

# INF3510 Information Security

---

## Lecture 01:

- Course info
- Basic concepts in information security



University of Oslo, spring 2018

# Course information

- Course organization
- Prerequisites
- Syllabus and text book
- Lecture plan
- Home exam
- Assessment and exams
- Security education
- *AFSecurity*

# Course organisation

- Course activities
  - Attend 2 hours lectures per week
    - Lecture notes available at least one day prior to lecture
  - Work on the workshop questions
    - Will be discussed during the following week's workshop which follows immediately after the 2-hour lecture
  - Work on the home exam
    - Topic for the assignment can be freely chosen.
- Not just about facts, you also need to
  - understand concepts
  - apply those concepts
  - think about implications
  - understand limitations

# Course Resources

- Learning material is available at:
  - <http://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/>
  - lecture presentations, workshop questions, etc.
  - List of English security terms translated to Norwegian
- Assignment topic for home exam on:
  - <https://wiki.uio.no/mn/ifi/INF3510-2018>
- Various online resources
  - E.g. NIST special computer security publications  
<http://csrc.nist.gov/publications/PubsSPs.html>

# Lecturer



- Prof. Audun Jøsang,
- Education
  - CISSP 2005, CISM 2010,
  - PhD Information Security, NTNU, 1998
  - MSc Information Security, Royal Holloway College, London, 1993
  - BSc Telematics, NTH 1987
  - Baccaalaureat, Lycée Corneille, France, 1981
- Work
  - Professor, UiO, 2008 →
  - Associate Professor, QUT, Australia, 2005-2007
  - Research Leader, DSTC, Australia 2000-2004
  - Associate Professor, NTNU, 1998-1999
  - System design engineer, Alcatel, Belgium 1988-1992

# Prerequisites

- Prerequisites
  - Basic computer and network technology
  - Basic mathematics
- Theoretic focus on a basic level
  - Discrete mathematics, number theory, modular arithmetic
  - Information theory
  - Probability calculus
  - Computer and network architecture

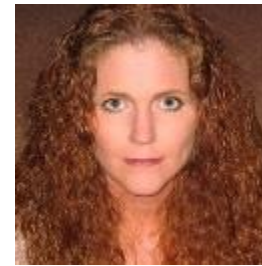
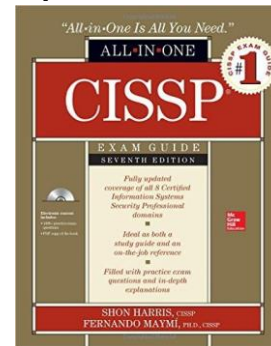
# Syllabus and text book

- The syllabus for this course consists of the material presented during the lectures, as described in the lecture notes.
- Adequate comprehension of the material requires that you also
  - read parts of the text book and other documents
  - work out answers to the workshop questions
  - follow the lectures.

- Text book:

CISSP All-in-One Exam Guide  
7<sup>th</sup> Edition, 2016

Authors: Shon Harris (†) and  
Fernando Maymí



Shon Harris



Fernando Maymí

- The book covers the 8 CBK domains (Common Body of Knowledge) for the CISSP Exam (Certified Information Systems Security Professional).
- Easy to order book from amazon.com, price approx: US\$ 55  
<https://www.amazon.com/CISSP-All-One-Guide-Seventh/dp/0071849270>

# How to use Harris & Maymí's CISSP book (7th ed.)

- 1340 pages in total
  - But exclude
    - 50 pages of appendix, glossary and index
    - 300 pages of tips, Q&A
    - Parts of chapters
  - Around 700 pages of readable material
  - The book is very easy to read 😊
  - Sometimes long explanations and examples ☹️
- Each chapter has **Main Sections** (big font) and **Subsections** (small font), but no numbering
  - The lack of numbering of subsections can be confusing



| <b>Week</b> | <b>Date</b>         | <b>#</b>                                      | <b>Topic</b>                                     |
|-------------|---------------------|-----------------------------------------------|--------------------------------------------------|
| W04         | 22.01.2018          | 1                                             | Course Information. Basic Concepts in IS         |
| W05         | 29.01.2018          | 2                                             | IS Management, Human Factors for IS              |
| W06         | 05.02.2018          | 3                                             | Cryptography                                     |
| W07         | 12.02.2018          | 4                                             | Key Management and PKI                           |
| W08         | 19.02.2018          | 5                                             | Risk Management and Business Continuity Planning |
| W09         | 26.02.2018          | 6                                             | Computer Security                                |
| W10         | 05.03.2018          | 7                                             | Incident Response and Digital Forensics          |
| W11         | 12.03.2018          | 8                                             | User Authentication                              |
| W12         | 19.03.2018          | 9                                             | Identity Management and Access Control           |
| W13         | <i>Easter break</i> |                                               |                                                  |
| W14         | <i>Easter break</i> |                                               |                                                  |
| W15         | 09.04.2018          | 10                                            | Network Communication Security                   |
| W16         | 16.04.2018          | 11                                            | Network Perimeter Security                       |
| W17         | 23.04.2018          | 12                                            | System Development and Application Security      |
| W18         | <i>No lecture</i>   |                                               |                                                  |
| W19         | <i>No lecture</i>   |                                               |                                                  |
| W20         | 22.05.2018          |                                               | Review                                           |
| W21         | <i>No lecture</i>   |                                               |                                                  |
| W22         | 01.06.2018          | Digital exam, time: 09:00h - 13:00h (4 hours) |                                                  |

# Home Exam

- Write an essay on a security topic chosen by you
- Individual, or in group of 2 or 3 students
- Select topic and specify group on wiki  
<https://wiki.uio.no/mn/ifi/INF3510-2018/>
- Length: 5000 - 10000 words (approx. 10 – 15 pages)
- Due date: 07.05.2018
- Assessment criteria:
  - Structure and presentation: weight  $\frac{1}{4}$
  - Scope and depth of content: weight  $\frac{1}{4}$
  - Evidence of independent research and analysis: weight  $\frac{1}{4}$
  - Proper use of references: weight  $\frac{1}{4}$

# Assessment and Marking

- Course weight: 10 study points
- Assessment items:
  - Home exam: weight 0.4
  - Digital exam: weight 0.6
- Required to get a pass score on both assessment items
  - At least 40% on home exam and 40% on written exam
  - Relatively easy to get a high score on home exam
  - Relatively difficult to get a high score on written exam
- Academic dishonesty (including plagiarism and cheating) is actively discouraged
  - See: <https://www.uio.no/english/studies/admin/examinations/cheating/>
  - Should be no problem 😊

# Exam statistics from previous years

| Year | # students | # A (%)                                                                        | # B (%)  | # C (%)  | # D (%)    | # E (%)   | # F (%)    |
|------|------------|--------------------------------------------------------------------------------|----------|----------|------------|-----------|------------|
| 2017 | 138        | 9 (6%)                                                                         | 47 (34%) | 66 (49%) | 4 (3%)     | 3 (2%)    | 9 (6%)     |
| 2016 | 147        | 6 (4%)                                                                         | 39 (37%) | 59 (40%) | 9 (6%)     | 10 (7%)   | 24 (16%)   |
| 2015 | 121        | 10 (9%)                                                                        | 30 (25%) | 45 (37%) | 9 (7%)     | 9 (7%)    | 18 (15%)   |
| 2014 | 103        | 4 (4%)                                                                         | 8 (7.5%) | 45 (44%) | 14 (13.5%) | 9 (4.5%)  | 23 (22.5%) |
| 2013 | 0          | For the 2013 spring semester the course was cancelled due to faculty politics. |          |          |            |           |            |
| 2012 | 34         | 2 (6%)                                                                         | 6 (18%)  | 14 (41%) | 0 (0.0%)   | 6 (17.5%) | 6 (17.5%)  |
| 2011 | 70         | 1 (2%)                                                                         | 10 (14%) | 33 (47%) | 9 (13%)    | 10 (14%)  | 7 (10%)    |

# Other security courses at IFI

- IN4XXX: Ethical Hacking
  - Laszlo Erdödi (autumn)
- IN5XXX: Security by Design
  - Lillian Røstad (spring)
- UNIK4220: Introduction to Cryptography
  - Leif Nilsen (autumn, taught at IFI)
- UNIK4250: Security in Distributed Systems
  - Nils Nordbotten (spring)
- UNIK4270: Security in OS and Software
  - Audun Jøsang (Autumn, taught at IFI)
- UNIK4740: InfoSec in Industrial Sensor and Mobile Systems
  - Judith Rossebø (autumn)
- INF5150 - Unassailable IT-systems
  - Ketil Stølen (autumn)
- ITLED4230 Ledelse av informasjonssikkerhet
  - Audun Jøsang (autumn) (for professionals, fee NOK 25K)

# Why study information security ?

- Being an IT expert requires knowledge about IT security
  - Analogy: Building architects must have knowledge about fire safety
- Developing IT systems without considering security will lead to vulnerable IT systems
- IT experts without security skills are part of the problem
- Learn about IT security to become part of the solution !
- Security by Design is a prerequisite for privacy by design which is a legal requirement for processing personal data
- Information security is a political issue
  - Often seen as a cost, but saves costs in the long term
  - Often given low priority in IT industry and IT education

# Certifications for IS Professionals

- Many different types of certifications available
  - vendor neutral or vendor specific
  - from non-profit organisations or commercial for-profit organisations
- Certification gives assurance of knowledge and skills,
  - needed in job functions
  - gives credibility for consultants, applying for jobs, for promotion
- Sometimes required
  - US Government IT Security jobs
- Knowledge domains reflect current topics in IT Security
  - Generally kept up-to-date

# ISACA Certifications

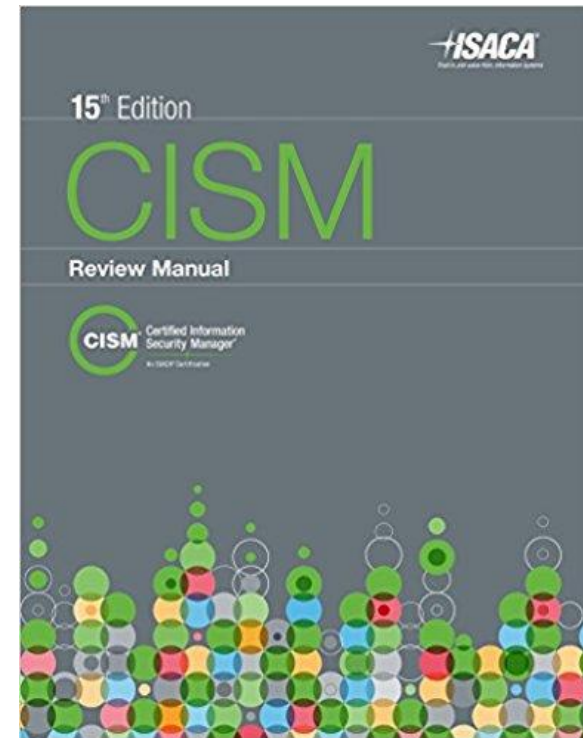
(Information Systems Audit and Control Association)

- ISACA provides certification for IT professionals
  - CISM - Certified Information Security Manager
  - CISA - Certified Information System Auditor
  - CGIT - Certified in the Governance of Enterprise IT
  - CRSIC - Certified in Risk and Information Systems Control
- CISM is the most popular ISACA security certification
- IT auditors and consultants commonly have ISACA certifications
- ISACA promotes IT governance framework COBIT  
(Control Objectives for Information and Related Technologies)



# CISM: Certified Information Security Manager

- Focuses on 4 domains of IS management
  1. Information Security Governance
  2. Information Risk Management
  3. Information Security Program Development and Management
  4. Information Security Incident Management
- Official prep manual published by ISACA
  - <https://www.isaca.org/bookstore/>
  - Price: US \$115 (\$85 for ISACA members)



# CISM Exam

- Exams normally twice per year worldwide
- Next exam in Oslo (and worldwide): June 2018
  - Deadline for registering: April 2018
  - Register for exam at [www.isaca.org](http://www.isaca.org)
  - Exam fee approx. US \$500
  - Multiple choice exam
  - Requires 5 years professional experience
  
  - Yearly CISM maintenance fee approx. US \$100
  - Requires 120 hours “practice time” per 3 years

# (ISC)<sup>2</sup> Certifications

## International Information Systems Security Certification Consortium

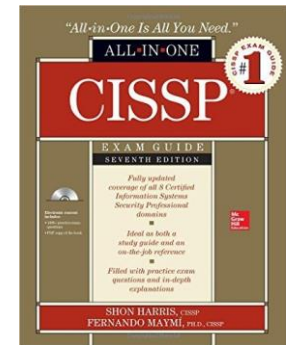
- (ISC)<sup>2</sup> provides certification for information security professionals
  - CISSP - Certified Information Systems Security Professional
  - ISSAP - Information Systems Security Architecture Professional
  - ISSMP - Information Systems Security Management Professional
  - ISSEP - Information Systems Security Engineering Professional
  - CAP - Certification and Accreditation Professional
  - SSCP - Systems Security Certified Practitioner
  - CSSLP - Certified Secure Software Lifecycle Professional
- CISSP is the most common IT security certification
  - Most IT Security Consultants are CISSP

# CISSP Exam: Certified Information System Security Professional

- Many different books to prepare for CISSP exam
- e.g. text book used for INF3510 course

CISSP All-in-One Exam Guide  
7<sup>th</sup> Edition, 2016

Author: Shon Harris and Fernando Maymí



- € 560 fee to sit CISSP exam
- Exam through <http://www.pearsonvue.com/isc2/>
- Test Centre in Oslo: <http://www.glasspaper.no/>  
Brynsveien 12, Bryn, Oslo
- Most of the of the material presented in the INF3510 course is taken from the syllabus of the CISSP CBK (Common Body of Knowledge).

# CISSP CBK (Common Body of Knowledge)

## 8 domains

- 1. Security and Risk Management** (Security, Risk, Compliance, Law, Regulations, and Business Continuity)
- 2. Asset Security** (Protecting Security of Assets)
- 3. Security Engineering** (Engineering and Management of Security)
- 4. Communication and Network Security** (Designing and Protecting Network Security)
- 5. Identity and Access Management** (Controlling Access and Managing Identity)
- 6. Security Assessment and Testing** (Designing, Performing, and Analyzing Security Testing)
- 7. Security Operations** (Foundational Concepts, Investigations, Incident Management, and Disaster Recovery)
- 8. Software Development Security** (Understanding, Applying, and Enforcing Software Security)

# Security Surveys

Useful for knowing the trend and current state of information security threats and attacks

- Verizon Data Breach Report:  
<http://www.verizonenterprise.com/DBIR/>
- PWC security survey:  
<http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html>
- Mnemonic Security Report  
<https://www.mnemonic.no/security-report/>
- Mørketallsundersøkelsen;  
<http://www.nsr-org.no/moerketall/>
  - New report in December every 2 years (even years).

+ many others

# Security Advisories

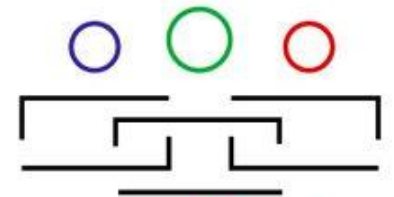
- Useful for managing threats and vulnerabilities
    - NorCERT: For government sector: <https://www.nsm.stat.no/>
    - NorSIS: For private sector: <http://www.norsis.no/>
    - FinansCERT: <http://www.finanscert.no/>
    - KraftCERT: <https://www.kraftcert.no/>
    - HelseCERT:  
<https://www.nhn.no/tema/sikkerhet/HelseCERT/Sider/default.aspx>
    - UNINETT-CERT: <https://www.uninett.no/cert>
    - UiO-CERT: <http://www.uio.no/english/services/it/security/cert/>
    - US CERT: <http://www.cert.org/>
    - Australia AusCERT: <http://www.auscert.org.au/>
- + many others

# Academic Forum on Security

- Monthly seminar on information security
- <https://wiki.uio.no/mn/ifi/AFSecurity/>
- Guest expert speakers
  
- Next AF *Security* seminar:
  - **Topic:** *History of Cryptology in Norway*
  - **Speaker:** *Sondre Rønjom, NSM*
  - **Time:** January 2018
  - **Place:** Kristen Nygaards sal, 5<sup>th</sup> floor, OJD
  
- All interested are welcome !
  
- Organised by SecurityLab



UiO • University of Oslo



SecurityLab



# Information Security

## Basic Concepts

---

# Good and bad translation

## English

- Security
- Safety
- Certainty



- Security
- Safety
- Certainty



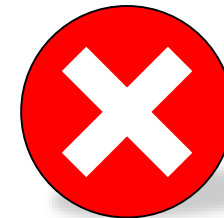
## Norwegian

- Sikkerhet
- Trygghet
- Visshet

- Sikkerhet



*Good*



*Bad*

# What is security in general

- Security is about protecting assets from damage or harm
- Focuses on all types of assets
  - Example: your body, possessions, the environment, the nation
- Security and related concepts
  - National security (political stability)
  - Safety (health)
  - Environmental security (clean environment)
  - Information security
  - etc.

# What is Information Security

- *Information* Security focuses on protecting *information assets* from damage or harm
- What are the assets to be protected?
  - Example: data files, software, IT equipment and infrastructure
- Covers both intentional and accidental events
  - Threat agents can be people or acts of nature
  - People can cause harm by accident or by intent
- Information Security defined:
  - The preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved. (ISO27000 Information Security Management Systems - Overview and Vocabulary)

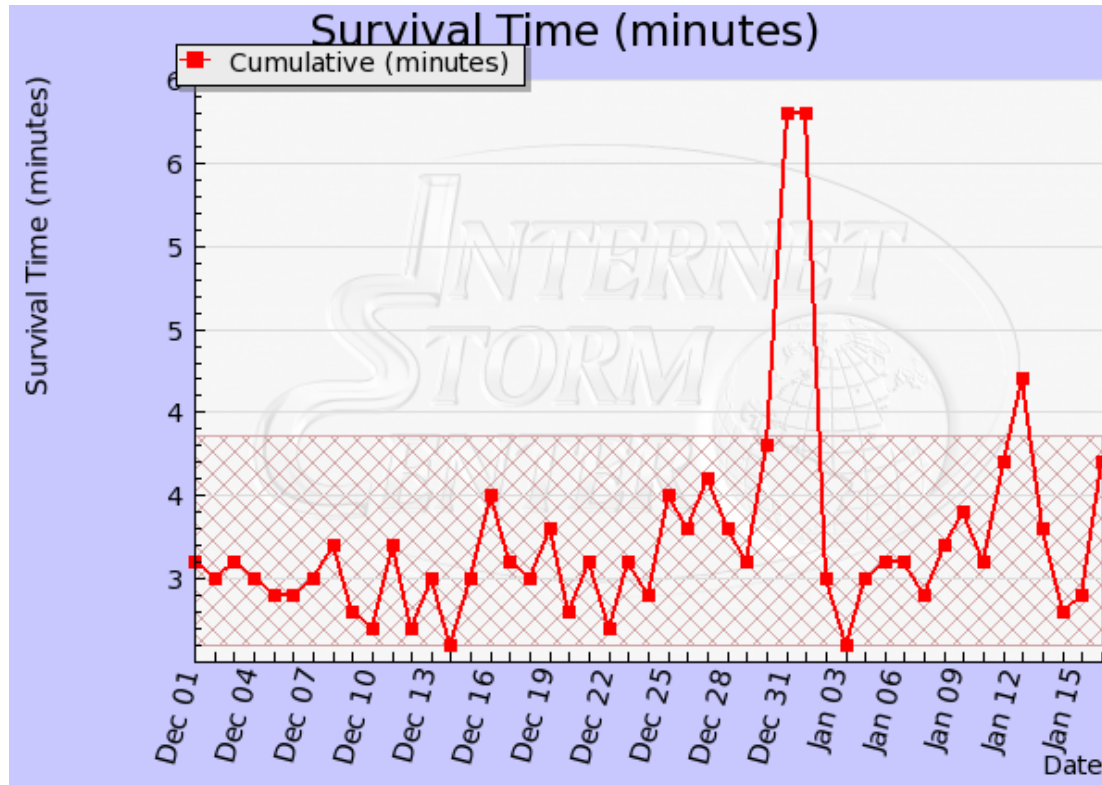
# Scope of information security

- IS management has as goal to avoid damage and to control risk of damage to information assets
- IS management focuses on:
  - Understanding threats and vulnerabilities
  - Managing threats by reducing vulnerabilities or threat exposures
  - Detection of attacks and recovery from attacks
  - Investigate and collect evidence about incidents (forensics)

# The Need for Information Security

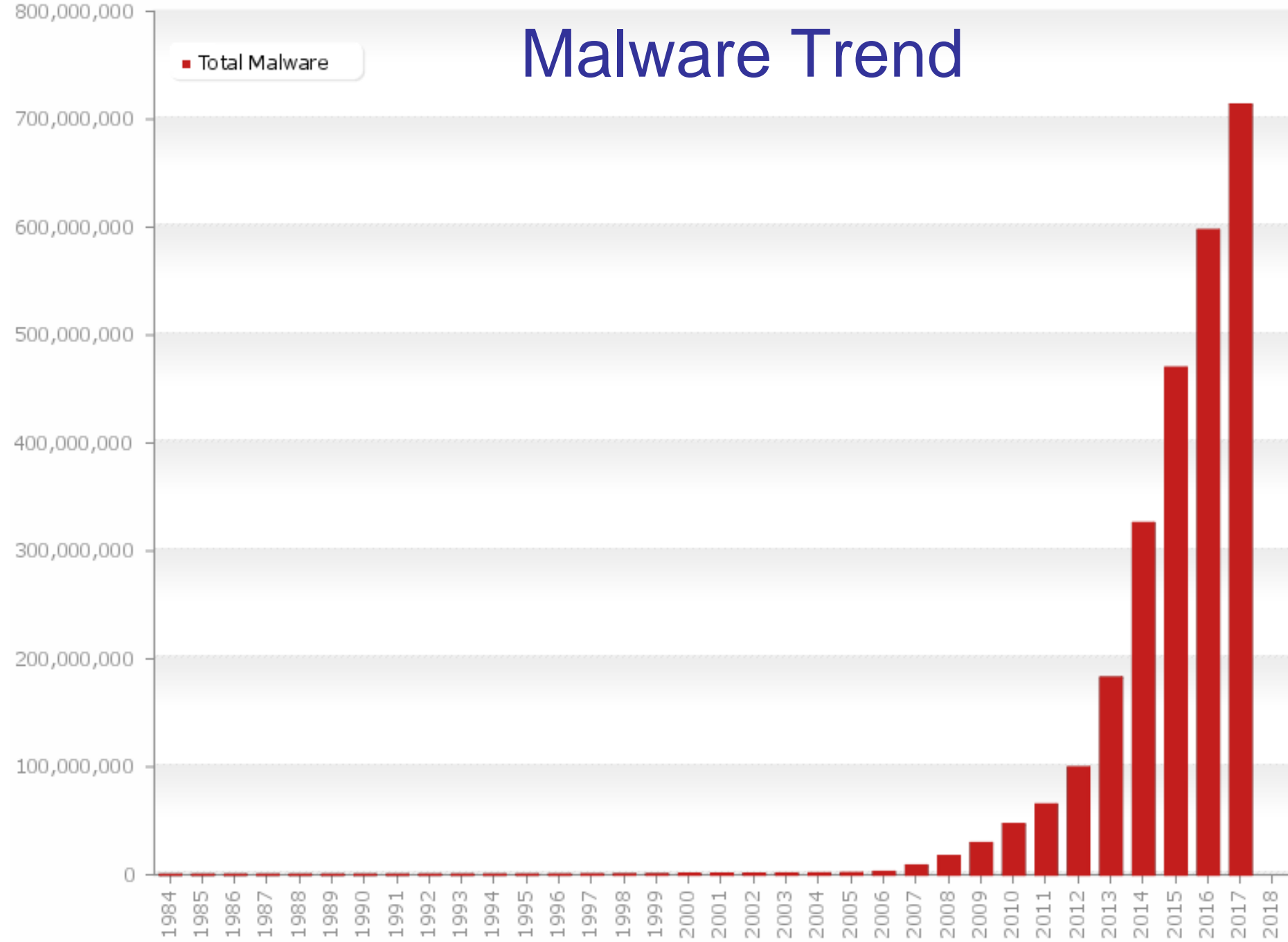
- Why not simply solve all security problems once for all?
- Reasons why that's impossible:
  - Rapid innovation constantly generates new technology with new vulnerabilities
  - More activities go online
  - Crime follows the money
  - Information security is a second thought when developing IT
  - New and changing threats
  - More effective and efficient attack technique and tools are being developed
- Conclusion: Information security doesn't have a final goal, it's a continuing process

# Internet Storm Survival Time Measure



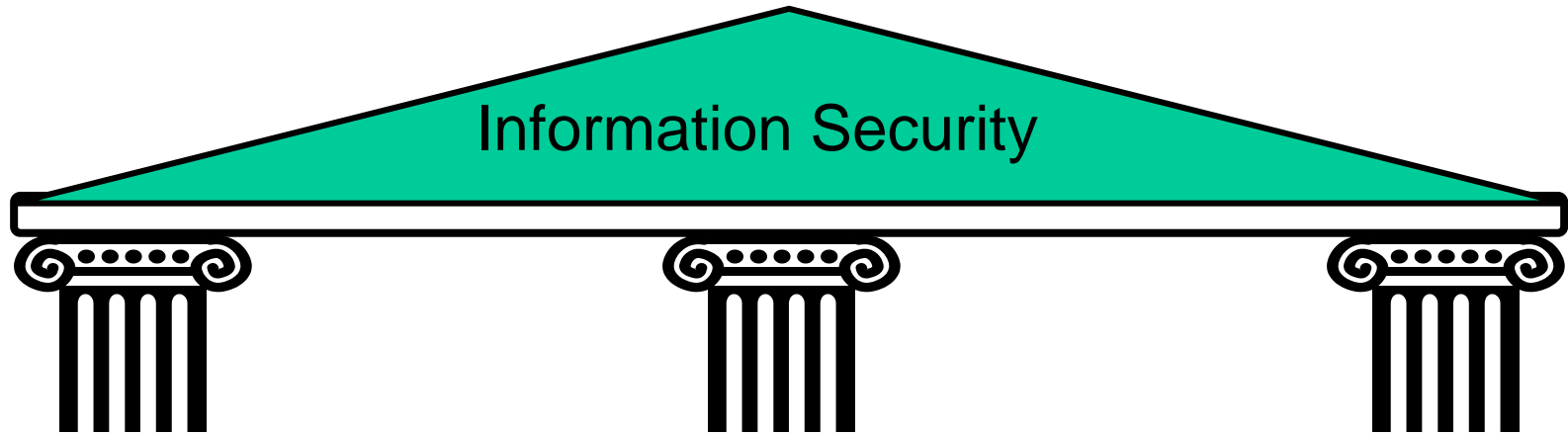
The survival time is calculated as the average time between attacks against average target IP address.  
<http://isc.sans.org/survivaltime.html>

# Malware Trend





# Security control categories



## **Physical controls**

- Facility protection
- Security guards
- Locks
- Monitoring
- Environmental controls
- Intrusion detection

## **Technical controls**

- Logical access control
- Cryptographic controls
- Security devices
- User authentication
- Intrusion detection
- Forensics

## **Administrative controls**

- Policies & standards
- Procedures & practice
- Personnel screening
- Awareness training
- Secure System Dev.
- Incident Response

# Security control functional types

- **Preventive** controls:
  - prevent attempts to exploit vulnerabilities
    - Example: encryption of files
- **Detective** controls:
  - warn of attempts to exploit vulnerabilities
    - Example: Intrusion detection systems (IDS)
- **Corrective** controls:
  - correct errors or irregularities that have been detected.
    - Example: Restoring all applications from the last known good image to bring a corrupted system back online
- Use a combination of controls to help ensure that the organisational processes, people, and technology operate within prescribed bounds.



# Controls by Information States

- Information security involves protecting information assets from harm or damage.
- Information is considered in one of three possible states:

- During storage

- Information storage containers
- Electronic, physical, human



- During transmission

- Physical or electronic



- During processing (use)

- Physical or electronic

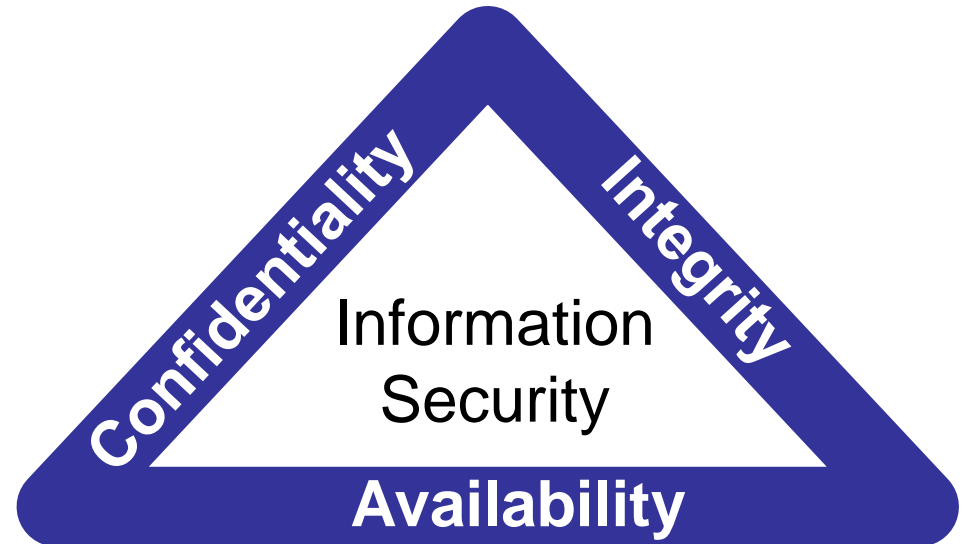


- Security controls for all information states are needed

# Security Services and Properties

- A security service provides a high level security property
- The traditional definition of information security is to preserve the three CIA properties for data and services:

- **C**onfidentiality:
- **I**ntegrity
- **A**vailability:



- CIA are the three main security properties/services
- Data privacy is an additional property which assumes CIA

**Data Privacy**

# Security services and controls

- Security services (aka. goals or properties)
  - implementation independent
  - supported by specific controls
- Security controls (aka. mechanisms)
  - Practical mechanisms, actions, tools or procedures that are used to provide security services



## Security services:

e.g. Confidentiality – Integrity – Availability

support

## Security controls:

e.g. Encryption – Firewalls – Awareness



# Confidentiality

- The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (ISO 27000)
- Can be divided into:
  - Secrecy: Protecting business data
  - Privacy: Protecting personal data
  - Anonymity: Hide who is engaging in what actions
- Main threat: Information theft, unintentional disclosure
- Controls: *Encryption, Access Control, Perimeter defence*  
As general controls, also include:  
*Secure Systems Development, Incident Response*

# Integrity

- **Data Integrity:** The property that data has not been altered or destroyed in an unauthorized manner.  
(X.800: Security Architecture for OSI)
- **System Integrity:** The property of accuracy and completeness (ISO 27000).  
Can include the accountability of actions.
- Threats: Data and system corruption, loss of accountability
- Controls:
  - *Hashing, cryptographic integrity check and encryption*
  - *Authentication, access control and logging*
  - *Software digital signing*
  - *Configuration management and change control (system integrity)*

As general controls, also include:

*Secure System Development, Incident Response*

# Availability

- The property of being accessible and usable upon demand by an authorized entity. (ISO 27000)
- Main threat: Denial of Service (DoS)
  - The prevention of authorized access to resources or the delaying of time critical operations
- Controls:
  - *Redundancy of resources,*
  - *Load balancing,*
  - *Software and data backups*

As general controls, also include:

*Secure System Development and Incident Response*





# Data Privacy



To protect specific aspects of information that may be related to natural persons (personal information).

- Prevent unauthorized collection and storage of personal information
- Prevent unauthorized use of collected personal information
- Make sure your personal information is correct
- Ensure transparency and access for data subjects
- Provide adequate information security (CIA) around personal information
- Define clear responsibilities around personal information
- GDPR becomes EU law on 25 May 2018  
(General Data Protection Regulation)



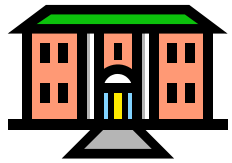
# Authenticity (Security Service)

The CIA properties are quite general security services. Other security services are often mentioned. Authentication is very important, with various types:



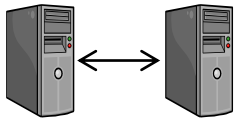
- **User authentication:**

- The process of verifying a claimed identity of a (legal) user when accessing a system or an application.



- **Organisation authentication:**

- The process of verifying a claimed identity of a (legal) organisation in an online interaction/session



- **System authentication (peer entity authentication):**

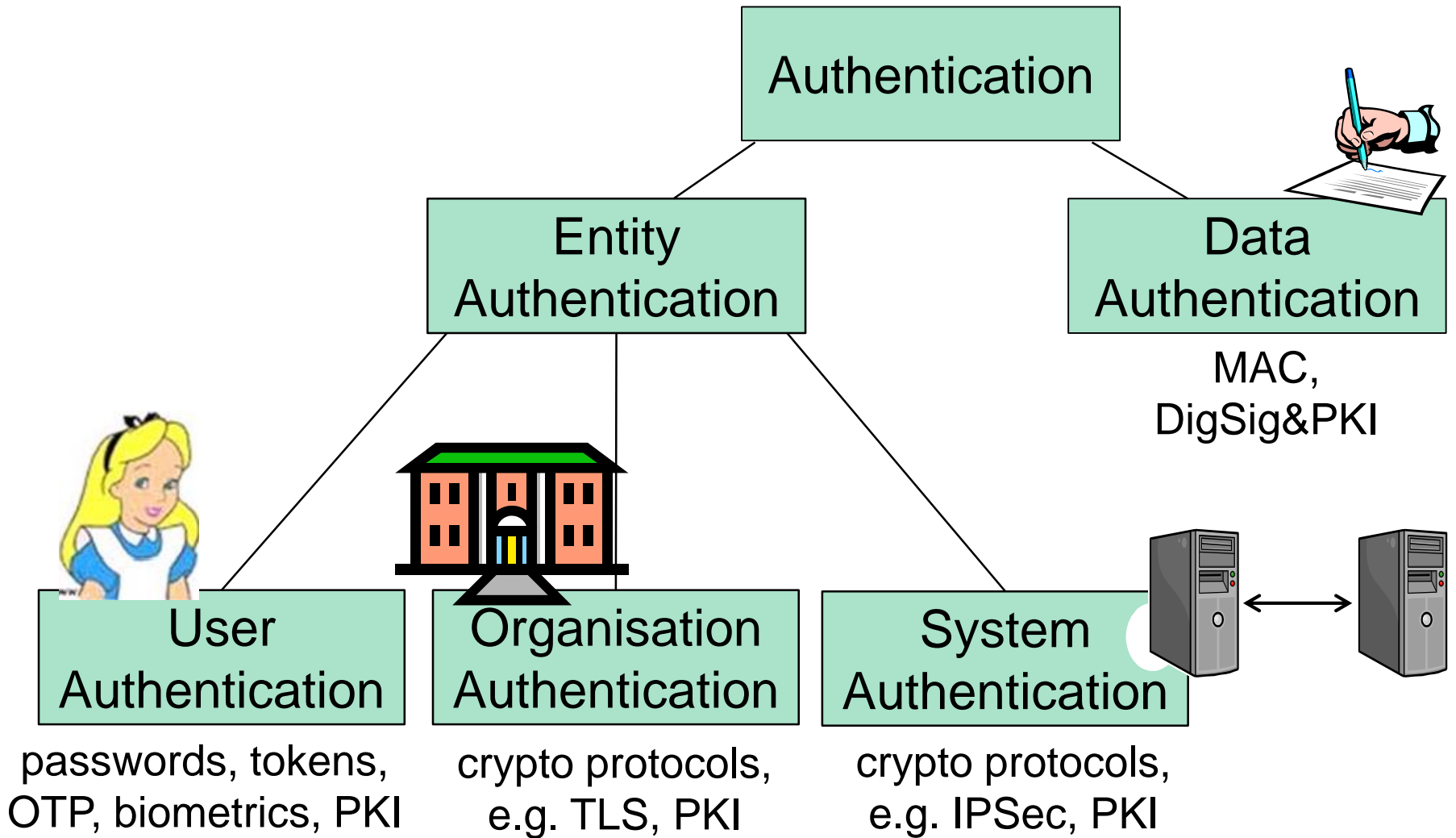
- The corroboration (verification) that a peer entity (system) in an association (connection, session) is the one claimed (X.800).



- **Data origin authentication (message authentication):**

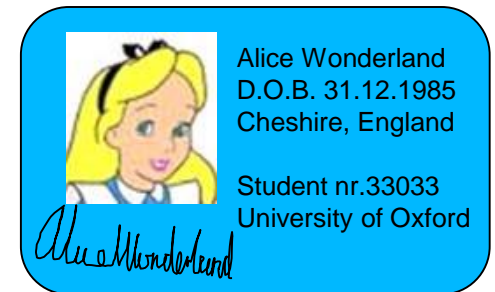
- The corroboration (verification) that the source of data received is as claimed (X.800).

# Taxonomy of Authentication



# User Identification and Authentication

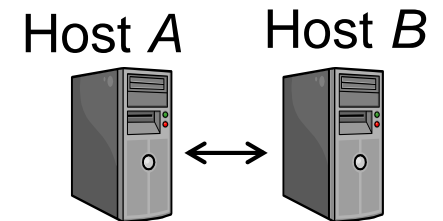
- Identification
  - Who you claim to be
  - Method: (user)name, biometrics
- User authentication
  - Prove that you are the one you claim to be
- Main threat: Unauthorized access
- Controls:
  - *Passwords,*
  - *Personal cryptographic tokens,*
    - OTP generators, etc.
  - *Biometrics*
    - Id cards
  - *Cryptographic security/authentication protocols*



Authentication token

# Organisation/System Authentication

- Goal
  - Establish the correct identity of organisations/remote hosts
- Main threat:
  - Network intrusion
  - Masquerading attacks,
  - Replay attacks
  - (D)DOS attacks
- Controls:
  - *Cryptographic authentication protocols based on hashing and encryption algorithms*
  - *Examples: TLS, VPN, IPSEC*



# Data Origin Authentication (Message authentication)

- Goal: Recipient of a message (i.e. data) can verify the correctness of claimed sender identity
  - But 3<sup>rd</sup> party may not be able to verify it
- Main threats:
  - False transactions
  - False messages and data
- Controls:
  - *Encryption with shared secret key*
  - *MAC (Message Authentication Code)*
  - *Security protocols*
  - *Digital signature with private key*
  - *Electronic signature,*
    - i.e. any digital evidence



# Non-Repudiation

## (Strong form of Data Authentication)

- Goal: Making sending and receiving messages undeniable through unforgible evidence.
  - Non-repudiation of origin: proof that data was sent.
  - Non-repudiation of delivery: proof that data was received.
  - NB: imprecise interpretation: Has a message been received and read just because it has been delivered to your mailbox?
- Main threats:
  - Sender falsely denying having sent message
  - Recipient falsely denying having received message
- Control: *digital signature*
  - Cryptographic evidence that can be confirmed by a third party
- Data origin authentication and non-repudiation are similar
  - Data origin authentication only provides proof to recipient party
  - Non-repudiation also provides proof to third parties

# Accountability

(Can be considered as a part of System integrity)

- Goal: Trace action to a specific user and hold them responsible
  - *Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party*  
(TCSEC/Orange Book)
- Main threats:
  - Inability to identify source of incident
  - Inability to make attacker responsible
- Controls:
  - *Identify and authenticate users*
  - *Log all system events (audit)*
  - *Electronic signature*
  - *Non-repudiation based on digital signature*
  - *Forensics*



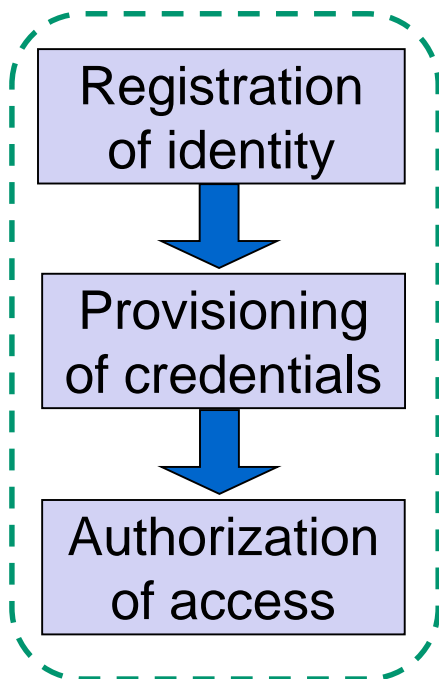


# Authorization

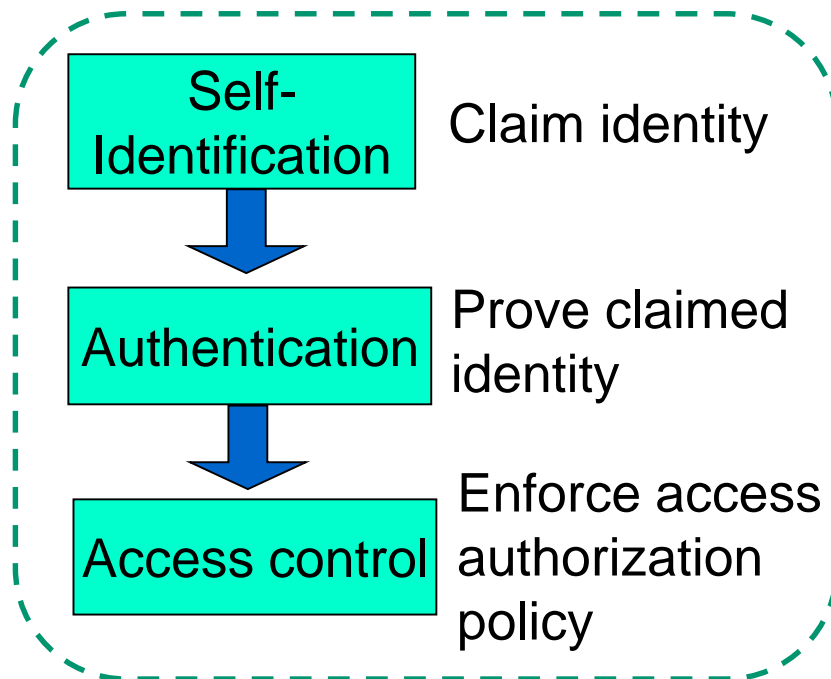
- Authorization is to specify access and usage permissions for entities, roles or processes
  - Authorization policy normally defined by humans
  - Issued by an authority within the domain/organisation
- Authorities authorize, systems don't
- Authority can be delegated
  - Management → Sys.Admin
  - Implemented in IT systems as configuration/policy

# Identity and Access Management (IAM) Phases

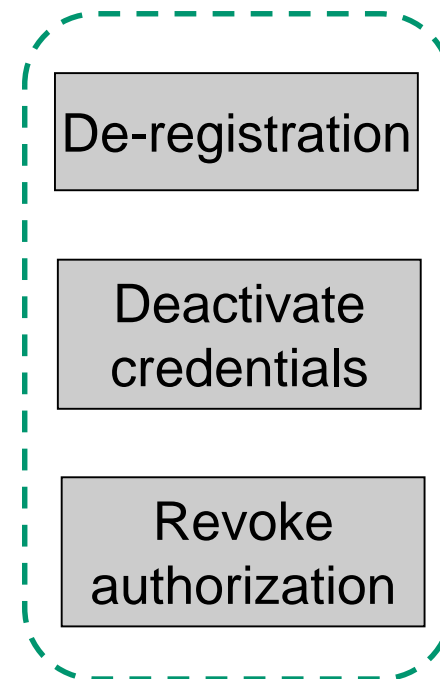
## Configuration phase



## Operation phase



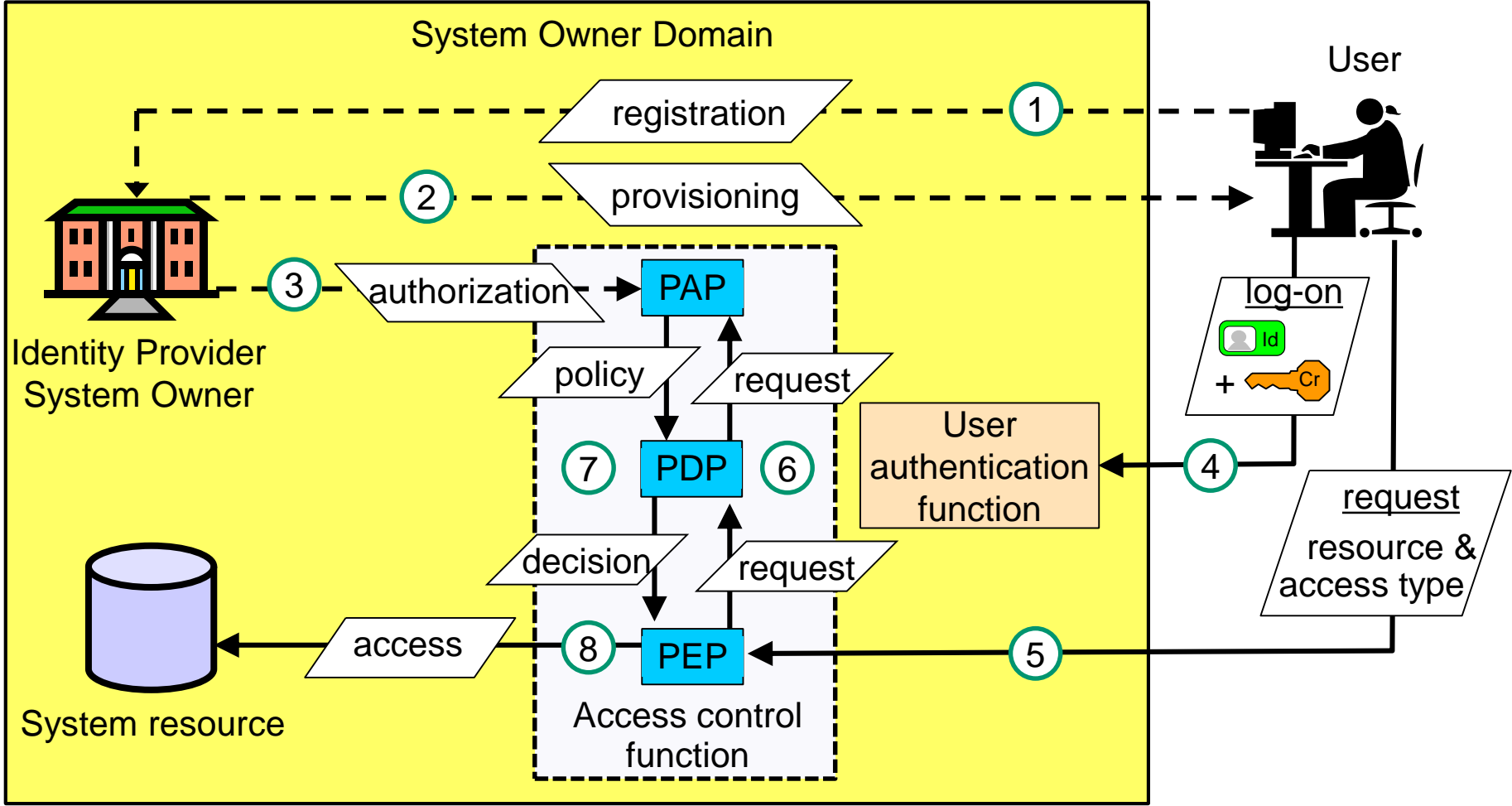
## Termination phase



# Confusion about Authorization

- The term “authorization” is often wrongly used in the sense of “access control”
  - e.g. misleading figure on p.725 in Harris 7<sup>th</sup> ed.
  - Common in text books and technical specifications (RFC 2196 ...)
  - Cisco AAA Server (Authentication, Authorization and Accounting)
- Wrong usage of “authorization” leads to absurd scenario:
  1. You get somebody’s password, and uses it to access account.
  2. Login screen gives warning: *“Only authorized users may access this system”*.
  3. You get caught and taken to the police
  4. You argue: *“Text books in security state that a system authorizes the user when typing the right password, hence I was authorized because I typed the right password”*.
  5. Case dismissed, you go free.

# Identity and Access Management Concepts



PAP: Policy Administration Point

PEP: Policy Enforcement Point

← - - Registration

PDP: Policy Decision Point

IdP: Identity Provider

← Operations

End of lecture

