Data Security

Content of the Course

1st week: Information security foundation, theories and future vision.

2nd – 3rd week: Introduction to information security technique

4th – 5th week: Symmetric ciphers

6th – 7th week: Block ciphers and the Data Encryption Standard

8th week: Confidentiality using symmetric encryption

9th week: Midterm exam

10th – 12th week: Public key encryption and hash function

13th – 15th week: Network security application

16th week: Final exam

Course Learning Outcome

1. **Remembering** and **Understanding** the information security foundation and readiness of developing countries to accept security technologies.
2. **Remembering**, **Understanding**, **Applying**, **Analyzing** and **Evaluating** techniques and technologies to preserve the security in the system based on the use cases, environments, regulation and agreement.

Biography of the lecturer

- **Name**: TITH Dara
- **Latest degree**: Doctor of Engineering of Information and Communication at Tokyo Institute of Technology
- **Doctoral research theme**: “Data Sharing and Consent Management of Electronic Health Record based on the Blockchain Technology”, ***Information security and Application design***
- **Master research theme**: “Predicting methods: predicting access goal based on user’s access history”, ***Information security and Data mining***

Introduction to Information Security Foundations, Theories and Future Visions

Content

1. Introduction
2. Defining the problem
3. Security threats and protection
4. Appreciating the breadth of information security
5. Conclusion

1. Introduction

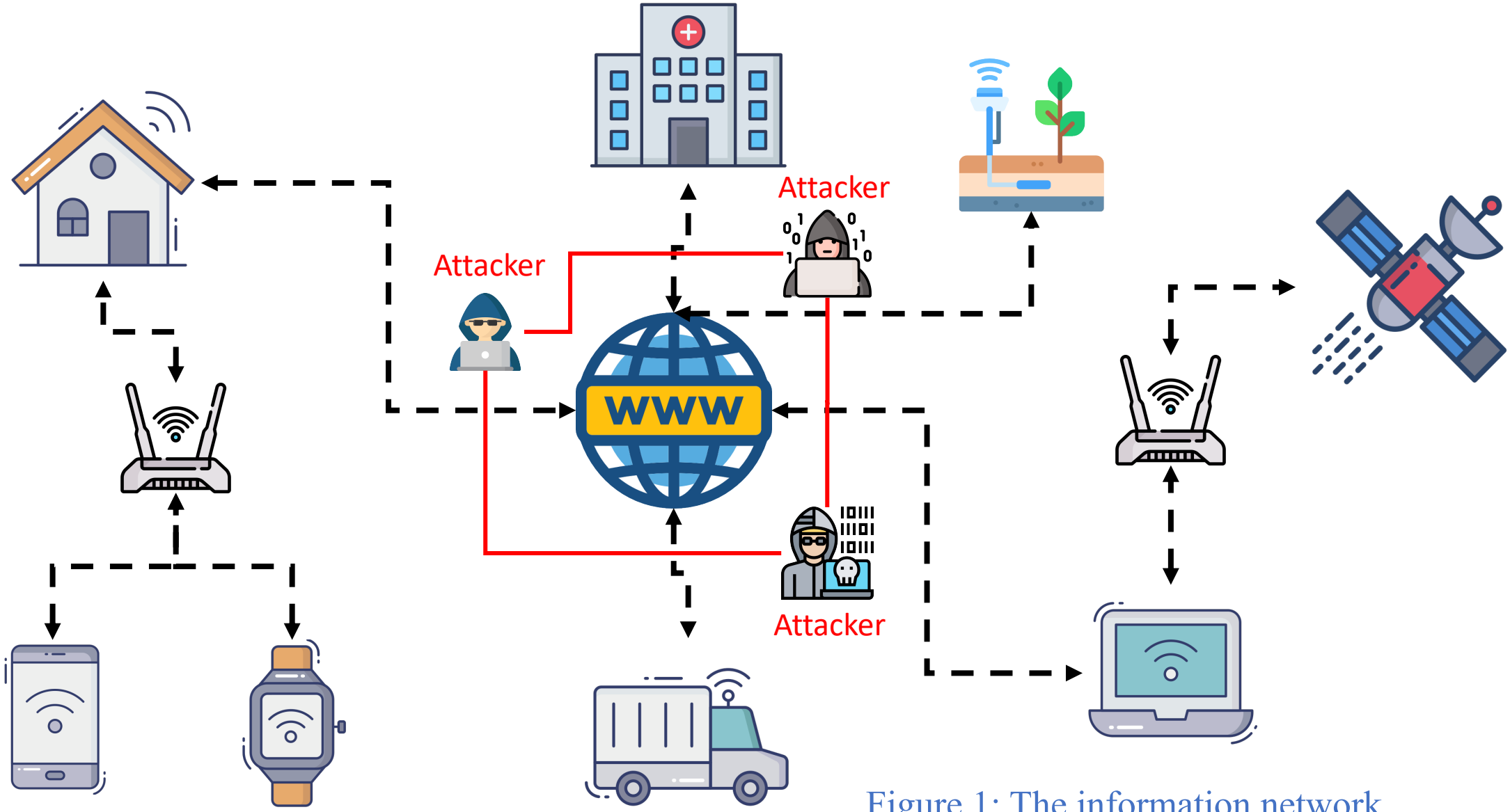


Figure 1: The information network

2. Defining the problem

- Based on the Oxford dictionary, "***Cyber***" refers to relating to electronic communication networks and virtual reality.
- Based on the Oxford dictionary, ***"Security"*** refers to the state of being free from danger or threat.

- **Cyber Security** or **Cybersecurity** (The US naming convention): is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

International Telecommunication Union

ITU-T X.1205, Overview of Cybersecurity, 2008

2. Defining the problem (Cont.)

- **Cybersecurity**: The process of protecting information by preventing, detecting, and responding to attacks.

National Institute of Standards and Technology (USA)

Framework for Improving Critical Infrastructure Cybersecurity, 2014

- **Information assurance**: Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include provision for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Committee on National Security Systems (USA)

National Information Assurance Glossary, 2010

2. Defining the problem (Cont.)

- **Information security**: Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

International Organization for Standardization

ISO/IEC 27000 – Overview and Vocabulary, 2016

- **Security of network and information systems**: The ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.

European Union

Directive on Security of Network and Information Systems, 2016

2. Defining the problem (Cont.)

- In considering these definition, it is relevant to what they want to account.
- The National Institute of Standards and Technology (NIST) definition, we can see that cybersecurity is specifically defined in terms of ‘protecting information’, and so infosec would clearly work as a synonym here.

So, is cybersecurity really something different?

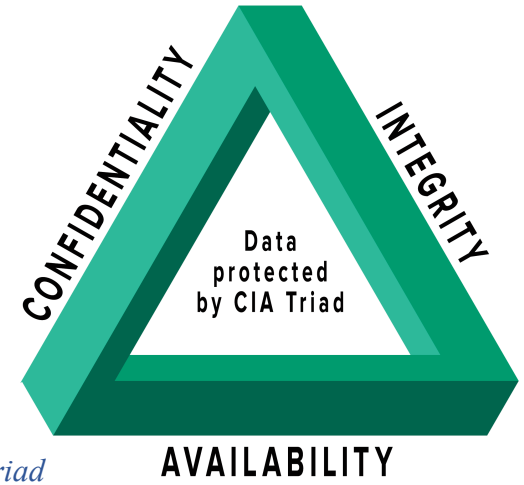
Free icon from : www.flaticon.com

2. Defining the problem (Cont.)

- To build the information system, it has to follow the fundamental of security technique which is called *CIA Triad*.

i. What is CIA Triad?

- These three principles form the cornerstone of any organization's security infrastructure; in fact, they (should) function as goals and objectives for every security program.
- *CIA Triad* refers to ***Confidentiality***, ***Integrity*** and ***Availability***.

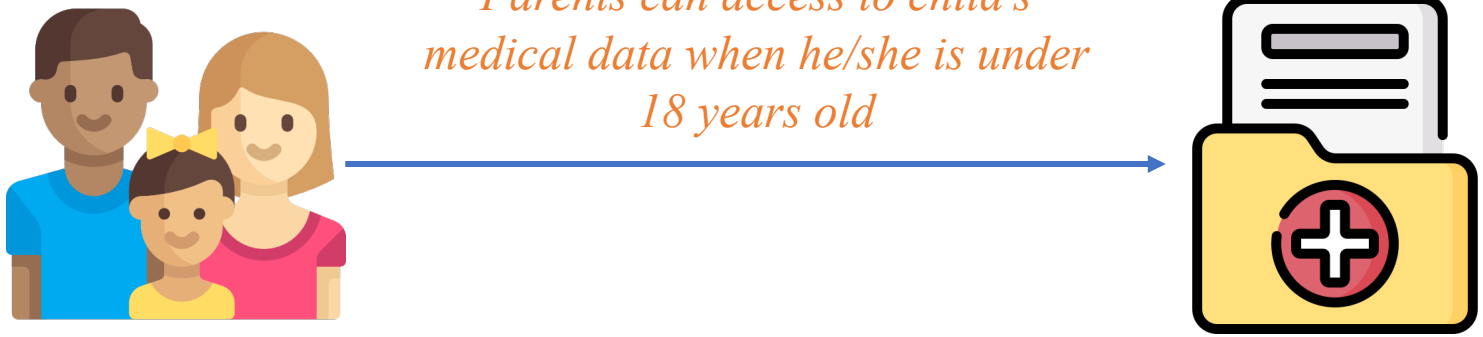


https://www.f5.com/labs/articles/education/what-is-the-cia-triad

2. Defining the problem (Cont.)

I choose to explain the definition of these three principles based on the ISO definition rather than from NIST definition.

- **Confidentiality**: Property that information is not made available or disclosed to unauthorized individuals, entities or processes. To say it shortly "to make data private or secret".



Free icon from : www.flaticon.com

2. Defining the problem (Cont.)

- **Integrity**: Property of accuracy and completeness.

After reaching the agreement, members in the group sign on the agreement documents then copy it to all members for securing the integrity of the information.

2. Defining the problem (Cont.)

- **Availability**: Property of being accessible and usable upon demand by an authorized entity.

A nurse can access to her patient's medical data for any situations 24h/day.

2. Defining the problem (Cont.)

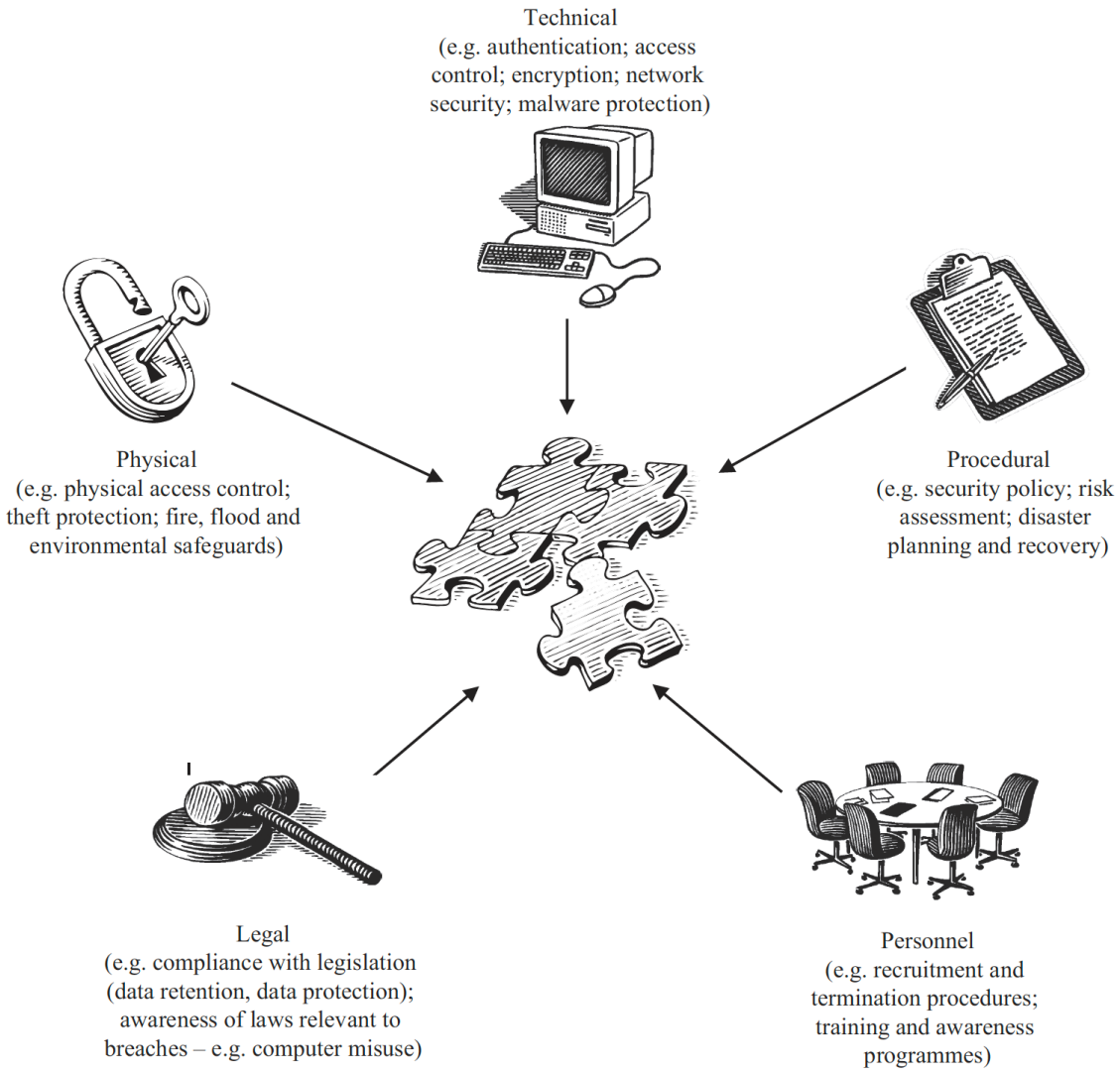


Figure 2: Elements of information security puzzle

3. Security threats and protection

- ***Threats*** are basically anything that can go wrong in order to violate the principles of security.
- During 1980s, the threats to IT system are categorised very few. For instance, the reporting categories in the UK Audit Commission's Computer Fraud Survey in 1981, it had only two categories of related incident: fraud and theft.
- Until 2005, categories of related incident are increased : accessing pornographic/inappropriate material; hacking; invasion of privacy; sabotage; use of unlicensed software and virus/denial of service [1].

[1] Audit Commission. ICT fraud and abuse 2004 – An Update to Yourbusiness@ risk. Public Sector Update. June 2005. ISBN 186240 507 7.

3. Security threats and protection

- The impacts on the data can be of four types [2]:
  - disclosure – data is disclosed to an unauthorized party;
  - denial of access – data, or a system containing it, becomes unavailable;
  - modification – data is changed as a result of the breach;
  - destruction – data is lost as a result of the breach.

[2] Maguire S. 'Identifying risks during information system development: managing the process'. Information Management & Computer Security. 2002;10(3): 126–134.

3. Security threats and protection

- Consequences of the ***Threat*** on the data:
  - disclosure of commercial information/breach of commercial confidentiality;
  - infringement of personal privacy;
  - embarrassment, loss of reputation or goodwill;
  - disruption to activities;
  - financial loss;
  - failure to meet legal obligations;
  - danger to personal safety.

3. Security threats and protection

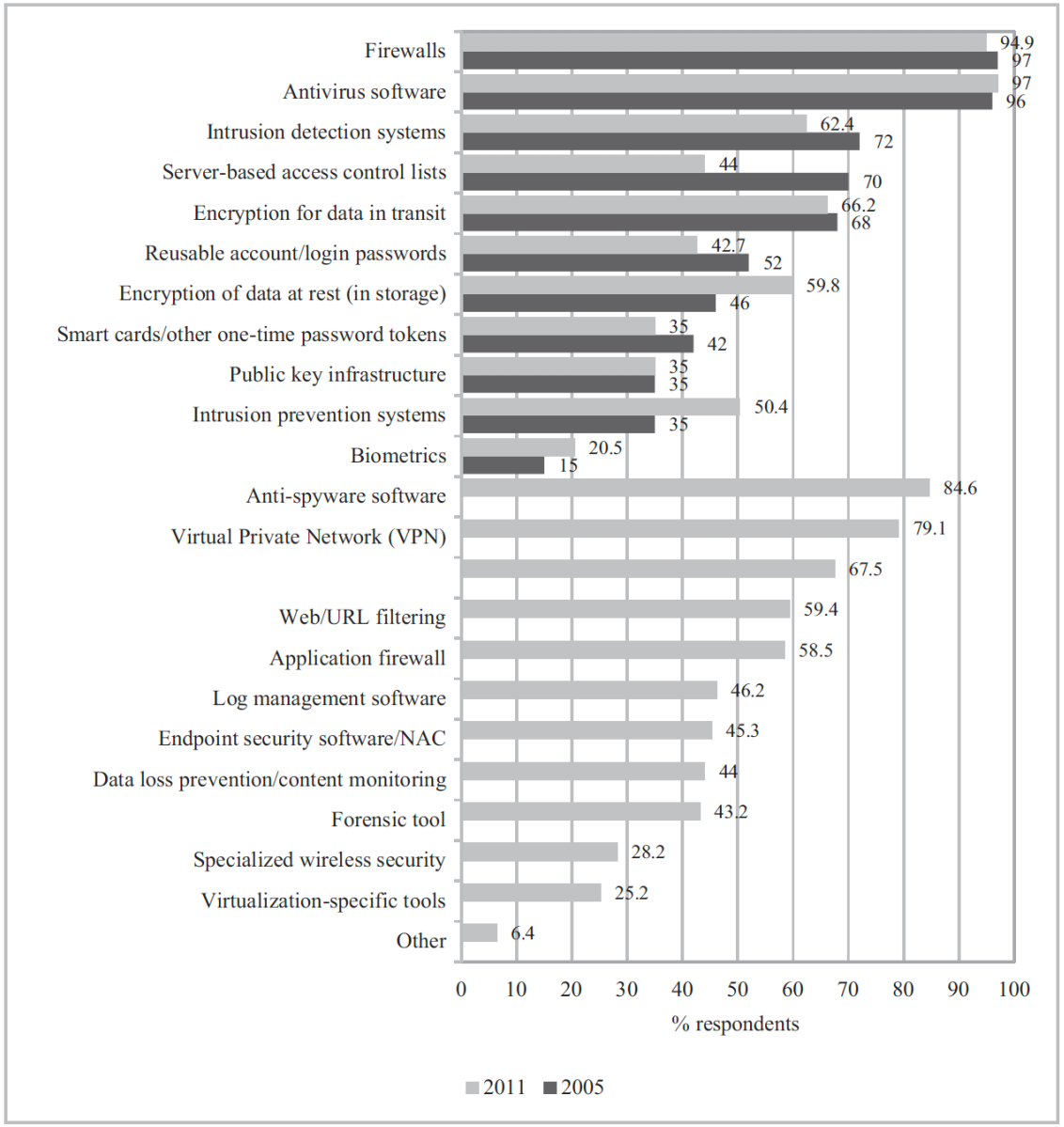


Figure 3: Evolving use of security technologies
Source: CSI Surveys.

3. Security threats and protection

Issue	Users should understand …	Users should be able to …
Authentication	The role of authentication in preventing unauthorised access	Choose and use suitable passwords, and then follow good practice in terms of managing them
Backup	The risks to systems and devices that may result in data loss, and the impact that such a loss may have for them	Utilise appropriate means to backup their data and devices, and appreciate the need for these to be stored away from the original copies
Malware protection	The potential impacts of malware and the possible routes for infection	Check that appropriate antivirus protection is installed and enabled
Mobile devices	The risks that devices can face from both technical threats and the physical environment	Employ available features for security and privacy, and take appropriate precautions to safeguard devices when on the move
Privacy and data leakage	The sensitivity of different types of data, and the ways in which they could be misused (e.g. to support identity theft)	Configure privacy and access settings in contexts where personal data may be most readily shared (e.g. in social networks, between apps or within cloud services), and make informed decisions about what to divulge
Safe Internet access and web browsing	The existence of threats such as phishing, malicious sites and unsafe downloads	How to spot the signs of scams and social engineering, alongside recognising the indicators that denote security and trustworthiness
Secure networking	The risks posed by using unprotected or unknown networks	Ensure that their own networks are protected and make informed decisions about when it is safe to connect to others
Software updates	The reason why software updates are released and the importance of patching vulnerabilities	Configure the system to handle updates in the most appropriate manner

Figure 4: Examples of baseline security literacy for end-users

4. Appreciating the breadth of information security

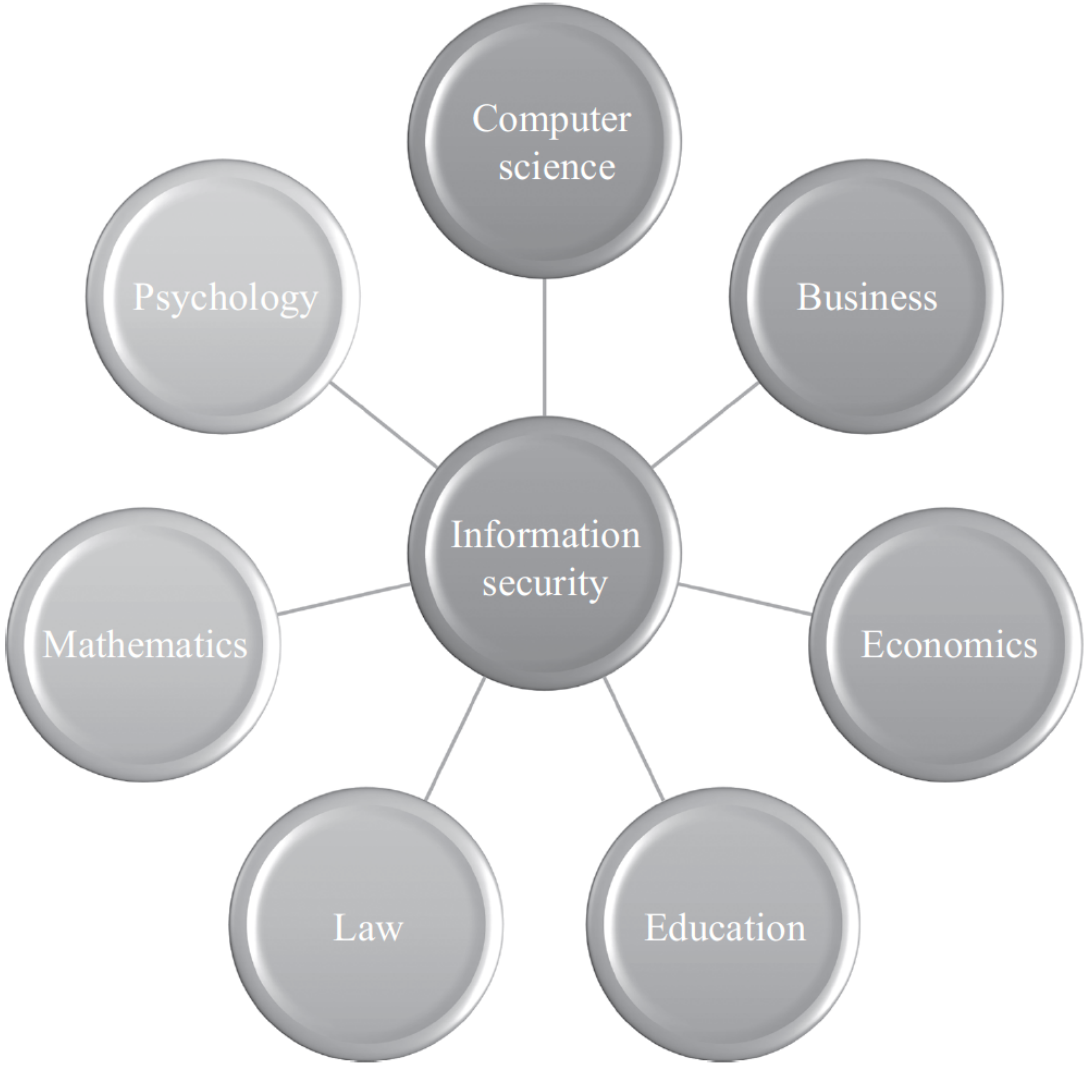


Figure 5: Disciplines contributing to information security

4. Appreciating the breadth of information security

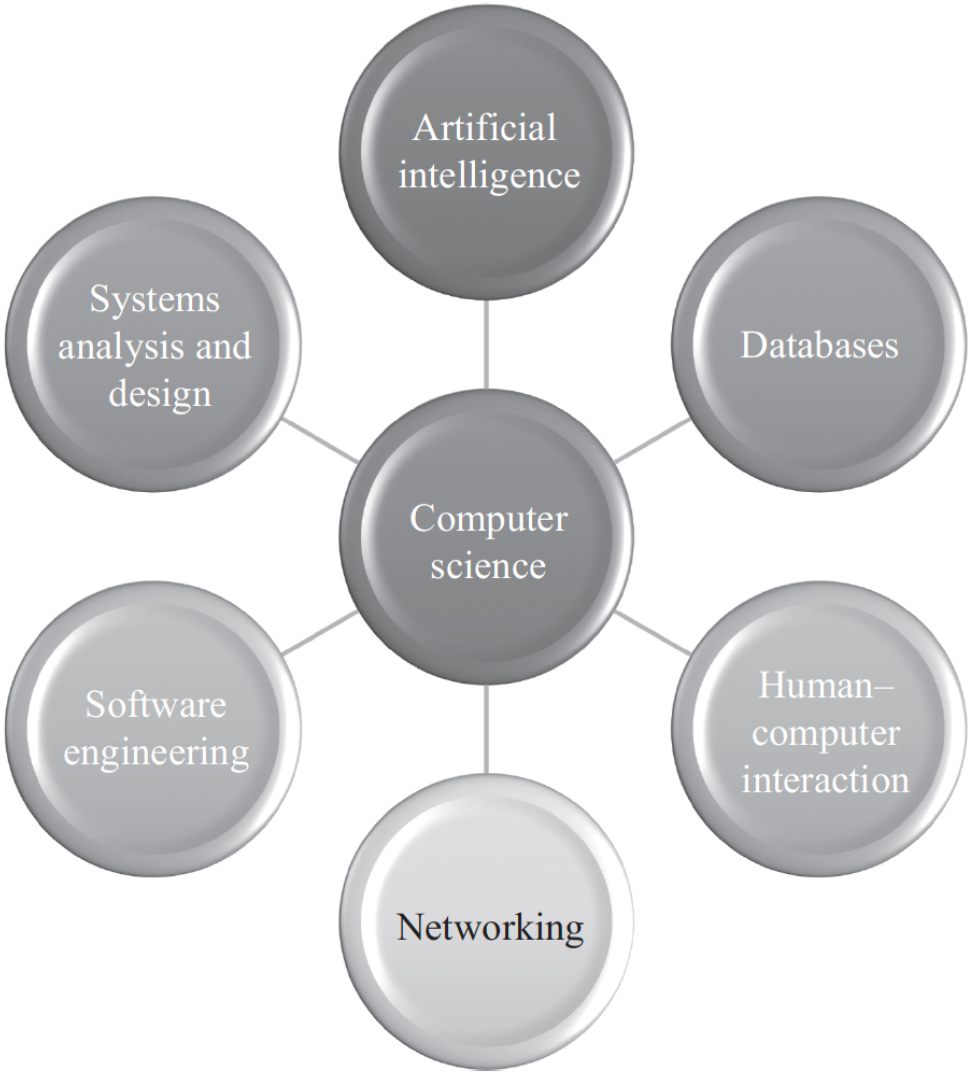


Figure 6: Security-related aspects of computer science

5. Conclusion

- The scope of security changes as the technology changes
- As computing has evolved from mainframes, through PCs and mobile devices, to the Cloud and the Internet of Things, all have required security in some way.

Reference

"Information Security: Foundations, technologies and applications", Edited by Ali Ismail Awad and Michael Fairhurst