Security Attacks

- A passive attack attempts to learn or make use of information from the system but does not affect system resources.

- An active attack attempts to alter system resources or affect their operation.

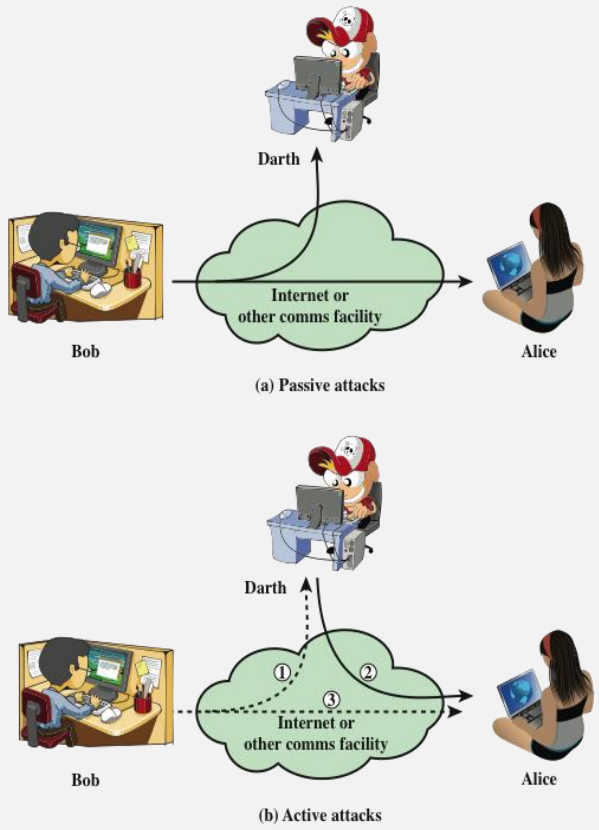


Figure 1.2 Security Attacks

Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions.

- **Goal of the opponent**
  obtain information that is being transmitted.

- **Our Goal:**
  the emphasis in dealing with passive attacks is on prevention rather than detection

- Two types of passive attacks are:
  - The release of message contents
  - Traffic analysis

Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them

Active Attacks (four categories)

- **Masquerade**
  - Takes place when one entity pretends to be a different entity Usually includes one of the other forms of active attack.

    Example: logon ID and password

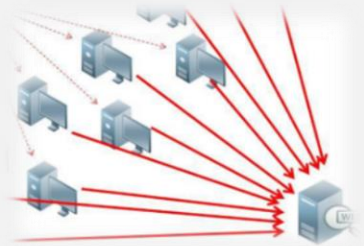
- **Replay**
  - Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

- **Modification of messages**
  - Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect.

    Example: "Allow John Smith to read confidential file accounts" is modified to say, "Allow Fred Brown to read confidential file accounts."

- **Denial of service (DoS)**
  - Prevents or inhibits the normal use or management of communications facilities.

    Example: disabling the network or by overloading it with messages



Security bug

- A security bug or security defect is a software bug that can be exploited to gain unauthorized access or privileges on a computer system. Security bugs introduce security vulnerabilities by compromising one or more of:
  - Authentication of users and other entities
  - Authorization of access rights and privileges
  - Data confidentiality
  - Data integrity

authentication **is the process of verifying who someone is, whereas** ***authorization*** **is the process of verifying what specific applications, files, and data a user has access to**

Basic security analysis

How do you secure X? Is X secure?

1. What are we protecting?
2. Who is the adversary?
3. What are the security requirements?
4. What security approaches are effective?

Basic security analysis

How do you secure X? Is X secure?

1. **What are we protecting?**
2. Who is the adversary?
3. What are the security requirements?
4. What security approaches are effective?

- Enumerate assets and their value
- Understand architecture of system
- Useful questions to ask
  - What is the operating value, i.e., how much would we lose per day/hour/minute if the resource stopped?
  - What is the replacement cost? How long would it take to replace it?

Basic security analysis

How do you secure X? Is X secure?

1. What are we protecting?
2. **Who is the adversary?**
3. What are the security requirements?
4. What security approaches are effective?

- Identify potential attackers
- Estimate attacker resources
- Estimate number of attackers, probability of attack

Basic security analysis

How do you secure X? Is X secure?

1. What are we protecting?
2. Who is the adversary?
3. **What are the security requirements?**
4. What security approaches are effective?

- Confidentiality: Protecting information from unauthorized access.
- Integrity: Ensuring that information is accurate and complete.
- Authenticity: Verifying the identity of users and devices.
- Availability: Ensuring that assets are accessible to authorized users when they need them.
- Auditability: Tracking and recording user activity for security auditing purposes.
- Access control: Restricting access to assets to authorized users.
- Privacy: Protecting the privacy of personal information.

Basic security analysis

How do you secure X? Is X secure?

1. What are we protecting?
2. Who is the adversary?
3. What are the security requirements?
4. **What security approaches are effective?**

- **No security**
  - Legal protection
- **Build strong security defense**
  - Use cryptographic mechanisms
  - Perimeter defense (firewall), VPN (virtual private network)
- **Resilience to attack**
  - Multiple redundant systems
- **Detection and recovery**
  - Intrusion detection system

Securing Your Systems: Think like an attacker

- Adversary is targeting assets, not defenses
- Will try to exploit the weakest part of the defenses
  - E.g., bribe human operator, social engineering, steal (physically) server with data

Part 2

Encryption basics

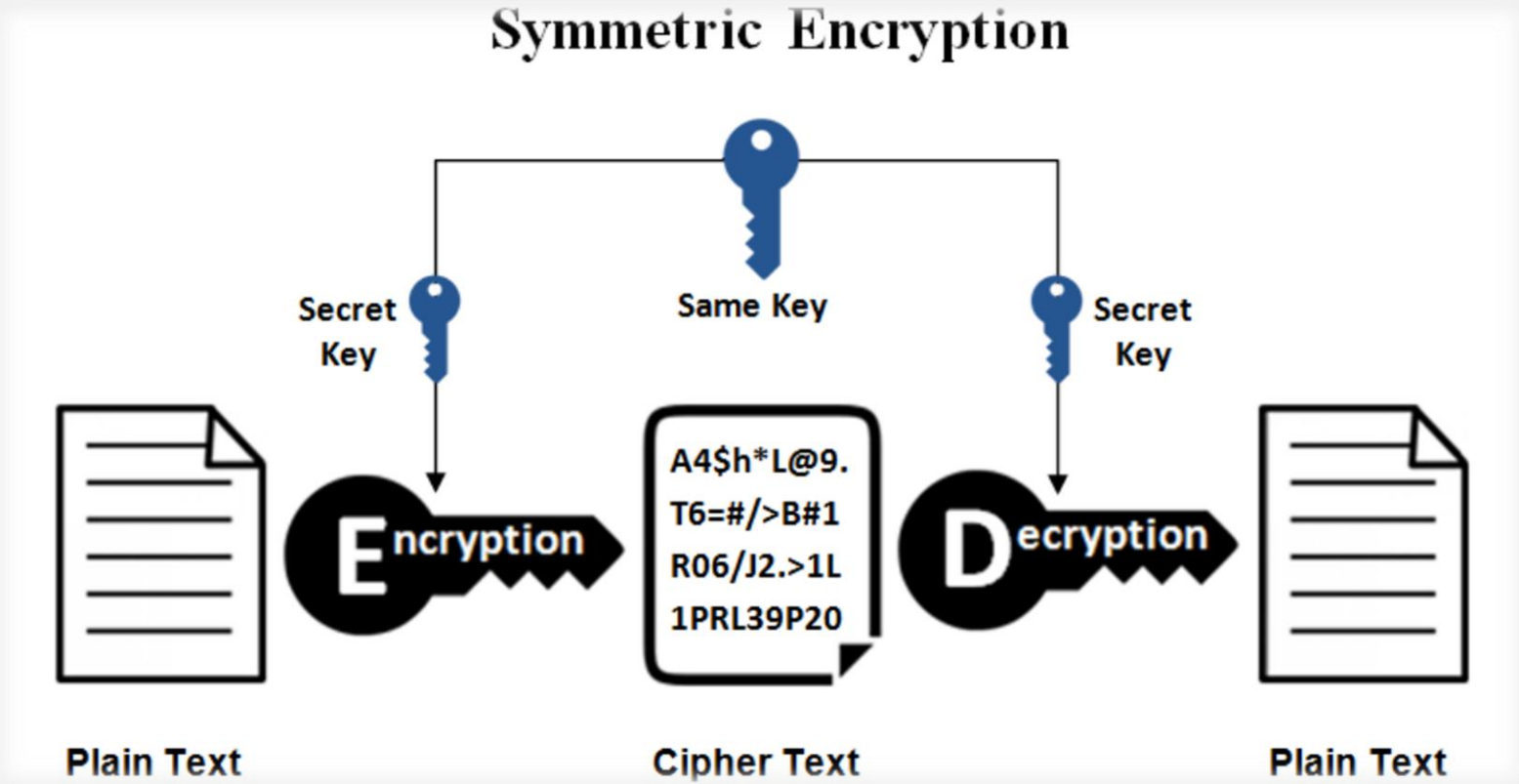
Encryption is a tool that can help achieve many security properties

Encryption basics

- Putting a message in code so that other people can't read it.

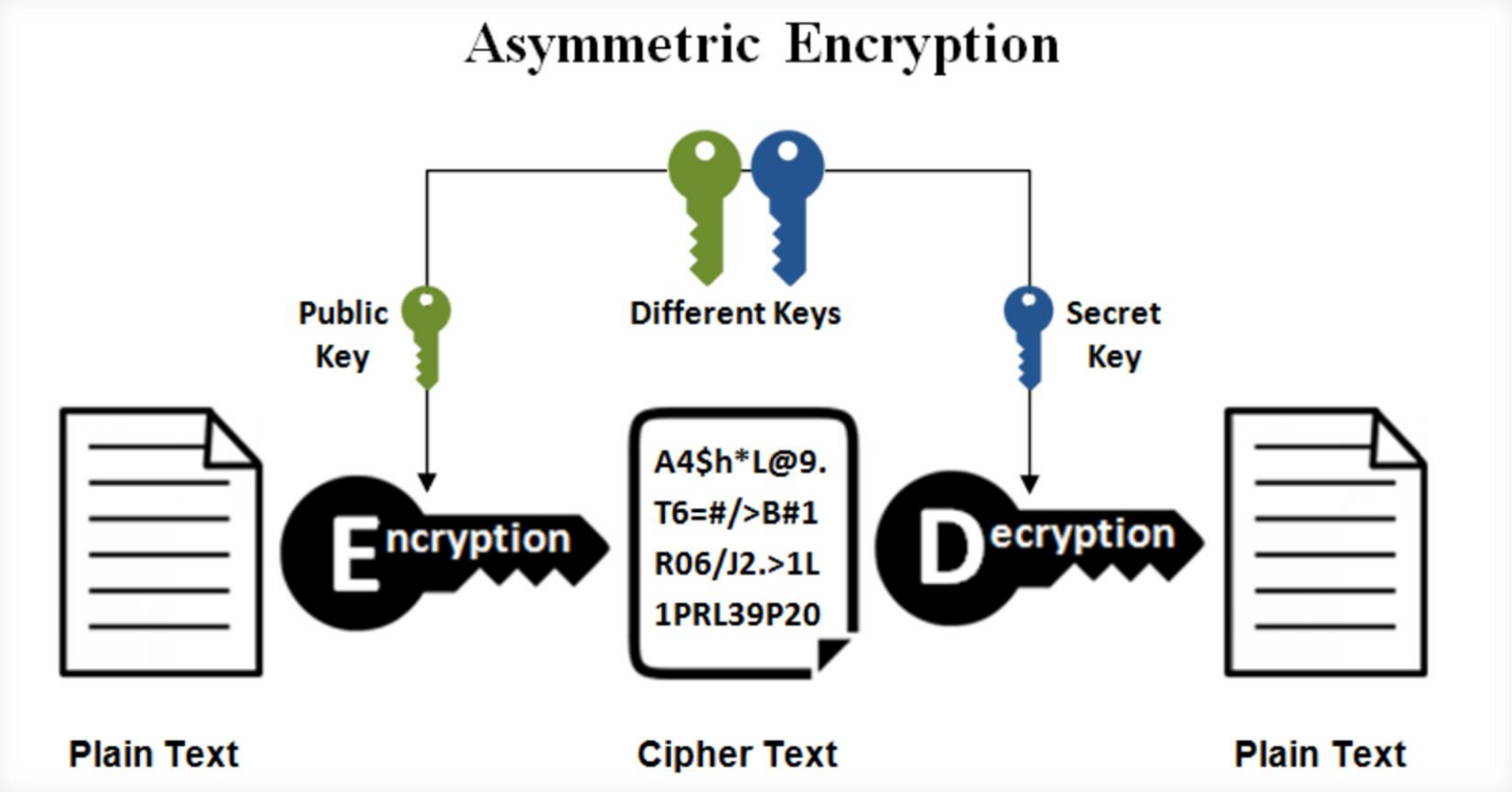
- Two main approaches:
  - Symmetric encryption (same key used for encryption and decryption)
  - Asymmetric encryption (keypair: public key and private key)

Encryption basics



https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Encryption basics



https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

What might you want to encrypt?

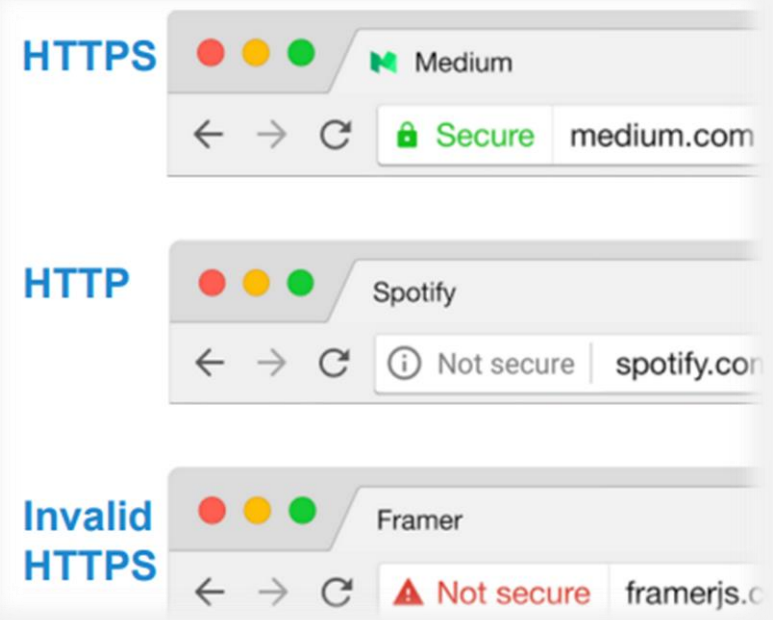
- Hard drive (or some part of it), disks, USB
- Messages you send (text messages)
- “Everything” you’re sending when you’re browsing the web
- etc

Usability problems

- Encryption is rarely configured by default
- You need a good password
  - …and you can't lose it or forget it
- Public/private key encryption
  - How to get someone's public key?
  - How do I make it work on my phone?

Connection security indicators

- What do proposed symbols indicate?
- What are the security properties of HTTPS?
  - Secrecy – message is encrypted
  - Authenticity – message has a valid certificate
  - Integrity – message has not been tampered

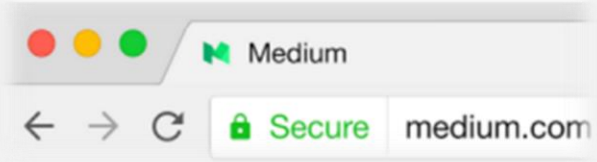


HTTPS: **H**ypertext **T**ransfer **P**rotocol **S**ecure

A.P. Felt, R.W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M.E. Acer, E. Morant, and S. Consolvo. Rethinking Connection Security Indicators. SOUPS 2016

What can still go wrong at secure site?

- Malware on site
- Key logger on user's computer
- Malicious third-party ads or trackers
- Certificate authority was compromised and issued invalid certificate



References

- Prof. Lorrie Cranor's lecture notes
- Stallings & Brown's PowerPoint slides