Introduction

Presentation by:
V. Balasubramanian
SSN College of Engineering

Course objectives

- Learn how crypto primitives work
- Learn how to use them correctly and reason about security

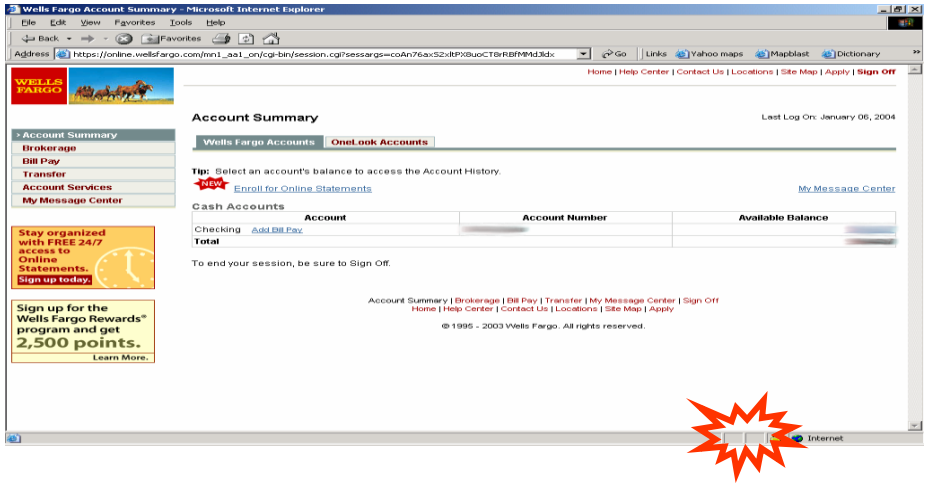
Objectives

- To define three security goals
- To define security attacks that threaten security goals
- To define security services and how they are related to the three security goals
- To define security mechanisms to provide security services
- To introduce two techniques, cryptography and steganography, to implement security mechanisms

Cryptography is everywhere

- Secure communication:
- web traffic: HTTPS
- wireless traffic: 802.11i WPA2 (and WEP), GSM, Bluetooth
- Encrypting files on disk: EFS, TrueCrypt
- Content protection (e.g. DVD, Blu-ray): CSS, AACS
- User authentication
- … and much much more

Secure communication



no eavesdropping
no tampering

Secure Sockets Layer / TLS

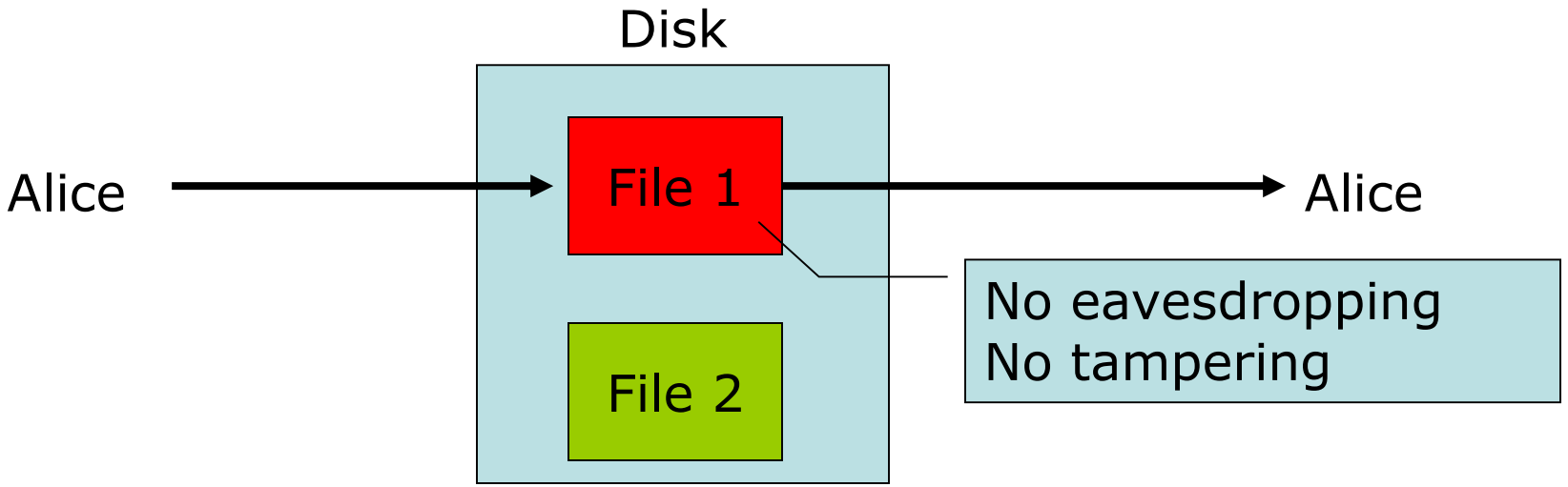
Two main parts

1. Handshake Protocol: **Establish shared secret key using public-key cryptography** (2nd part of course)

2. Record Layer: **Transmit data using shared secret key**

   Ensure confidentiality and integrity (1st part of course)

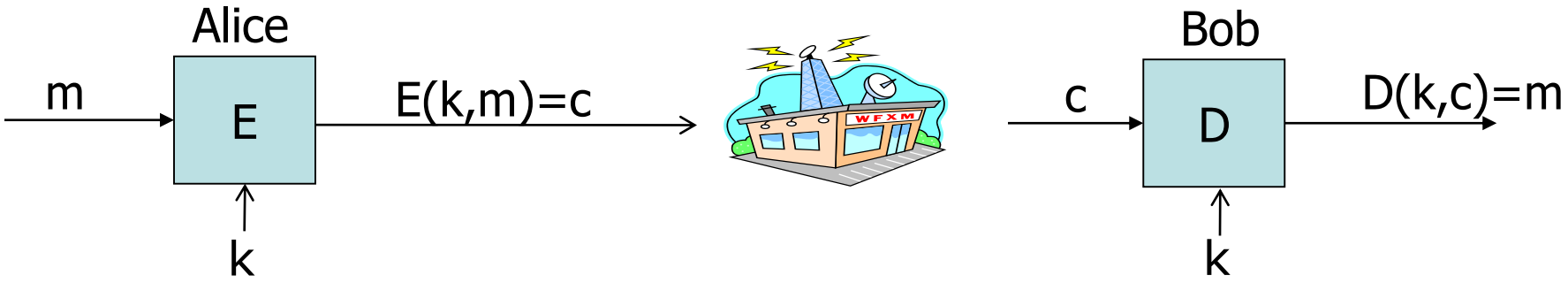
Protected files on disk



Analogous to secure communication:

Alice today sends a message to Alice tomorrow

Building block: sym. encryption



E, D: cipher k: secret key (e.g. 128 bits)
m, c: plaintext, ciphertext

Encryption algorithm is publicly known

- Never use a proprietary cipher

Things to remember

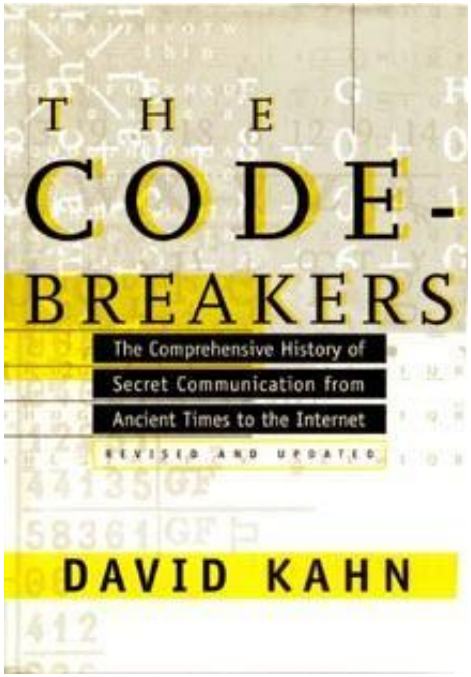
Cryptography is:

- A tremendous tool
- The basis for many security mechanisms

Cryptography is not:

- The solution to all security problems
- Reliable unless implemented and used properly
- Something you should try to invent yourself
  - many many examples of broken ad-hoc designs

- David Kahn, "The code breakers" (1996)



Price Water Cooper

Increased Security Breaches

81% more in 2015

90% of large organisations

74% of small businesses

had a security breach.

▲ Up from 81% a year ago.

▲ Up from 60% a year ago.

£1.46m - £3.14m is the average cost to a large organisation

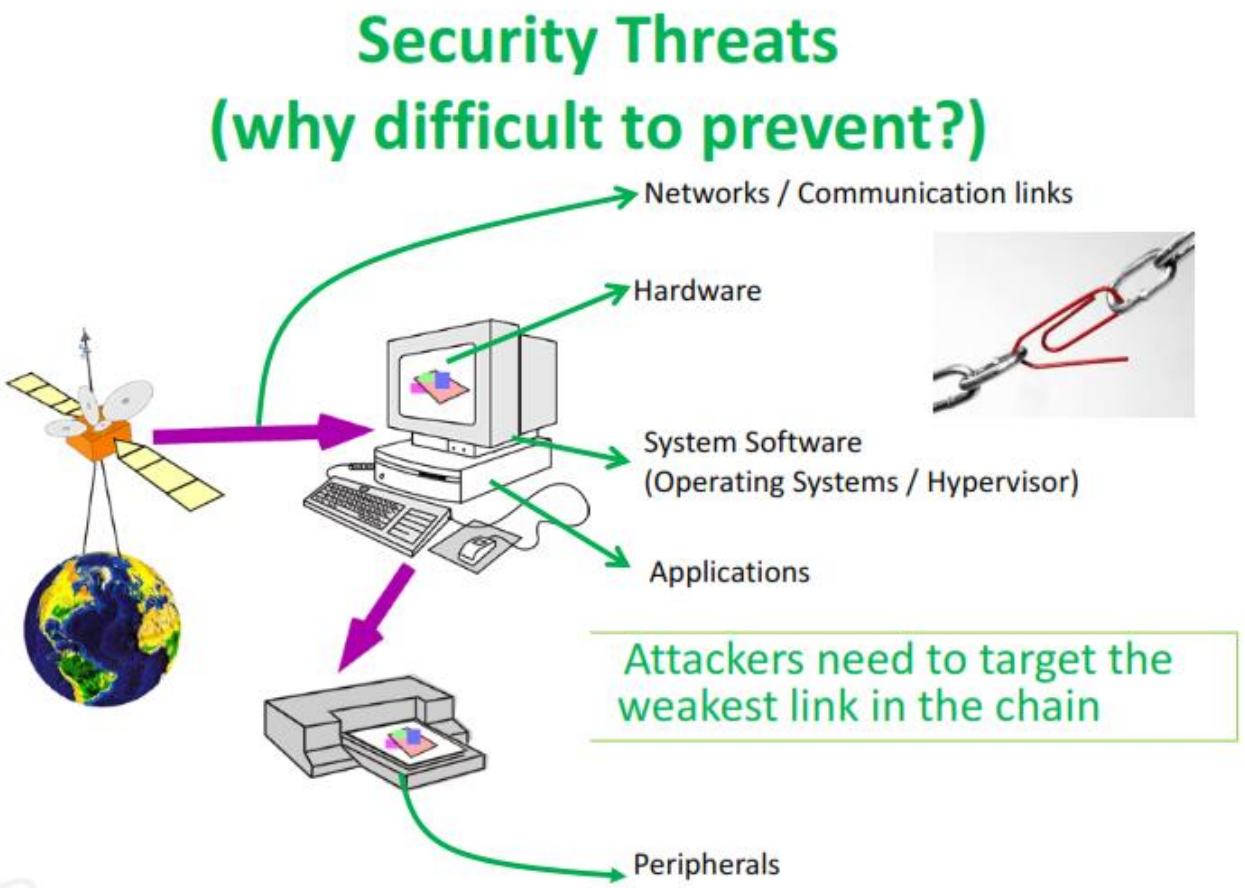
£75k - £311k is the average cost to a small business

44% of large organisations

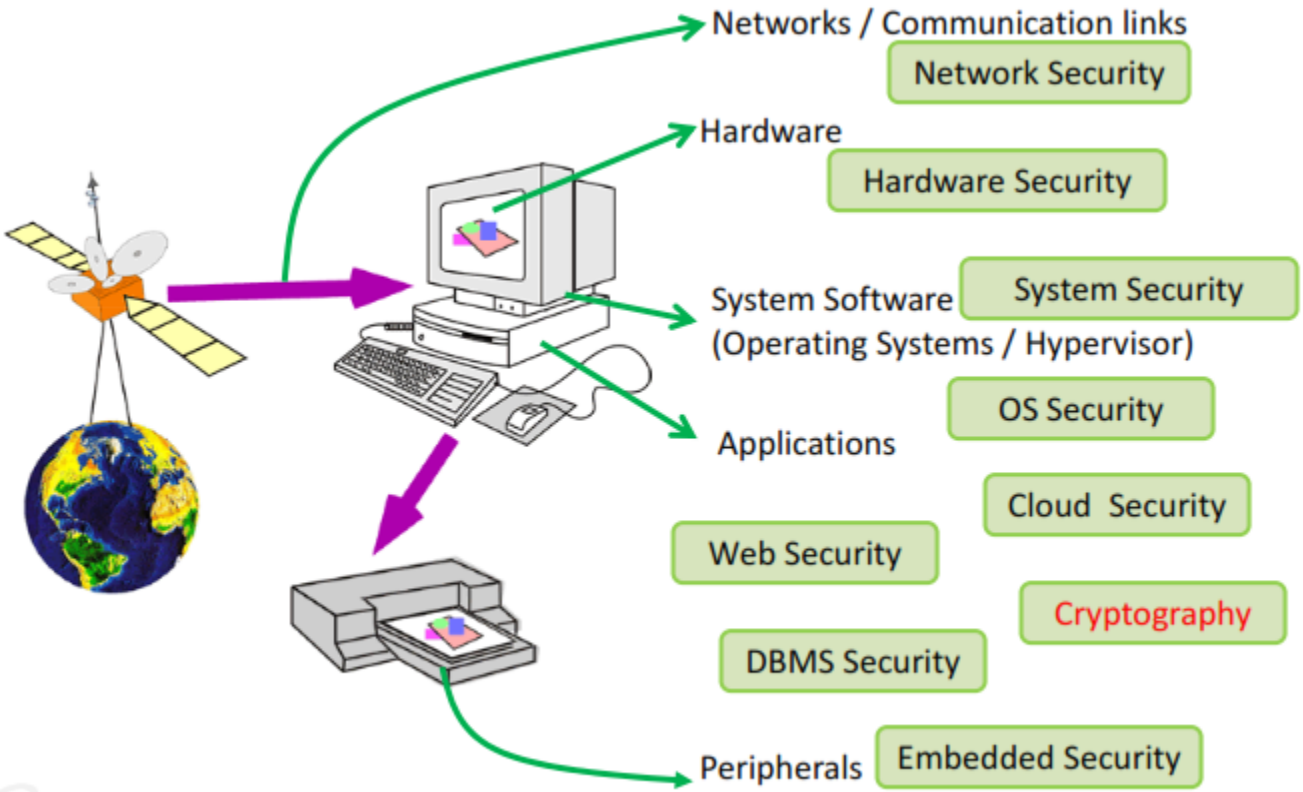
44% of small businesses

increased information security spend in the last year.

Security Threats

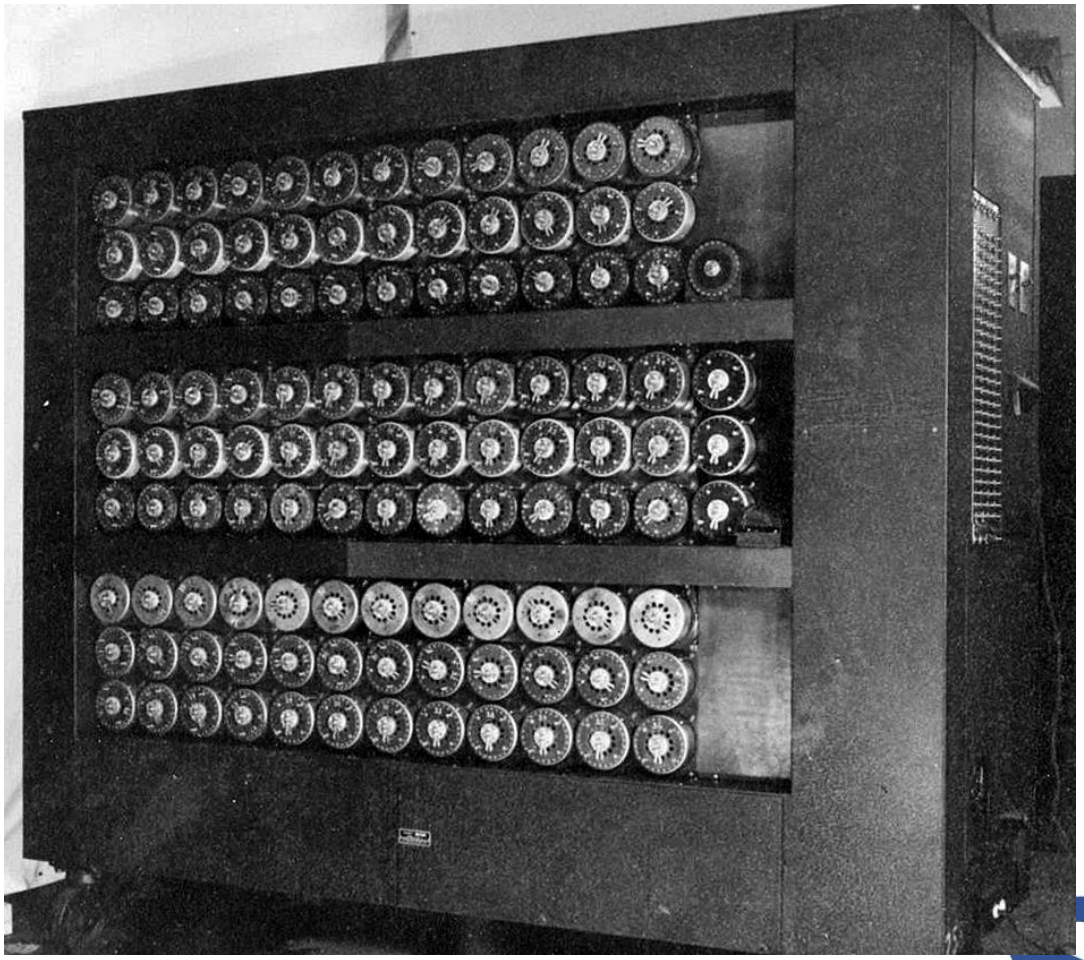


Security Study



Enigma

Bombe



Turing Award

CIA Triad

Data


Data on your computing devices
Financial Data
Medical Data
Your Data
Education Data
Employment
Your Identity
Information Online

Security Breach

Security Breach

- The online password manager, LastPass, detected unusual activity on its network in July 2015.
- The high tech toy maker for children, Vtech, suffered a security breach to its database in November 2015.
- Equifax Inc. is one of the nationwide consumer credit reporting agencies in the United States.

CyberWarfare

- State-sponsored attack involved the Stuxnet malware that was designed to damage Iran’s nuclear enrichment plant.

Confidentiality

- Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

Integrity

- Information needs to be changed constantly. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.

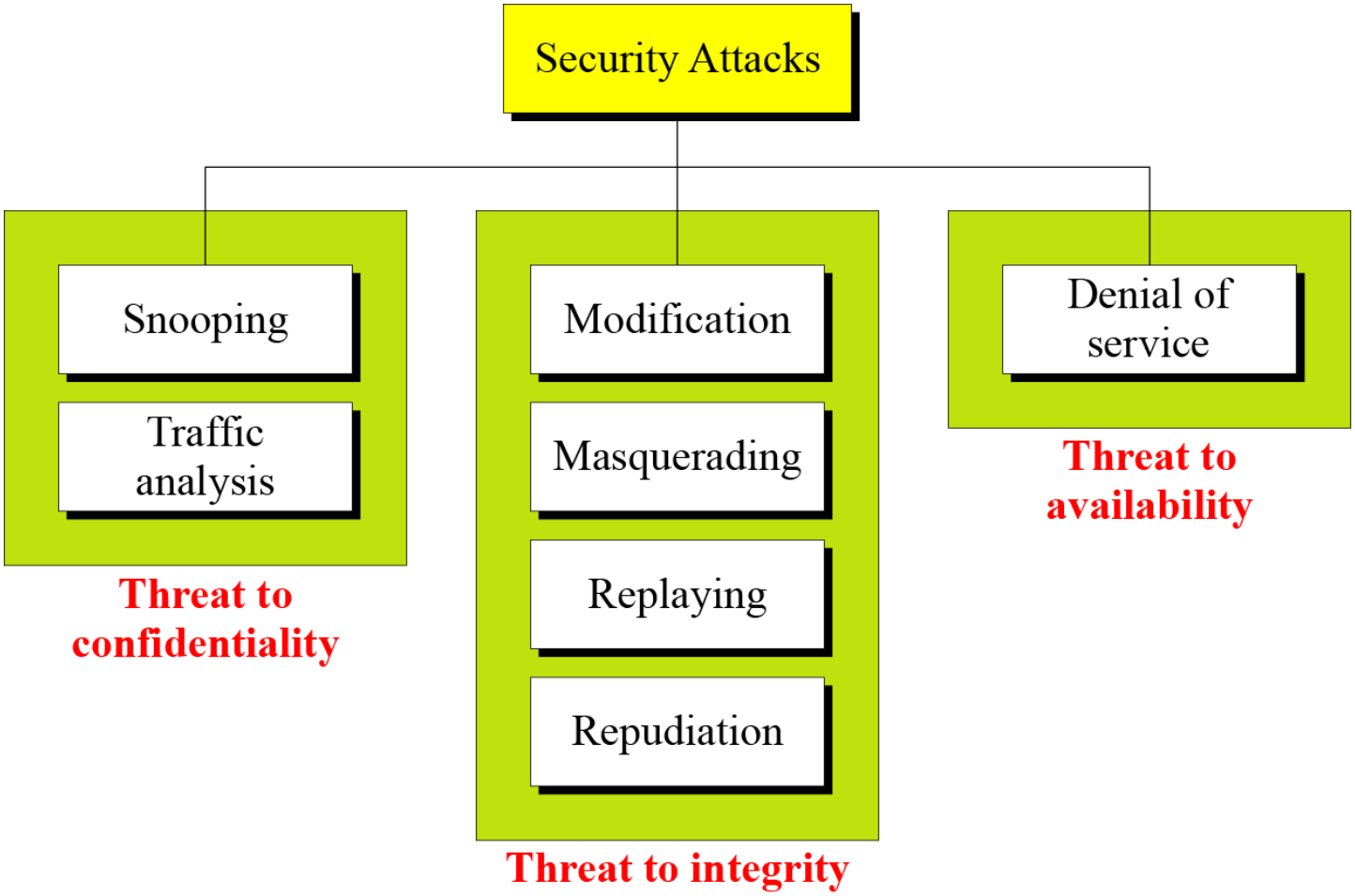
Availability

- The information created and stored by an organization needs to be available to authorized entities. Information needs to be constantly changed, which means it must be accessible to authorized entities.

Attacks

- Attacks Threatening Confidentiality
- Attacks Threatening Integrity
- Attacks Threatening Availability
- Passive versus Active Attacks

Taxonomy


Security Attacks
Snooping
Traffic analysis
Threat to confidentiality
Modification
Masquerading
Replaying
Repudiation
Threat to integrity
Denial of service
Threat to availability