Introduction into Cyber Security

Chapter 1: Introduction

WiSe 18/19

Chair of IT Security

Organizational

- V4/Ü2, 8 ECTS points
  - Compulsory course for Cyber Security program
  - Elective course for
    - Computer Science
    - Information and Media Technology
    - …
- Lectures (Prof. A. Panchenko)
  - Tue 3:30pm ZHG HSC (room changed)
  - Thu 9:15am ZHG HSB
- Exercises (Torsten Ziemann and Eric Strehle)
  - Wed 1:45pm ZHG SR1
    (05.11.18 - 26.11.08 on Mon 3:30pm in VG1C/0.03)

Organizational (cont'd)

- Consultation hours:
  - Lecture: after the lecture
  - Exercise: Wed 11:00-12:00
- Offices: VG1C, room 2.34, 2.36
- Material will be made available in moodle
  - Please register for the course
- Exercises will consist of two types
  - Theoretical exercises
  - Practical tasks / lab
- You need to successfully complete all the practical tasks to get admitted to the exam

Teaching Offer WiSe 18/19

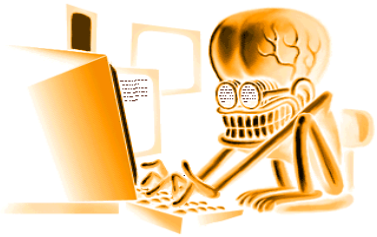
- Lecture: Introduction into Cyber Security (8 ECTS)
- Seminar: Advanced Topics in Network and System Security (6 ECTS)
  - Fr 15:30
- Study Project: Adversarial Machine Learning (8 ECTS)
  - Wed 15:30

Focus of this Course

- Cryptographic Basics
  - Symmetric Cryptography
  - Authentication and Key Agreement
  - Asymmetric Cryptography
  - Certificates and Public Key Infrastructures
- Network Security
  - Security Protocols on different network layers
- Related topics
  - Spam, Botnets, Phishing

Based on IT Security course at RWTH Aachen University (Prof. Meyer)
and the one taught here before (Prof. König)

Introduction - ITSec 1 – Network Security



Related

DNSsec, SSH, SMTP
SSL/TLS
IPsec

Protocols

Encryption Algorithms
Integrity Protection
Digital Signatures
Certificates and PKIs

Basics

Focus of this Course (cont'd)

- Only cursory overview of cryptography
- To dive deeper into cryptography attend
  - Cryptography of Prof. Meer (SoSe)
  - Compulsory course for Cyber Security students

- Foundations for further specialization in more advanced topics
- Cryptographic protocols (SoSe)
  - Continuation of this course
  - Elective course for Cyber Security Methods

Cyber Security

- What is Cyber?

  "Relating to or characteristic of the culture of computers, information technology, and virtual reality." Oxford dictionary

  "of, relating to, or involving computers or computer networks (such as the Internet)" Miriam Webster

  Origin: 1980s: abbreviation of cybernetics

- What is Security?

  Computer Security
  Network Security
  Internet Security

  Protection Measure
  deter, protect, detect and correct security violation

Definitions

- Computer Security
  - Generic name for the collection of tools
  - Designed to protect data and to thwart hackers

(prevent (someone) from accomplishing something.)

- Network Security
  - Measures to protect data during their transmission

- Internet Security
  - Measures to protect data during their transmission
  - Over a collection of interconnected networks

- Protection measures include measures
  - To deter, prevent, detect, and correct security violations
  - That involve the transmission & storage of information

Definitions

- What is privacy?

  "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others" [Westin 68]

  Right to digital self-determination

- Anonymity

  not identifiable for a set of subjects called anonymity set.

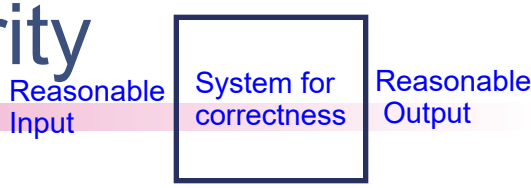
  "The state of being not identifiable within a set of subjects, the anonymity set" [Pfitzmann]

- Steganography
  - Conceals the existence of the message

Who needs privacy?

- Privacy-aware individuals
- Journalists and political dissidents in oppressive regimes (inflicting harsh and authoritarian treatment.)
- Organizations and companies (a person who opposes official policy, especially that of an authoritarian state.) (a system or ordered way of doing things.)
- Law enforcement
- Government, intelligent agencies, and military
- You?

Correctness versus Security



What is the difference between System correctness and security?

- System correctness: system satisfies specification
  - For reasonable input, get reasonable output
- System security: system properties preserved in face of attack
  - For unreasonable input, output not completely disastrous
- Main difference: interference from adversary
  (the action of interfering or the process of being interfered with.)
  (one's opponent in a contest, conflict, or dispute.)

- Note: Security is a property of a system that can only be defined negatively
  - A system is secure as long as there are no attacks against it

Safety vs. Security

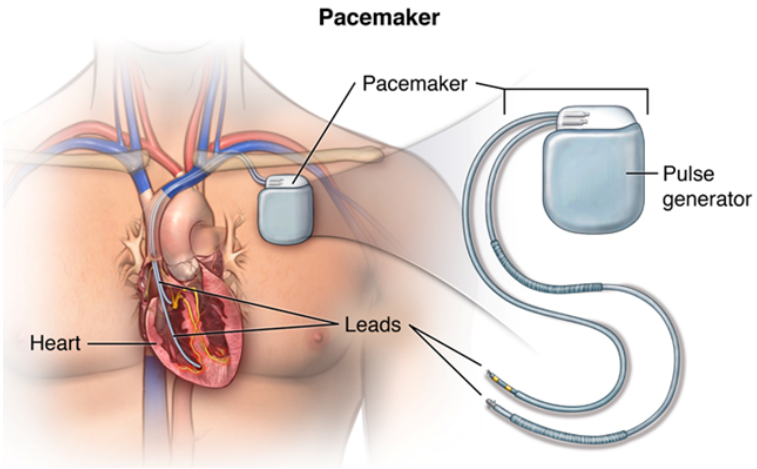
Safety - threat to the person, materials and infrastructure
Security - effect or risk of misuse by the aforementioned

Safety incidents and security vulnerabilities have vice versa cause and effect.

What is the difference between Safety and Security?

- Safety addresses the trustworthiness (the ability to be relied on as honest or truthful.) of the IT system whether it does not pose a threat to its environment [present or constitute (a problem or danger).] (persons, material, infrastructure)
- Security addresses the trustworthiness of the IT system to the effect that it does not pose any risk of misuse by the environment (information, services)
  - Security vulnerabilities can lead to safety incidents (an instance of something happening; an event or occurrence.) (e.g., security violation causes functional failure of the system)
  - Safety incidents can lead to security vulnerabilities that can be exploited in attacks (e.g., logical system error that grants access rights)

Why do we need Security?



Wirelessly controlled pacemaker / defibrillator

BBC Sign in News Sport Weather Shop Earth

NEWS

Home Video World UK Business Tech Science Stories Entertainment

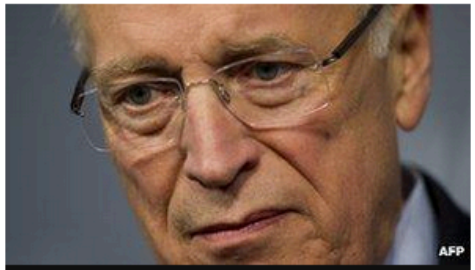
Technology

Dick Cheney: Heart implant attack was credible

21 October 2013

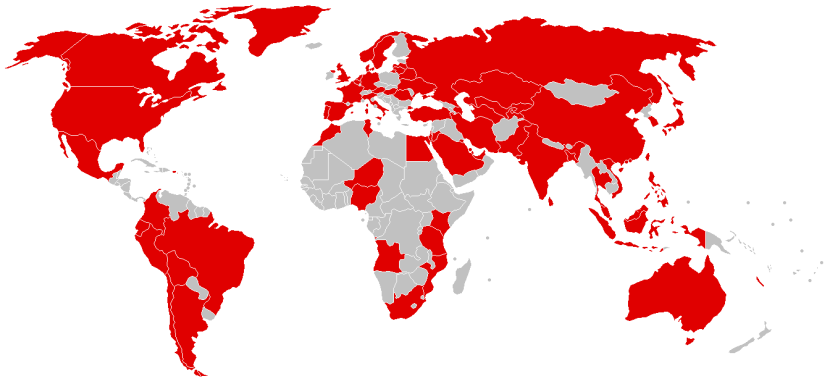
Dick Cheney, the former US vice-president, has revealed that he had his heart implant modified for fear of terrorist attack.

Mr Cheney's doctor disabled the heart defibrillator's wireless function in 2007 to prevent would-be assassins from interfering with it and causing a fatal heart attack.



Former US vice-president Dick Cheney has suffered from heart problems for much of his life.

Why do we need Security? (cont'd)



WannaCry ransomware 12.5.2017
Infected more than 250.000 Windows PCs in 150 countries

Cash only payments in China on 20,000 gas stations because of WCRY

Img sources: Wikipedia

Why do we need Security (cont'd)

- Internet is an open system
- Increasing connection of systems to the Internet
  - Internet of Things (sensors, objects)
  - Information systems, proprietary systems
  - Smartphones, tablets, …
- Growing threats to critical infrastructures (those with an essential importance for the society)
  - Energy supply networks
  - Telecommunication, transport and traffic system
  - Water supply, sewage
  - Healthcare, food supply

(expressing adverse or disapproving comments or judgements.)

Why do we need Security?
1. Increasing connection to the Internet which is open system
2. Threats to critical infrastructure of society
3. Increasing threat potential
4. Essential prerequisite to protect the IT systems/infrastructures

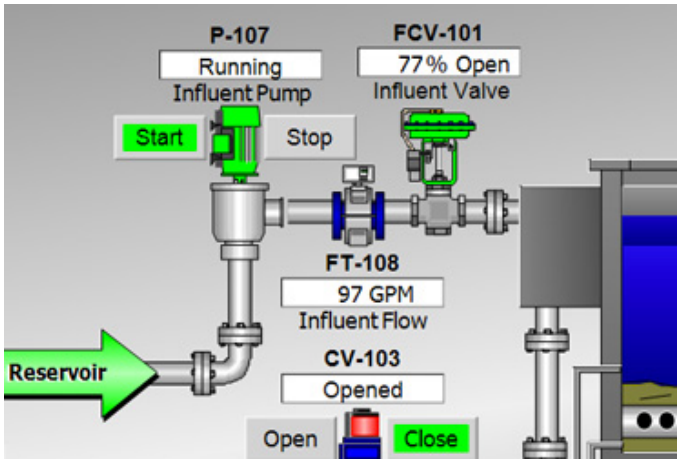
⇒Steadily increasing threat potential (having or showing the capacity to develop into something in the future.)

⇒Protection of IT systems / infrastructures is an essential prerequisite for their use and acceptance

(absolutely necessary; extremely important.)

SCADA Security

- Supervisory Control and Data Acquisition (SCADA)
  - Industrial control system
  - Hierarchical structure
  - Trend towards using standard Internet Protocol



Reasons for Security Issues

Security Issues:

1. Design(specification & feature) and implementation(configuration) errors
2. Careless system users
3. Abuse by Internal and external people
4. Interconnected system via Internet

- Design and implementation errors
  - Specification gaps
  - Feature orientation
  - Implementation errors
  - Configuration errors
- Careless behavior of system users
- Abuse by people
  {use (something) to bad effect or for a bad purpose; misuse.}
  - Internal (employees – curiosity, revenge, espionage) plural noun: spies, for Spy
    [the practice of spying or of using spies, typically by governments to obtain political and military information.]
    - Legal system access, inside the firewall
    - Familiar with policies and system architectures
  - External (hackers, spies, terrorists) a person employed by a government or other organization to secretly obtain information on an enemy or competitor.
- System interconnectivity via the Internet

Preventive vs. Reactive Security

c) Cybersecuritydistinguishesbetweenpreventiveandreactivesecurity. Definethetwoareas from each other and name two examples of measures for each area.

Two complementary approaches

- (prevention) Preventive - by means of encryption, authentication, access control, firewall, cryptographic hash functions.
  - Measures to prevent security violations (e.g., encryption, authentication, access control, firewalls, cryptographic hash functions)
- (detection) Reactive - by intrusion detection system, virus scanner, honeypots
  - Measures to detect security violations and limit their effect (e.g., intrusion detection system, virus scanner, honeypots)

{a honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.}

Network Defenses

Systems

Implementations

Firewalls, intrusion detection…

Blueprints

Protocols and policies

SSL, IPSec, access control…

Building blocks

Cryptographic primitives

{belonging to or characteristic of an early stage of development}

RSA, AES, HMAC, SHA-3…

- The defense mechanisms on **all abstraction layers** have to be **"secure"**

{a general idea rather than one relating to a particular object, person, or situation.}

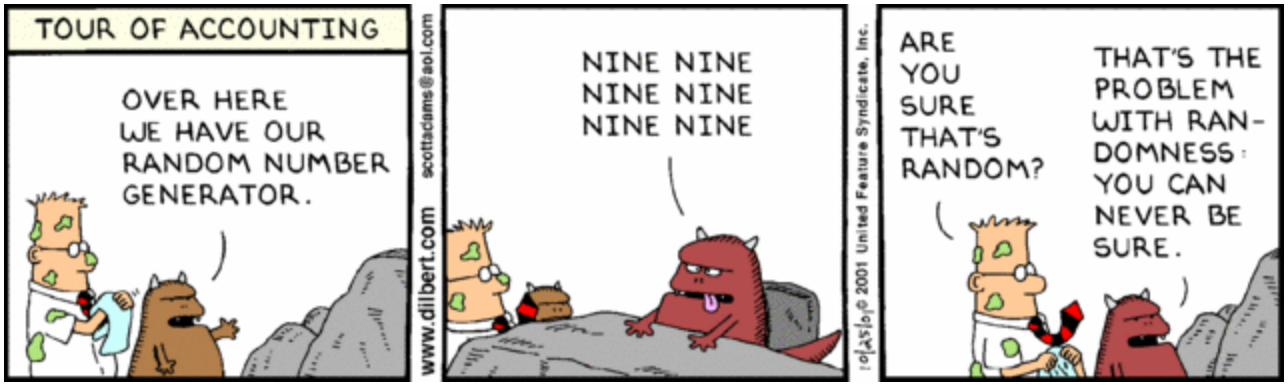
- They have to **interact properly** → **modular design** difficult

Modular design, or "modularity in design", is a design approach that subdivides a system into smaller parts called modules or skids, that can be independently created and then used in different systems.

Example Problems

- OpenSSL bug: implementation problem on Debian-based systems
  - Not a vulnerability in the protocol design
  - "Just" a problem in the implementation of the pseudo-random function
  - Lead to only 32,767 different keys
- Wired equivalent privacy problem in Wireless LAN
  - Not a vulnerability of the RC4 cipher itself
  - Problem(s) how RC4 is used → protocol design
- Total break of the encryption algorithm A5/2 in GSM
  - Weakness in the cryptographic building block itself
  - Combined with the fact that encryption is done after error correction

OpenSSL BugOpenSSL Bug



Dilbert ©2009, United Feature Syndicate, Inc.

Bad News

- Security often not a primary consideration
  - Performance, usability, and cost take precedence

{the condition of being considered more important than someone or something else; priority in importance, order, or rank.}

- Feature-rich systems are often poorly understood
  - Higher-level protocols make wrong assumptions
- Implementations are buggy
  - Buffer overflows are the “vulnerability of the decade”
- Networks are more open and accessible than ever
  - Increased exposure, easier to cover tracks

{the state of having no protection from something harmful}

- Many attacks are not even technical in nature
  - Phishing, impersonation, etc.

{an act of pretending to be another person for the purpose of entertainment or fraud.}

Better News

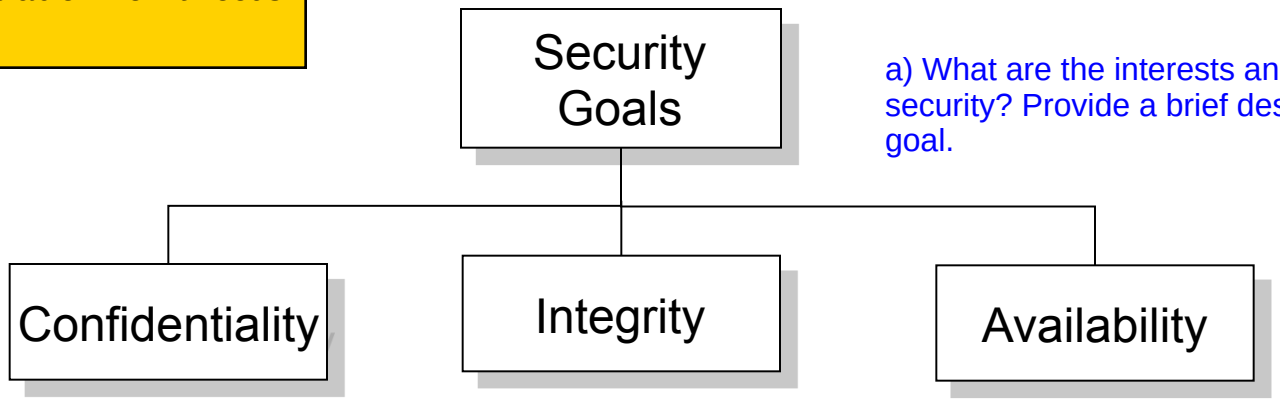
- There are a lot of defense mechanisms
  - We'll study some, but by no means all, in this course
- It's important to understand their limitations
  - "If you think cryptography will solve your problem, then you don't understand cryptography… and you don't understand your problem" -- Bruce Schneier
- Many security holes are based on misunderstanding
  - Security awareness and user "buy-in" help {Employee buy-in is when employees are committed to the mission and/or goals of the company,}
- Other important factors: usability and economics
- For cyber security studies also ethics

Objectives of this Chapter

- Define security goals
- Define security attacks that threaten security goals
- Define security services and their relation to the security goals
- Define security mechanisms to provide security services
- Define models for network and access security
- Provide an overview on the rest of the course

Security Goals
Confidentiality: Authorized persons can access only.
Integrity: No change of information without authorized persons
Availability: System available when it needs to the available.

Security Goals



a) What are the interests and goals of data security? Provide a brief description for each goal.

- Confidentiality
  - Ensure only authorized entities obtain information
  - Applies to storage and transmission of information
- Integrity
  - Changes to data on storage or during transmission only by authorized persons or processes
- Availability
  - Information stored by an organization needs to be available to authorized entities

An Attack is...

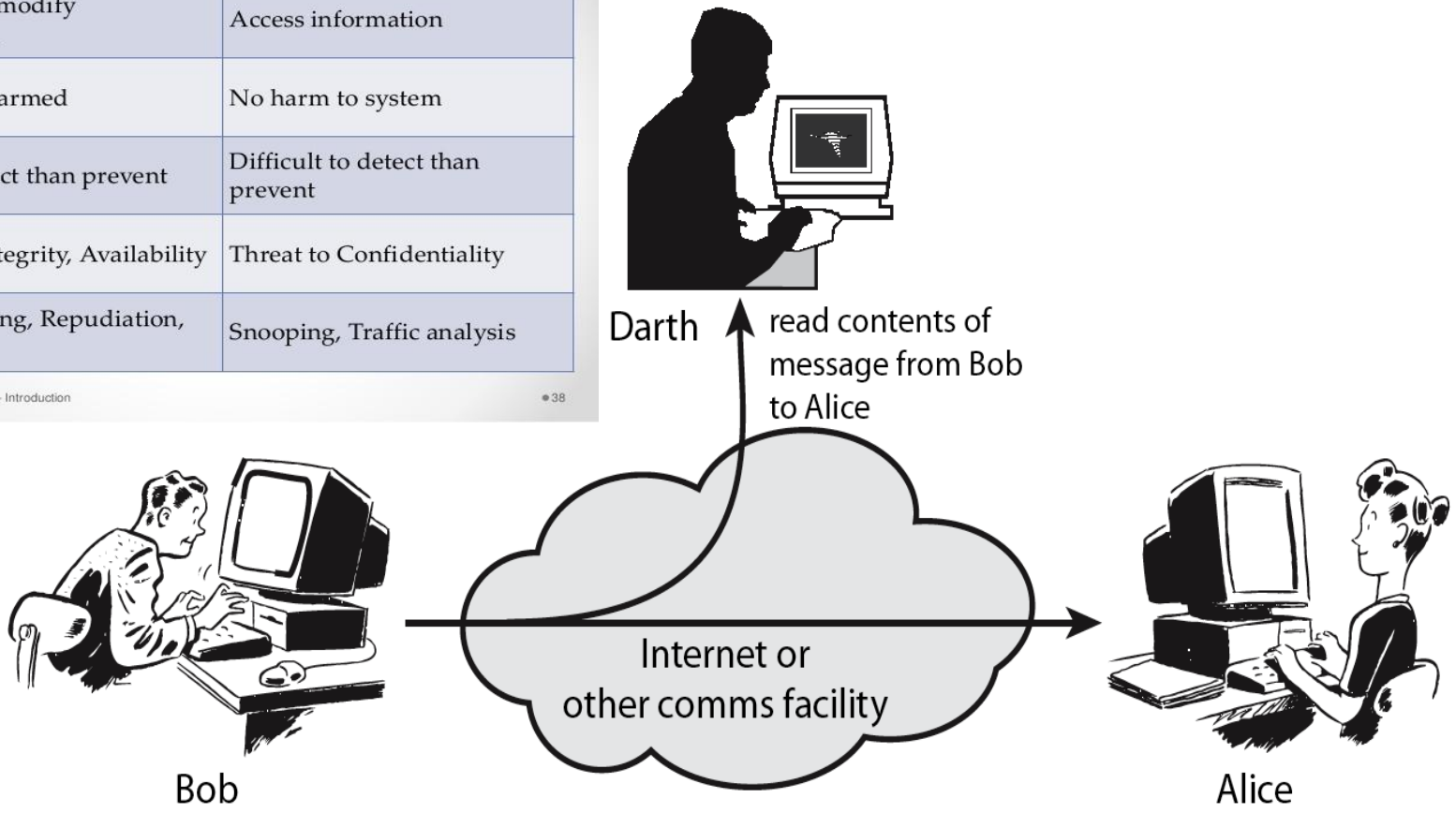
Attack is...
to compromises the security of information.

Generic 2 types
1. Passive Attacks
2. Active Attacks.

- …any action that compromises the security of information owned by an organization
- Information security is about how to
  - prevent attacks, or, failing that, to
  - detect attacks on information-based systems
- Often threat & attack are used to mean same thing
- There is a wide range of attacks
- We will - for now - focus on generic types of attacks
  - passive
  - active

Passive Attacks

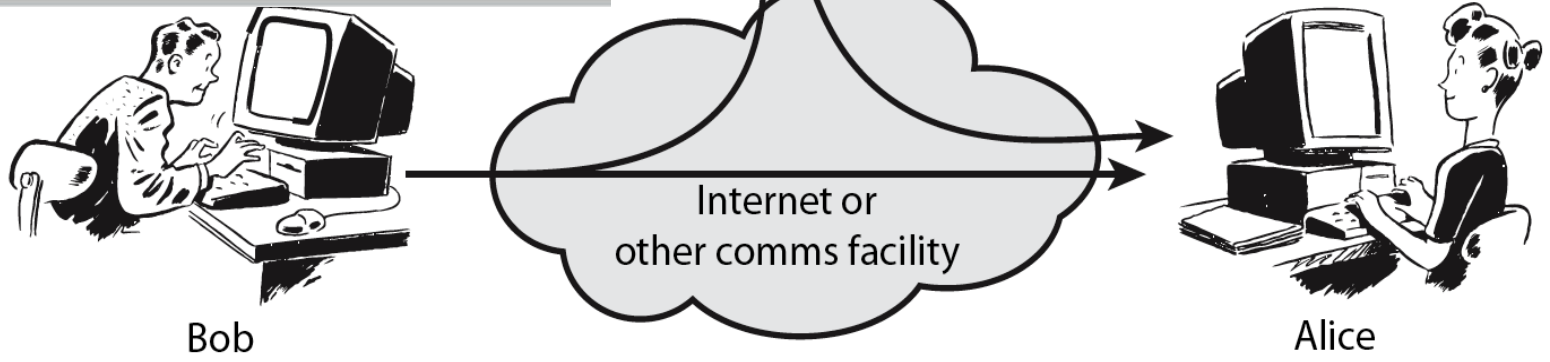
Active Attack	Passive Attack
Access and modify information	Access information
System is harmed	No harm to system
Easy to detect than prevent	Difficult to detect than prevent
Threat to Integrity, Availability	Threat to Confidentiality
Masquerading, Repudiation, DOS	Snooping, Traffic analysis



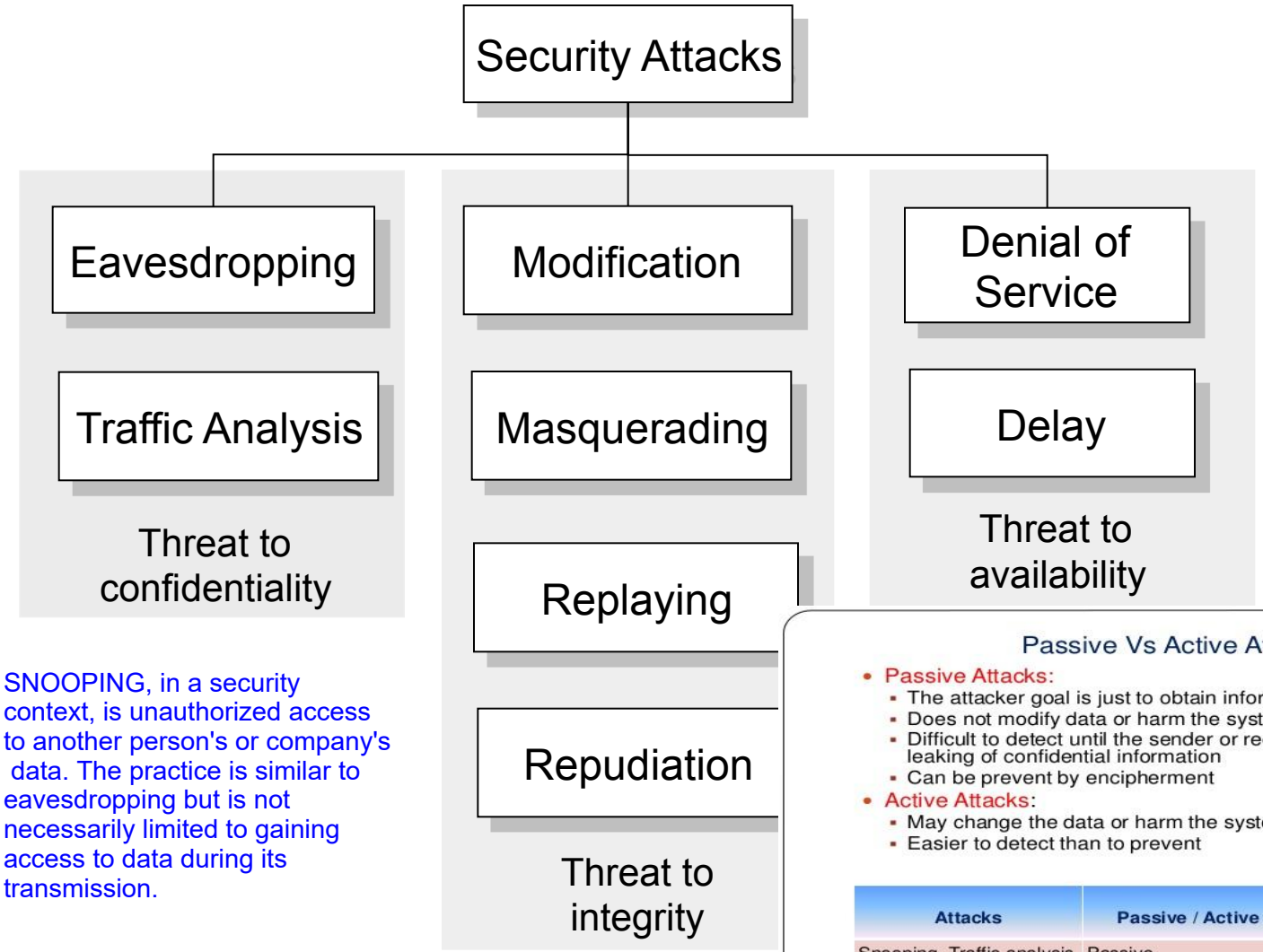
Active Attacks

Passive and Active Attacks

- Passive attacks attempt to learn or make use of information from the system but does not affect system resources
  - eavesdropping/monitoring transmissions
  - difficult to detect
  - emphasis is on prevention rather than detection
  - two types:
    - release of message contents
    - traffic analysis
- Active attacks involve modification of the data stream
  - goal is to detect them and then recover
  - four categories:
    - masquerade
    - replay
    - modification of messages
    - denial of service



Taxonomy of Attacks



SNOOPING, in a security context, is unauthorized access to another person's or company's data. The practice is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission.

Passive Vs Active Attacks

- Passive Attacks:
  - The attacker goal is just to obtain information
  - Does not modify data or harm the system
  - Difficult to detect until the sender or receiver finds out about leaking of confidential information
  - Can be prevent by encipherment
- Active Attacks:
  - May change the data or harm the system
  - Easier to detect than to prevent

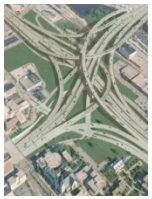
Attacks	Passive / Active	Threatening
Snooping, Traffic analysis	Passive	Confidentiality
Modification, Masquerading, Replay, Repudiation	Active	Integrity
Denial of Services	Active	Availability

Attacks Threatening Confidentiality

- Eavesdropping
  - Unauthorized access to or interception of data
  - Traffic Analysis

(the process of receiving electronic transmissions before they reach the intended recipient.)

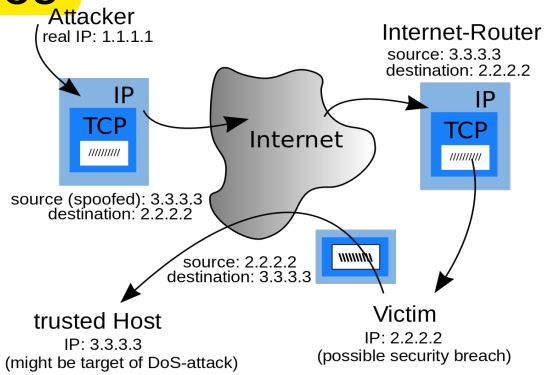
  - Monitoring online traffic may reveal confidential information
  - E.g. email address of sender/receiver



- Note: in this lecture we use eavesdropping, intercepting and recording in the following way
  - Eavesdropping = recovering the plaintext
  - Interception = cipher-text
  - Recording = cipher-text

Attacks Threatening Integrity

- Modification
  - After intercepting or accessing information, the attacker modifies the information to make it beneficial to himself
  - Includes simple deletion or delay of messages
- Masquerading (pretend to be someone, one is not.)
  - Also called spoofing
  - An attacker impersonates somebody else
- Replaying
  - An attacker obtains a copy of a message sent by an entity and later on tries to replay it to the receiver



Replay

- Similar to an active man-in-the-middle attack
- Whereas an active man-in-the-middle attack changes the contents of a message before sending it on, a replay attack only captures the message and then sends it again later
- Takes advantage of communications between a network device and a file server

JURINNOV eDiscovery & eSecurity

Attacks Threatening Integrity

- Repudiation
  - The sender of a message later on denies that he has sent it
  - The receiver of a message later on denies that he has received it
- As of today repudiation is often not technically guaranteed
  - E.g. phone bills: call detail records exchanged between cell phone providers can be legally repudiated by subscribers

Attacks Threatening Availability

- Denial of Service
  - Slows down or totally interrupts the service of a system
  - Attacker may e.g.
  - send bogus requests to a server such that the server crashes because of the heavy load
  - Intercept and delete a server's response to a client, making the client believe that the server is not responding
  - Block the requests from a client such that the client sends requests many times
- …

Categorization in Active and Passive

Attack	Passive/Active	Threatening
Snooping **Traffic Analysis**	**Passive**	**Confidentiality**
Modification	**Active**	**Integrity**
Masquerading		
Replaying		
Repudiation	**Active / Passive**	**Integrity / Availability**
Denial of Services	**Active**	**Availability**

Further Definitions

(having or showing the capacity to develop into something in the future.)

- Threat: is a potential event or sequence of events that could lead to an abuse or malfunction of the IT system
- Attack: implementation of a threat that exploits a vulnerability

[make full use of and derive benefit from (a resource).]

- Exploit: program that executes the attack
- Incident: executed attack

Objective of IT security is to compensate and minimize the risks and threats existing in the respective application environment

Security Mechanisms and Services

- Security Mechanism
  - A mechanism that is designed to detect, prevent, or recover from a security attack.
- Security Service
  - A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Security Mechanism: detect, prevent or recover from a security attack

Security Service: makes use of one or more security mechanism to enhance the data processing systems and information transfers.

Security Services

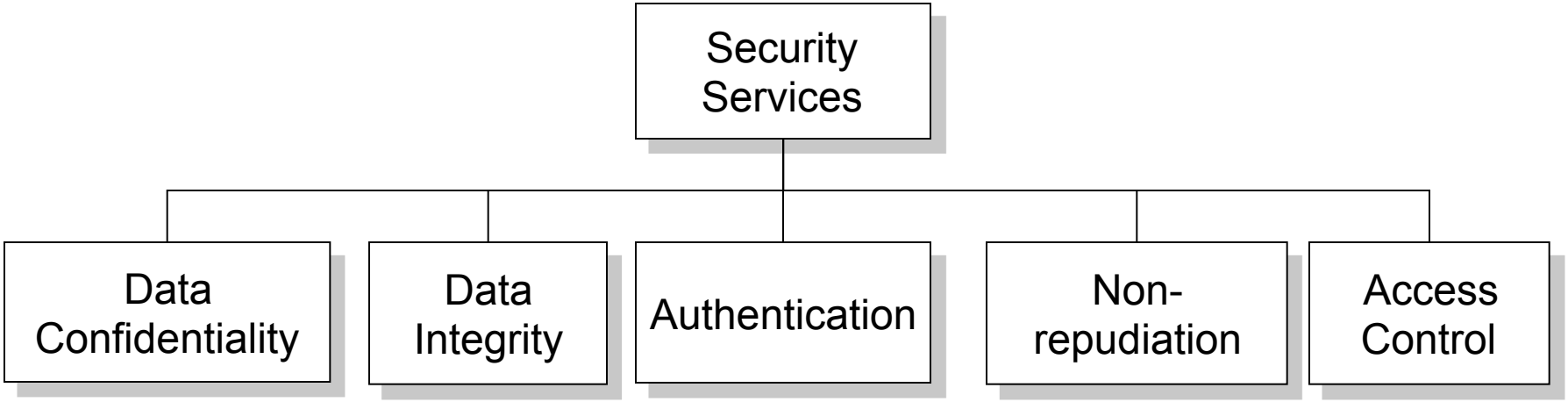
- Definitions of Security Services
- ITU-T X.800:

  "A service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers"

- IETF RFC 2828:

  "A processing or communication service provided by a system to give a specific kind of protection to system resources"

Security Services



- Data Confidentiality - protection of data from unauthorized disclosure
- Data Integrity - assurance that data received is as sent by an authorized entity

List concurrent requirements regarding the information exchange

Security Services

b) What additional goals are pursued in the concept of multilateral data security? Explain these protection goals briefly and explain how they might conflict with the classical ones.

- Authentication - assurance that the communicating entity is the one claimed
- Access Control - prevention of the unauthorized use of a resource
- Data Confidentiality - protection of data from unauthorized disclosure
- Data Integrity - assurance that data received is as sent by an authorized entity
- Non-Repudiation - protection against denial by one of the parties in a communication

Security Mechanisms: ITU-T X.800

- Specific security mechanisms:
  - encryption, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization

((especially of an unwelcome influence or physical effect) spreading widely throughout an area or a group of people.)

- Pervasive security mechanisms:
  - trusted functionality, security labels (indicate how sensitive or critical system resources are), event detection, security audit trails (chronological record of system activities), security recovery

2 Types of Security Mechanisms as per ITU-T X.800

1. Specific Security Mechanism such as, encryption, access control, traffic padding, routing control, etc.

2. Pervasive Security Mechanism such as, trusted functionality, event detection, security audit trails, etc.

Security Mechanisms

- Encryption – hides or covers complete or partial data, may additionally bind data blocks together
- Data integrity – appends check value to data
- Digital Signatures – mechanism by which a sender can electronically sign data and the receiver can check the signature, contains integrity
- Authentication exchange – proofs the identity of an entity to another entity
- Key agreement – allows two or more parties to agree upon secret keys, used to ensure continuous authenticity, typically required for all other mechanisms

Security Mechanisms

- Traffic padding – inserting bogus data into traffic to thwart traffic analysis
- Routing control – continuously changing available routes between sender and receiver to prevent opponent from eavesdropping on a particular route
- Notarization – selecting a third party to control the communication between two entities e.g. to thwart repudiation
- Access Control – method to prove that an entity has access right to the data or resource owned by a system and to guarantee that only authorized entities can access the data or resource

Model for Network Security

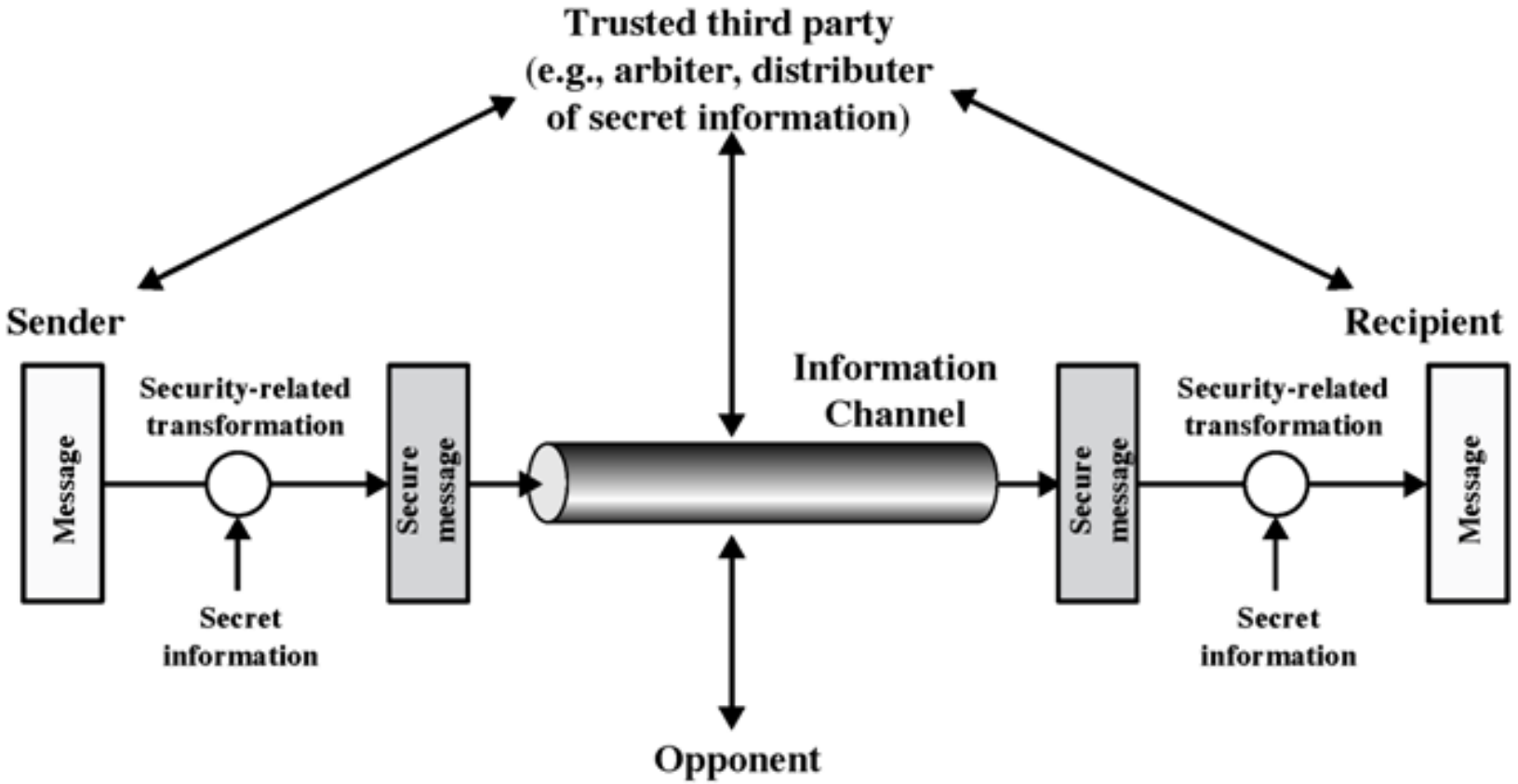


Figure 1.5 Model for Network Security

Model for Network Security

- Using this model requires us to:
  - Design a suitable algorithm for the security transformation
  - Generate the secret information (keys) used by the algorithm
  - Develop methods to distribute and share the secret information
  - Specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Access Control

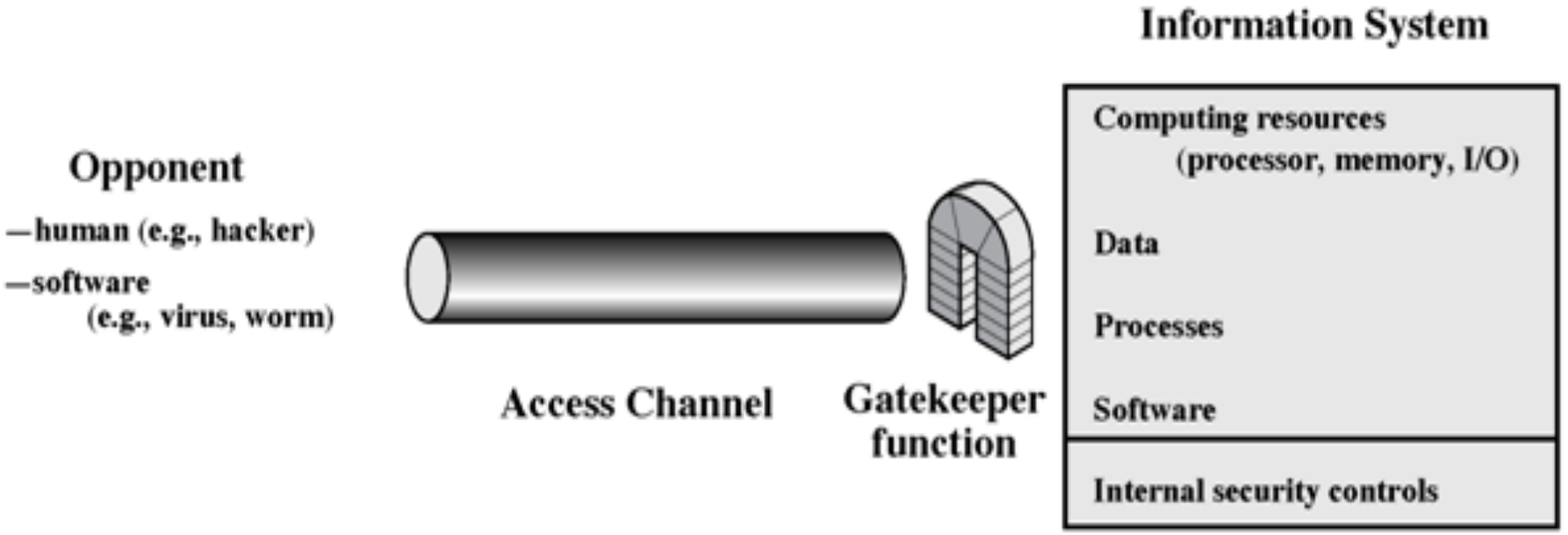


Figure 1.6 Network Access Security Model

Model for Network Security

- Using this model requires us to:
  - Select appropriate gatekeeper functions to identify users
  - Implement security controls to ensure only authorized users access designated information or resources
- Trusted computer systems may be useful to help implement this model

A Note on Policies

- A security policy is a statement of what is, and what is not allowed
- A security policy is typically derived from analyzing and evaluating the potential threats to a system
- A security mechanism is a method, tool or procedure for enforcing a security policy

Who are Attackers and What Drives them?

1. Criminals - For financial gain, spread spam, destroy copy protection or extort money,
2. Crackers - achieve fame and glory in blackhat,
3. Insiders eg. have access to confidential data like administrator and last but not the least,
4. Security services, Terrorist, Military Personal

- Criminals
  - Put up a fake financial website, collect users' logins and passwords, empty out their accounts
  - Insert a hidden program into unsuspecting users' computers, use them to spread spam
  - Subvert copy protection, gain access to music and video files
  - Stage denial of service attacks on websites, extort money

(to try to destroy or damage something)

[obtain (something) by force, threats, or other unfair means.]

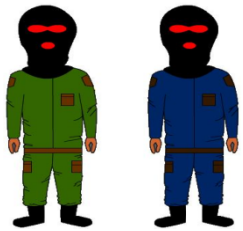
- Crackers
  - Wreak havoc, achieve fame and glory in the blackhat community

(cause the destruction of (a ship) by sinking or breaking up.)

[confusion and lack of order, especially causing damage or trouble: The storm wreaked (= caused) havoc in the garden, uprooting trees and blowing a fence down.]

Who are Attackers and What Drives them?

- Insiders (criminal as well as harmless ones!!)
  - E.g. anyone authorized to access confidential data
  - E.g. administrators, regular personnel
- Secret Services, Terrorists, Military Personal



Offender Classes

- Insiders vs. outsiders
- Users of a system/software
- Provider of a system/software
- Maintenance service
- Developers of a system
- Producers of design and development tools

⇒*In IT Security, no one is excluded as a potential offender*

White-Hat (idealists, hobby)

Grey-Hat (also accepts legal violations)

Black-Hat (destructive, espionage) hackers

Next Topics

Symmetric Encryption

Integrity Protection

Asymmetric Crypto

Authentication and Key Agreement

Certificates and PKI

Kerberos

E-Mail Security

Overview on Chapters - Basics

Chapter 2
Symmetric Encryption

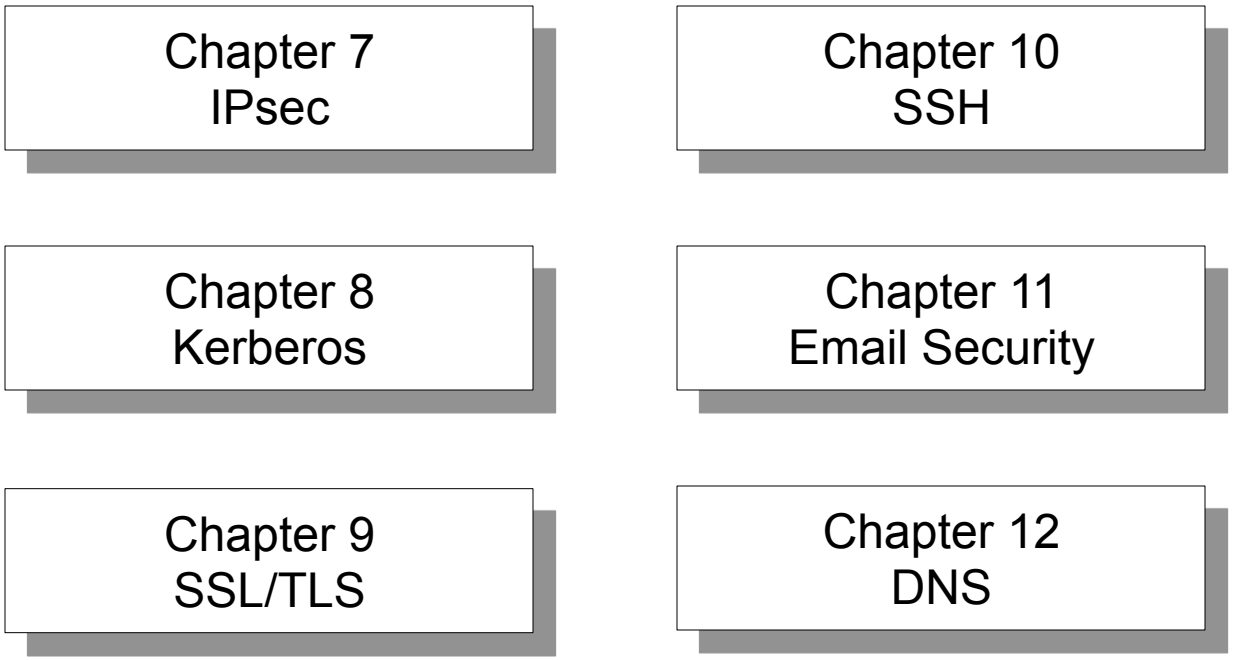
Chapter 3
Integrity Protection

Chapter 4
Asymmetric Crypto

Chapter 5
Authentication and
Key Agreement

Chapter 6
Certificates and PKI

Overview on Chapters - Protocols



Overview on Chapters – Related Topics

Chapter 13
SPAM

Chapter 14
Botnets

Chapter 15
Phishing

Some Notable Standardization Bodies

- ANSI - American National Standards Institute
  - http://www.ansi.org
- X9 - Standards for Financial Services Industry
  - http://www.x9.org
- X.509 – Public Key Certificates
- IEEE - Institute of Electrical and Electronics Engineers
  - http://www.ieee.org
- P1363 - Specifications for Public-Key Cryptography
  - http://grouper.ieee.org/groups/1363
- SC 27 - Information Technology – Security Techniques
  - http://www.jtc1sc27.din.de (joint work of ISO and IEC)
- ISO - International Organization for Standardization
  - http://www.iso.ch
- IEC - International Electronic Commission
  - http://www.iec.ch

More Notable Standardization Bodies

- NIST — National Institute of Standards and Technology
  - http://www.nist.gov
- FIPS — Federal Information Processing Standards
  - http://www.itl.nist.gov/fipspubs
- IETF — Internet Engineering Task Force
  - http://www.ietf.org/
- PKCS — Public-Key Cryptography Standards
  - http://rsa.com/rsalabs/

Some Links to Software

- GNU MP: http://gmplib.org/, license free
  - Efficient modular arithmetic
- MIRACL: http://www.shamus.ie/, license free
  - Cryptographic primitives (symmetric, asymmetric, elliptic curves)
- NTL: http://www.shoup.net/ntl/
  - C++ library, polynomials, finite fields, etc.
- OpenSSL: http://www.openssl.org
  - Open Source Toolkit, including SSL v2/v3, TLS v1, Crypto-library

Recommended Reading

- Book chapters for this chapter
  - Introductory chapter of Stallings: Cryptography and Network Security: Principles and Practices
  - Introductory chapter of Forouzan: Introduction to Cryptography and Network Security

- Image sources:
  - Stallings: Cryptography and Network Security: Principles and Practices (active / passive attacks)
  - Forouzan: Introduction to Cryptography and Network Security (inspirational)