IN2120 Information Security

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

Audun Jøsang

University of Oslo, Autumn 2019

Course information

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

Course organisation and learning

- Learning activities
  - Attend 2-hour lecture on Thursdays 14:15h – 16:00h
    - Lecture notes available at least one day prior to lecture
    - Podcast available the day after the lecture
  - Attend 1-hour workshop on Tuesdays 12:15 – 13:00h
    - Study and answer workshop questions after each lecture
    - Will be discussed during the following week's workshop
  - Read sections from text book, corresponding to each 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/h19/
  - 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/IN2120-2019
- 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

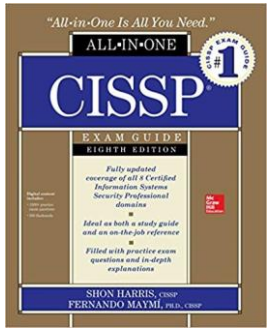
- Prerequisites
  - Basic computer and network technology
  - Basic (discrete) mathematics
- Theoretic focus on a basic level
  - Discrete mathematics, number theory, modular arithmetic
  - Information theory
  - Probability calculus
  - Computer and network architectures

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




Shon Harris


Fernando Maymí

- The book covers the 8 CBK domains (Common Body of Knowledge) for the CISSP (Certified Information Systems Security Professional) exam.
- Sold by e.g. Akademika and Amazon

  https://www.akademika.no/cissp-all-one-exam-guide-eighth-edition/harris-shon/maymi-fernando/9781260142655

- Reading sections in the text book
  - For each lecture a set of relevant pages in the text book is specified in the document “Detailed Reading” on the course web page.
  - The purpose is to give deeper understanding of topics from lectures

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

Preliminary Course Schedule

Week	Date	L#	Topic
W34	22.08.2019	1	Course Information. Basic Concepts in IS
W35	29.08.2019	2	Cryptography
W36	05.09.2019	3	Key Management and PKI
W37	12.09.2019	4	Network Security
W38	18.09.2019	5	IS Management, and Human Factors for IS
W39	26.09.2019	6	Incident Response and Digital Forensics
W40	03.10.2019	7	Risk Management and Business Continuity Planning
W41	10.10.2019	8	Computer Security
W42	17.10.2019	9	User Authentication
W43	24.10.2019	10	Identity and Access Management
W44	31.10.2019	11	Ethical Hacking / Penetration Testing
W45	07.11.2019	12	Secure System Development and Application Security
W46	*No lecture*		
W47	21.11.2019		Review
W48	*No lecture*		
W49	*No lecture*		
W50	11.12.2019	Digital exam, time: 09:00h - 13:00h (4 hours)	

Home Exam

- Write a report/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/IN2120-2019/
- Length: 5000 - 10000 words (approx. 10 – 15 pages)
- Due date: 03.11.2019
- 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 Grading

- Course weight: 10 study points
- Assessment items
  - Home exam: normally carries relative weight 0.4
  - Digital exam: normally carries relative weight 0.6
- Adjustments
  - Weight on home exam is reduced when digital-exam score < 50%
  - Weight on home exam is 0 when digital-exam score < 40%
- 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
- Stay clear of dishonesty (including plagiarism and cheating)
  - See: https://www.uio.no/english/studies/admin/examinations/cheating/
  - Should be no problem ☺

Exam Statistics IN2120 (2018→) and INF3510 (→2018)

Year	# studs	# A (%)	# B (%)	# C (%)	# D (%)	# E (%)	# F (%)
2018	241	28 (12%)	92 (38%)	87 (36%)	6 (2%)	9 (4%)	19 (8%)
2018	152	20 (13%)	50 (33%)	64 (42%)	10 (7%)	1 (1%)	7 (5%)
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 (8%)	45 (44%)	14(13%)	9 (9%)	23 (22%)
2013	0	INF3510 was cancelled in 2013 due to faculty politics.					
2012	34	2 (6%)	6 (18%)	14 (41%)	0 (0.0%)	6 (17.5%)	6 (17.5%)

Other security courses at IFI

- IN3210 Network Security
  - Nils Gruschka (Autumn)
- IN5290: Ethical Hacking
  - Laszlo Erdödi (Autumn)
- IN5280: Security by Design
  - Lillian Røstad (Spring)
- IN5130 - Unassailable IT-systems
  - Ketil Stølen (Autumn)
- TEK4500: Introduction to Cryptography
  - Leif Nilsen (Autumn)
- TEK5500: Security in Distributed Systems
  - Nils Nordbotten (Spring)
- TEK5510: Security in Operating Systems and Software
  - Trond-Arne Sørby (Autumn)
- TEK9550 Advanced Topics in Cryptology
  - Thomas Gregersen (Spring)
- ITLED4230 Ledelse av informasjonssikkerhet
  - Audun Jøsang (Autumn) (professional 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
- *"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
  - The Government states the importance of producing of IT-security skills in higher education
  - Stortinget wants information security to be mandatory in IT education

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

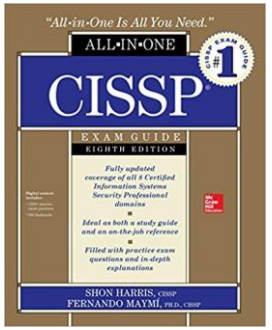
Security Certifications for Professionals

- 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



- € 560 fee to sit CISSP exam
- You also need several years professional experience to be certified
- 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)

Information Security Surveys

- Mørketallsundersøkelsen:
  http://www.nsr-org.no/moerketall/
  - New report in December every 2 years (latest report from 2018)
- Mnemonic Security Report:
  https://www.mnemonic.no/security-report/
- PWC security survey:
  http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html
- UK Cyber Security Survey:
  https://www.ipsos.com/ipsos-mori/en-uk/uk-cyber-security-survey-2019

+ many others

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

Security Advisory Bodies

- NorCERT: For government sector: https://www.nsm.stat.no/norcert
- NorSIS: For citizens and small-business sector: https://www.norsis.no/
- Nordic Financial CERT: https://www.nfcert.org/
- KraftCERT: https://www.kraftcert.no/
- HelseCERT: https://www.nhn.no/helsecert/
- UNINETT-CERT: https://www.uninett.no/cert
- UiO-CERT: http://www.uio.no/english/services/it/security/cert/
- CISA US CERT: https://www.us-cert.gov/
- Australia AusCERT: https://www.auscert.org.au/

+ many others

They provide advice and assistance for managing threats and vulnerabilities

Academic Forum on Security

- Monthly seminar on information security
- https://wiki.uio.no/mn/ifi/AFSecurity/
- Guest expert speakers
- Next AF*Security* seminar:
  - **Title:** Privacy Threat of Keystroke Profiling on the Web
  - **Speaker:** *Denis Migdal* (ENSICAEN)
  - **Time:** 21 August 2019, 14:00h
  - **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

- Security
- Safety
- Certainty

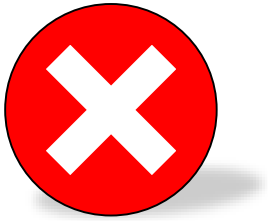
Norwegian

- Sikkerhet
- Trygghet
- Visshet

Good

- Security
- Safety
- 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 of property)
- **Societal security** (security of critical infrastructures)
- **National security** (political stability and national integrity)
- **Safety** (security of life and health)
- **Environmental security** (stop pollution and invasive species)
- **Information security and data protection**

What is *Information Security*

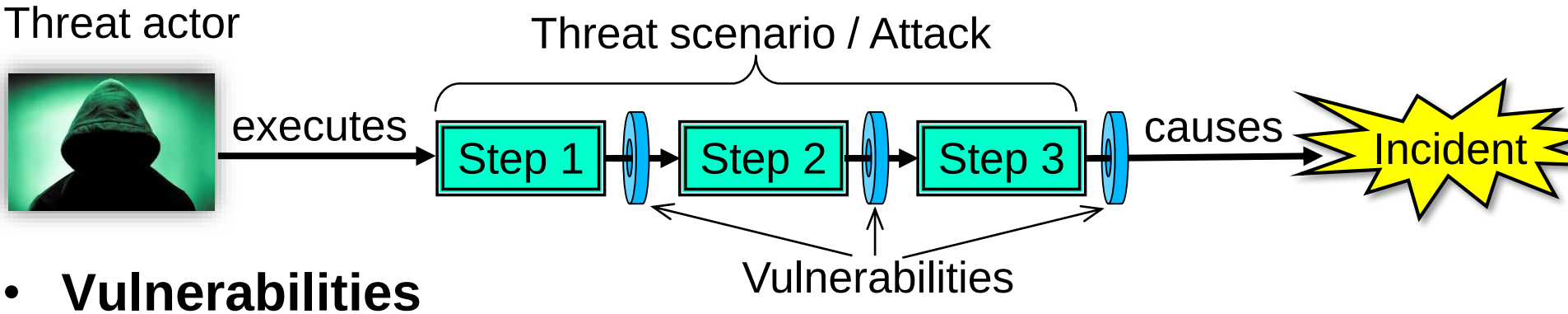
- *Information Security* is the protection of *information assets* from damage or harm
- What are the assets to be protected?
  - Example: data files, software, IT equipment and infrastructure
- Covers both intentional and accidental events
  - Threat agents can be humans or acts of nature
  - People 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)

Information Security Management

- IS management consists of activities to control and reduce risk of damage to information assets
- IS management focuses on:
  - Evaluate threats, vulnerabilities and risks
  - Control security risks by reducing vulnerability to threats
  - Detection and response to attacks
  - Recovery from damage caused by attacks
  - Investigate and collect evidence about incidents (forensics)

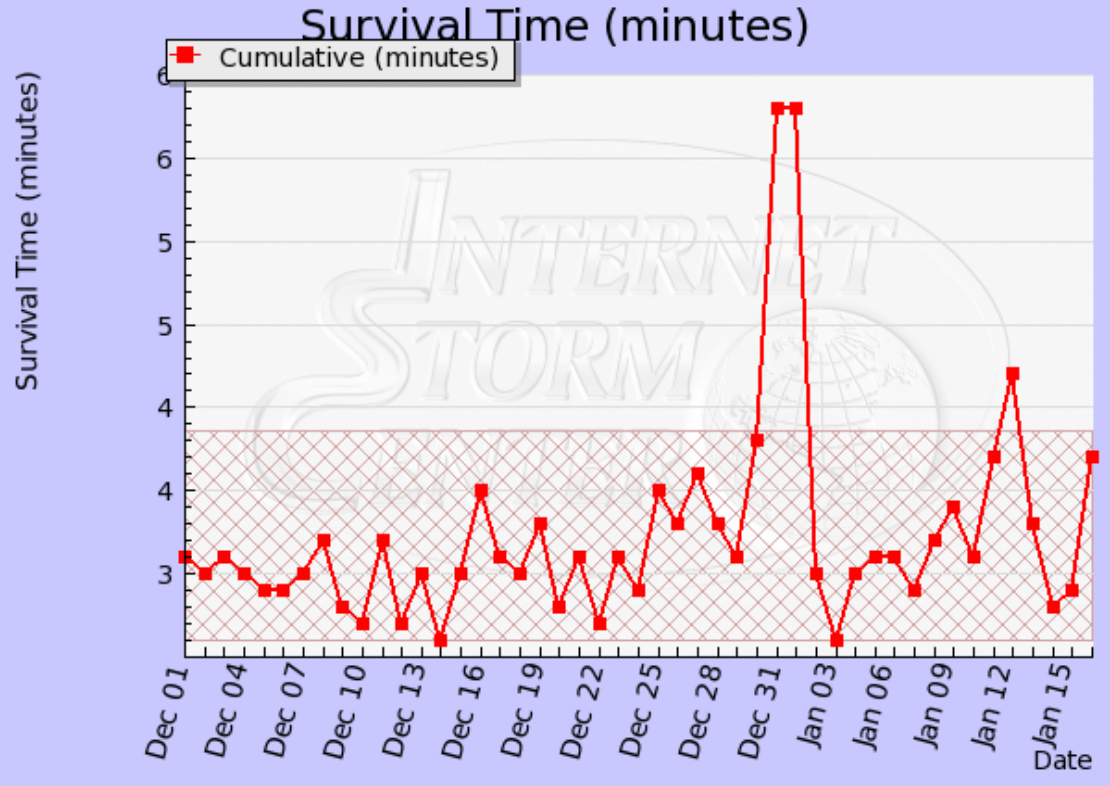
Threat, Vulnerability, Risk and Control

- **Threat**
  - **Threat Actor:** An active entity which can execute a threat scenario.
  - **Threat Scenario:** The set of steps executed in a (potential) cyber attack.
  - When simply using the term “threat”, it usually means a threat scenario.



- **Vulnerabilities**
  - Weaknesses or opportunities allowing a threat scenario to be executed
- **Security Risk**
  - Likelihood (ease of executing a threat scenario), combined with the potential damage in case of an incident (successful attack)
- **Security Control**
  - A method for removing vulnerabilities and reducing security risk

Internet Storm Survival Time Measure



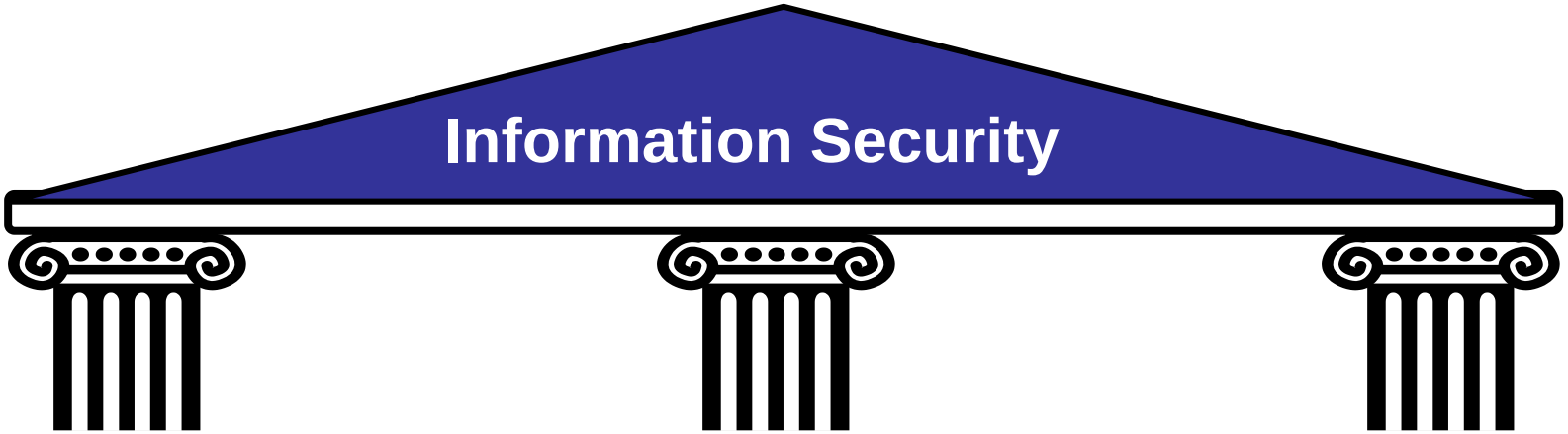
The survival time is calculated as the average time between attacks against average target IP address. https://isc.sans.edu/survivaltime.html

The Need for Information Security

- Can we remove all vulnerabilities once and for all?
- No we can't! Reasons why that's impossible:
  - Rapid innovation and new technology creates new vulnerabilities
  - Information security is (still) often ignored when developing IT
  - New threats that exploit vulnerabilities are invented every day
  - More effective attack technique and tools are being developed
  - Increased value of online digital assets makes attacks more attractive

- Conclusion: Information security doesn't have a final goal, it's a continuing process

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 Controls by 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

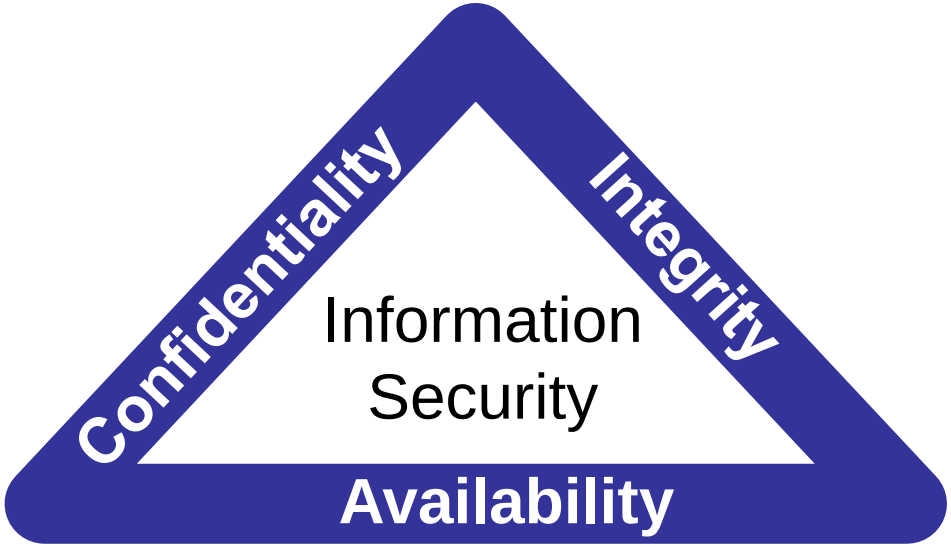
  - During transmission
    - Physical or electronic

  - During processing (use)
    - Physical or electronic

- Security controls for all information states are needed

Security Services and Goals

- A security service supports a general security goal
- The traditional definition of information security is to ensure the three CIA security services/goals for data and systems:
  - **Confidentiality**:
  - **Integrity**
  - **Availability**:



- CIA are the three main security services and goals
- Data privacy is an additional goal which relies on CIA
  - **Privacy**:

Data Privacy

Security Services and Controls

- Security services (aka. security goals or properties) are
  - implementation independent
  - supported by specific controls
- Security controls (aka. mechanisms) are
  - 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 (Security Service/Goal)

- 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 (Security Service/Goal)

- **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 (Security Service/Goal)

- 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

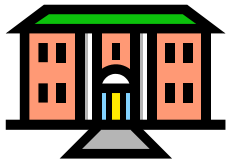
To protect specific aspects of information that may be related to natural persons (personal information).

- 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
- 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 “Personopplysningsloven” on 20 July 2018.

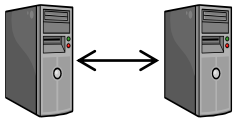
Authenticity (Security Service/Goal)

The CIA services/goals are quite general.
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.



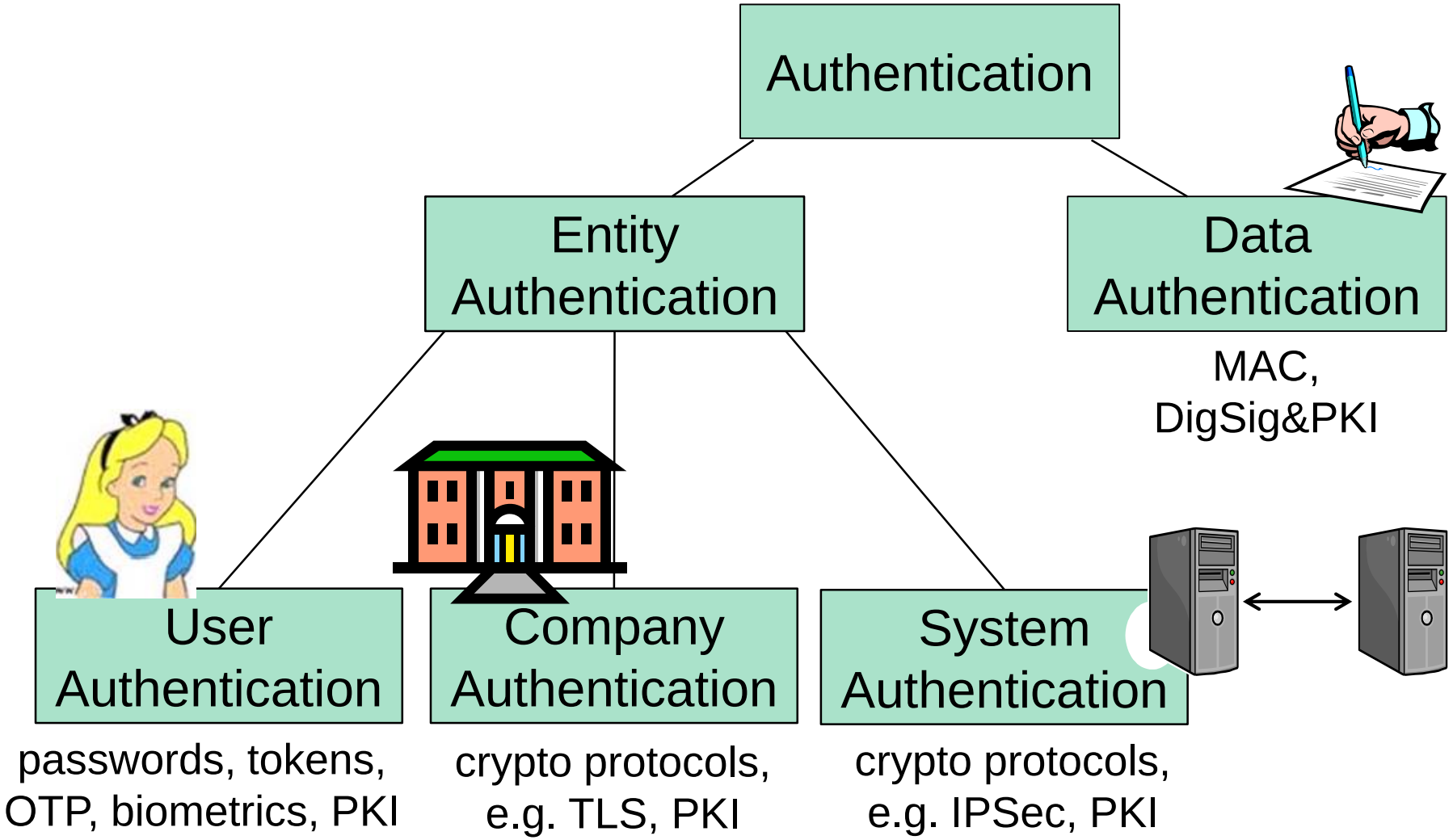
- Organisation authentication:
  - The process of verifying a claimed identity of a (legal) organisation in an online interaction/session



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

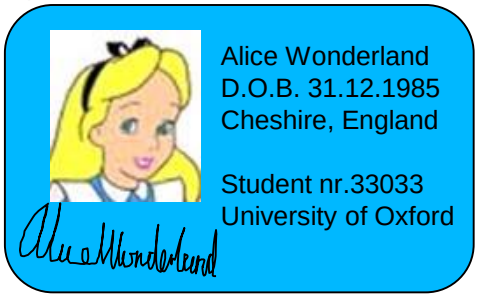
- Data origin authentication (message authentication):
  - The corroboration (verification) that the source of data received is as claimed (X.800).

Taxonomy of Authentication



User Identification and Authentication

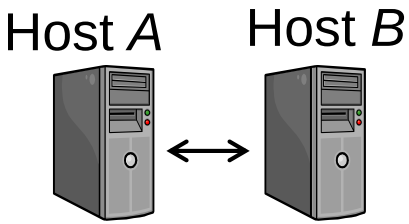
- Identification
  - Who you claim to be
  - Method: (user)name, biometrics
- User authentication
  - Prove that you are the one you claim to be
- Main threat: Spoofed identity and false login
- Controls:
  - *Passwords,*
  - *Personal cryptographic tokens*,
    - OTP generators, etc.
  - *Biometrics*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



Authentication token

System/Company 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)

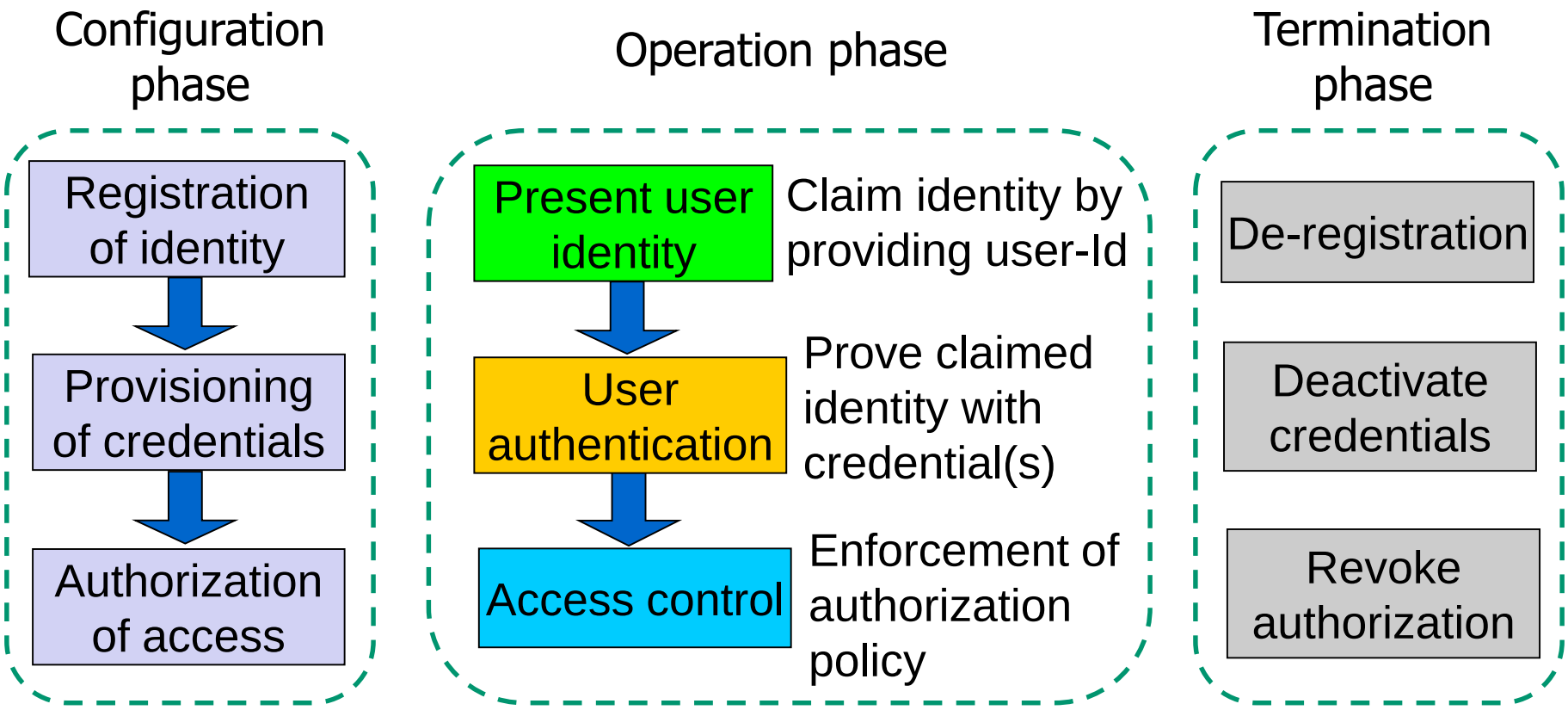
- Goal: Trace action to a specific user and hold them responsible
  - *Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party*

    (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*

Access Authorization

- Access Authorization is to specify access and usage permissions for entities, roles or processes
  - Authorization policy is 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

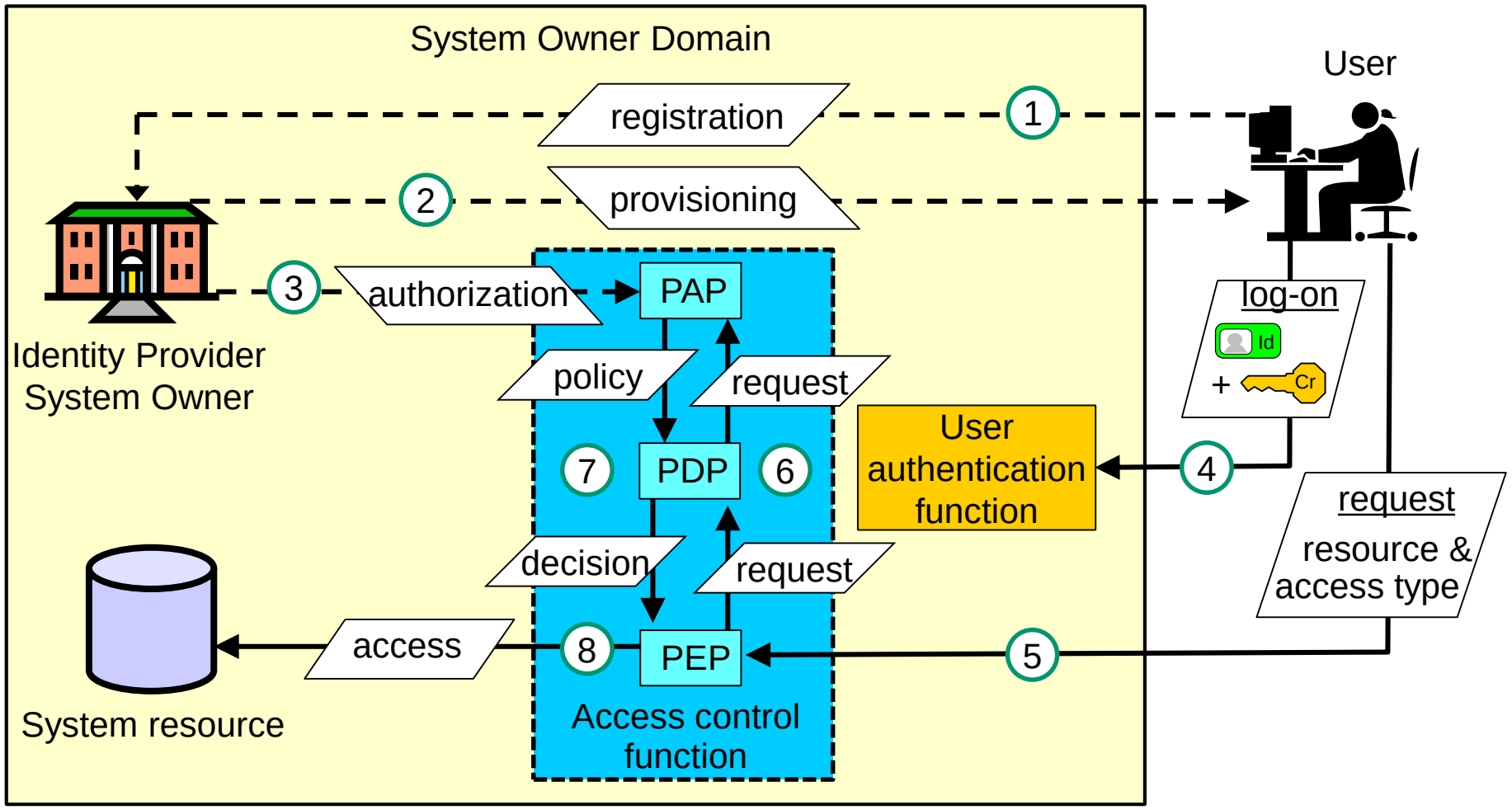
Identity and Access Management (IAM) Phases



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.733 in Harris 8th ed.
  - Common error in text books and specifications (RFC 2196 …)
  - E.g. Cisco AAA (Authentication, Authorization and Accounting)
- Wrong use of “authorization” gives meaningless security:
  1. You steal 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 book 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 Scenario



PAP: Policy Administration Point

PDP: Policy Decision Point

PEP: Policy Enforcement Point

IdP: Identity Provider

Configuration

Operation