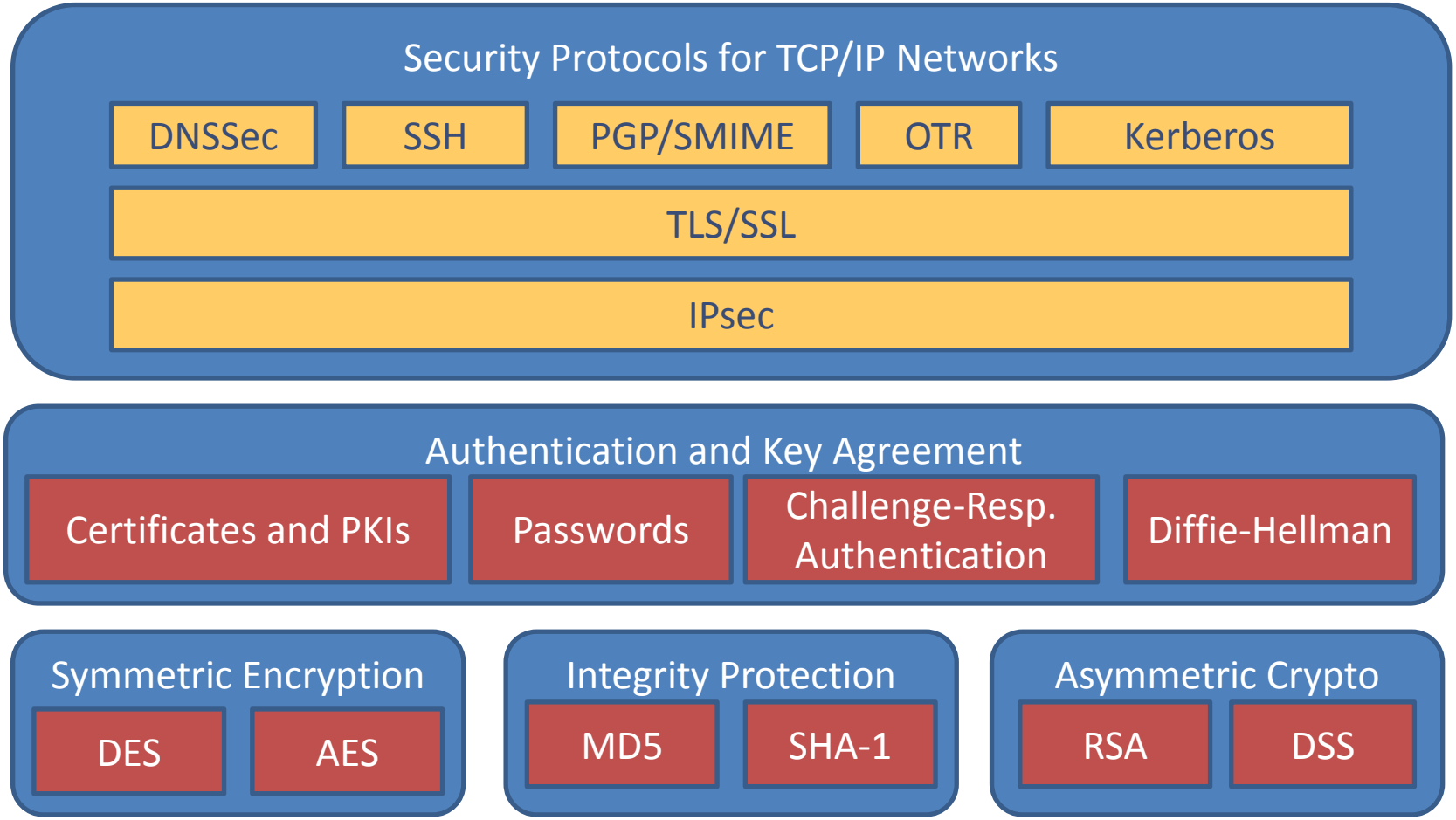
IT-Security 1

Chapter 1: Introduction

Prof. Dr.-Ing. Ulrike Meyer

WS 15/16

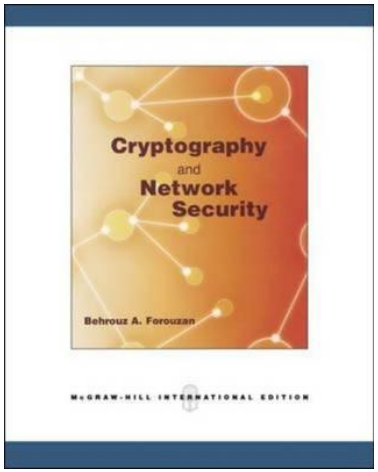
IT-Security 1: What this Course is About



IT-Security 1: The Destructive Part

What Knowledge Do You Need to Follow

- Basic Knowledge on TCP/IP Networks
- No problem for those who attended DatKom or DCIT during bachelor or master studies
- If you did not attend DatKom or DCIT
  - A very brief introduction to TCP/IP can be found in the appendix of this book by Forouzan



What This Course is NOT About

- Only overview of most important cryptographic primitives
  - To dive deeper into cryptography attend one of the following
  - Algorithmic Cryptography of Dr. Unger
  - Cryptography 1+2 with Prof. Mathar
- No systems security issues, no secure hardware, no intrusion detection, no firewalls, no malware
  - Take the lecture IT-Security 2 – System Security with us for these issues
- No security of mobile / wireless networks such as GSM, UMTS, LTE, WLAN, Bluetooth, RFID,…
  - Take the lecture Mobile Security with us for these issues

Terms

- Computer Security
  - generic name for the collection of tools designed to protect data and to thwart hackers

- Network Security
  - measures to protect data during their transmission
  - measures to protect data stored on networked devices

- Internet Security
  - measures to protect data during their transmission over a collection of interconnected networks
  - measures to protect data stored on devices connected to the internet

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

Correctness versus 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

- Note: Security is a property of a system that can only be defined negatively, namely:
  - A system is secure as long as there are no attacks against it
  - Typically only possible to proof that system is secure against particular attacks but not that there aren't any other attacks

Network Protection

Systems

Blueprints

Building blocks

Implementations

Firewalls, intrusion detection…

Protocols and policies

SSL, IPSec, access control…

Cryptographic primitives

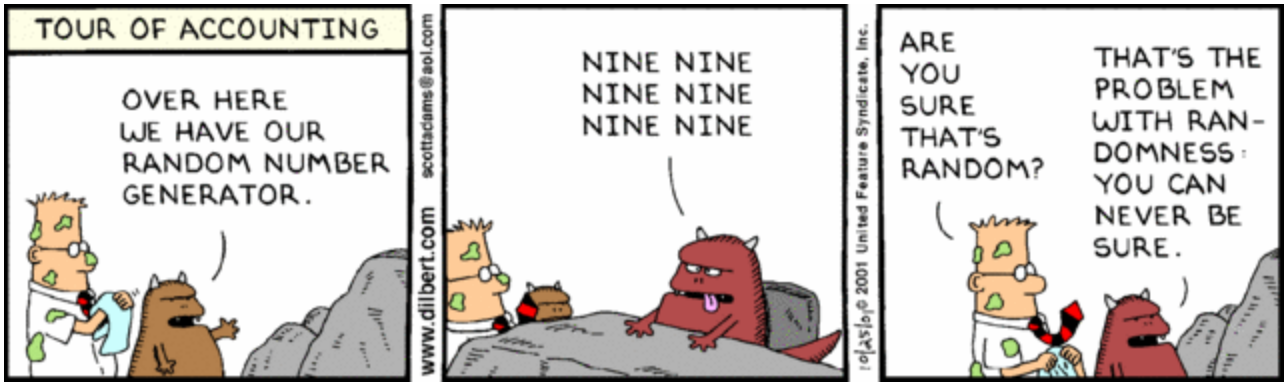
RSA, DSS, HMAC, SHA-1…

- The defense mechanisms on all abstraction layers have to be "secure"
- They have to interact properly → modular design difficult

Example Problems

- 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 bug: implementation problem on Debian-based systems
  - Lead to only 32,767 different keys
  - Not a vulnerability in the protocol design
  - “Just” a problem in the implementation of the pseudo-random function

OpenSSL Bug


TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
www.dilbert.com scottadams@aol.com
NINE NINE NINE NINE NINE NINE
© 2001 United Feature Syndicate, Inc.
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RAN-DOMNESS: YOU CAN NEVER BE SURE.

Example Problem: Backward Compatibility

Forscher demonstriert Lücke im PGP-Standard

08.10.2015 09:39 Uhr – Jürgen Schmidt vorlesen

Durch die Rückwärtskompatibilität könnten Angreifer verschlüsselte und signierte Nachrichten nachträglich manipulieren. Immerhin geben aktuelle GnuPG-Versionen dann einen Hinweis auf mögliche Probleme.

Example Problem: Backdoors in Cryptosystems

Crypto Wars 3.0: Obama will Verschlüsselung nicht per Gesetz schwächen

09.10.2015 10:18 Uhr – Martin Holland

vorlesen

US-Präsident Barack Obama (Bild: dpa, Aude Guerrucci)

Die US-Regierung will vorerst keine Gesetze anstreben, die eine Schwächung von Verschlüsselung vorschreiben würden. IT-Unternehmen sollen stattdessen davon überzeugt werden, Ermittlern Zugänge zu Daten ihrer Kunden zu öffnen.

Example Problem: The Human Factor

Google vergisst interne Zugangsdaten auf ausrangiertem Router

06.10.2015 11:04 Uhr – Ronald Eikenberg vorlesen

Ein deutscher Online-Shop hat einen generalüberholten Router verkauft, der zuvor offenbar für Google Dienst schob. Das Gerät hat den Internetriesen mit allerhand sensiblen Informationen verlassen, welche die neuen Besitzer problemlos auslesen konnten.

Bad News

- Security often not a primary consideration
  - Performance, usability, and cost take precedence
- 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
- Many attacks are not even technical in nature
  - Phishing, social engineering, etc.

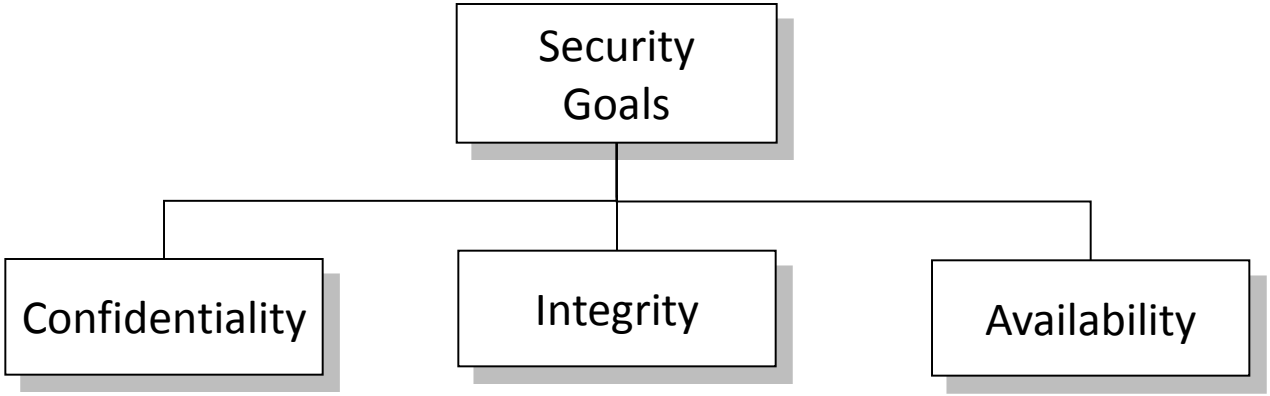
Better News

- 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
- Security awareness is continuously on the rise
  - Even on regular news!
- Security experts currently have good job opportunities
- Research projects in networking and other areas that do not take security and privacy into account are currently often rejected

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
- Provide an overview on the rest of the course

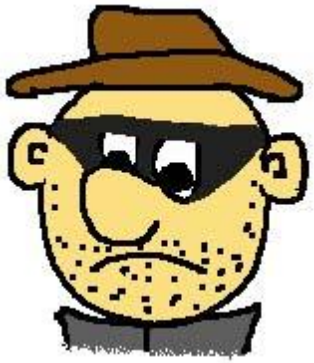
Security Goals



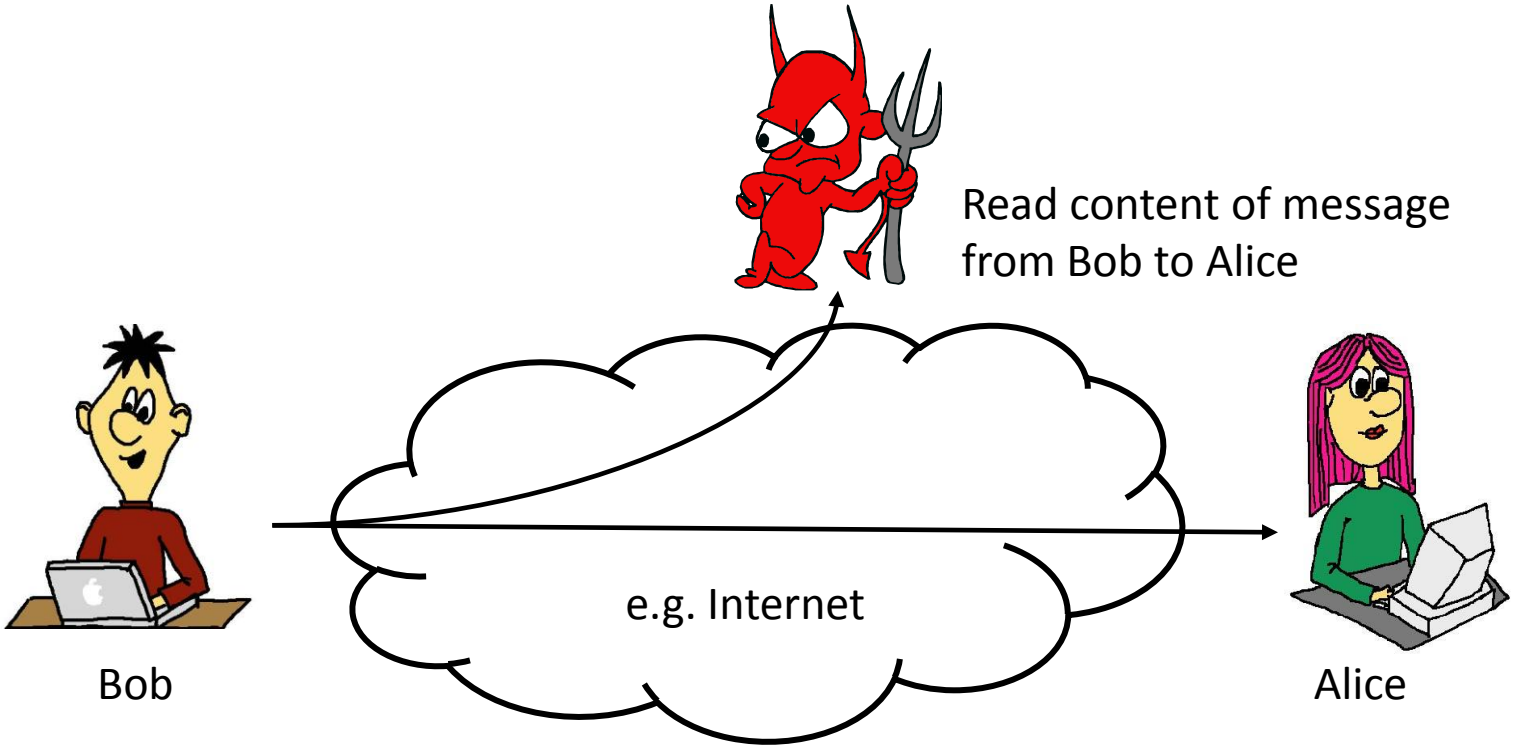
- Confidentiality
  - Ensure only authorized entities obtain information
  - Applies to storage and transmission of information
- Integrity
  - Changes to data on storage or during transmission only by authorized persons or processes
- Availability
  - Information stored by an organization needs to be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

An Attack is...

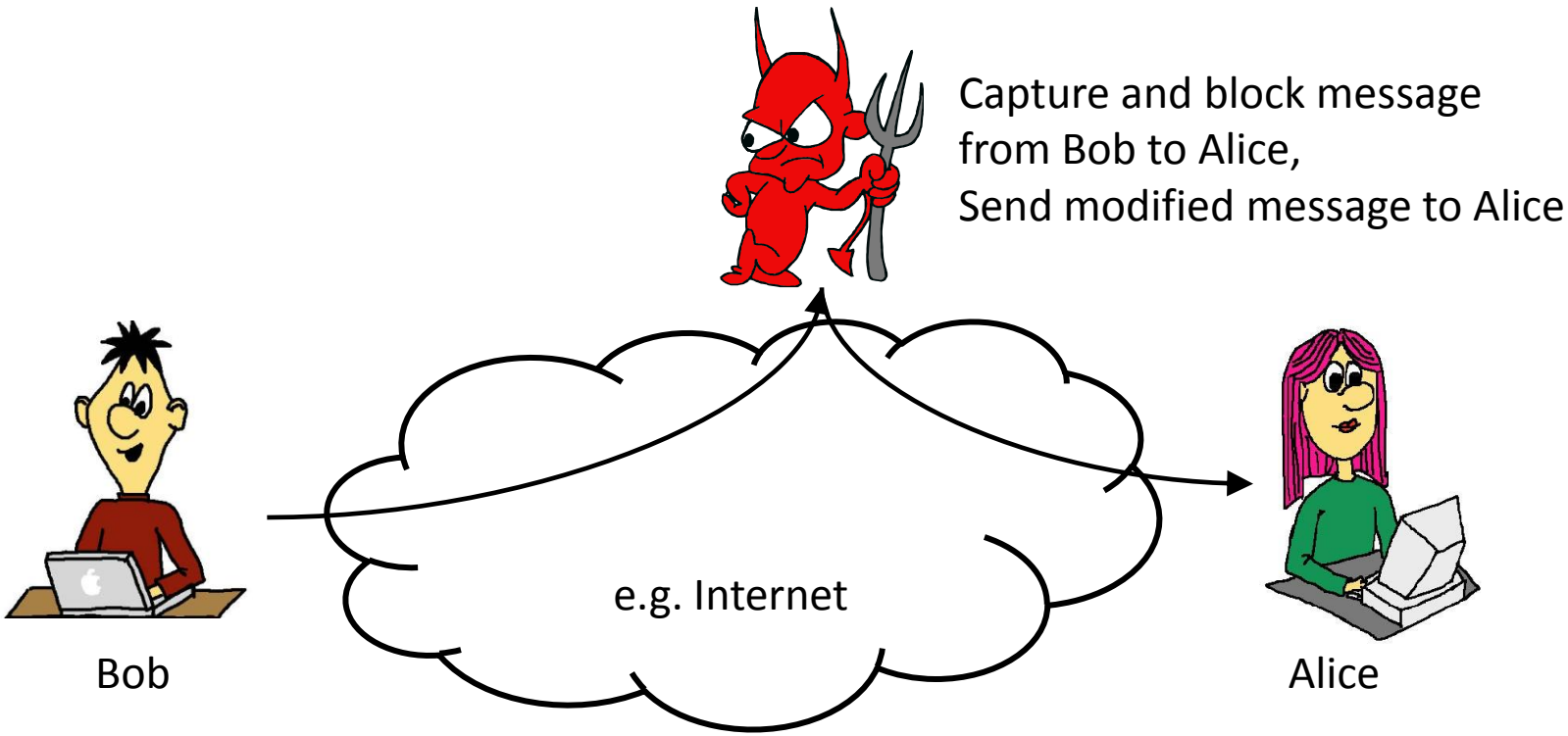
- …any action that compromises a security goal with respect to information owned by an organization
- Often threat & attack are used to mean same thing
- There is a wide range of attacks
- One way to classify them on is
  - Passive attacks
  - Active attacks



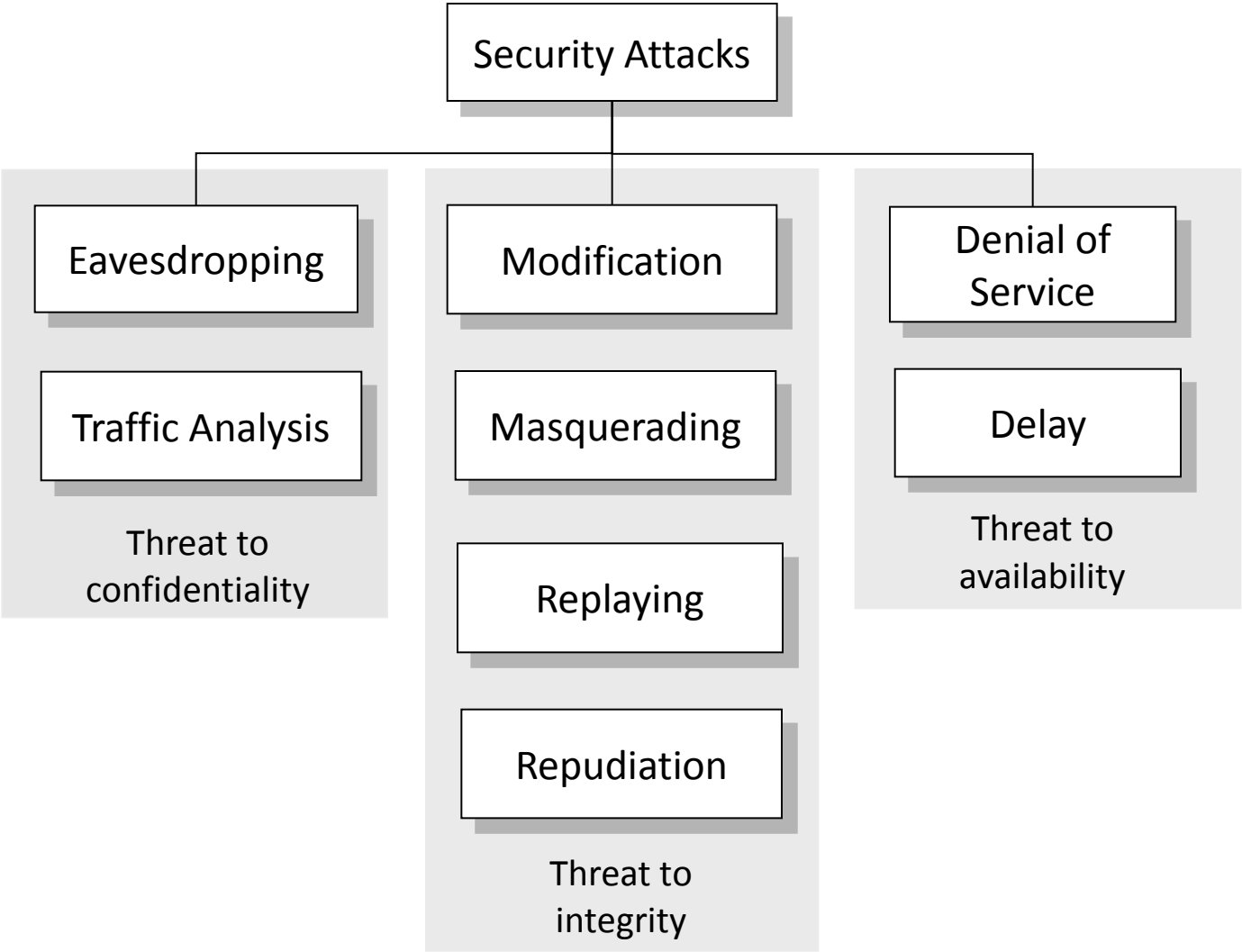
Passive Attacks - Example Eavesdropping



Active Attacks – Example: Modifying



Taxonomy of Attacks



Attacks Threatening Confidentiality

- Eavesdropping
  - Unauthorized access to or interception of data

- Traffic Analysis
  - Monitoring traffic may reveal confidential information even if traffic is encrypted
  - Information can be deduced by analyzing address information, timings, frequencies etc.

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
  - 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

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

- Protection against repudiation is often done by non-technical means
  - 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**

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 Services

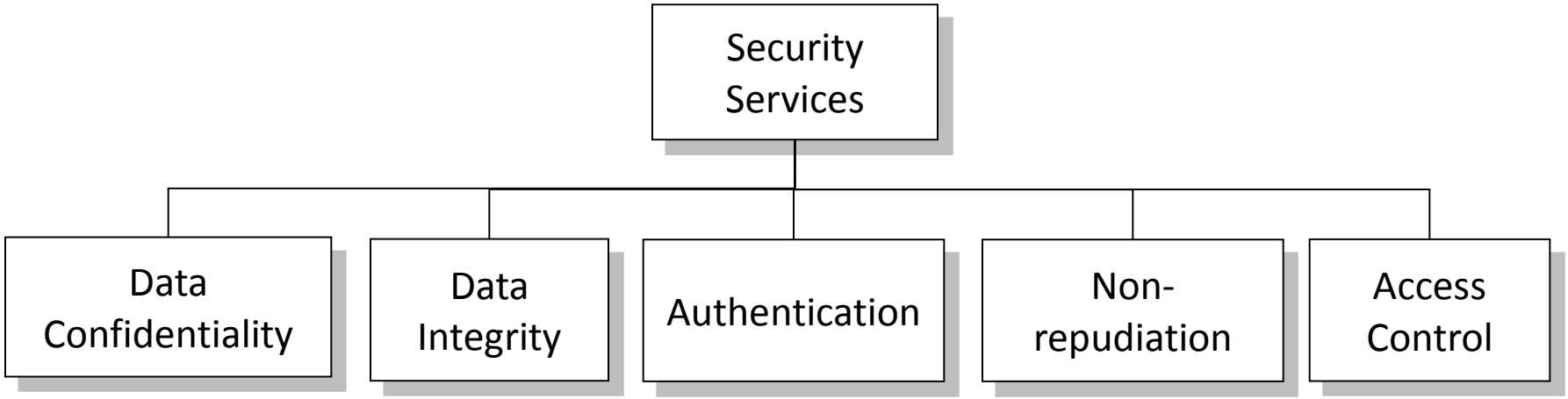
- ITU-T X.800:

  "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:

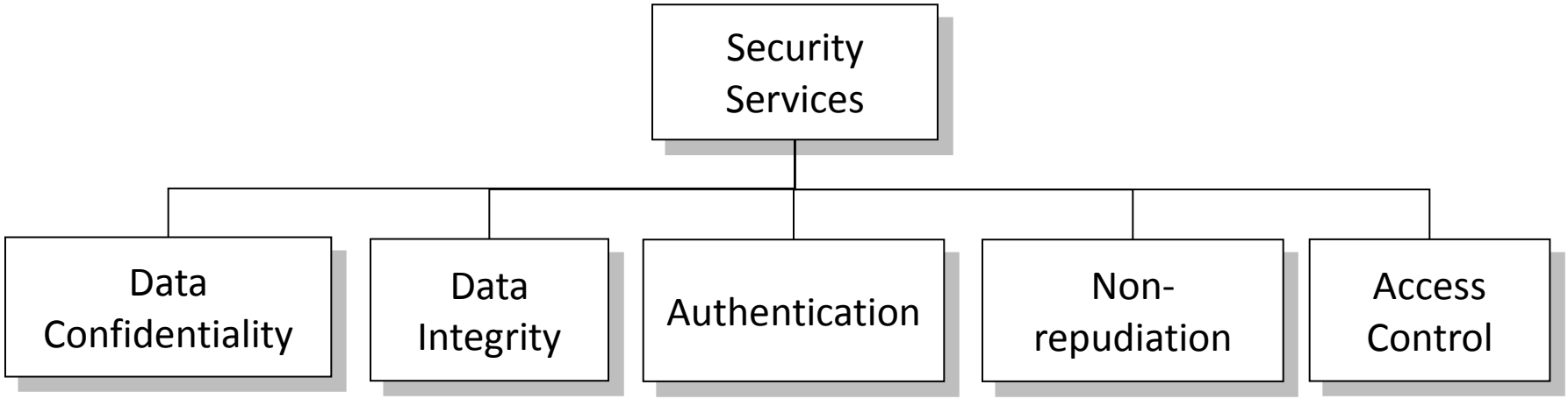
  "A processing or communication service provided by a system to give a specific kind of protection to system resources"

Security Services



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

Security Services



- Authentication - assurance that the communicating entity is the one claimed
- Non-Repudiation - protection against denial by one of the parties in a communication
- Access Control - prevention of the unauthorized use of a resource

Security Mechanisms: ITU-T X.800

- Specific security mechanisms:
  - encryption, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- Pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery

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

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?

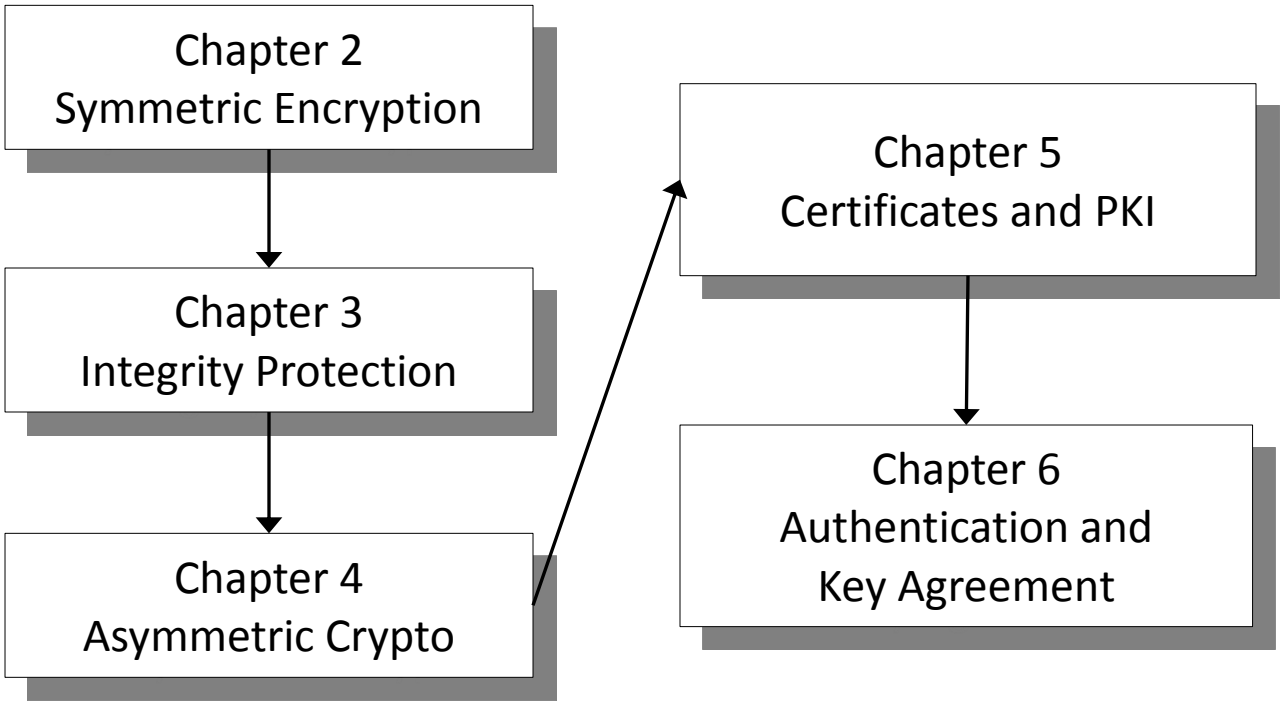
- Criminals
  - Put up a fake financial website, collect users' logins and passwords, empty out their accounts
  - Insert a hidden program into unsuspecting users' computers, use them to spread spam
  - Subvert copy protection, gain access to music and video files
  - Stage denial of service attacks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

- Crackers
  - Achieve fame and glory in the blackhat community

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
- Innocent end users
  - That do not protect their computers
- Secret Services, Terrorists, Military Personal

Overview on Chapters – Cryptographic Basics



Overview on Chapters – Protocols & Co

Chapter 12

Chapter 7
Kerberos

Chapter 8
IPsec

Chapter 9
SSL/TLS

Chapter 10
Phishing

Chapter 11
Email Security

Mo 21st of December
Physical Security

Chapter 12
SPAM

Chapter 13
OTR

Chapter 14
DNS and Security

Chapter 15
SSH

Chapter 16
Anonymous Comm.

Chapter 17
SMPC

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
- Bouncy Castle Crypto APIs: http://www.bouncycastle.org/
  - A lightweight cryptography API for Java and C#.

Recommended Reading

- Book chapters for this chapter
  - Introductory chapter of Stallings
  - Introductory chapter of Forouzan