# IN2120 Information Security

## Lecture 01:
## - Course info
## - Basic concepts in information security

Audun Jøsang

University of Oslo,  Autumn 2018

# Course information

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

# 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/IN2120/h18/
  - lecture presentations, workshop questions, etc.
  - List of English security terms translated to Norwegian
- Suggested security topics for home exam on:
  - https://wiki.uio.no/mn/ifi/IN2120-2018
- Various online resources
  - E.g. NIST special computer security publications
    http://csrc.nist.gov/publications/PubsSPs.html

- Previous version of the course: INF3510 Information Security
  - https://www.uio.no/studier/emner/matnat/ifi/INF3510/
  - 3rd year Bachelor course, Spring semester
  - Same scope as IN2120

# Lecturers

- Prof. Audun Jøsang,
  - Professor, UiO, 2008 →
  - Associate Professor, QUT, Australia, 2000-2007
  - Telecommunications engineer, Alcatel, Belgium 1988-1993
  - PhD Information Security, NTNU, 1997
  - MSc Information Security, Royal Holloway College, London, 1993
  - MSc Telecommunications, NTH 1987
- Nils Gruschka
  - Associate Professor, UiO, 2018 →
  - Professor, Kiel Univ. of Applied Science, 2012-2017
  - Senior Research, NEC Labs Europe, 2008-2011
  - PhD, Network Sec., Chr-Albrechts University, Kiel, 2008
  - System Design Engineer, T-Systems, 2000-2002
  - MSc, Comp.Sc., Chr-Albrechts University, Kiel, 2000

# Prerequisites

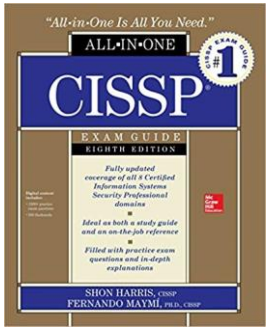
- Prerequisites
  - Basic computer and network technology
  - Basic (discrete) mathematics

- 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 main learning material is presented during the lectures.
- In addition use the text book:

  CISSP All-in-One Exam Guide
  8th Edition, 2018
  Authors: Shon Harris (✝) and
  Fernando Maymí


"All-in-One Is All You Need."
ALL-IN-ONE
CISSP
#1
EXAM GUIDE
EIGHTH EDITION
Fully updated coverage of all 8 Certified Information Systems Security Professional domains
Ideal as both a study guide and an on-the-job reference
Filled with practice exam questions and in-depth explanations
SHON HARRIS, CISSP
FERNANDO MAYMÍ, PH.D., CISSP

Shon Harris

Fernando Maymí

- The book covers the 8 CBK domains (Common Body of Knowledge) for the CISSP (Certified Information Systems Security Professional) exam.
- https://www.amazon.com/CISSP-All-One-Guide-Eighth/dp/1260142655
- The 8th edition will be published in October 2018. It is possible to use the 7th edition from 2016, but we recommended to wait until October and buy the 8th edition. Until then the lecture notes and other learning material will be sufficient for studying this course.
- Detailed reading of sections in the text book
  - For each lecture a set of relevant pages in the text book is specified
  - Before the 8th edition is published, refer to the 7th edition (wiki pages)
  - New overview of detailed reading when the 8th edition is published

# How to use Harris & Maymí's CISSP book

- 1000+ 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

| Week | Date | # | Topic |
|---|---|---|---|
| W34 | 21.08.2018 | 1 | Course Information. Basic Concepts in IS |
| W35 | 28.08.2018 | 2 | Cryptography |
| W36 | 04.09.2018 | 3 | Key Management and PKI |
| W37 | 11.09.2018 | 4 | Network Communication Security |
| W38 | 18.09.2018 | 5 | IS Mgment, and Human Factors for IS. |
| W39 | 25.09.2018 | 6 | Incident Response and Digital Forensics |
| W40 | 02.10.2018 | 7 | Computer Security. |
| W41 | 09.10.2018 | 8 | Risk Management and Business Continuity Planning |
| W42 | 16.10.2018 | 9 | User Authentication |
| W43 | 23.10.2018 | 10 | Identity and Access Management |
| W44 | 30.10.2018 | 11 | Network Perimeter Security |
| W45 | 06.11.2018 | 12 | System Development and Application Security |
| W46 | *No lecture* | | |
| W47 | *No lecture* | | |
| W48 | 27.11.2018 | | Review |
| W49 | *No lecture* | | |
| W50 | 11.12.2018 | Digital exam, time: 14:30h - 18:30h (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/IN2120-2018/
- Length: 5000 - 10000 words (approx. 10 – 15 pages)
- Due date: 04.11.2018
- Assessment criteria:
  - Structure and presentation: weight ¼
  - Scope and depth of content: weight ¼
  - Evidence of independent research and analysis: weight ¼
  - Proper use of references: weight ¼

# 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 ☺

# INF3510 Exam Statistics

| Year | # students | # A<br>(%) | # B<br>(%) | # C<br>(%) | # D<br>(%) | # E<br>(%) | # F<br>(%) |
|---|---|---|---|---|---|---|---|
| 2018 | 152 | 20<br>(13%) | 50<br>(33%) | 64<br>(42%) | 10<br>(7%) | 1<br>(1%) | 7<br>(5%) |
| 2017 | 138 | 9<br>(6%) | 47<br>(34%) | 66<br>(49%) | 4<br>(3%) | 3<br>(2%) | 9<br>(6%) |
| 2016 | 147 | 6<br>(4%) | 39<br>(37%) | 59<br>(40%) | 9<br>(6%) | 10<br>(7%) | 24<br>(16%) |
| 2015 | 121 | 10<br>(9%) | 30<br>(25%) | 45<br>(37%) | 9<br>(7%) | 9<br>(7%) | 18<br>(15%) |
| 2014 | 103 | 4<br>(4%) | 8<br>(7.5%) | 45<br>(44%) | 14<br>(13.5%) | 9<br>(4.5%) | 23<br>(22.5%) |
| 2013 | 0 | For the 2013 spring semester INF3510 was cancelled due to faculty politics. | | | | | |
| 2012 | 34 | 2<br>(6%) | 6<br>(18%) | 14<br>(41%) | 0<br>(0.0%) | 6<br>(17.5%) | 6<br>(17.5%) |

# Other security courses at IFI

- IN5290: Ethical Hacking
  - Laszlo Erdödi (Autumn)
- IN5280: Security by Design
  - Lillian Røstad (Spring)
- IN5300: Network Security and Applied Cryptography
  - Nils Gruschka (Spring)
- TEK4500: Introduction to Cryptography
  - Leif Nilsen  (Autumn)
- UNIK4250: Security in Distributed Systems
  - Nils Nordbotten (Spring)
- TEK5510: Security in Operating Systems and Software
  - Trond-Arne Sørby (Autumn)
- IN5130 - Unassailable IT-systems
  - Ketil Stølen (Autumn)
- ITLED4230 Ledelse av informasjonssikkerhet
  - Audun Jøsang (Autumn) (for professionals, course fee NOK 25K)

# Why study information security ?

- You can not be an IT expert without also knowing IT security
  - Analogy: Building architects must have knowledge about fire safety
- Developing IT systems without considering security will lead to vulnerable IT systems
- System developers with insufficient security skills build security vulnerabilities into the systems they design
- *“Security by design”* is a requirement in system design and is a prerequisite for privacy by design which is a legal requirement for processing personal data
- Information security is a political issue
  - National Government expresses the importance of production of security skills in higher education
  - Stortinget made information security mandatory in IT education

https://www.tekna.no/aktuelt/tekna-gjennomslag-om-ikt-sikkerhet-i-utdanningen/

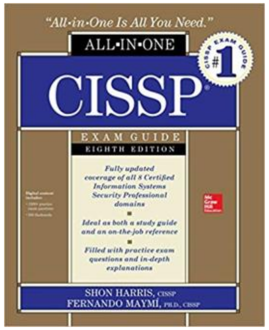
# Certifications for IS Professionals

- Many different types of certifications available
  - vendor neutral or vendor specific, profit or non-profit, e.g.
    - (ISC)$^2$ https://www.isc2.org/
    - ISACA https://www.isaca.org/
    - SANS https://www.sans.org/
    - CISCO https://www.cisco.com/c/en/us/training-events/training-certifications/overview.html
- 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
- Certification types reflect current topics in IT Security
  - Generally kept up-to-date

# CISSP Certification from (ISC)$^2$: Certified Information System Security Professional

- Many different books to prepare for the CISSP exam
- e.g. text book used for IN2120 course

  CISSP All-in-One Exam Guide
  8th Edition, 2018
  Author: Shon Harris and Fernando Maymí


"All-in-One Is All You Need."
ALL•IN•ONE
CISSP
EXAM GUIDE
EIGHTH EDITION
Fully updated coverage of all 8 Certified Information Systems Security Professional domains
Ideal as both a study guide and an on-the-job reference
Filled with practice exam questions and in-depth explanations
SHON HARRIS, CISSP
FERNANDO MAYMÍ, PH.D., CISSP

- € 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 IN2120 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:** *Multi-Factor Authentication*
  - **Speaker:** *Prof. Dipankar Dasgupta*
  - **Time:** 31 August 2018, 10:00h
  - **Place:** Kristen Nygaards sal, 5th floor, OJD

- All interested are welcome !

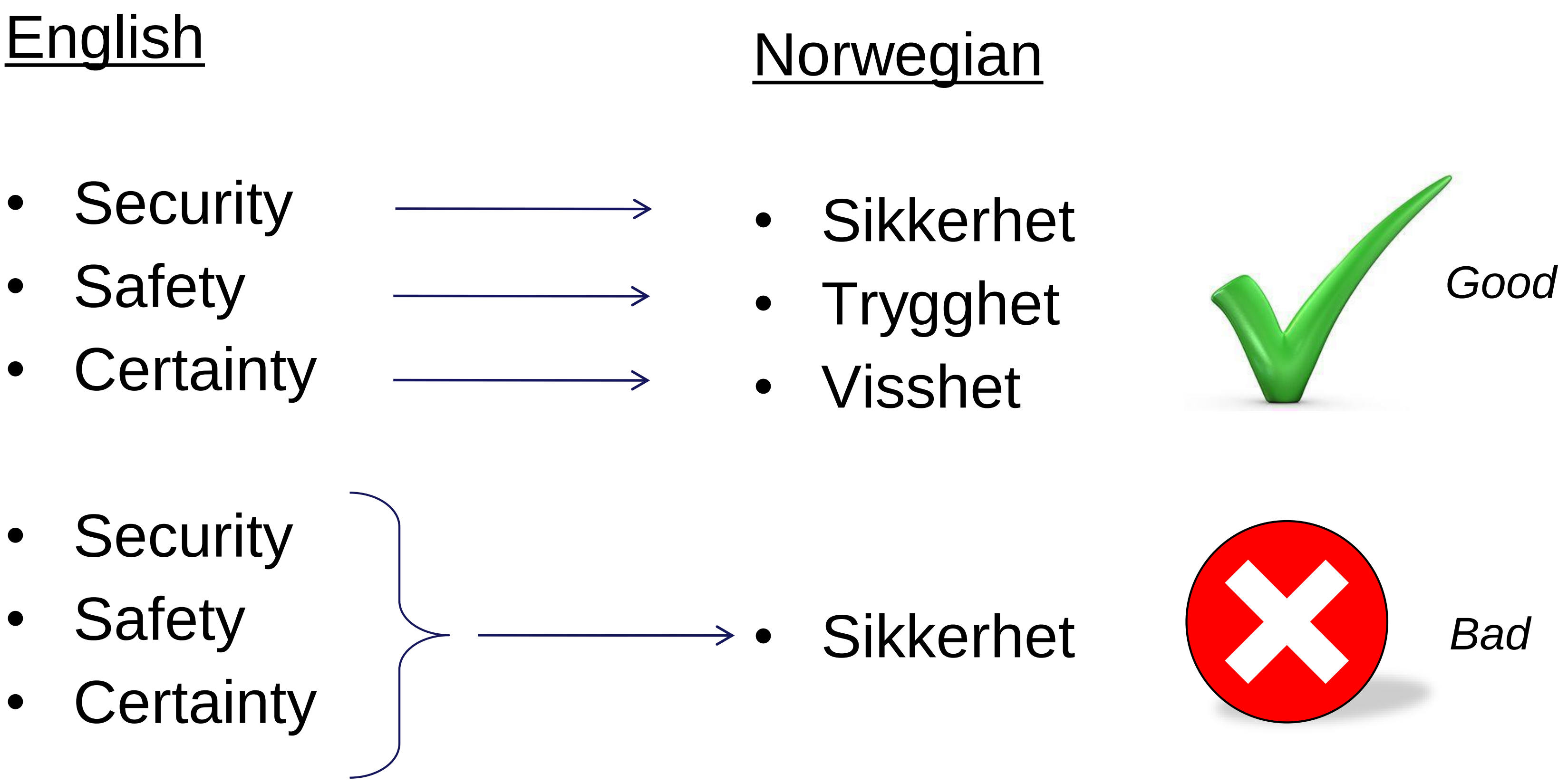
- Organised by the UiO SecurityLab

UiO : University of Oslo

SecurityLab

# Information Security
Basic Concepts

# Good and bad translation



| English | Norwegian | |
|---|---|---|
| Security | Sikkerhet | ✓ *Good* |
| Safety | Trygghet | |
| Certainty | Visshet | |
| Security<br>Safety<br>Certainty | Sikkerhet | ✗ *Bad* |

# Wat is security ?

Security is the protection of assets from harm

property, infrastructure, stability, life, environment, information

- **Physical security** (prevent burglary and theft)
- **Societal security** (security in critical infrastructure)
- **National security** (political stability)
- **Safety** (security of life and health)
- **Environmental security** (stop pollution and invasive species)
- **Information security and data protection**

# What is *Information Security*

- *Information Security* is the protection of *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)

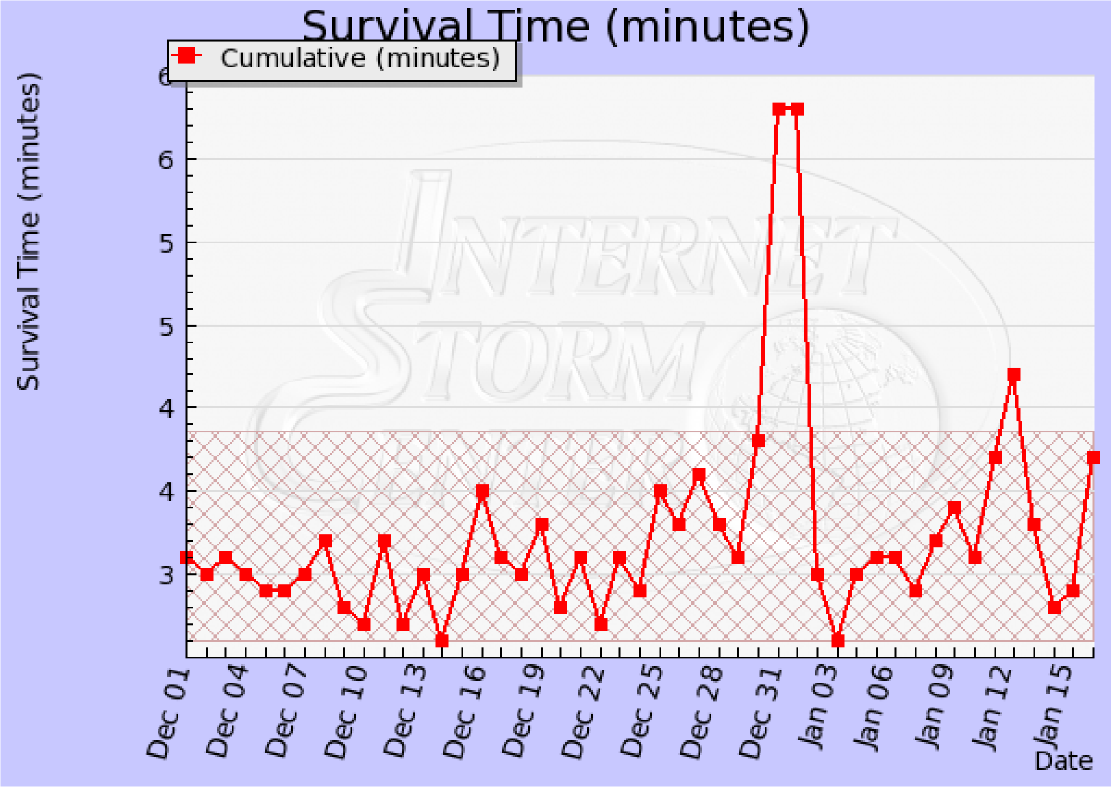
# Scope of information security management

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

# The Need for Information Security

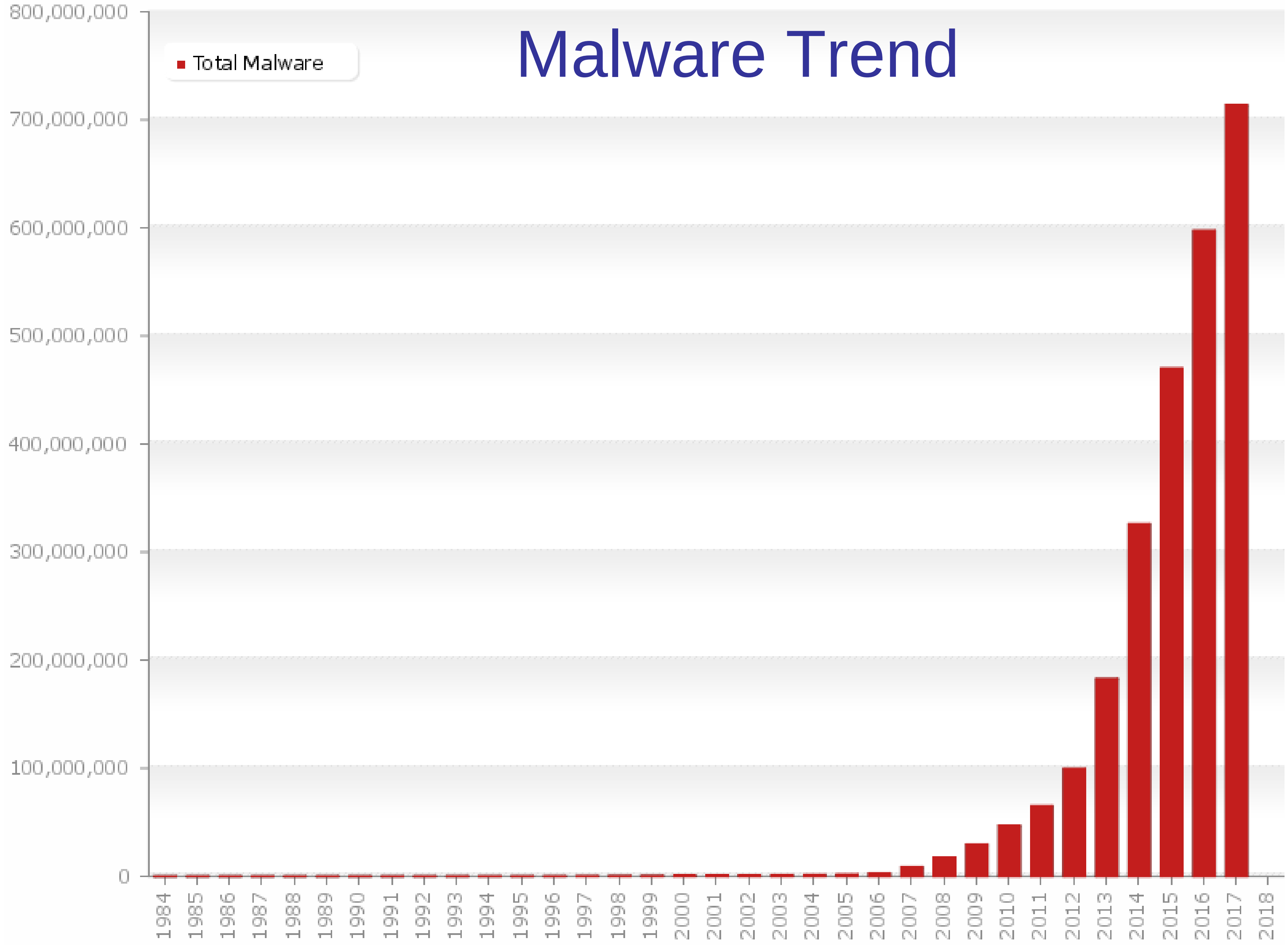
- Why not simply solve all security problems once for all?
- Reasons why that’s impossible:
  - Rapid innovation constantly generates new technology with new vulnerabilities
  - More activities go online
  - Crime follows the money
  - Information security is a second thought when developing IT
  - New 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

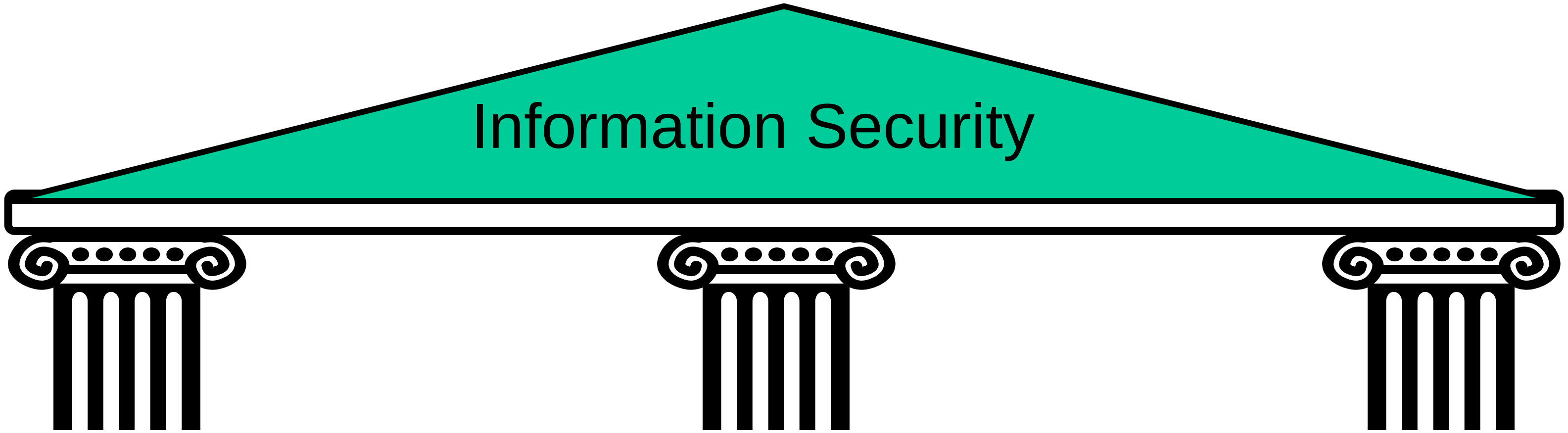
# Malware Trend



Last update: 12-18-2017 10:11

Copyright © AV-TEST GmbH, www.av-test.org

# 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

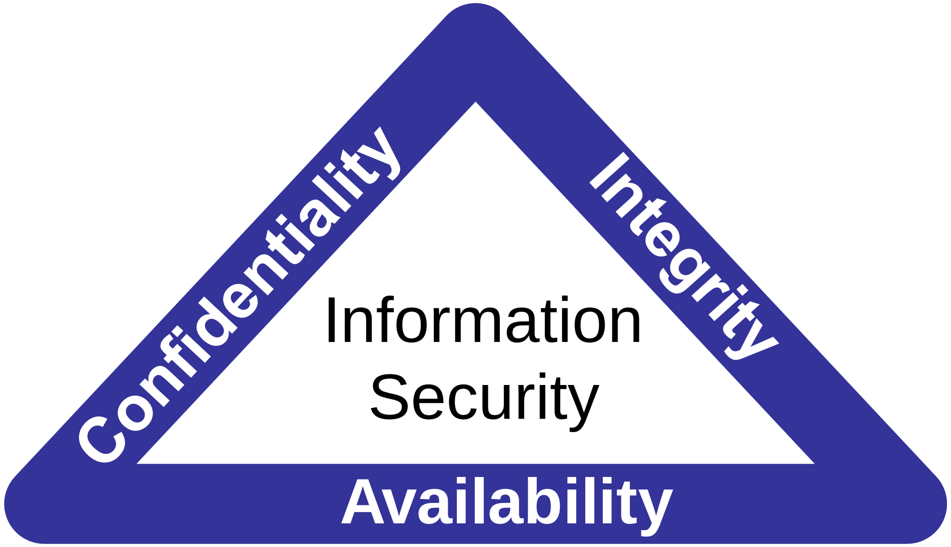
  - During transmission
    - Physical or electronic

  - During processing (use)
    - Physical or electronic

- Security controls for all information states are needed

# Security Services and Properties

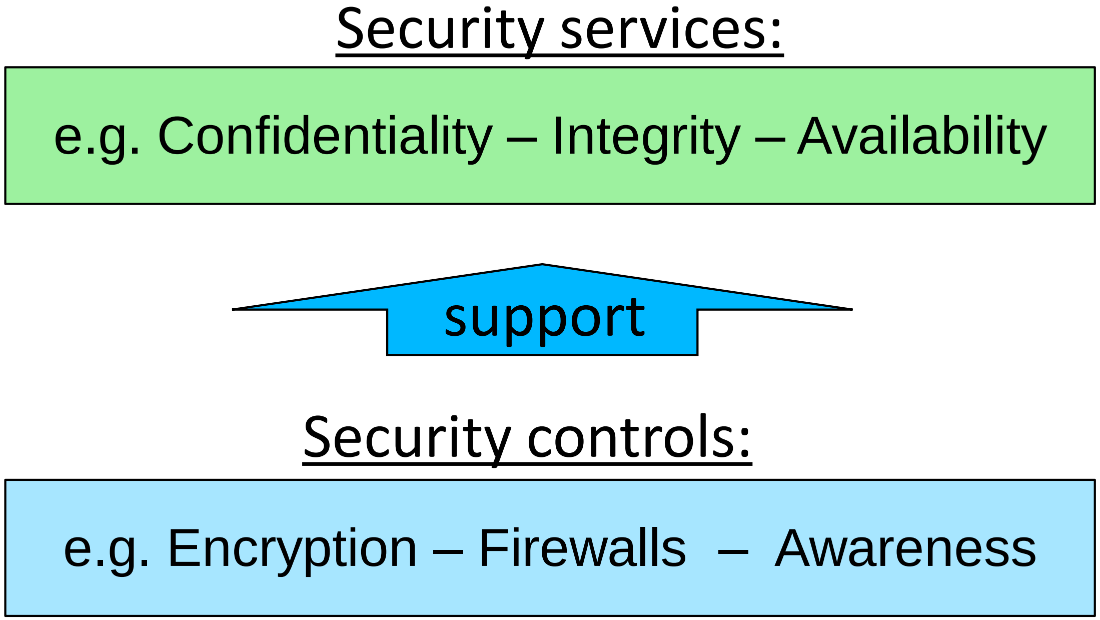
- A security service provides a high level security property
- The traditional definition of information security is to preserve the three CIA properties for data and services:
  - **Confidentiality**:
  - **Integrity**
  - **Availability**:



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

# 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*

Are you still there?
DENIAL OF SERVICE
Securely configure and harden networks against known DoS attacks.
Implement intrusion detection and monitor for unusual network behavior.

# Data Privacy

GDPR

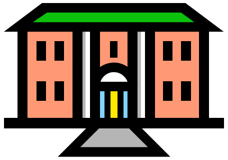
To protect specific aspects of information that may be related to natural persons (personal information).

- 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
- Adequate information security (CIA) of personal information
- Define clear responsibilities around personal information
- GDPR (General Data Protection Regulation) became EU law on 25 May 2018, its Norwegian translation became the new “Personopplysningslov” on 20 July 2018.

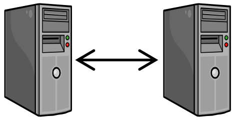
# Authenticity (Security Service)

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.



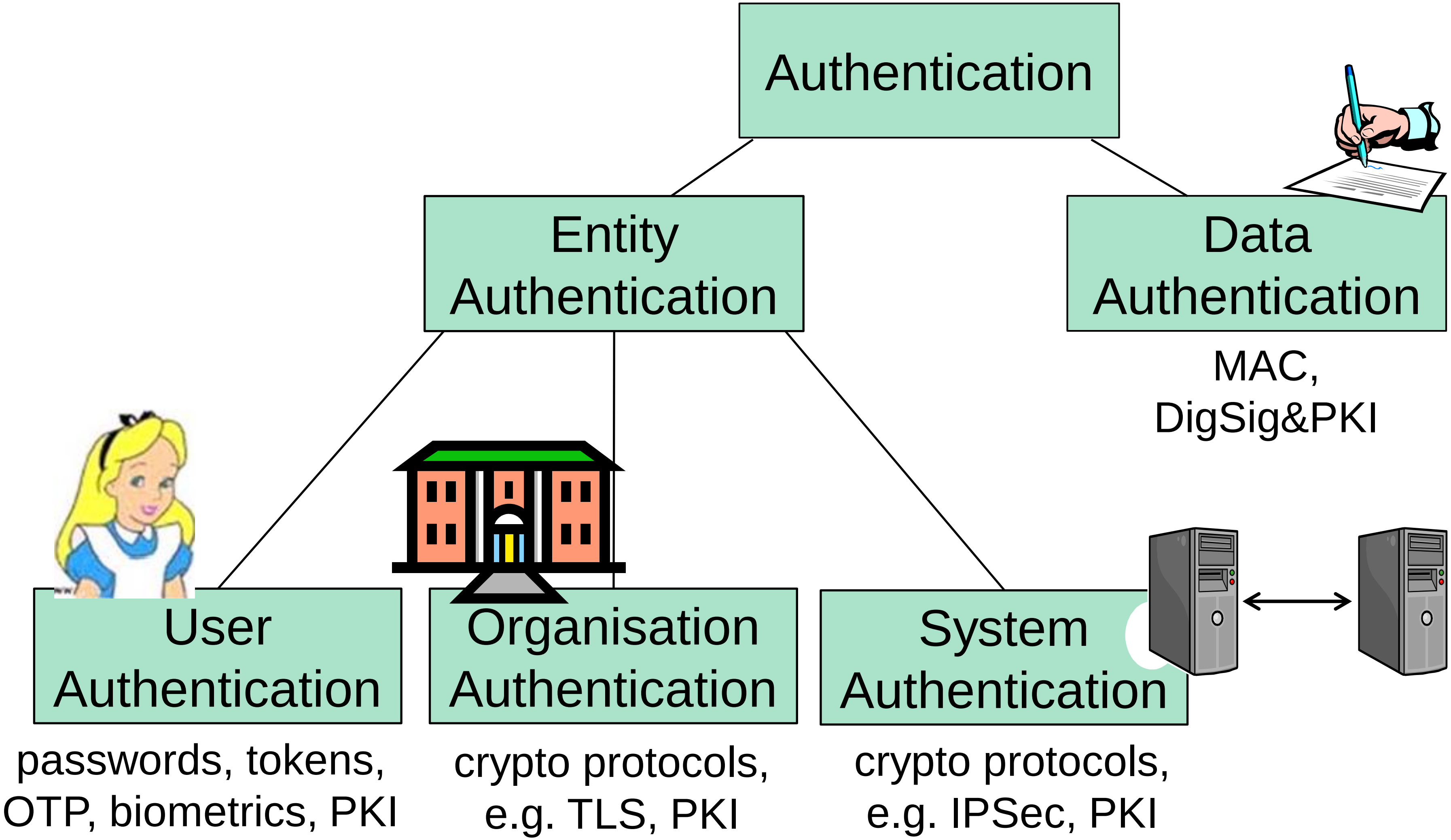
- Organisation authentication:
  - The process of verifying a claimed identity of a (legal) organisation in an online interaction/session



- 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


Authentication
Entity Authentication
Data Authentication
MAC, DigSig&PKI
User Authentication
passwords, tokens, OTP, biometrics, PKI
Organisation Authentication
crypto protocols, e.g. TLS, PKI
System Authentication
crypto protocols, e.g. IPSec, PKI

# 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: Spoofed identity and false login
- Controls:
  - *Passwords,*
  - *Personal cryptographic tokens*,
    - OTP generators, etc.
  - *Biometrics*
    - Id cards
  - *Cryptographic security/authentication protocols*

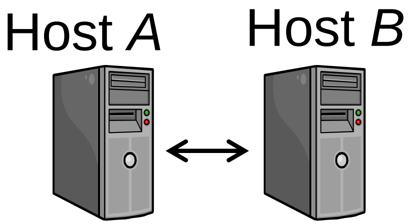
Alice Wonderland
D.O.B. 31.12.1985
Cheshire, England

Student nr.33033
University of Oxford

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 3rd 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)

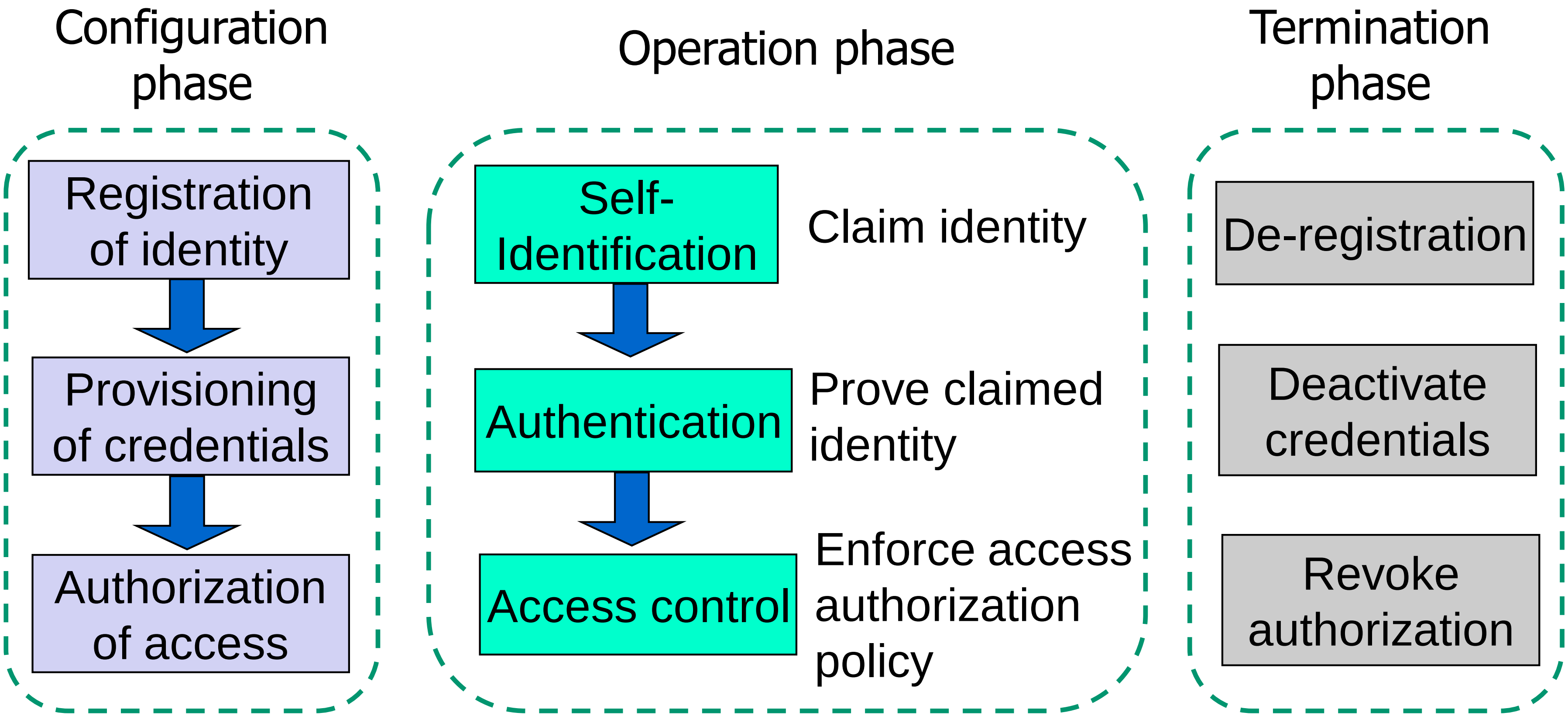
- Goal: Trace action to a specific user and hold them responsible
  - *Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party*

    (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

Registration of identity

Provisioning of credentials

Authorization of access

Operation phase

Self-Identification

Claim identity

Authentication

Prove claimed identity

Access control

Enforce access authorization policy

Termination phase

De-registration

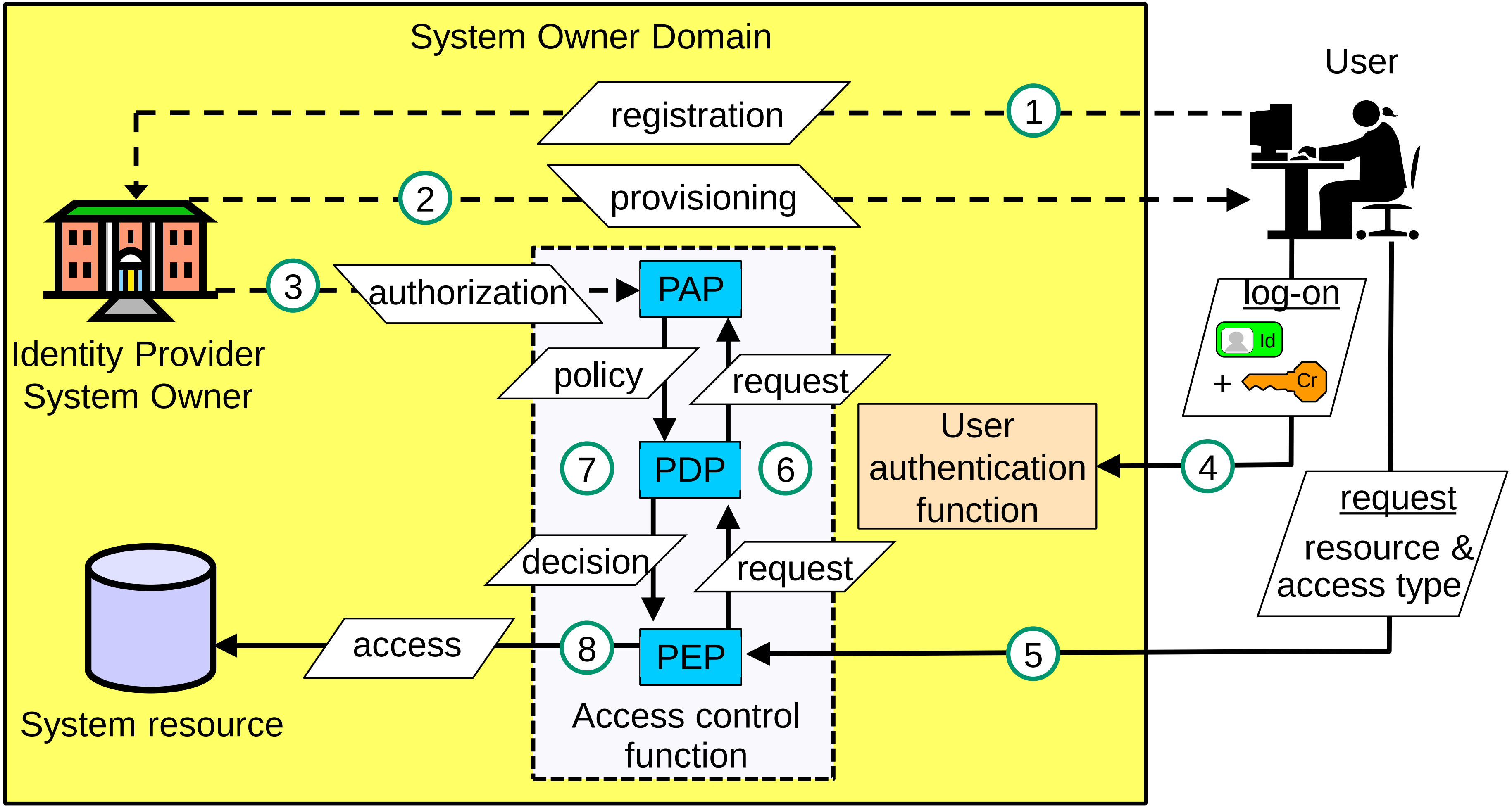
Deactivate credentials

Revoke authorization

# Confusion about Authorization

- The term “authorization” is often wrongly used in the sense of “access control”
  - e.g. misleading figure in Ch.5 IAM on p.725 in Harris 7th ed.
  - Common error in text books and specifications (RFC 2196 …)
  - E.g. Cisco AAA (Authentication, Authorization and Accounting)
- Wrong usage of “authorization” leads to absurd scenario:
  1. You obtain 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: *“This text books on information security states 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

PDP: Policy Decision Point

PEP: Policy Enforcement Point

IdP: Identity Provider

◄- - - Registration

◄—— Operations

# End of lecture