

## EITA25 Computer Security (Datasäkerhet)

Lectures and Course Responsibility  
Martin Hell ([martin.hell@eit.lth.se](mailto:martin.hell@eit.lth.se))

Projects  
Pegah Nikbakht Bideh ([pegah.nikbakht\\_bideh@eit.lth.se](mailto:pegah.nikbakht_bideh@eit.lth.se))

Laboratories  
Linus Karlsson ([linus.karlsson@eit.lth.se](mailto:linus.karlsson@eit.lth.se))

## Course Organisation

- ▶ Credits: 7,5 hp
- ▶ Lectures
  - 14 x 2 hours
    - See webpage/schedule for time and place
- ▶ Mandatory examination will give you grade 3
  - 2 Projects
  - 3 Labs
  - 3 online quizzes
- ▶ Optional examination for grade 4 or 5
  - Written exam
    - Friday, March 22, 14-19, MA8
- ▶ Web: <http://www.eit.lth.se/kurs/eita25>

EITA25 - Computer Security

2

## Projects and labs

- ▶ Laboratories: 2 students/computer
  - Lab 1: Windows security, week 4
  - Lab 2: Unix/Linux security, week 5
  - Lab 3: Network security, week 7
- ▶ Project 1
  - 3-4 students/group
  - Digital certificates. Set up a secure connection with SSL/TLS.
- ▶ Project 2
  - 3-4 students/group
  - Using your connection from project 1, implement a server and a client and perform a security evaluation.
- ▶ You sign up in pairs or alone, then we form groups
- ▶ Group list will be posted on webpage when we know who is active on the course

EITA25 - Computer Security

3

## Quizzes

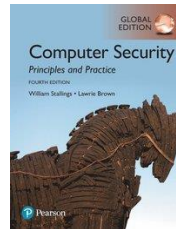
- ▶ Will be released when topics have been covered on lectures
- ▶ Open 14 days, you get one attempt per 16 hours
- ▶ You have 90 minutes to finish a quiz
- ▶ 80% needed for passing each quiz
- ▶ You may consult book, internet, slides, notes etc, but you must do it yourself

EITA25 - Computer Security

4

## Course Book

- ▶ W. Stallings and L. Brown: Computer Security, Principles and Practice, 4th edition, Pearson, 2018, ISBN: 9781292220611



- ▶ Course content is defined by
  - Book (the parts that are lectured)
  - Lectures + Lecture slides
  - Project material
  - Laboratory material

EITA25 - Computer Security

5

## Security Courses

### Basic Courses

- ▶ **Computer Security (G1)**
  - VT1
  - 7.5 credits
- ▶ **Web Security (G2)**
  - HT1
  - 4 credits

### Advanced Courses

- ▶ **Secure Systems Engineering**
  - NEW 2020
  - VT1
  - 7.5 credits
- ▶ **Advanced Computer Security (A)**
  - HT1
  - 7.5 credits
- ▶ **Advanced Web Security (A)**
  - HT2
  - 7.5 credits
- ▶ **Cryptology (A)**
  - HT2
  - 7.5 credits

EITA25 - Computer Security

6

## Content of this course

- ▶ General introduction to the very broad world of computer security
  - Basic cryptography
  - Access control
  - Operating system security
  - Network security
  - Mobile security
  - Software security

EITA25 - Computer Security

7

## About the course

### Advice from previous students

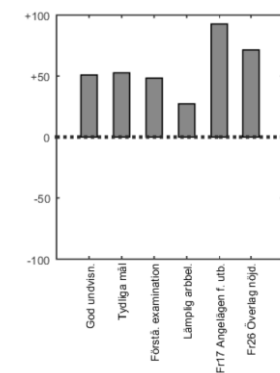
- ▶ Start doing the preparatory assignments for the second lab early
- ▶ Project 2 takes more time than project 1

### Common misconception

- ▶ There is too much programming in the course considering it is not a programming course

Do not see your education as a set of independent courses

CEQ 2018



8

## Prerequisites

- ▶ You should be comfortable with Java programming.

### Diversity among students

#### ▶ C Students

- Programmeringsteknik
- Programmeringsteknik – fördjupningskurs
- Kommunikationssystem
- Informationsöverföring
- Internetprotokoll

#### ▶ D students

- Programmeringsteknik
- Programmeringsteknik – fördjupningskurs
- Objektorienterad modellering och design
- Datorkommunikation
- Digitalteknik
- Datorteknik
- Algoritmer, datastrukturer och komplexitet

This has been taken into account. Similar for BME, E, F and I.

**You. Only. Need. To. Know. Some. Java.**

EITA25 - Computer Security

9

## Goal for this course

- ▶ Be familiar with the main concepts in computer security
  - Definitions, models, evaluation, etc...
- ▶ Have a basic understanding of means and methods that provide increased security
  - SSL, IPsec, key agreement protocols, etc...
- ▶ Have a basic understanding of security vulnerabilities
  - Attacks, implementation mistakes, etc...

- ▶ Get hands-on experience with digital certificates, secure connections, logon techniques, computer scanning, network sniffing, OpenSSL

**Laboratory and project part**

EITA25 - Computer Security

10

## Computer Security

Measures and controls that ensure **confidentiality**, **integrity**, and **availability** of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

The NIST Internal/Interagency Report NISTIR 7298  
(Glossary of Key Information Security Terms, May 2013)

- ▶ Confidentiality, Integrity, Availability - Sometimes memorized as CIA
- ▶ **Confidentiality**: prevent unauthorized disclosure of information.
- ▶ **Integrity**: prevent unauthorized modification of information.
- ▶ **Availability**: prevent disruption of access to or use of information.
- ▶ Other aspects:
  - **Authenticity**
  - **Accountability**
  - **Nonrepudiation**

EITA25 - Computer Security

11

## Confidentiality

- ▶ Prevent unauthorized disclosure of information
- ▶ Related to the *reading* of data
  - More generally – the *learning* of data
- ▶ Two aspects
  - **Data confidentiality**: protection of private and confidential information.
  - **Privacy**: Assures that individuals control or influence information related to them.
- ▶ Achieved by encryption, access control
- ▶ Confidentiality also applies to existence of data

EITA25 - Computer Security

12

## Integrity

- ▶ Prevent unauthorized modification of information.
- ▶ Related to the *writing* of data
- ▶ **Two aspects**
  - **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.
  - **System integrity:** Assures that a system performs its intended function, free from unauthorized manipulation.
- ▶ **Other definitions**
  - **ITSEC:** prevent unauthorized modification of information (prevent unauthorized writing).
  - **Clark and Wilson:** No user of the system, even if authorized, may be permitted to modify data items in such a way that assets or accounting records of the company are lost or corrupted.
  - **Orange Book:** Data Integrity - The state that exists when computerized data is the same as that in the source document and has not been exposed to accidental or malicious alteration or destruction.

EITA25 - Computer Security

13

## Integrity cont'd

- ▶ **Integrity in communications:** detection (and correction) of modifications of transmitted data, including both intentional modifications and random transmission errors.
- ▶ **In the most general sense:** make sure that everything is as it is supposed to be; the data in a computer system should correctly reflect some reality outside the computer system.
- ▶ Integrity is a prerequisite for many other security services. Operating systems security has a lot to do with integrity.
  - Circumventing confidentiality protection can be done by circumventing integrity protection
- ▶ Integrity can be achieved by CRCs, hash functions, Message Authentication Codes (MACs), Digital Signatures
  - All have different properties

EITA25 - Computer Security

14

## Availability

- ▶ Assures that systems work promptly and service is not denied to authorized users
- ▶ **CTCPEC:** The property that a product's services are accessible when needed and without undue delay.
- ▶ **ISO 7498-2:** The property of being accessible and usable upon demand by an authorized entity.
- ▶ **Denial of Service (DoS):** The prevention of authorized access of resources or the delaying of time-critical operations.
  - Send malformed network packets to crash a computer
  - Utilize all capacity of a given host
  - Registering the domain with the name of a company may affect the availability for that company.

EITA25 - Computer Security

15

## Accountability and Authentication

- ▶ We can not prevent authorized actions
- ▶ Users should be held responsible for their actions
- ▶ **Accountability (Orange Book):** audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party.
- ▶ Users are *identified* and *authenticated* to have a basis for access control decisions.
- ▶ The security system keeps an audit log (audit trail) of security relevant events to detect and investigate intrusions.
  - Access to the log must be controlled so that no one can change previous entries

EITA25 - Computer Security

16

## Nonrepudiation

- ▶ A way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
- ▶ Divided into (from common criteria)
  - **Nonrepudiation of origin:** Ensures that the originator of information cannot successfully deny having sent the information.
  - **Nonrepudiation of receipt:** Ensures that the recipient of information cannot successfully deny having received the information.
- ▶ **Example:** You should not be able to deny having signed a contract.
- ▶ Can be achieved by *digital signatures*

## Assets of Computer System

Security is about protecting assets!

**Hardware** – Computer system, storage and storage devices, communications devices

**Software** – Operating system and applications

**Data** – Files and databases

**Communication lines and networks** – LAN/WAN communication links, bridges, routers

## Vulnerabilities, Threats and Attacks

### Threats

- ▶ Threats are hypothetical events capable of exploiting vulnerabilities
  - Can create loss of confidentiality, integrity and/or availability
- ▶ Potential security harm to an asset or a resource
  - Person or event
  - Deliberate, accidental or act of nature

## Examples of Threats

	Availability	Confidentiality	Integrity
<b>Hardware</b>	Equipment is stolen or disabled, thus denying service.	An unencrypted DVD or USB device is stolen.	Hardware is modified to perform unintended tasks
<b>Software</b>	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to have it do some unintended task
<b>Data</b>	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
<b>Communication lines and networks</b>	Messages are destroyed or deleted. Communications lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

## Vulnerabilities, Threats and Attacks

### Vulnerabilities

- ▶ A vulnerability is an issue that can result in a successful attack
- ▶ Inherent weakness in the design, implementation, configuration or management of a system
- ▶ Something that allows the threat to be realized
- ▶ Categories
  - Corruption – loss of integrity
  - Leaky – loss of confidentiality
  - Unavailable or very slow – loss of availability

## Example, CVE

- ▶ Common Vulnerabilities and Exposures
- ▶ Administered by Mitre
- ▶ NIST provides a database with more information and analysis of each vulnerability
- ▶ Includes severity rating
- ▶ Database includes more than 100 000 vulnerabilities

### CVSS v3.0 Severity and Metrics:

Base Score: 6.1 MEDIUM

Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N (V3 legend)

Impact Score: 2.7

Exploitability Score: 2.8

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): Required

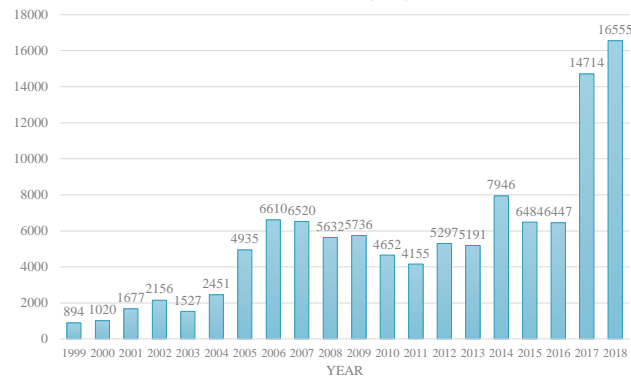
Scope (S): Changed

Confidentiality (C): Low

Integrity (I): Low

Availability (A): None

New Vulnerabilities (CVE)



## Vulnerabilities, Threats and Attacks

### Attack

- ▶ Threat that is carried out – sometimes taking advantage of a vulnerability
  - Also called *threat action*
  - Done by *attacker* or *threat agent*
- ▶ Passive vs. active attacks
  - *Passive attack* - attempt to learn or make use of information from the system without affecting system resources
  - *Active attack* - attempt to alter system resources or affect their operation
- ▶ Insider vs. outsider attacks (attack origin)
  - *Insider* - Initiated by an entity inside the security perimeter
  - *Outsider* - Initiated from outside the perimeter, by an unauthorized or illegitimate user of the system

## Example of Passive Attack (2018)

### Tinder App

**Threat to confidentiality:** Someone might read the data sent on the network in order to obtain information about users' actions



#### Vulnerability:

User profile pictures taken from unencrypted HTTP  
→ Can be eavesdropped

Swipe gestures submitted to encrypted API

#### Expected result:

An eavesdropper can see who you are viewing, but not your decision

#### Vulnerability:

- Left swipe gives 278 byte response from API
- Right swipe gives 374 byte response
- Match gives 581 byte response

#### Actual result:

An eavesdropper can see who you are viewing and your decision for that person

#### Attack:

1. Connect to same network as victim
2. Eavesdrop and analyze data

EITA25 - Computer Security

25

## Computer Security Strategy

### Three aspects

#### 1. Specification/Policy – Description of desired behavior. Considerations:

- What assets are being protected?
- System vulnerabilities.
- Potential threats and likelihood of attacks.
- Ease of use versus security.
- Cost of security versus cost of failure.

#### 2. Implementation – How to obtain the desired behavior. Divided into

- Prevention
- Detection
- Response
- Recovery

#### 3. Assurance and evaluation – How to know that it actually works. A degree of confidence. Does the design meet the requirements? Does the implementation meet the specification?

EITA25 - Computer Security

26

## Implementation

### Example – Stolen passwords (service provider perspective)

#### Prevention:

- Use up-to-date software (*perhaps obvious to most*)
- Protect the actual passwords (*We will talk about this in detail*)
- Validate all user input coming from web forms and open APIs (*Details in web security course, some aspects in this course*)

#### Detect:

- Reports from users about strange activity in their account
  - provide an easy way for users to file these reports
- Password file published on Internet
  - Scan typical places where these are published

#### Response:

- Tell all users to change password (Who will do it? How will it be done?)
- Know how to handle media, e.g., say that the attackers were extremely sophisticated and it could have happened to anyone, even though you know it's bullshit. (Who will talk to media?)

#### Recovery:

- Analyze attack and look over the prevention mechanisms (Who will do that?)

EITA25 - Computer Security

27

## This does happen

### Some examples of attacks on passwords/accounts:

- ▶ **Feb 2008** – 24 000 hashed passwords from dataföreningen
- ▶ **April 2008** – 1 000 000 accounts on Spray stolen
- ▶ **Dec 2009** – 32 million RockYou passwords published on Internet
- ▶ **Oct 2011** – 93 000 hashed passwords to blogtoppen published on Internet
- ▶ **June 2012** – 6.5 million hashed passwords from LinkedIn published on Internet
- ▶ **July 2012** – 450 000 passwords from Yahoo published on Internet
- ▶ **Oct 2013** – 150 000 000 encrypted passwords from Adobe published on Internet
- ▶ **Aug 2015** – 36 000 000 hashed passwords from Ashley Madison published on Internet
- ▶ **June 2018** – 92 300 000 hashed passwords were leaked from MyHeritage

EITA25 - Computer Security

28

## Example, cont'd

- ▶ With good **prevention** the attacks (at least some) could have been avoided
- ▶ With good **detection** the attacks could have been detected before passwords reached wide spread
- ▶ With good **response and recovery** users might stay with the provider
- ▶ Example, Spray attack April 2008. (One) **response**

*...vi håller faktiskt just nu på att byta leverantör på vårt mejlsystem så det här kommer inte att kunna hända oss igen.*

Article in Aftonbladet, April 20, 2008

- ▶ Spray was hacked again in May 2008. (One) **response**

*Hackare kommer alltid på nya sätt att attackera sidor. Det går inte att skydda sig till hundra procent.*

Article in SvD, May 30, 2008

## Assurance and Evaluation

### Who Should Evaluate?

- ▶ **Alternative 1:** One government body
  - Fair, since the same body does all evaluations
  - Not all products are accepted for evaluation
  - Slow, for the same reason
- ▶ **Alternative 2:** Private evaluators
  - More difficult to make it fair: Will evaluations be consistent?
    - **Repeatability:** re-evaluation by the same team
    - **Reproducibility:** re-evaluation by a different team
  - Formulation of criteria is important so there is no room for interpretation
  - More evaluators → faster evaluation

## Functionality vs. Assurance

- ▶ Functionality is evaluated – Assurance is the result
- ▶ Two contrasting approaches

### Orange Book (TCSEC)

- U.S. Department of defense 1983
- Primarily for operating systems
- Evaluation service offered for free (sometimes with long delays)
- Evaluation performed by government body

Evaluation level **combined** functionality and degree of assurance

**Only recognized in the U.S.**

### ITSEC

- European initiative 1990
- EU recommendation 1995
- Suitable for both systems and products (TOE)
- Fee for evaluation
- National bodies issued certificates and controlled and approved evaluators

Evaluation level **only based on assurance** – functionality completely flexible

**Only recognized in Europe**

## Common Initiative – Common Criteria

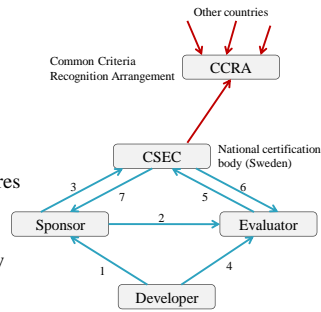
- ▶ A common standard is more commercially attractive
- ▶ Common Criteria initiated in 1998 (ISO 15408)
- ▶ Similar to ITSEC in that it separates functionality and assurance
- ▶ Uses **protection profiles (PP)** to identify and collect security requirements relevant to certain areas, e.g., operating systems, databases, firewalls, smart cards, etc
- ▶ **Evaluation Assurance Level (EAL)** is used to define the degree of confidence
  - EAL1 – EAL7
- ▶ CC evaluation required by some public sector customers

### Criticism

- ▶ Expensive (sometimes 10% - 40% of development cost)
- ▶ Time delay
- ▶ Only applies to one version and one configuration
  - "Assurance continuity" allows minor changes

## CC – Evaluation and Certification

1. Evaluation Agreement. Developer not needed for EAL1.
2. Evaluation order – produce a certification application together
3. Certification order – application is sent
4. Send documentation, source code etc.
5. Evaluation report – Evaluator follows procedures given in Common Criteria in the evaluation process
6. Report is approved after an independent review of the report
7. Send certificate and a certificate report



EITA25 - Computer Security

33

## Some Problems in Computer Security

- ▶ Some secret information has to be stored somewhere
  - Keys, passwords, etc...
- ▶ The designer has to eliminate ALL weaknesses – an attacker only needs to find ONE weakness
- ▶ Security solutions might be very different even between products that seem similar. New solutions means new potential weaknesses.
- ▶ A system is only as secure as its weakest link
- ▶ Even if the system, product, computer, protocol etc, is completely secure, there are humans using them.
- ▶ Some people tend to design their own security without proper knowledge.

EITA25 - Computer Security

34