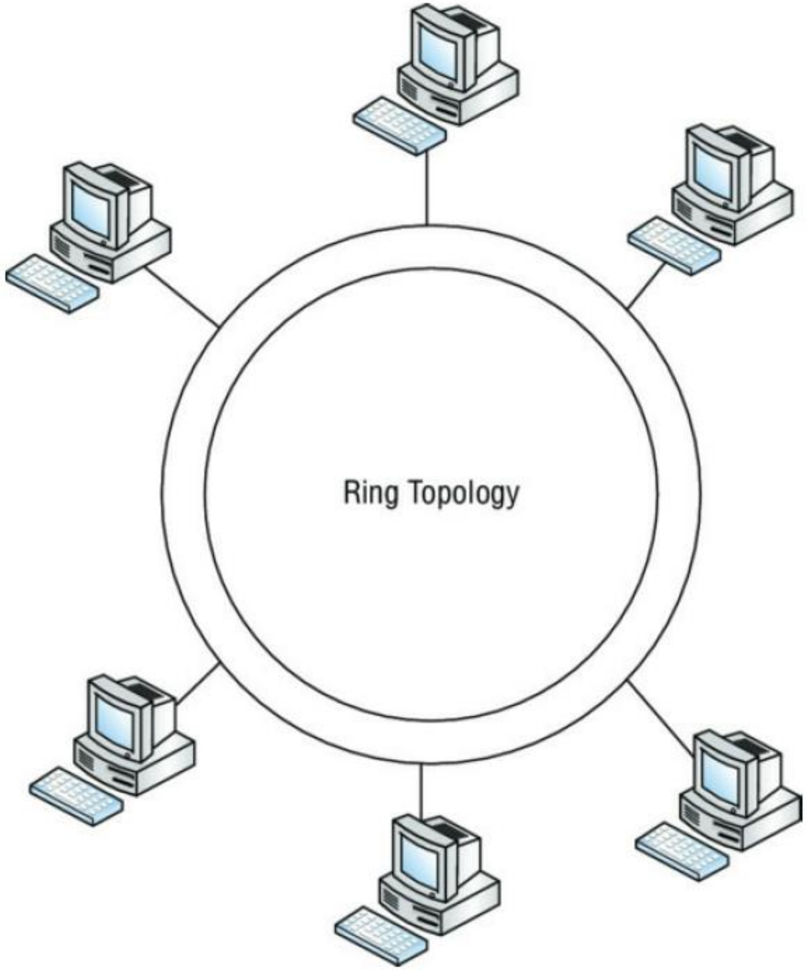


Figure 2.2 Ring topology

Network topologies

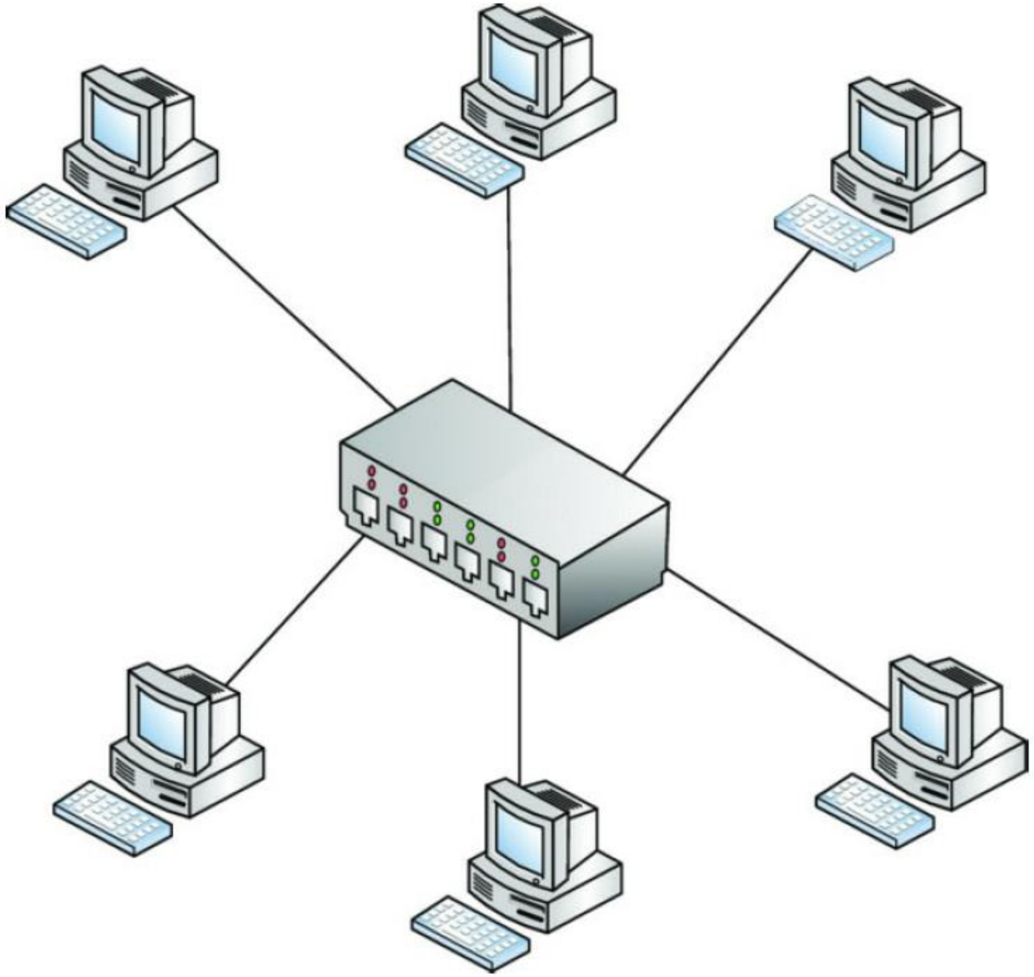


Figure 2.3 Star topology

Network topologies

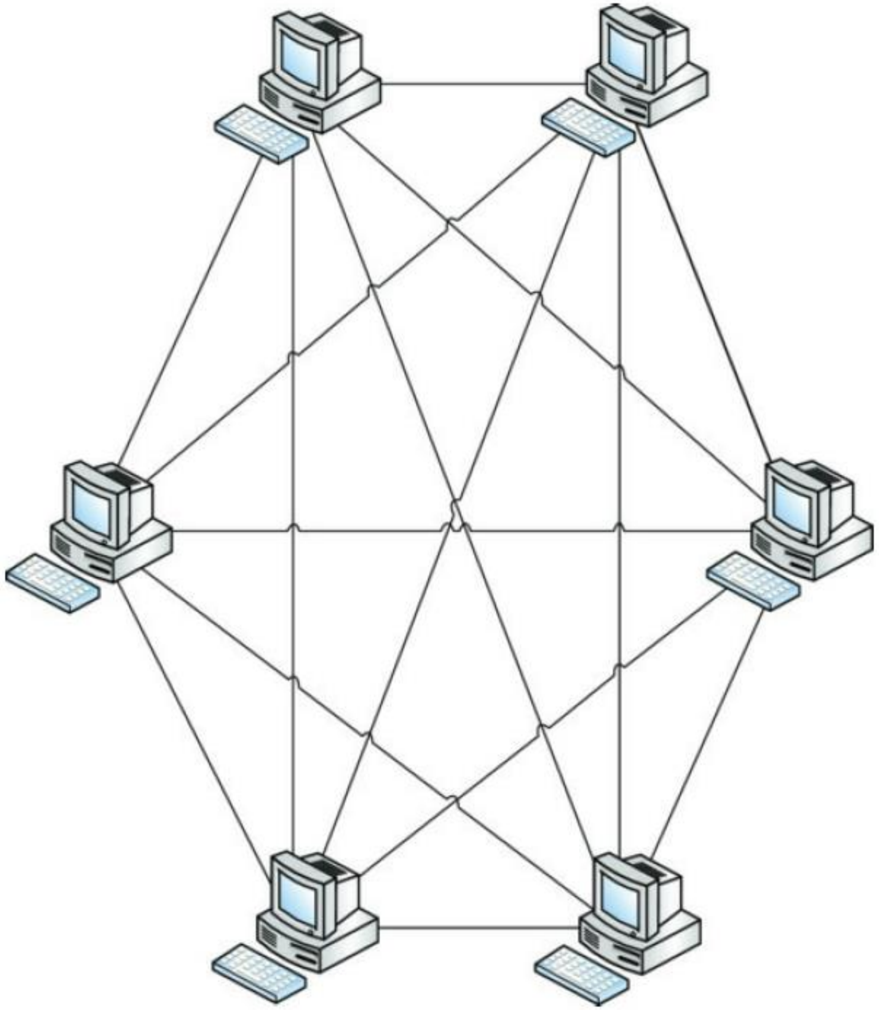


Figure 2.4 Mesh topology

Network topologies

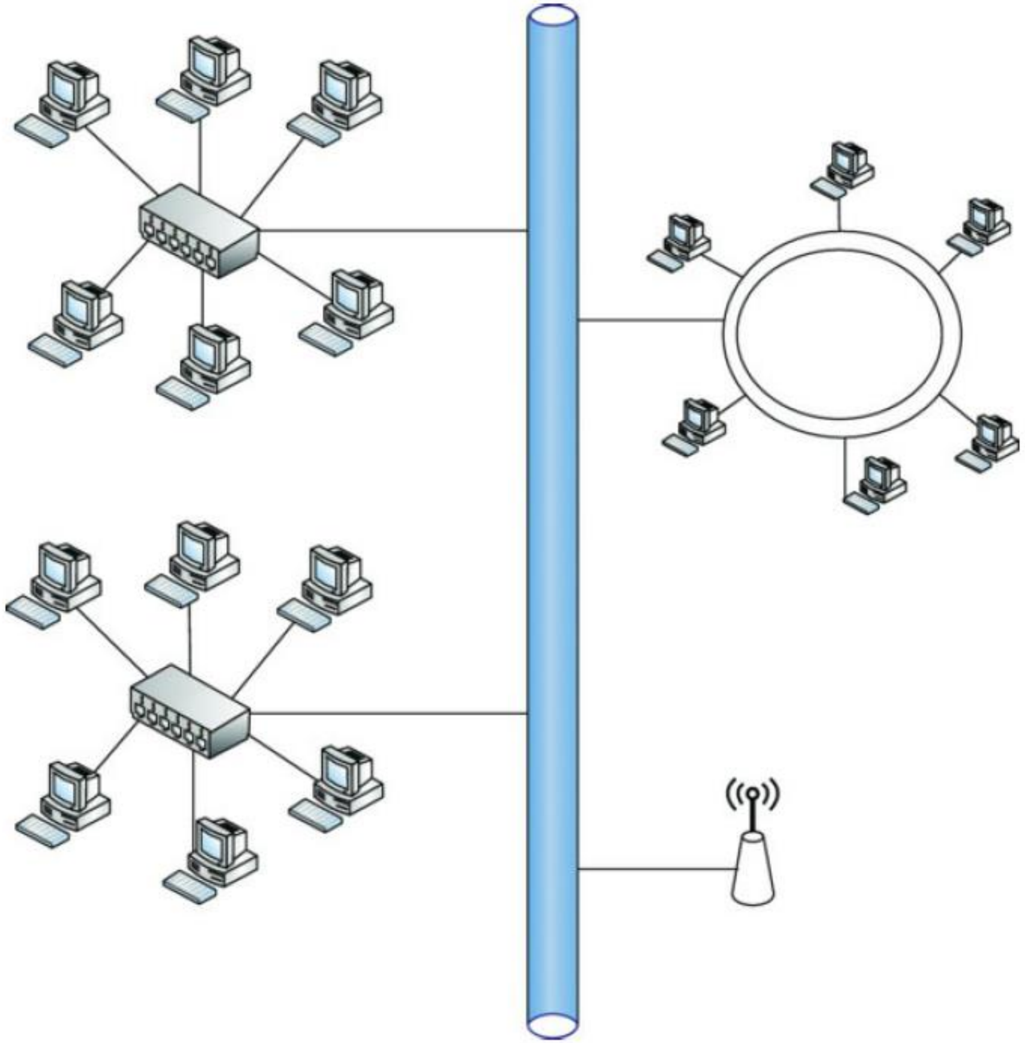
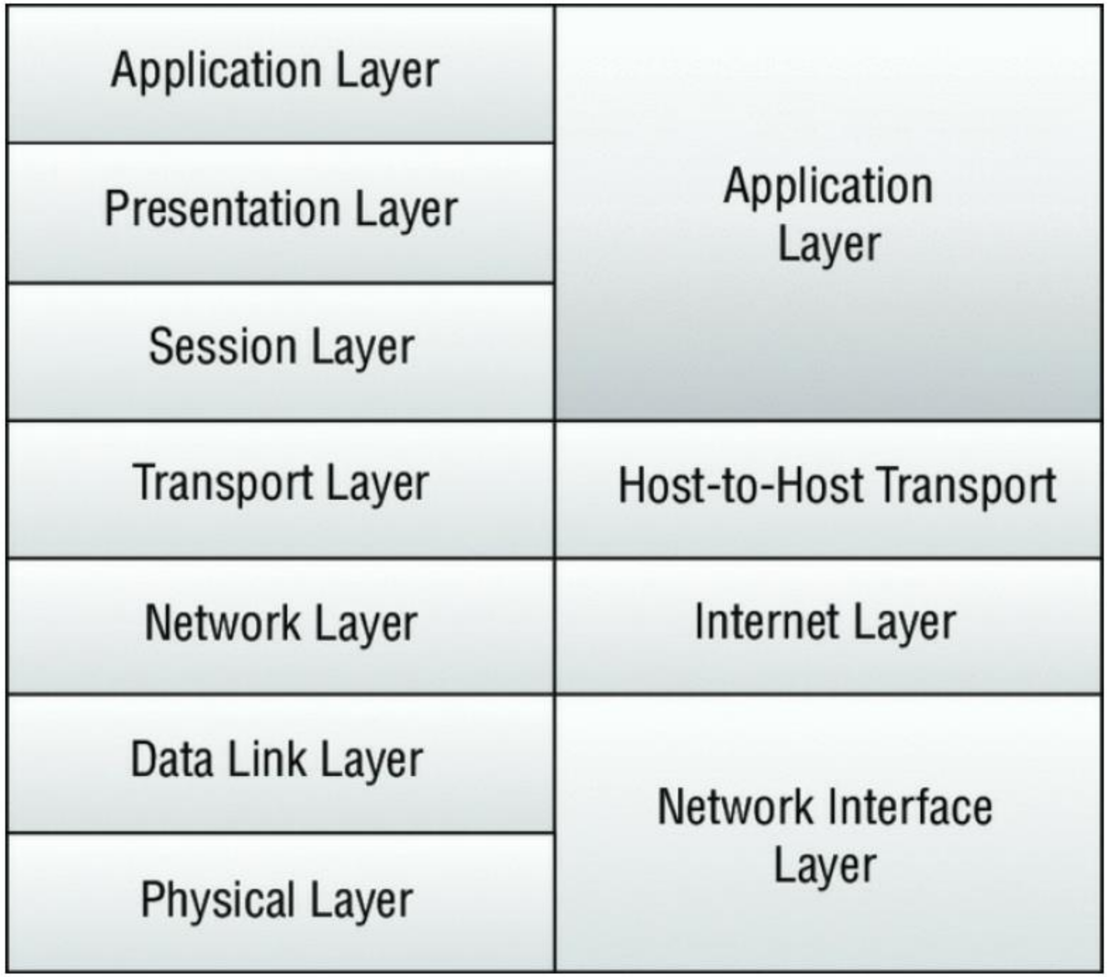


Figure 2.5 Hybrid topology

OSI – Open System Interconnection Model



Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transport Layer	Host-to-Host Transport
Network Layer	Internet Layer
Data Link Layer	Network Interface Layer
Physical Layer	

Figure 2.6 OSI TCP/IP comparative model

OSI layers

- Layer 1: Physical – cables, connections
- Layer 2: Data link – data in frames to ensure it is free of errors
  - Includes protocols for Ethernet and Wi-Fi
- Layer 3: Network – determines the path of data packets
  - Includes IP addressing
- Layer 4: Transport – ensures transport or sending is successful
  - Includes TCP and UDP
- Layer 5: Session – identifies established sessions between entities
- Layer 6: Presentation – translates data to the receiving layer
  - Includes SSL
- Layer 7: Application – enables user and processes to access resources

TCP/IP

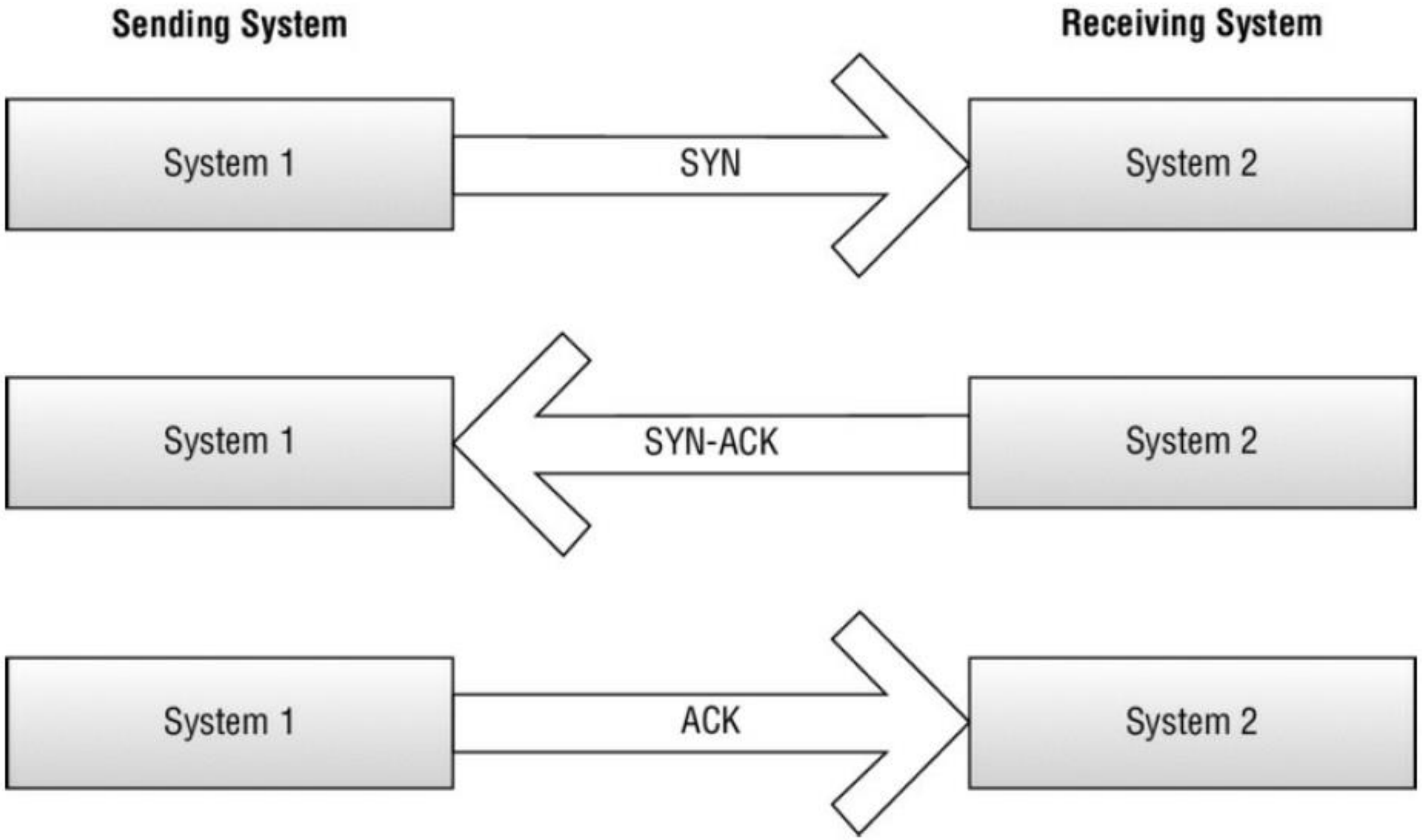


Figure 2.7 TCP three-way handshake

TCP/IP

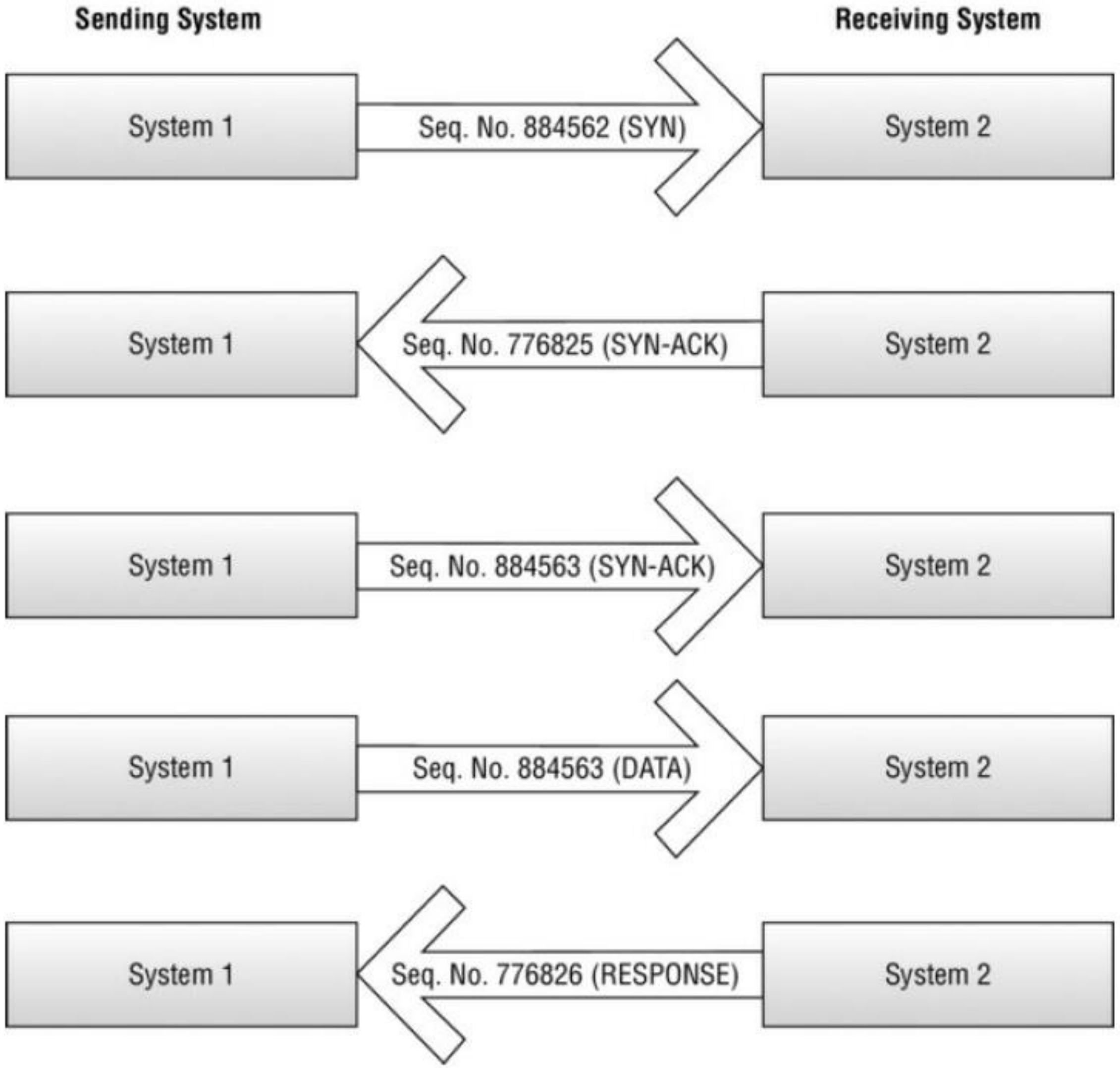


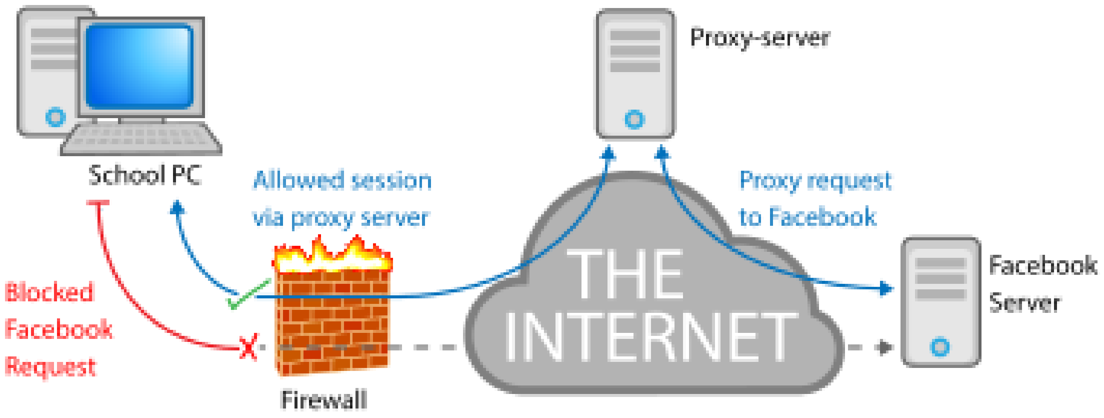
Figure 2.8 TCP sequencing

Network devices

- Routers
    - Direct layer 3 packets to the appropriate location based on network addressing
    - Uses the IP protocol
    - Gateway between different kinds of networks
    - Allow for Network Address Translation
        - Sharing a single IP address for access to the outside world
- Switches
    - Delivers data based on hardware addresses
        - MAC – media access control – addresses
        - This is burned into each network interface card
    - Works on layer 2, dealing strictly with MAC addresses

Proxies and firewalls

- Proxy server
  - Intermediate server
  - Entry point to the internet
  - May filter traffic
  - Work on layer 7 – application
- Firewalls
  - Packet filtering based on rules, e.g. IP addresses
  - Stateful packet filtering based on legitimacy of connection



Intrusion Prevention and Intrusion Detection Systems

- Intrusion detection system (IDS)
  - Detects suspicious network activity
  - Reacts passively
  - Sends a notification to administrator
- Intrusion Prevention System (IPS)
  - Detects suspicious network activity
  - Reacts proactively and preventive
  - Takes steps to prevent further damage and thwarts further attacks

Network security

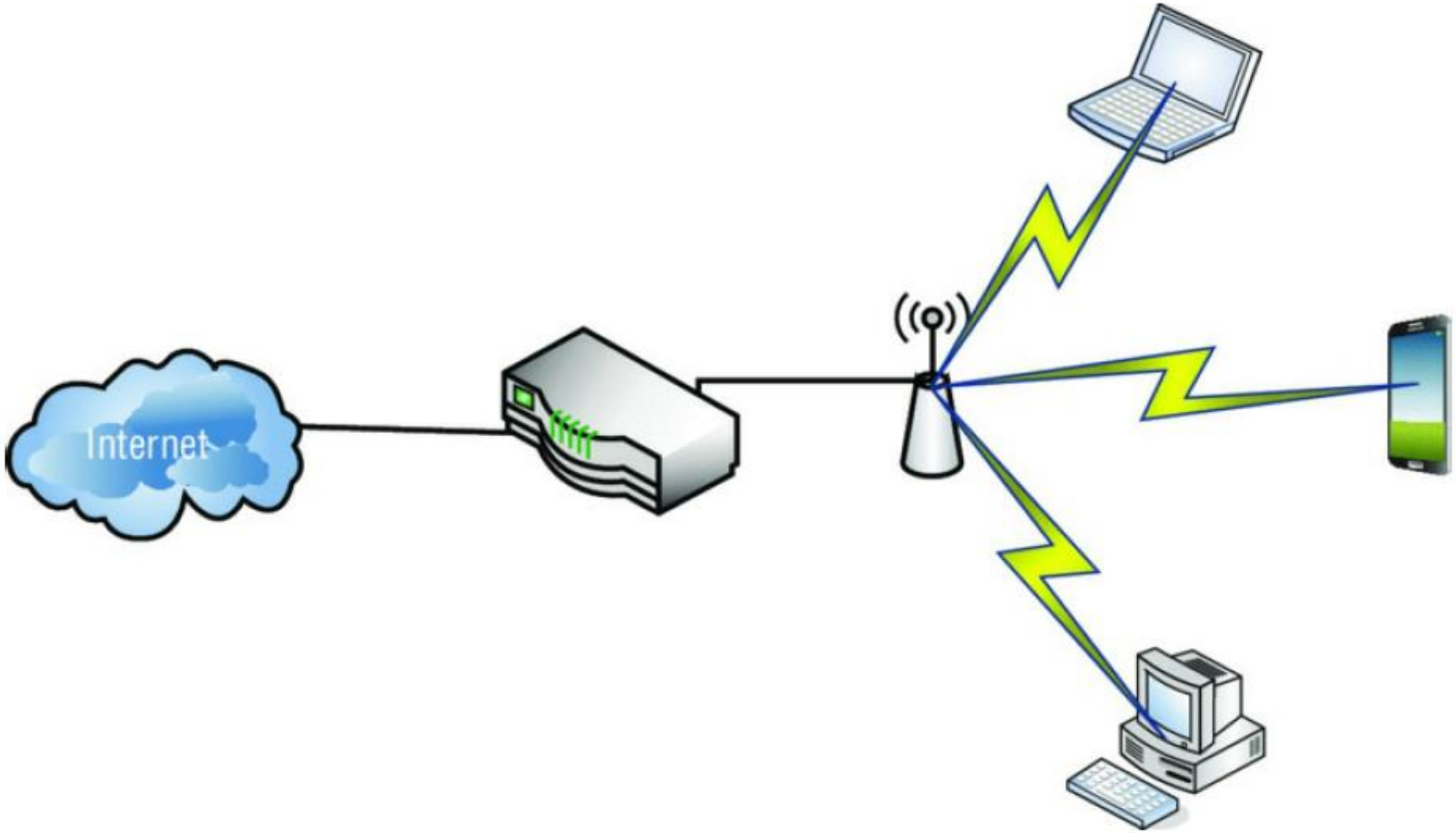


Figure 2.9 Residential network setup

Network security

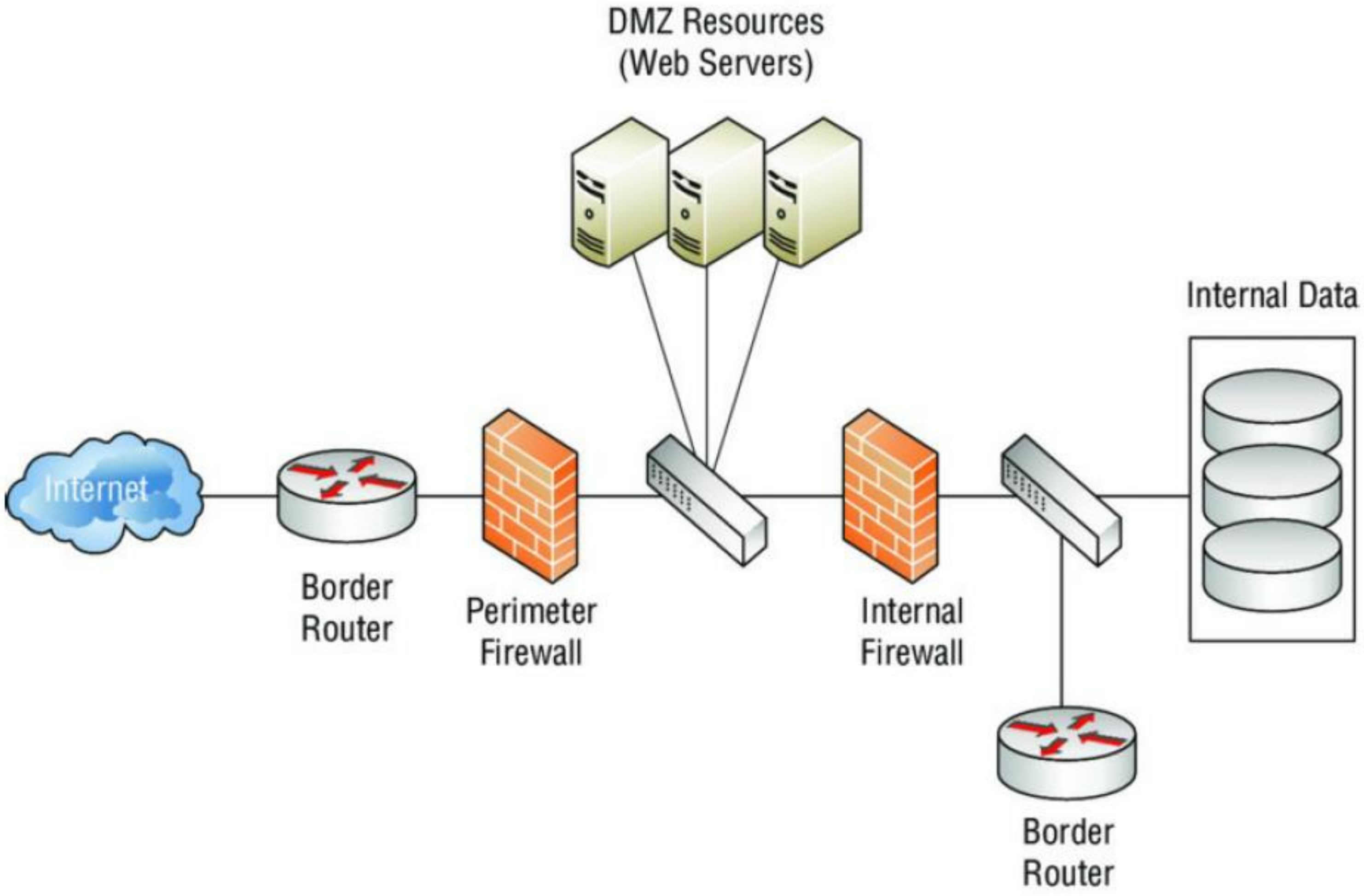


Figure 2.10 Typical enterprise network

Operating systems

- Microsoft Windows
  - Often patches, however, not always installed, may even cause issues
  - Support terminates at some point
  - Program installation may keep ports open
  - May run with administrator privileges
  - Allows for firewalls and virus detection to be disabled
- MAC OS
  - Thought to be un-susceptible to attacks – they are not!
  - Many features on standard installation – possible points of attack
  - Does not play well with windows – may cause admins to circumvent security

Operating systems

- Android
  - Popular on devices
  - Built on Linux
  - Counterfeit devices may include malware
  - Fake apps can make their way to Google play
- Linux
  - Popular open source OS
  - Users must know what they are doing
  - In that case, it is very safe
  - Separates administrator tasks from user accounts
  - It is open, anyone can check out the source code and attempt to tamper

Backup

- Full backup
  - Resets archive bit of all files and backs up accordingly
- Differential backup
  - Backs up all files changed since the last full backup
  - Does not reset archive bits
  - Changes are backed up – and backed up – and backed up…
  - For a system restore only last full backup and last differential needed
  - However, differentials can get huge!
- Incremental backup
  - Backs up all files changed since the last full backup
  - Does reset archive bits
  - Based on last incremental backup
  - Lots of small backups with the latest changes
  - For restore, full backup and all incremental backups needed

Cryptography

Applications of cryptography

- Confidentiality
  - Keeping information a secret
- Integrity
  - Messages has not been tampered with
- Authentication
  - Identify a person, object, or party
- Nonrepudiation
  - Positive ID of source
- Key Distribution
  - For use in encryption/decryption algorithms

Symmetric cryptography

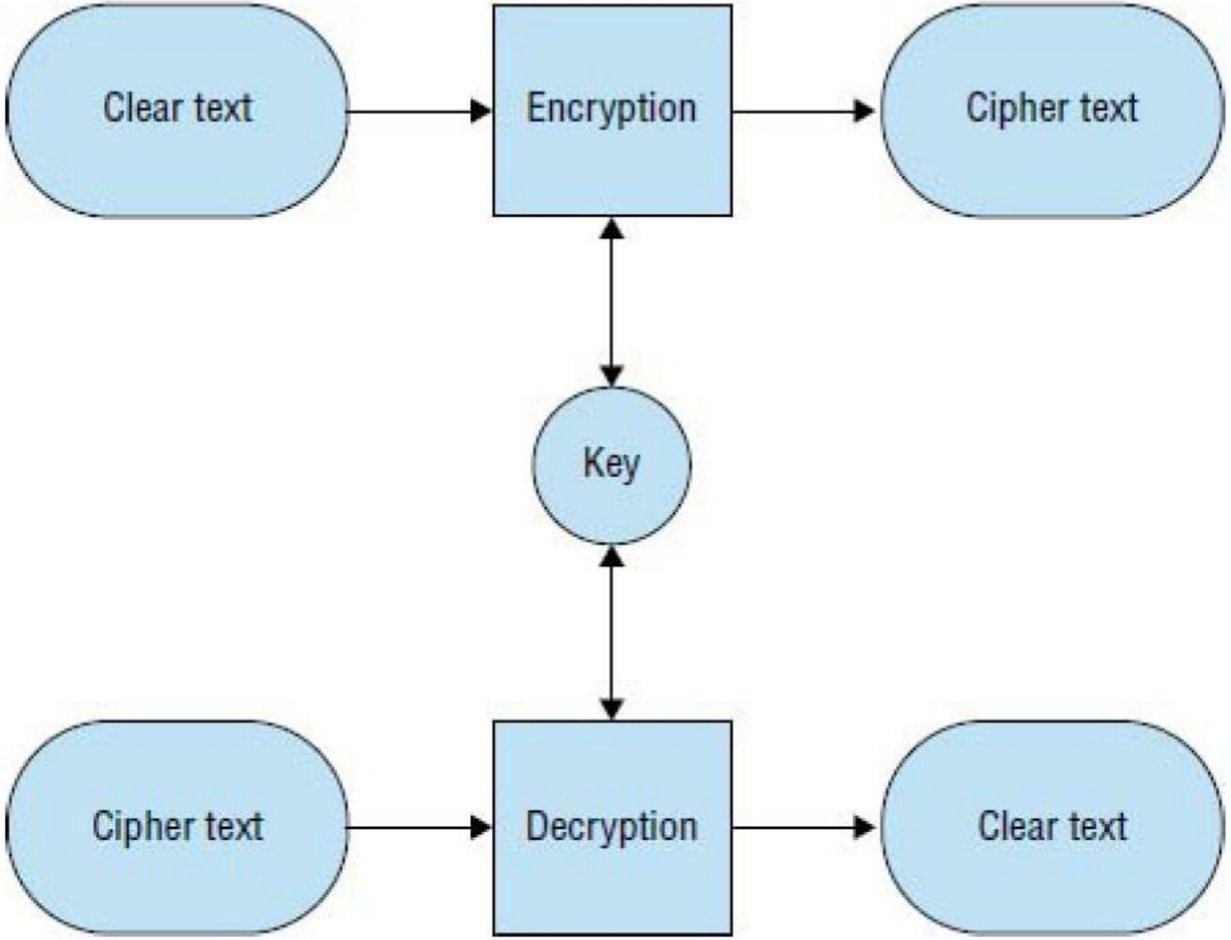


Figure 3.2 Symmetric encryption

Asymmetric cryptography

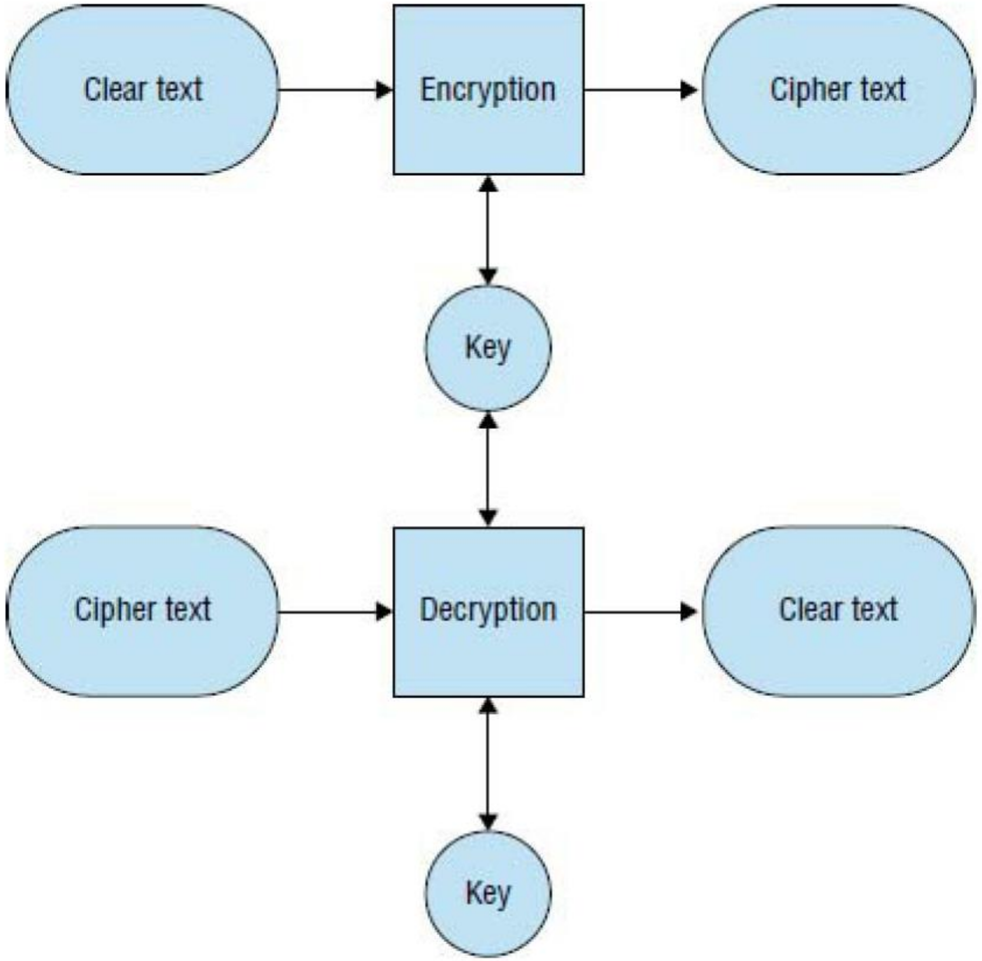
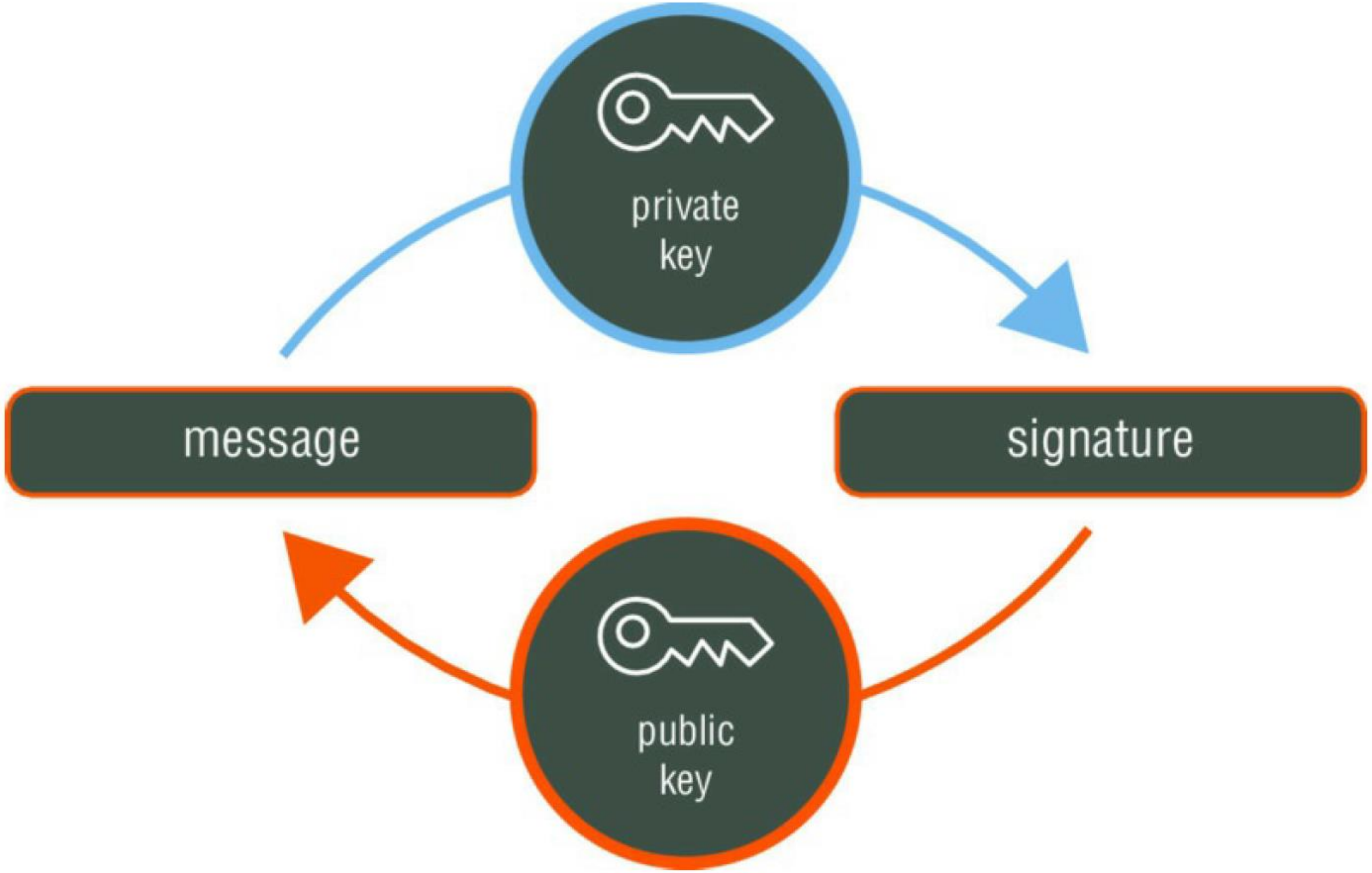


Figure 3.3 Asymmetric encryption

Signatures



Hashing

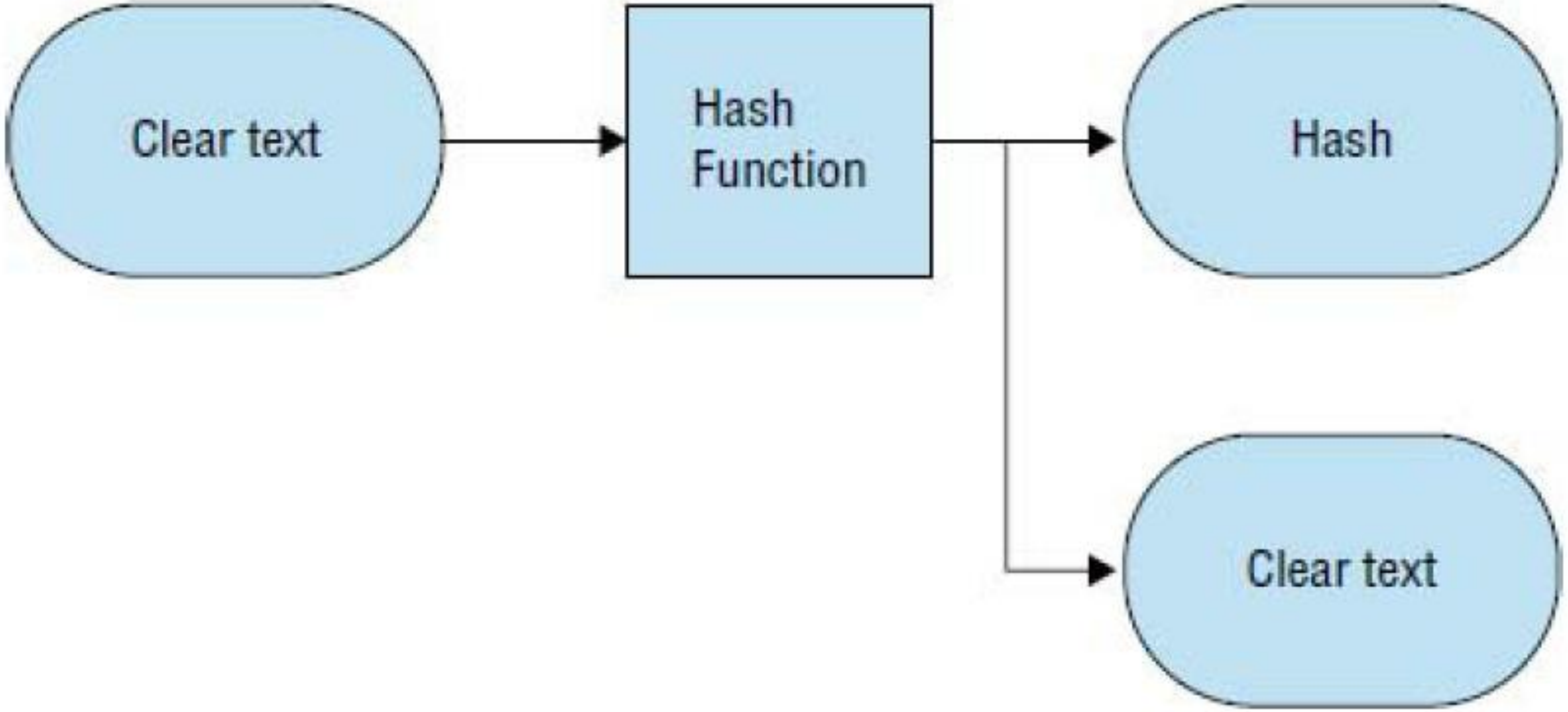


Figure 3.6 Hash generated from “Hello World” using MD5

Footprinting

Footprinting

- Information obtained through footprinting:
  - IP address ranges
  - Namespaces
  - Employee information
  - Phone numbers
  - Facility information
  - Job information

Footprinting steps

- Footprinting generally entails the following steps to ensure proper information retrieval:
  - **Collect information** that is publicly available about a target (for example, host and network information).
  - **Ascertain the operating system(s)** in use in the environment, including web server and web application data where possible.
  - **Issue queries** such as Whois, DNS, network, and organizational queries.
  - **Locate existing or potential vulnerabilities or exploits** that exist in the current infrastructure that may be conducive to launching later attacks.

Information gathered using footprinting

- Information about an organization’s **security posture** and where potential **loopholes** may exist. This information will allow for adjustments to the hacking process that makes it more productive.
- A **database** that paints a detailed picture with the maximum amount of information possible about the target. This may be from an application such as a web application or other source.
- A **network map** using tools such as the Tracert utility to construct a picture of a target’s Internet presence or Internet connectivity. Think of the network map as a roadmap leading you to a building; the map gets you there, but you still have to determine the floor plan of the building.

What to look for when footprinting

- Network information
- Operating system information
- Organization information, such as CEO and employee information, office information,
- contact numbers, and email
- Network blocks
- Network services
- Application and web application data and configuration information
- System architecture
- Intrusion detection and prevention systems
- Employee names
- Work experience

Network information

- Domain names the company uses to conduct business or other functions, including research and customer relations
- Internal domain name information
- IP addresses of available systems
- Rogue or unmonitored websites that are used for testing or other purposes
- Private websites
- TCP/UDP services that are running
- Access control mechanisms, including firewalls and ACLs
- Virtual private network (VPN) information
- Intrusion detection and prevention information as well as configuration data
- Telephone numbers, including analog and Voice over Internet Protocol (VoIP)
- Authentication mechanisms and systems

Operating system information

- User and group information and names
- Operating system versions
- System architecture
- Remote system data
- System names
- Passwords

Information gathering types

- Active information gathering
  - Actively engaging in information gathering, e.g. social engineering
- Passive (open source) information gathering
  - Passively obtaining information from public, open sources
- Pseudonymous Footprinting
  - Using pseudonyms for obtaining info, e.g. pretending to be an insider
- Internet Footprinting
  - Using the internet, e.g. search engines, to obtain information

Threats Introduced by Footprinting

- Social Engineering
  - Simply ask for information, pretend to be someone else
- Network and System Attacks
  - Gather information related to these
- Information Leakage
  - Information getting into the wrong hands
- Privacy Loss
  - Gather private data – could lead to lawsuit
- Revenue Loss
  - No trust equals no business

The Footprinting Process

- Using Search Engines
  - People search
  - Google Hacking
    - Using internal tools
    - Including location/geography using Google maps/earth
    - Including finding live cameras/webcams
- Social Networks
  - Facebook, linkedIn, Instagram…
- Financial Services
  - Job sites, competitive analysis
- Working with email
- Gaining Network Information
- Human hacking
  - Eavesdropping, phishing, shoulder surfing, dumpster diving

Footprinting tools

- Google operators – all kinds of filters, specifications
- Netcraft – server version, IP, OS, subdomain…
- Link extractor – locates and extracts internal and external URLs
- Google earth/maps – geographic/location information
- Webcams – live information
- People search - Spokeo, ZabaSearch, Wink, and Intelius.
- Social media – You know these, lots and lots of information
  - Echosec – location based, finds attached social media
  - Maltego – visualization of social media and other sources of information

Footprinting tools

- Job sites
  - Jobindex (dk), LinkedIn, Monster.com, Dice.com, or even Craigslist.com
- PoliteMail, WhoReadMe
  - Email tools (use with caution!)
- Company info
  - CVR – register (dk), www.sec.gov/edgar.shtml, www.cnbc.com...
- Network information
  - Whois, ping, nslookup, tracert
- Build information
  - Built With: https://builtwith.com/

Exercises