

Network Security (NetSec)



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Summer 2015

Chapter 01: Fundamentals

Module 01: Information Security 101



Prof. Dr.-Ing. Matthias Hollick

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science
Center for Advanced Security Research Darmstadt - CASED

Prof. Dr.-Ing. Matthias Hollick
matthias.hollick@seemoo.tu-darmstadt.de

Mornewegstr. 32
D-64293 Darmstadt, Germany
Tel.+49 6151 16-70922, Fax. +49 6151 16-70921
<http://seemoo.de> or <http://www.seemoo.tu-darmstadt.de>



Information Security 101

Learning Objectives

Obtain a common understanding of information security

- Identify the most important basic concepts of information security
- Have thorough understanding of security terminology
- Discuss basic attack principles and classify attacks
- Discuss security policies & mechanisms

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—The Art of War, Sun Tzu

Overview of this Module



- (1) Some basic definitions
- (2) Security goals and objectives
- (3) Actors in communication security
- (4) Attack classification
- (5) Recommended readings

Chapter 01, Module 01

Some Terms & Definitions

Security goals/objectives

- Abstract guard/protection goals to be achieved

Risks

- Vulnerabilities: security flaws in systems
 - Flaws in design, implementation, operation
- Attacks: means of exploiting vulnerabilities
 - Attacks have implicit concept of “intent”, try to violate security
- Threats: motivated adversaries capable of mounting attacks which exploit vulnerabilities

Countermeasures

- Technical or procedural means of addressing vulnerabilities or thwarting specific attacks

Questions & Definitions

To be answered at home:

- How can “security” be defined?
- How can “attack” be defined?
- How can “threat” be defined?

- Please look for definitions (colloquial, technical, ...)
- There is a wiki on the learning platform: please enter one definition (per course participant) of choice for one of the above terms and cite the source. If someone else has already taken “your” definition, please look for another one
 - Technical comment:
 gives you a line-break in the wiki
 - We will in the end have a number of definitions per term

Security is ...



Source: thesilverliningblog.com

Questions & Definitions

To be answered at home:

- How can “security” be defined?
- Please look for definitions (colloquial, technical, ...)
- There is a wiki on the learning platform: please enter one definition (per course participant) of choice and cite the source. If someone else has already taken “your” definition, please look for another one

To be answered in class:

- What are security goals (sometimes referred to as “security objectives”)? Which ones do you know?

Security Goals/Objectives

Authentication

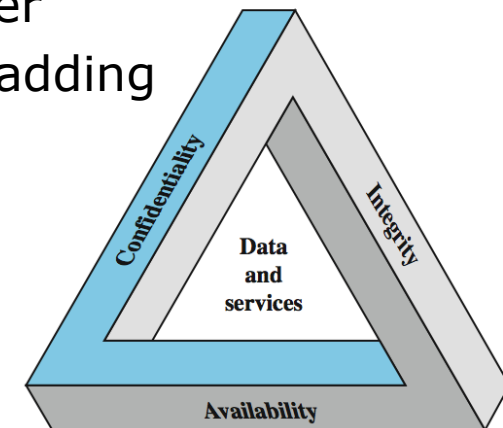
- User: Proven identity of communication partners
- → Need for means of user authentication
- Message: Information associated to communication partner
- → Need for means of message authentication

Confidentiality

- Information accessible only for sender and receiver
- → Need for cryptography, encipherment, traffic padding

Integrity

- Information not altered during transmission
- → Need for message integrity checks



Security Goals/Objectives

Non-Repudiation

- Ex post denial of communication not possible
- → Need for digital signatures, “notarization”

Availability

- Resistance against denial of service attacks
 - → Need for access control, routing control
-
- One can find (formal) definitions of these security goals in textbooks & standards
 - A good place to start looking are ISO, IETF, etc



Source: cabletrix.co.uk

OSI Security Architecture

ITU-T X.800 Security Architecture for OSI

- Defines a systematic way of defining and providing security requirements
- For us it provides a useful, yet abstract, overview of concepts we will study
- X.800 defines security services in 5 major categories

Services in X.800

- 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 Policy and Mechanisms (ISO X.800)



Pervasive security mechanisms:

- Trusted functionality
- Security labels
- Event detection
- Security audit trails
- Security recovery

Specific security mechanisms:

- Encipherment
- Digital signatures
- Access controls
- Data integrity
- Authentication exchange
- Traffic padding
- Routing control
- Notarization

Policy: a statement of what is, and is not allowed.

Mechanism: a procedure, tool, or method of enforcing a policy.

- Security mechanisms implement functions that help prevent, detect, and respond to recovery from security attacks.
- Security functions are typically made available to users as a set of security services through APIs or integrated interfaces.

Cryptography underlies many security mechanisms.

Friends & Foes

Friends ...



[Source: stumbled upon on
some tumblr.com blog]

... and Enemies

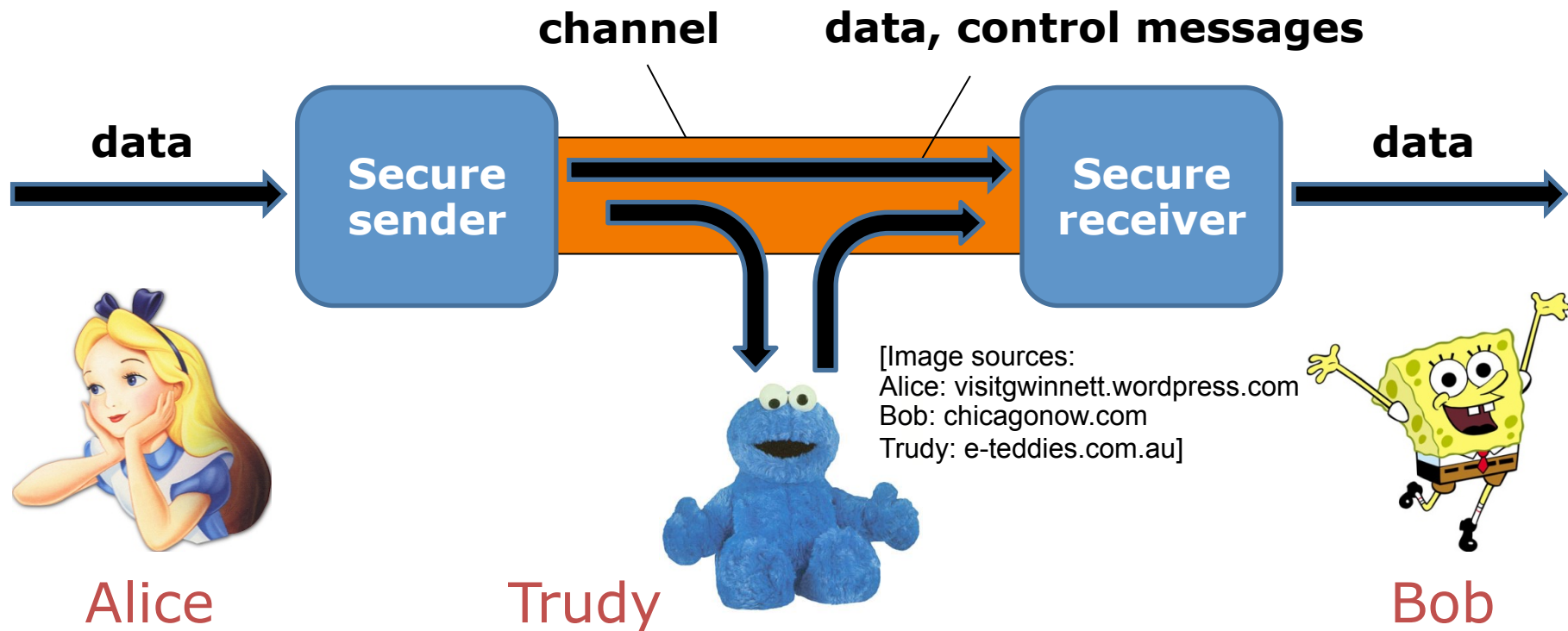


[Source: stumbled upon on some tumblr.com blog]

Meat Friends and Enemies: Alice, Bob, Trudy

The actors

- Bob, Alice (lovers!) want to communicate “securely”
- Trudy (intruder) may intercept, delete, add messages



What Bad Guys Do ...

Possible attacks on communication networks can be classified as

- Passive
- Active



- Which attacks do you know?

What Bad Guys Do ...

Possible attacks on communication networks are

- Passive
- Active

FIPS PUB 1 defines 3 levels of impact from a security breach

- Low, Moderate, High

Passive attacks

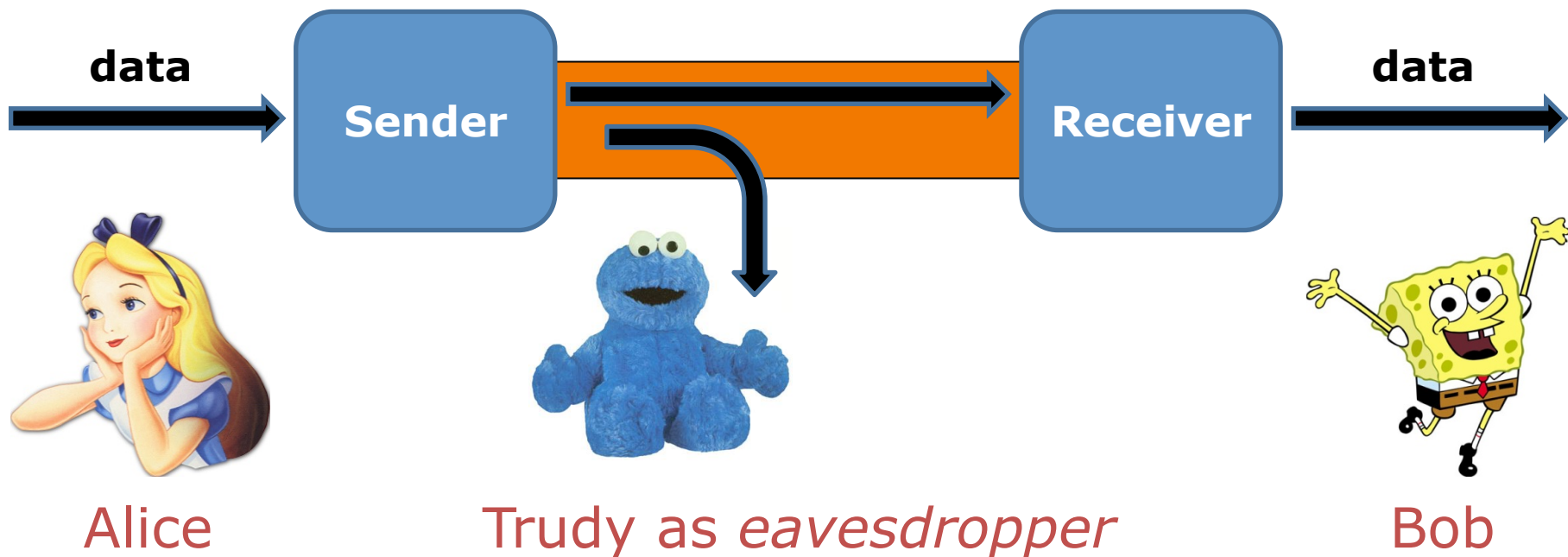
- Eavesdropping
 - Listening in communication of others
- Traffic analysis (monitor traffic flow)
 - E.g. trying to locate possible targets for further attacks



Eavesdropping Message Interception

Attack on Confidentiality

- Unauthorized access to information
- Packet sniffers and wiretappers
- Illicit copying of files and programs



What Bad Guys Do ...

Active attacks

- Changing messages of others (manipulation but also replaying)
 - E.g. manipulating the content of business e-mails
 - E.g. replaying previous messages
- Pretending to be someone else (impersonation)
 - E.g. buying something for someone's account without permission
- Denying a communication (repudiation)
 - E.g. lying about received prompt notes/signed contracts
- Disrupting someone else's services (denial of service)
 - E.g. bringing down websites
 - E.g. disconnecting others from networks

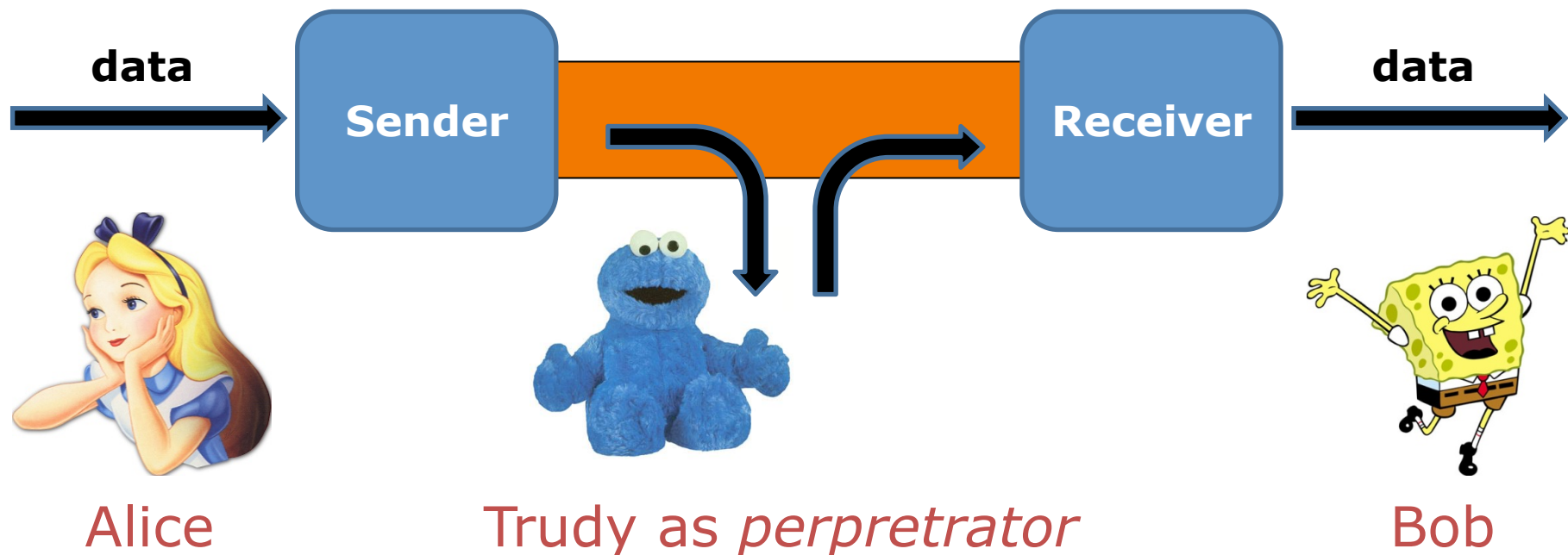


Integrity Attack

Tampering With Messages

Typically as man in the middle attack

- Stop the flow of the message
- Delay and optionally modify the message
- Release the message again



Authenticity Attack Fabrication

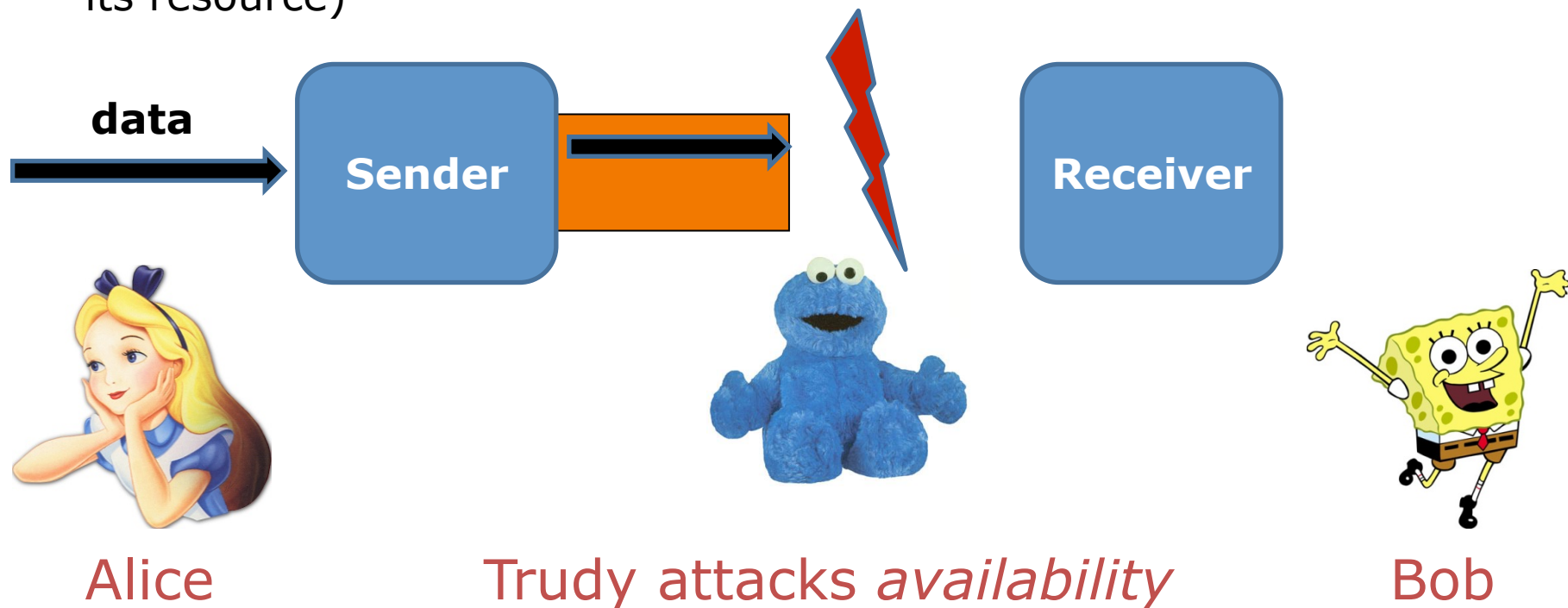
Typically as impersonation attack

- Unauthorized assumption of other's identity
- Generate and distribute objects under this identity



Attack on Availability




- Destroy hardware (cutting fiber) or software
- Modify software in a subtle way (alias commands)
- Corrupt packets in transit
- Denial of service (DoS): Crashing or overwhelming the server (use up its resource)

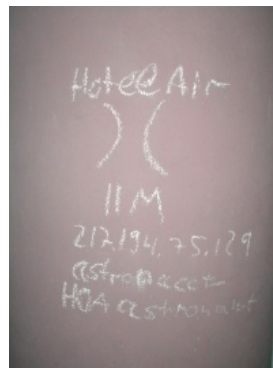


Example: Attacks on Wireless LANs

Scrounging

- Using someone else's WLANs often easily possible
 - Due to disabled security mechanisms (Factory defaults)
- Ever been or seen warchalking?

let's warchalk..!	
KEY	SYMBOL
OPEN NODE	<div>ssid</div>  <div>bandwidth</div>
CLOSED NODE	<div>ssid</div> 
WEP NODE	<div>ssid</div> <div>access contact</div>  <div>bandwidth</div>
blackbeltjones.com/warchalking	



Source: ocf.berkeley.edu

Enabling Security

Fundamental Methods Enabling Network Security



Cryptography

- Means "secret writing" (Greek origin)
- Can be categorized (for our needs) into
 - Symmetric cryptography
 - Public-key cryptography

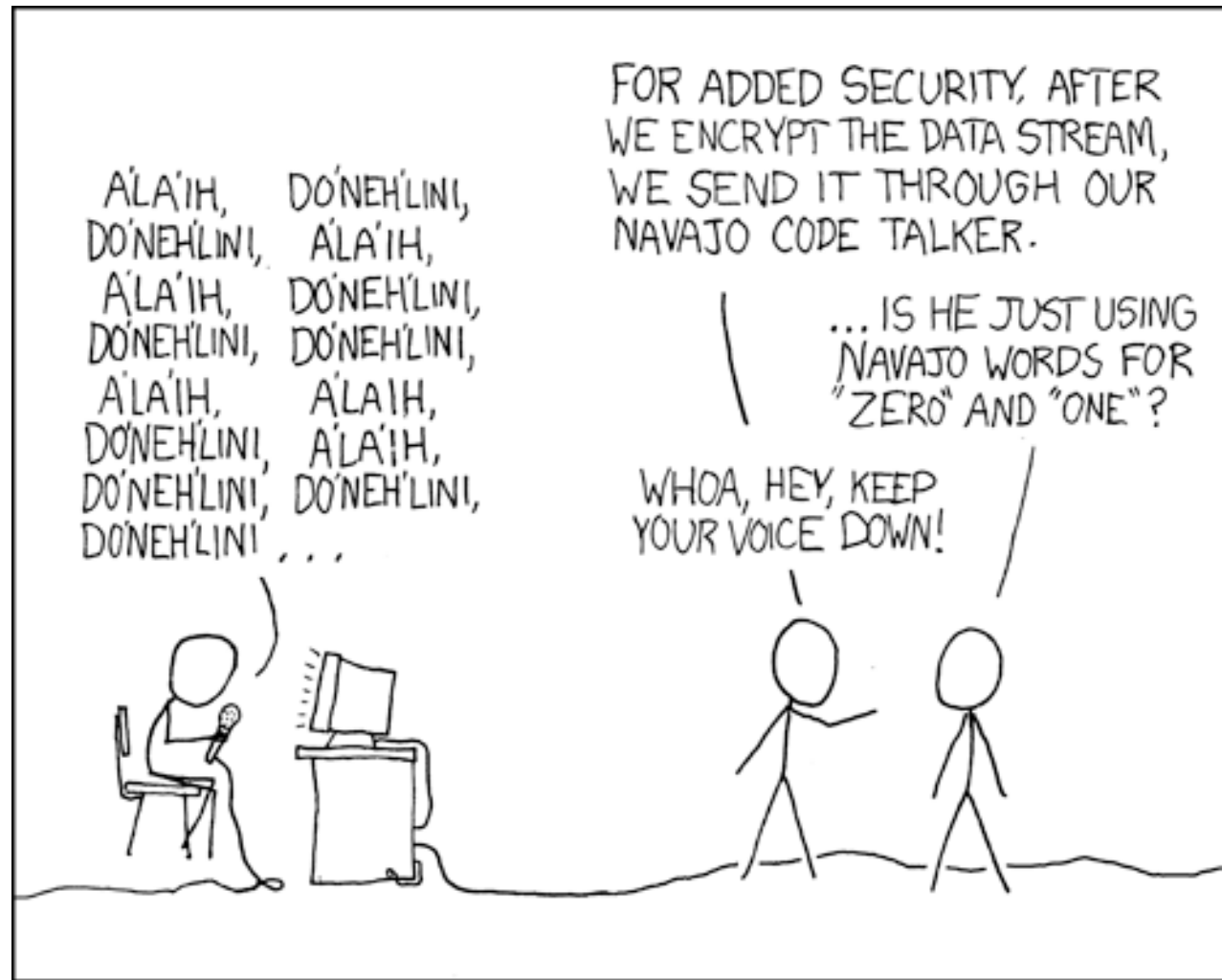
Message Authentication & Integrity

- Build the fundament for reaching security objectives of
 - Authentication, integrity, and non-repudiation

User Authentication

- Needed to verify identity of communication partner
- Fundamental for further security mechanisms
 - Confidentiality, access control, accounting, ... hard to achieve when identity of communication partner is unknown

Crypto as Cure-all?



Source: <http://xkcd.com/257/>

Security Services

Security Service

- X.800: *"a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers"*
- RFC 2828: *"a processing or communication service provided by a system to give a specific kind of protection to system resources"*
- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
 - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Summary



Forward from the Past (1981)

Computer criminals

Computers will make the world of tomorrow a much safer place. They will do away with cash, so that you need no longer fear being attacked for your money. In addition, you need not worry that your home will be burgled or your car stolen. The computers in your home and car will guard them, allowing only yourself to enter or someone with your permission.

However, there is one kind of crime which may exist in the future – computer crime. Instead of mugging people in the streets or robbing houses, tomorrow's criminal may try to steal money from banks and other organizations by using a computer. The computer criminal works from home, using his own computer to gain access to the memories of the computers used by the banks and companies. The criminal tries to interfere with the computers in order to get them to transfer money to his computer without the bank or company knowing that it has been robbed.

Computer crime like this in fact exists already. However, it is very difficult to carry out a successful robbery by computer. Many computers have secret codes to prevent anyone but their owners from operating them. As computers are used more and more, it is likely that computer crime will become increasingly difficult to carry out.



Nevertheless, a computer criminal may succeed now and then and the detectives of the future will have to be highly skilled computer operators. There will probably be police computer-fraud squads, specially trained to deal with computer crime. Here you can see a squad arriving at the home of a computer criminal and arresting him as he makes a dash for it. He is clutching a computer cassette that contains details of his computer crimes, and the police will need this as evidence to prove that he is guilty.

From *World of Tomorrow – School, Work and Play*, a book published in 1981 that envisioned what the world would look like in the future with the implementation of various technologies

Source:

<http://all-that-is-interesting.com/post/3997485945/computer-criminals-in-the-world-of-tomorrow>

Acks & Recommended Reading

Selected slides of this chapter courtesy of

- Yan Chen (northwestern.edu)
- Lawrie Brown (based on the book of William Stallings)
- André König

Bruce Schneier <http://www.schneier.com/> has an excellent blog

Recommended reading

- [KaPeSp2002] Charlie Kaufman, Radia Perlman, Mike Speciner: Network Security – Private Communication in a Public World, 2nd Edition, Prentice Hall, 2002, ISBN: 978-0-14-046019-6
- [Stallings2014] William Stallings, Network Security Essentials, 4th Edition, Prentice Hall, 2014, ISBN: 978-0-146-10805-4
- Security definitions from IETF RFC

Copyright Notice

This document has been distributed by the contributing authors as a means to ensure timely dissemination of scholarly and technical work on a non-commercial basis. Copyright and all rights therein are maintained by the authors or by other copyright holders, notwithstanding that they have offered their works here electronically.

It is understood that all persons copying this information will adhere to the terms and constraints invoked by each author's copyright. These works may not be reposted without the explicit permission of the copyright holder.

Contact



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Prof. Dr.-Ing. Matthias Hollick
Department of Computer Science

SEEMOO
Mornwegstr. 32
64293 Darmstadt/Germany
matthias.hollick@seemoo.tu-darmstadt.de

Phone +49 6151 16-70920
Fax +49 6151 16-70921
www.seemoo.tu-darmstadt.de