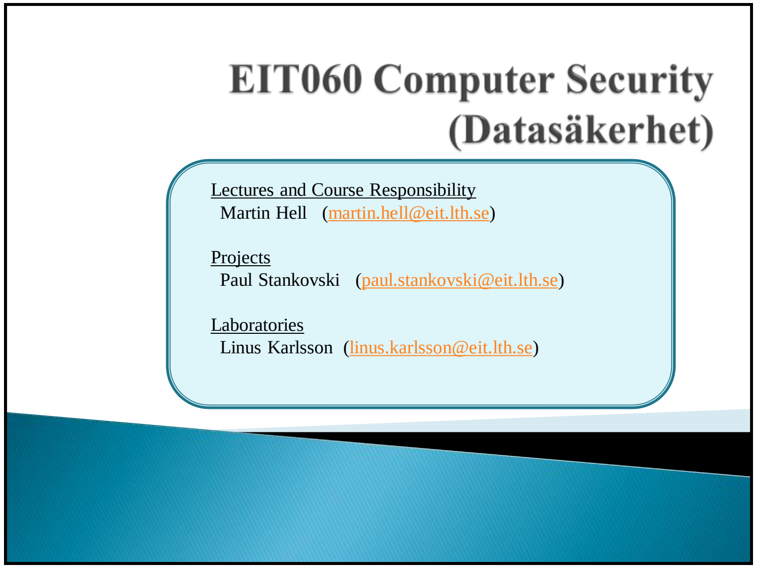
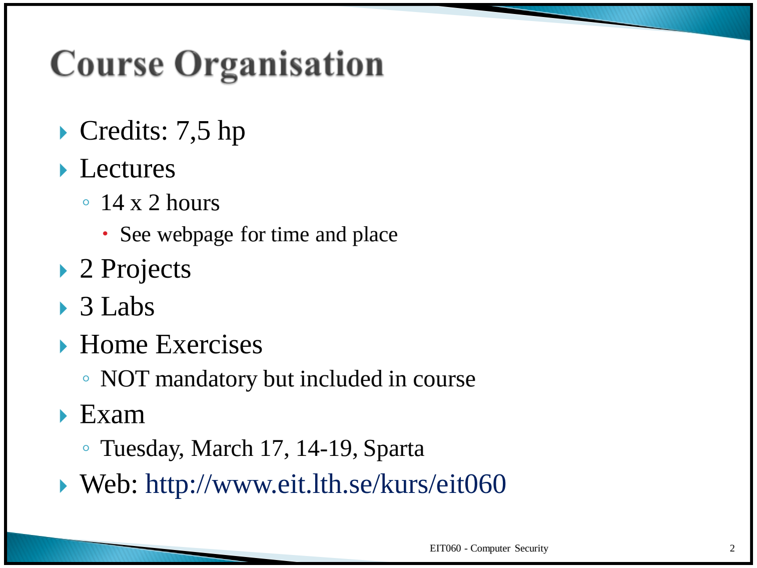


EIT060 Computer Security (Datasäkerhet)

Lectures and Course Responsibility
Martin Hell (martin.hell@eit.lth.se)

Projects
Paul Stankovski (paul.stankovski@eit.lth.se)

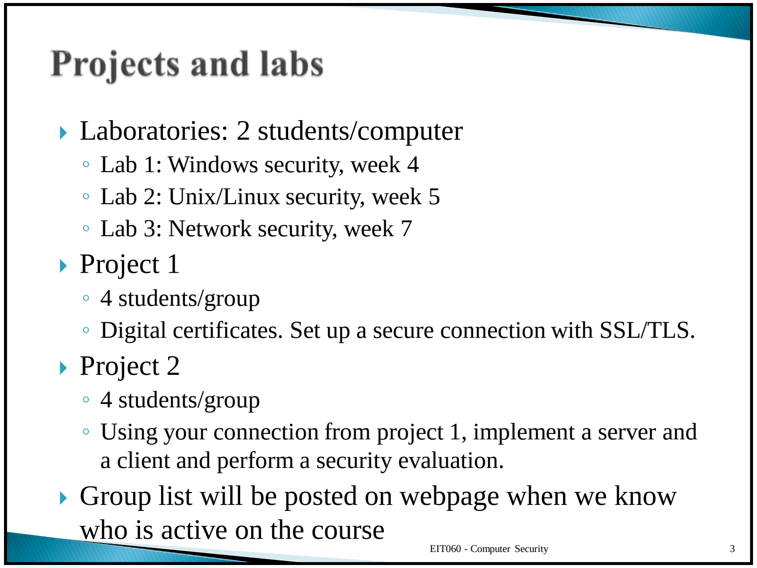
Laboratories
Linus Karlsson (linus.karlsson@eit.lth.se)



Course Organisation

- Credits: 7,5 hp
- Lectures
  - 14 x 2 hours
    - See webpage for time and place
- 2 Projects
- 3 Labs
- Home Exercises
  - NOT mandatory but included in course
- Exam
  - Tuesday, March 17, 14-19, Sparta
- Web: http://www.eit.lth.se/kurs/eit060

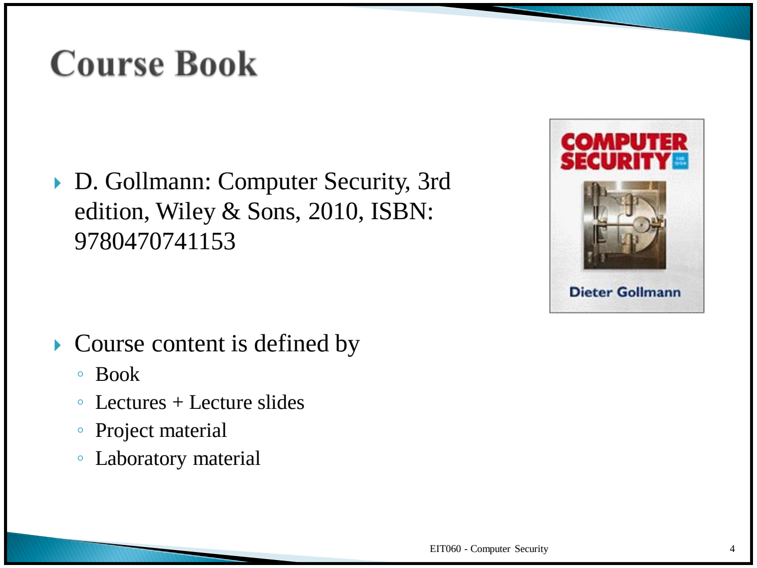
EIT060 - Computer Security 2



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
  - 4 students/group
  - Digital certificates. Set up a secure connection with SSL/TLS.
- Project 2
  - 4 students/group
  - Using your connection from project 1, implement a server and a client and perform a security evaluation.
- Group list will be posted on webpage when we know who is active on the course

EIT060 - Computer Security 3



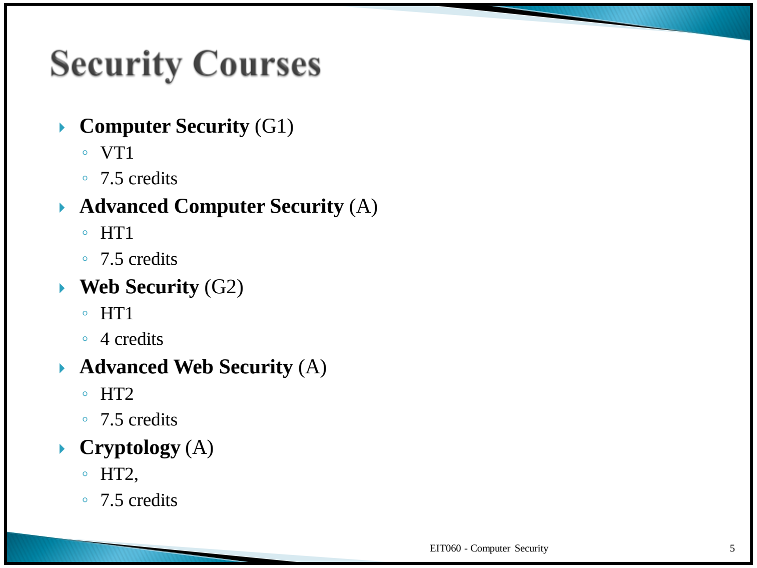
Course Book

- D. Gollmann: Computer Security, 3rd edition, Wiley & Sons, 2010, ISBN: 9780470741153

COMPUTER SECURITY
Dieter Gollmann

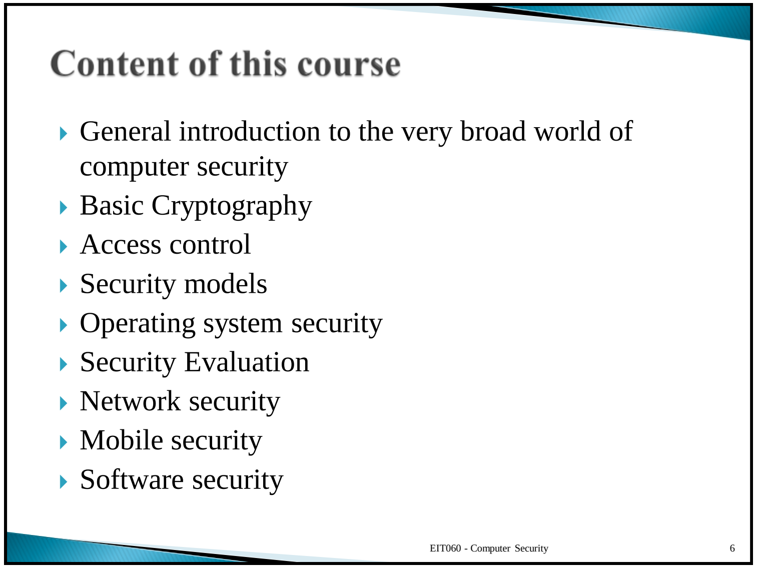
- Course content is defined by
  - Book
  - Lectures + Lecture slides
  - Project material
  - Laboratory material

EIT060 - Computer Security 4



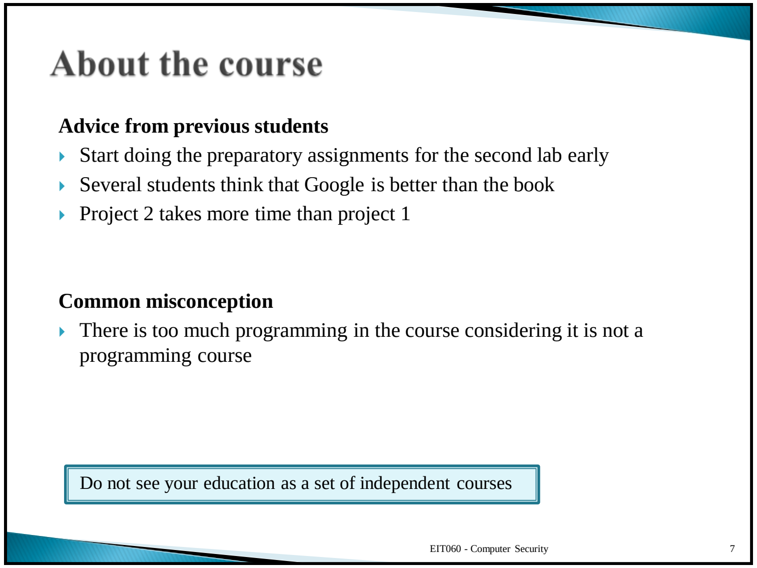
Security Courses

- **Computer Security** (G1)
  - VT1
  - 7.5 credits
- **Advanced Computer Security** (A)
  - HT1
  - 7.5 credits
- **Web Security** (G2)
  - HT1
  - 4 credits
- **Advanced Web Security** (A)
  - HT2
  - 7.5 credits
- **Cryptology** (A)
  - HT2,
  - 7.5 credits



Content of this course

- General introduction to the very broad world of computer security
- Basic Cryptography
- Access control
- Security models
- Operating system security
- Security Evaluation
- Network security
- Mobile security
- Software security



About the course

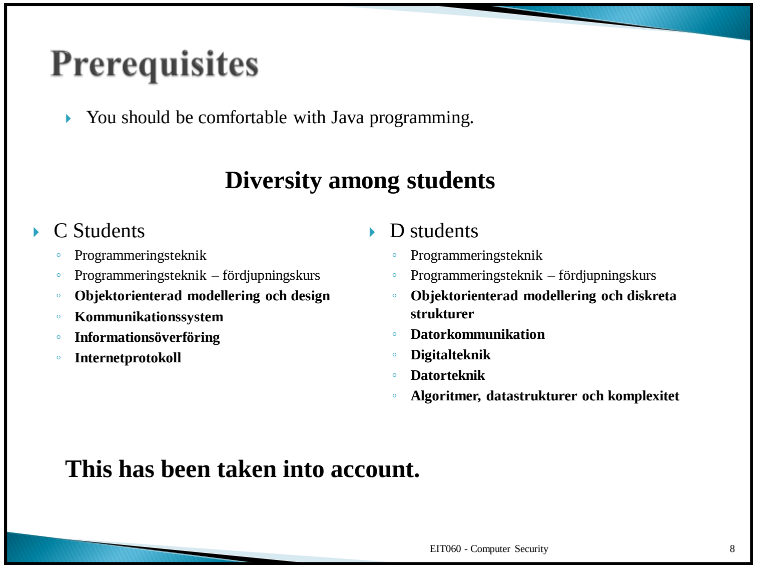
Advice from previous students

- Start doing the preparatory assignments for the second lab early
- Several students think that Google is better than the book
- 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



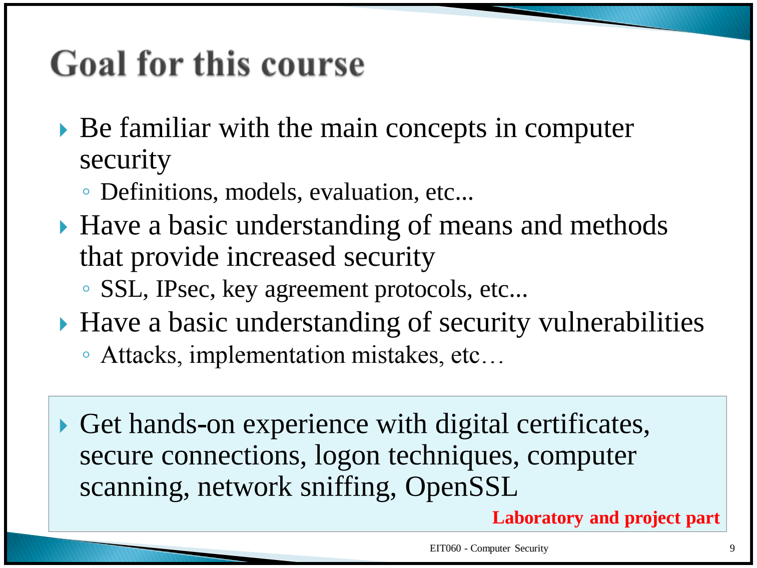
Prerequisites

- You should be comfortable with Java programming.

Diversity among students

- C Students
  - Programmeringsteknik
  - Programmeringsteknik – fördjupningskurs
  - **Objektorienterad modellering och design**
  - **Kommunikationssystem**
  - **Informationsöverföring**
  - **Internetprotokoll**
- D students
  - Programmeringsteknik
  - Programmeringsteknik – fördjupningskurs
  - **Objektorienterad modellering och diskreta strukturer**
  - **Datorkommunikation**
  - **Digitalteknik**
  - **Datorteknik**
  - **Algoritmer, datastrukturer och komplexitet**

This has been taken into account.

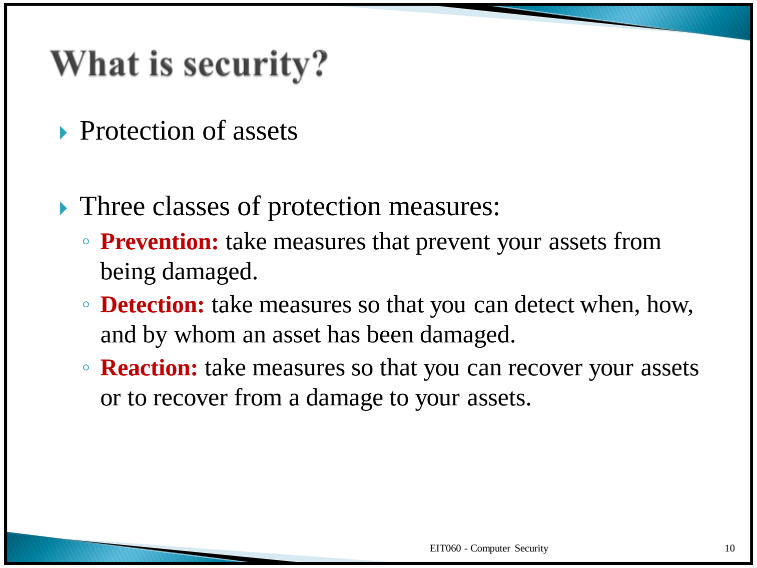


Goal for this course

- 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

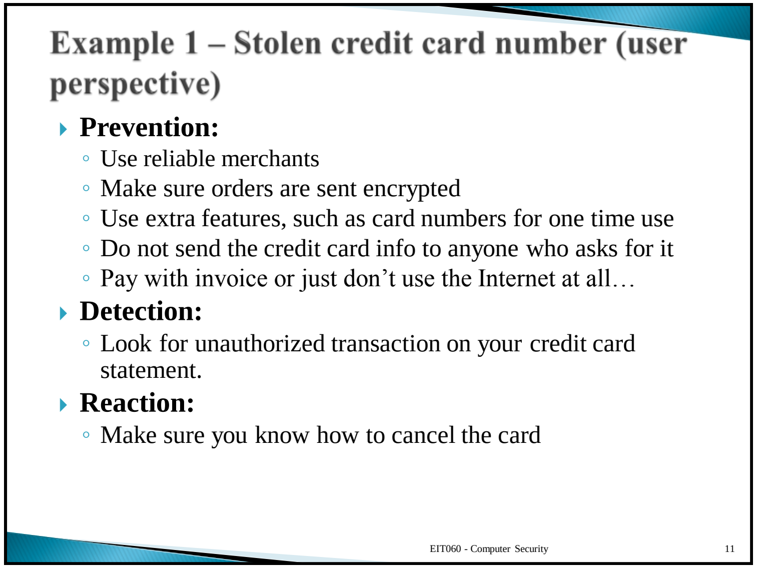
Laboratory and project part



What is security?

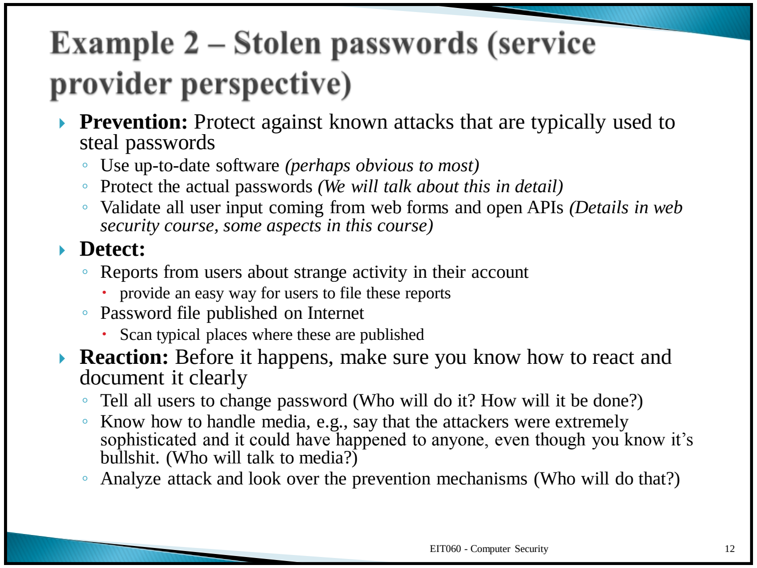
- Protection of assets

- Three classes of protection measures:
  - **Prevention:** take measures that prevent your assets from being damaged.
  - **Detection:** take measures so that you can detect when, how, and by whom an asset has been damaged.
  - **Reaction:** take measures so that you can recover your assets or to recover from a damage to your assets.



Example 1 – Stolen credit card number (user perspective)

- **Prevention:**
  - Use reliable merchants
  - Make sure orders are sent encrypted
  - Use extra features, such as card numbers for one time use
  - Do not send the credit card info to anyone who asks for it
  - Pay with invoice or just don't use the Internet at all…
- **Detection:**
  - Look for unauthorized transaction on your credit card statement.
- **Reaction:**
  - Make sure you know how to cancel the card



Example 2 – Stolen passwords (service provider perspective)

- **Prevention:** Protect against known attacks that are typically used to steal passwords
  - 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
- **Reaction:** Before it happens, make sure you know how to react and document it clearly
  - 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?)
  - Analyze attack and look over the prevention mechanisms (Who will do that?)

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 bloggtoppen 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

Security measures

- 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 **reaction** users will stay with the provider
- Example, Spray attack April 2008. (One) **reaction**

> *...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) **reaction**

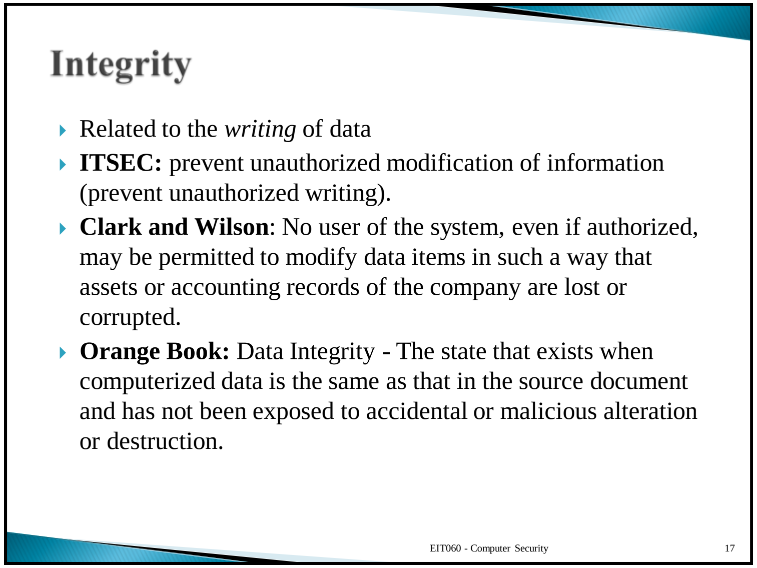
> *Hackare kommer alltid på nya sätt att attackera sidor. Det går inte att skydda sig till hundra procent.*
>
> Article in SvD, May 30, 2008

Aspects of Computer Security

- Confidentiality, Integrity, Availability
  - Sometimes memorized as CIA
- Definitions given in Gollman:
  - **Confidentiality:** prevent unauthorized disclosure of information.
  - **Integrity:** prevent unauthorized modification of information.
  - **Availability:** prevent unauthorized with-holding of information or resources .
  - **Other aspects:**
    - **Accountability**
    - **Authentication**
    - **Nonrepudiation**

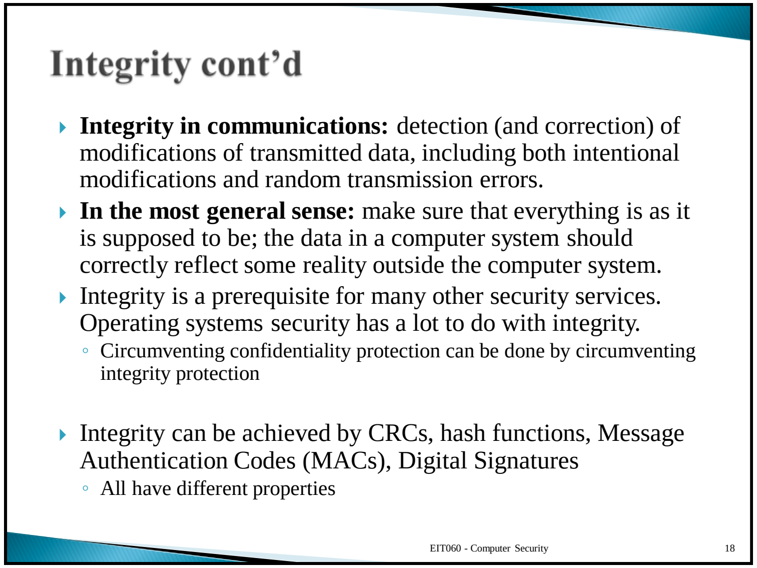
Confidentiality

- Prevent unauthorized disclosure of information
- Related to the *reading* of data
  - More generally – the *learning* of data
- Two aspects
  - **Privacy:** protection of personal data.
  - **Secrecy:** protection of data belonging to an organization.
- Achieved by encryption, access control
- Confidentiality also applies to existence of data



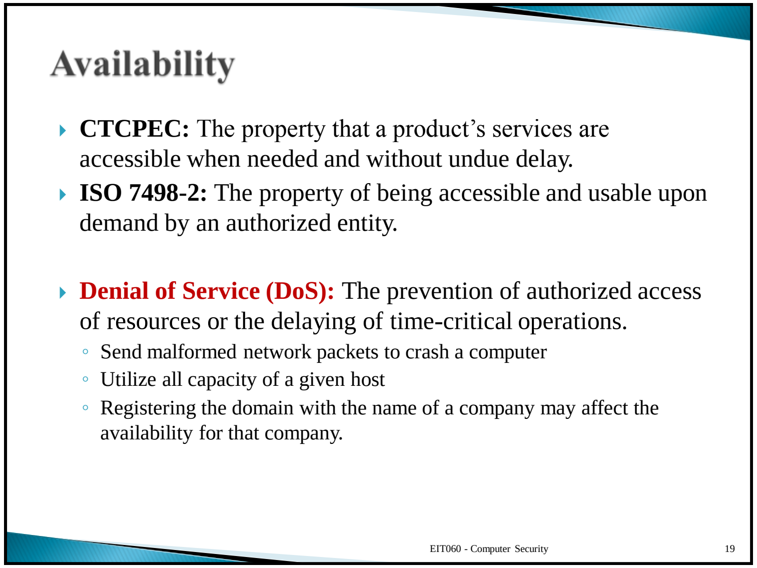
Integrity

- Related to the *writing* of data
- **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.



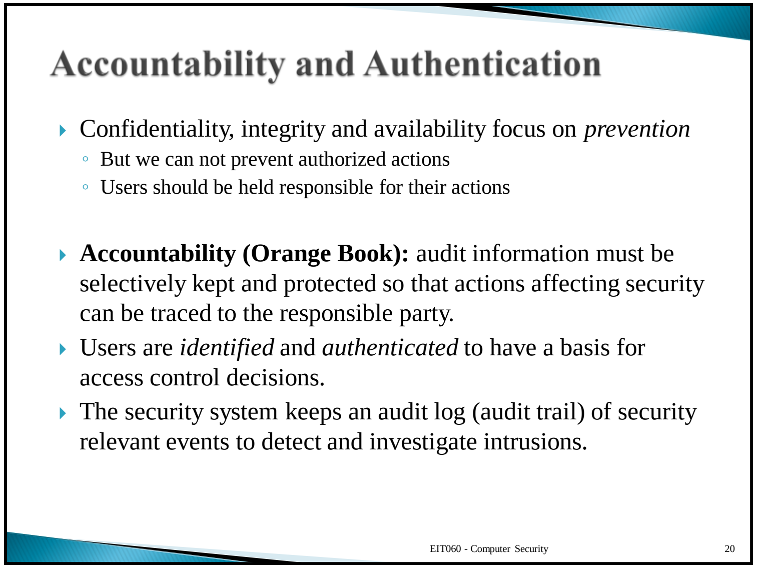
Integrity cont'd

- **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



Availability

- **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.



Accountability and Authentication

- Confidentiality, integrity and availability focus on *prevention*
  - But 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.

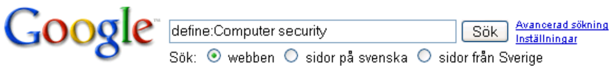
Nonrepudiation

- 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*

Definitions of Computer Security

- Deals with the prevention and detection of unauthorized actions by users of a computer system
- Concerned with the measures we can take to deal with intentional actions by parties behaving in some unwelcome fashion

- Security is the prevention of, or protection against, access to information by unauthorized recipients, and intentional but unauthorized destruction or alteration of that information – *Dictionary of Computing*



define:Computer security

Sök: ● webben ○ sidor på svenska ○ sidor från Sverige

- Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.
  https://ia.gordon.army.mil/iaso/lesson01.htm
- Technological and managerial procedures applied to computer systems to ensure the availability, integrity and confidentiality of information managed by the computer system.
  www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html
- The protection of a computer system and its data from harm. This is normally interpreted as being protection against losses of confidentiality, integrity and availability. Some security professionals also consider non-repudiation to be an integral component of computer security. ...
  www.nemesys.com/Content/Core/Glossary.php
- Methods or systems to prevent any event or action that could cause a loss of or damage to computer hardware, software, data and information
  en.wikibooks.org/wiki/SA_NCS_Computer_Application_Technology:Glossary
- Computer security is an application of Information Security to both theoretical and actual computer systems. For simplicity, issues of privacy and just causes to collect information should be handled under the subject of Information Privacy Rights. ...
  en.wikipedia.org/wiki/Computer security

The Main Conclusions

- There is no single definition of computer security.

- When reading a document, be careful not to confuse your *own* notion of security with that used in the document.

- A lot of time is being spent - and wasted - trying to define an unambiguous notation for security.

Five Fundamental Design Decisions

1. Where is the focus of security controls?
2. Where to place security controls ?
3. Complexity vs. Assurance.
4. Centralized or decentralized controls?
5. Blocking access to the layer below.

1. Where is the focus of security controls?

We can focus on

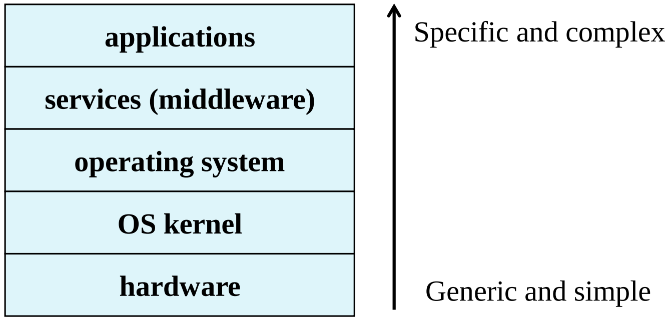
- Data
- Operations
- Users

How do we define the rules to follow?

Example: Integrity check – we control changes to data

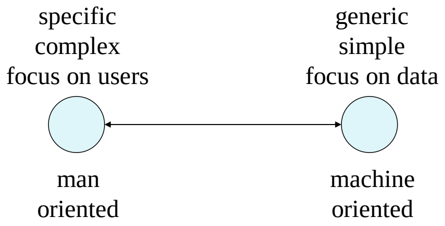
- **Data:** What is the format of the data? ”*This data can only be an integer*”
- **Operations:** What operations can be done on the data? ”*This data must be incrementred by 1 every 5 minutes*”
- **Users:** Who can write to the data? ”*Only Alice is allowed to make changes to the data*”

2. Where to place security controls?



The Man-Machine Scale

- Combining our first two design decisions, we refer to a *man-machine scale* for security mechanisms.



Data vs Information

- *Data* are physical phenomena
- The meanings we assign to data are called *information*.
- Data is used to transmit and store information and to derive new information by manipulating the data according to formal rules.
- Information and data correspond to the two ends of the man-machine scale.
- **Example:** Facebook (May 2013)
  - 4.75 billion pieces of content per day
  - 4.5 billion likes per day
  - 300 million photos per day

  } **Data**
- This data is processed…
- ...Facebook knows alot about you ← **Information**

Data vs Information cont'd

- Controlling access to *information* can be difficult and may have to be replaced by controlling access to *data*

Examples where this can be a problem

- *Covert channels*: response time or memory usage is used to signal information.
- *Inference in statistical databases*: combinations of statistical queries give information on individual entries.

3. Complexity vs Assurance

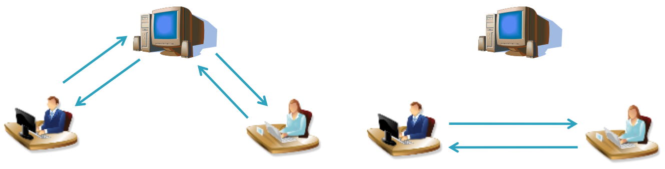
- There is a tradeoff between **complexity** and **assurance**
- **Evaluate a product:** High assurance means detailed and thorough examination → You want to keep it simple

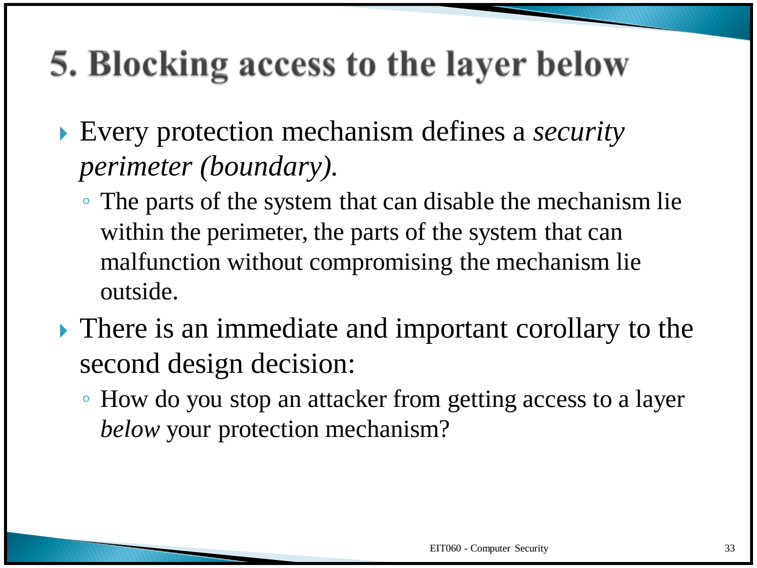
What do you want?

- *High assurance:* Simple mechanisms that are often generic
- *Lower assurance:* Complex, feature-rich and specific mechanisms

4. Centralised or Decentralised controls?

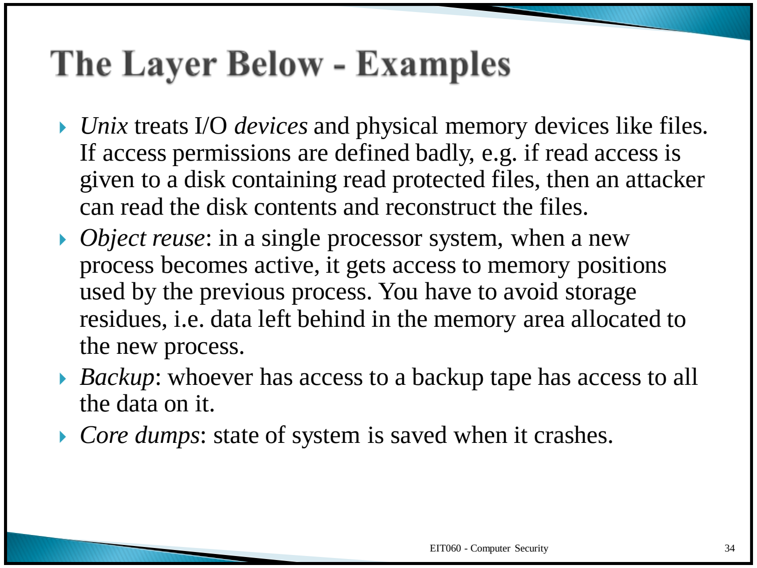
- If a single entity is in charge of security, then it is easy to achieve uniformity but this central entity may become a performance bottleneck. A distributed solution may be more efficient but you have to take added care to guarantee that different components enforce a consistent policy.
- Example: Encrypted communication





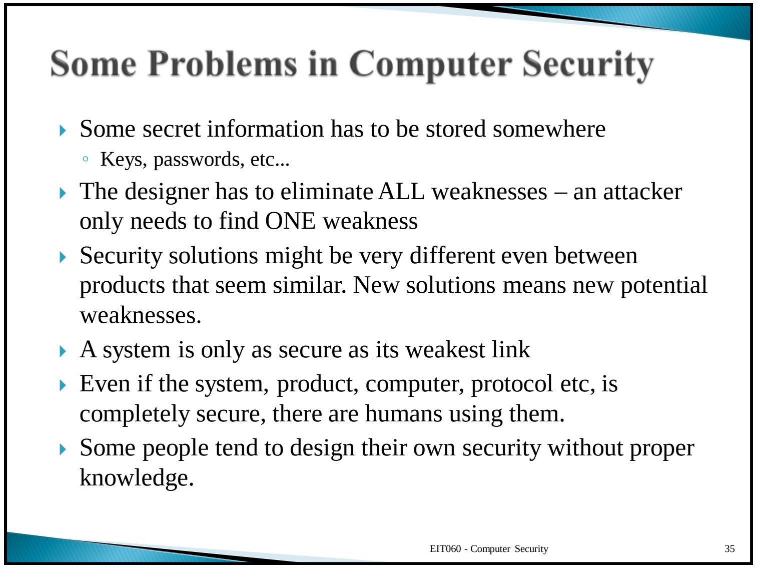
5. Blocking access to the layer below

- Every protection mechanism defines a *security perimeter (boundary).*
  - The parts of the system that can disable the mechanism lie within the perimeter, the parts of the system that can malfunction without compromising the mechanism lie outside.
- There is an immediate and important corollary to the second design decision:
  - How do you stop an attacker from getting access to a layer *below* your protection mechanism?



The Layer Below - Examples

- *Unix* treats I/O *devices* and physical memory devices like files. If access permissions are defined badly, e.g. if read access is given to a disk containing read protected files, then an attacker can read the disk contents and reconstruct the files.
- *Object reuse*: in a single processor system, when a new process becomes active, it gets access to memory positions used by the previous process. You have to avoid storage residues, i.e. data left behind in the memory area allocated to the new process.
- *Backup*: whoever has access to a backup tape has access to all the data on it.
- *Core dumps*: state of system is saved when it crashes.



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.