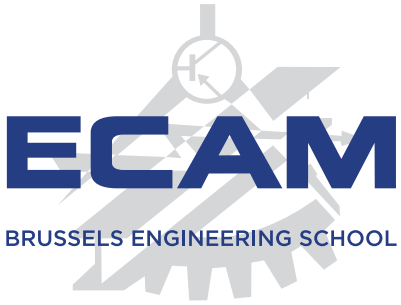


I5020 Computer Security

Session 1

Introduction to Computer Security

Sébastien Combéfis

Fall 2019

Objectives

- Computer security concepts and vocabulary
  - Main concepts in computer security
  - Principles and design requirements of a secure system
  - Attacks and security strategies
- Components and systems to secure

  Quick overview of parts to secure in a computer system
- How to analyse the security of a computer system

  Security agency, security audit of a computer system, and tools

Computer Security

Goal

- Measures implemented to reduce vulnerability

  Against accidental or intentional threats

- Requirements must be enforced on the system
  - On physical infrastructure *(machine, room...)*
  - On software *(update, security patch...)*
  - On architecture *(standard...)*
  - On user *(password, training...)*

Raised Questions

1. What are the assets that need to be protected?

   Hardware, software, documentation, license, access...

2. What are the threats to those assets?

   Attack, theft, falsification, misappropriation...

3. What can be done to counter those threats?

   Protection, authentication, encryption...

Definition

- National Institute of Standards and Technology (NIST)

  Promotes the economy by developing technologies/standards

- One possible definition of computer security of a system

  "The protection of information and systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide ***integrity, availability, and confidentiality****."*

Key Objectives

- Three objectives at the heart of computer security
  - **Confidentiality** covers data confidentiality and privacy
  - **Integrity** relates to data and system integrity
  - **Availability** ensures that the system works promptly
- Provide a guarantees pack for authorised users

  Possibility to access, to read and modify the data
- CIA triad embodies the fundamental security objectives

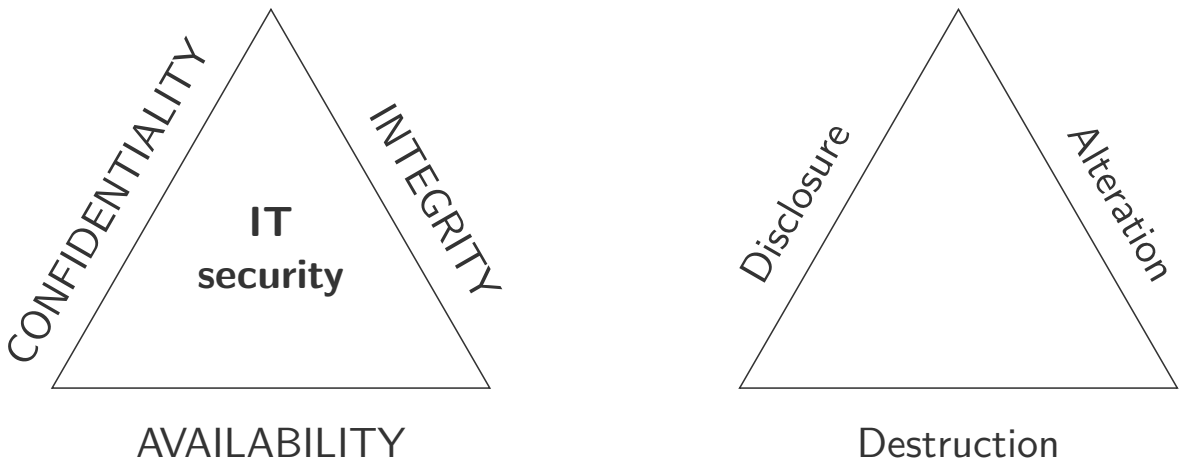
  For both data and for information and computing services

CIA Triad

- Right mix of CIA for an organisation is a balancing art

  Finding the right balance between security and usability

- Considering the CIA versus DAD opposition



Confidentiality

- Data confidentiality and privacy must be ensured
  - Private/confidential information not made available/disclosed
  - Users control collected, stored and disclosed information
- **Requirements**
  - Authorised restrictions on access and disclosure of information
  - Mean to protect personal privacy and proprietary information
- **In case of loss**

  Unauthorised disclosure of information

APPS MOBILE TECH

Twitter advising all 330 million users to change passwords after bug exposed them in plain text

67

There's apparently no evidence of any breach or misuse, but you should change your password anyway

By Chaim Gartenberg | @cgartenberg | May 3, 2018, 4:21pm EDT

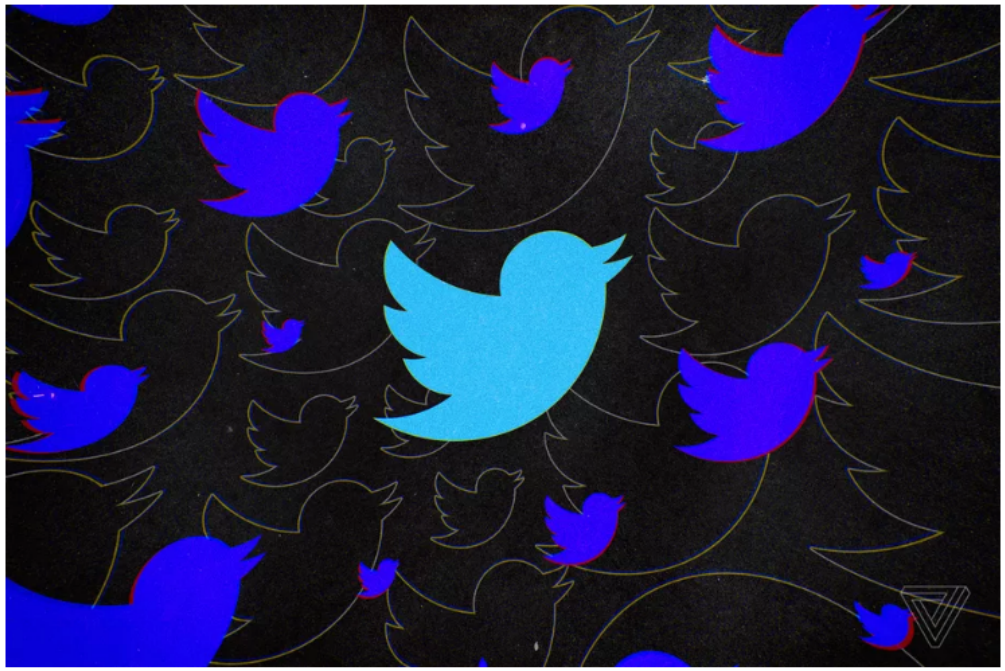


Illustration by Alex Castro / The Verge

Twitter is urging all of its more than 330 million users to immediately change their passwords after a bug exposed them in plain text. While Twitter's investigation showed that there was no evidence that any breach or misuse of the unmasked passwords occurred, the company is recommending that users change their Twitter passwords out of an "abundance of caution," both on the site itself and anywhere else they may have used that password,

Integrity

- Data Integrity and system integrity must be ensured
  - Data only changed in specified and authorised manner
  - Intended function, no unauthorised manipulation of the system
- **Requirements**
  - Guards against improper modification and destruction
  - Information nonrepudiation and authenticity
- **In case of loss**

  Unauthorised modification or destruction of information

Ransomware hits Johannesburg electricity supply

26 July 2019

The ransomware attack has affected the electricity company's ability to respond to power failures

A major electricity supplier in South Africa's largest city has suffered a ransomware attack, leaving some residents without power.

City Power revealed on Thursday that its IT systems had been shut down.

"It has encrypted all our databases, applications and network," **the company tweeted**, referring to the virus.

City Power's website remains offline and residents have reported problems via social media with their electricity supplies.

The ransomware attack initially affected customers' ability to buy pre-paid electricity and also hampered the firm's efforts to respond to localised blackouts.

Top Stories

Pelosi decries Trump 'racist attacks' on lawmaker

41 minutes ago

HK protesters defy police for second day

36 minutes ago

Kidnapped teen 'killed despite emergency calls'

27 July 2019

Features

French cyclists hit again by curse of Tour de France

How I'm helping stop Ebola from spreading

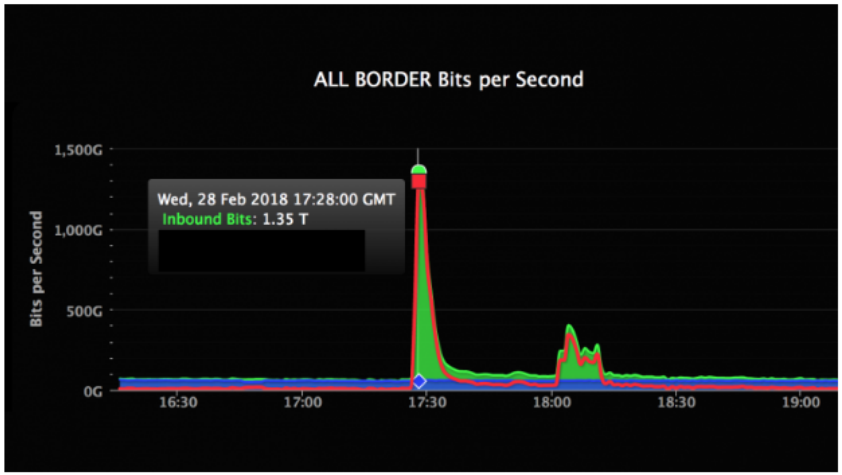
Availability

- Availability of the system and its services must be ensured
  - The system must work promptly and must respond to requests
  - Service of the system not denied to authorised users
- **Requirements**
  - Timely access to and use of information for the users
  - Reliable system and access to the system
- **In case of loss**

  Disruption of access to or use of information/system

Computing Mar 2, 2018

GitHub just suffered the world's biggest DDoS attack—and barely blinked



The site, which many developers use to store code, was knocked offline briefly this week by hackers who flooded it with fake traffic.

Terror-bytes: According to *Wired*, the attack peaked Wednesday at a whopping 1.35 terabits of data per second; the largest previous assault, launched in 2016 against a company called Dyn, hit 1.2 terabytes per second. GitHub was out of action for five minutes and suffered sporadic outages for several more.

Beware the memcrash: The attackers used "memcrashing," which involves exploiting memcache servers that companies use to speed up their web applications. Thousands of these machines have unsecured internet connections, and hackers can use them to boost fake traffic. In a blog post, GitHub said a memcache server can turn a single incoming byte into as much as 51 kilobytes aimed at a victim's servers.

Knight in shining code: Github routed its traffic flood to Prolexic, an automated anti-DDoS system run by Akamai that filtered out the attack. The whole thing was

CIAA Quartet

- Additional security objectives can be considered

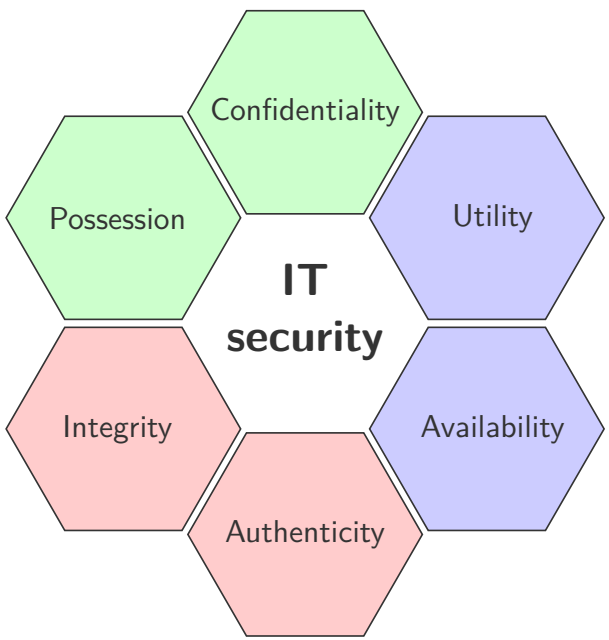
  Due to the evolution of protection goals

- CIAA model separates authenticity from integrity
  - Genuine, verifiable and trusted information/system
  - Confidence in the validity of a message (transmission)
  - Possibility to verify that users are who they say they are

Parkerian Hexad

- Three additional security attributes in the Parkerian hexad
  - **Authenticity**: veracity of claim of origin of the information
  - **Possession**: loss of control without breach of confidentiality
  - **Utility**: usefulness of the information

Controlling access



Continuity of operations

Information quality and validity

Accountability

- Accountability for traceability of actions to an entity

  Nonrepudiation, deterrence, fault isolation, intrusion detection/prevention, after-action recovery, legal action

- Being able to trace security breaches to a responsible party

  Since truly secured systems are not (yet?) an achievable goal

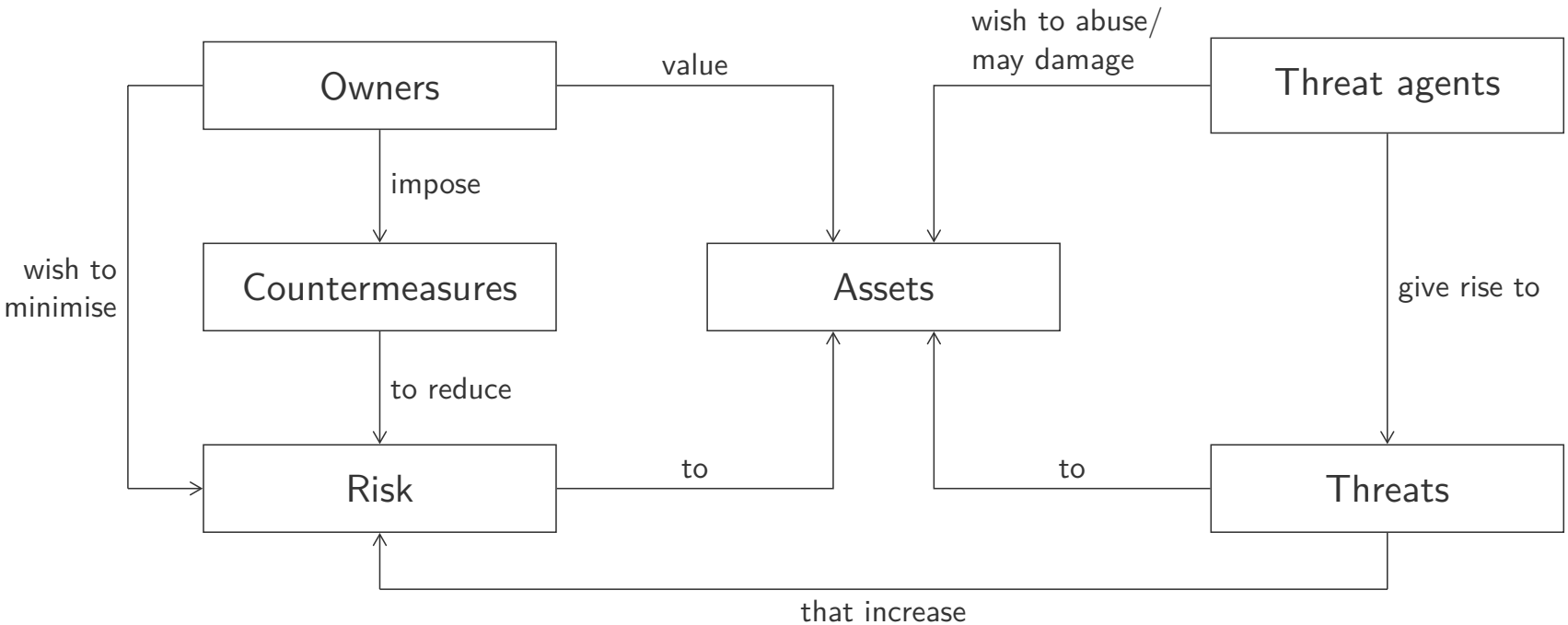
- Keep records of activity occurring on the system

  Useful for later forensics analysis, when needed

Computer Security Model

- Security concepts and relationships between them

  With the dynamic and the influence that exist



Terminology (1)

- An adversary (threat agent) attacks a system

  It can also be a threat to a system

- An attack is an assault on system security
  - Deliberate attempt that derives from an intelligent threat/act
  - Evade security services and violate security policy of a system

- A countermeasure reduces a threat, vulnerability or attack

  Can be an action, a device, a procedure or a technique

- A risk is an expectation of loss

  Probability that threat exploit a vulnerability with harmful result

Terminology (2)

- A security policy specifies/regulates security services provision

  Rules/practices to protect sensitive/critical system resources

- A system resource (asset) to be secured

  Data, service, system capability, item of equipment, facility

- A threat is a potential for violation of security

  There is a possible danger that might exploit a vulnerability

- A vulnerability is a flaw/weakness in the design of a system

  Could be exploited to violate the security policy of the system

Threat and Attack

- Four kinds of threat consequences with possible attack

  Following table built according to RFC 4949

Threat consequence	**Attack**	**CIA**
Unauthorised disclosure	■ Exposure ■ Interception ■ Inference ■ Intrusion	C
Deception	■ Masquerade ■ Falsification ■ Repudiation	I
Disruption	■ Incapacitation ■ Corruption ■ Obstruction	sI, A
Usurpation	■ Misappropriation ■ Miuse	sI

*sI: system integrity

Unauthorised Disclosure

- Unauthorised disclosure is a threat to confidentiality

  Sensitive data is made available to unauthorised entity

- Four types of attacks result in this threat consequence
  - **Exposure**: of sensitive information (deliberate/accidental)

    Student exam results posted before the deliberations
  - **Interception**: of exchanged messages during a communication

    Packets intended to another machine captured on a WLAN
  - **Inference**: of information by observing patterns of traffic

    Database information inferred with limited access
  - **Intrusion**: overcomes the access control of the system

    Unauthorised access to sensitive data gained

Deception

- Deception is a threat to data or system integrity

  False information sent to authorised entity believing they are true

- Three types of attacks result in this threat consequence
  - **Masquerade**: mimics an authorised user to gain his/her access

    Finding the logon/password of another user
  - **Falsification**: tampers/replaces valid or introduces false data

    Student alters his/her grades for some exams
  - **Repudiation**: user denies sending/receiving/possessing data

    Faking that a payment has failed

Disruption

- Disruption is a threat to availability or system integrity

  Interrupt or prevents correct operation of a system services

- Three types of attacks result in this threat consequence
  - **Incapacitation**: physical destruction or service deactivation

    Trojan disabling a system or some of its services
  - **Corruption**: modifies a system or corrupts data

    Exploiting backdoor logic illegitimate access
  - **Obstruction**: disables communication, overloads the system

    Sending spurious useless requests to a server

Usurpation

- Usurpation is a threat to system integrity

  System controlled by a unauthorised entity

- Two types of attacks result in this threat consequence
  - **Misappropriation**: theft of service

    Cryptocurrency mining in the browser with client code
  - **Misuse**: unauthorised access and security deactivation

    Malicious code or hacker gaining access to a system

Attack Surface (1)

- Exposed vulnerabilities of a system is its attack surface

  Reachable and exploitable by a threat agent

- Following examples enlarge the attack surface
  - Open ports (TCP/UPD...) with code listening on them
  - Services available on the inside of a firewall
  - Code systematically processing incoming data (email...)
  - Interfaces, SQL, web forms...
  - An employee with access to sensitive information

Attack Surface (2)

- Three categories of attack surfaces

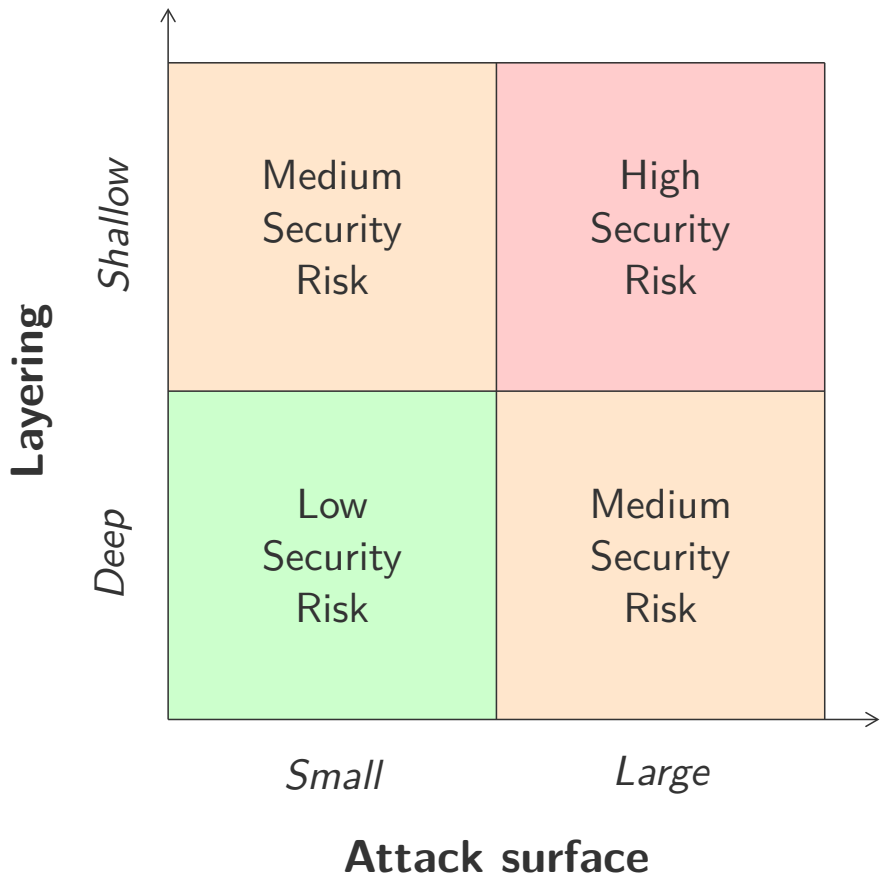
  Network, software or human surface attacks

- Attack surface analysis measures scale and severity of threats
  - Identify where security mechanisms are required
  - Think about ways to make the attack surface smaller
  - Provide guidance for testing, refactoring, maintenance

Security Risk Mitigation

- Defense in depth and attack surfaces reduction

  Best solution to mitigate security risks



Attack Tree

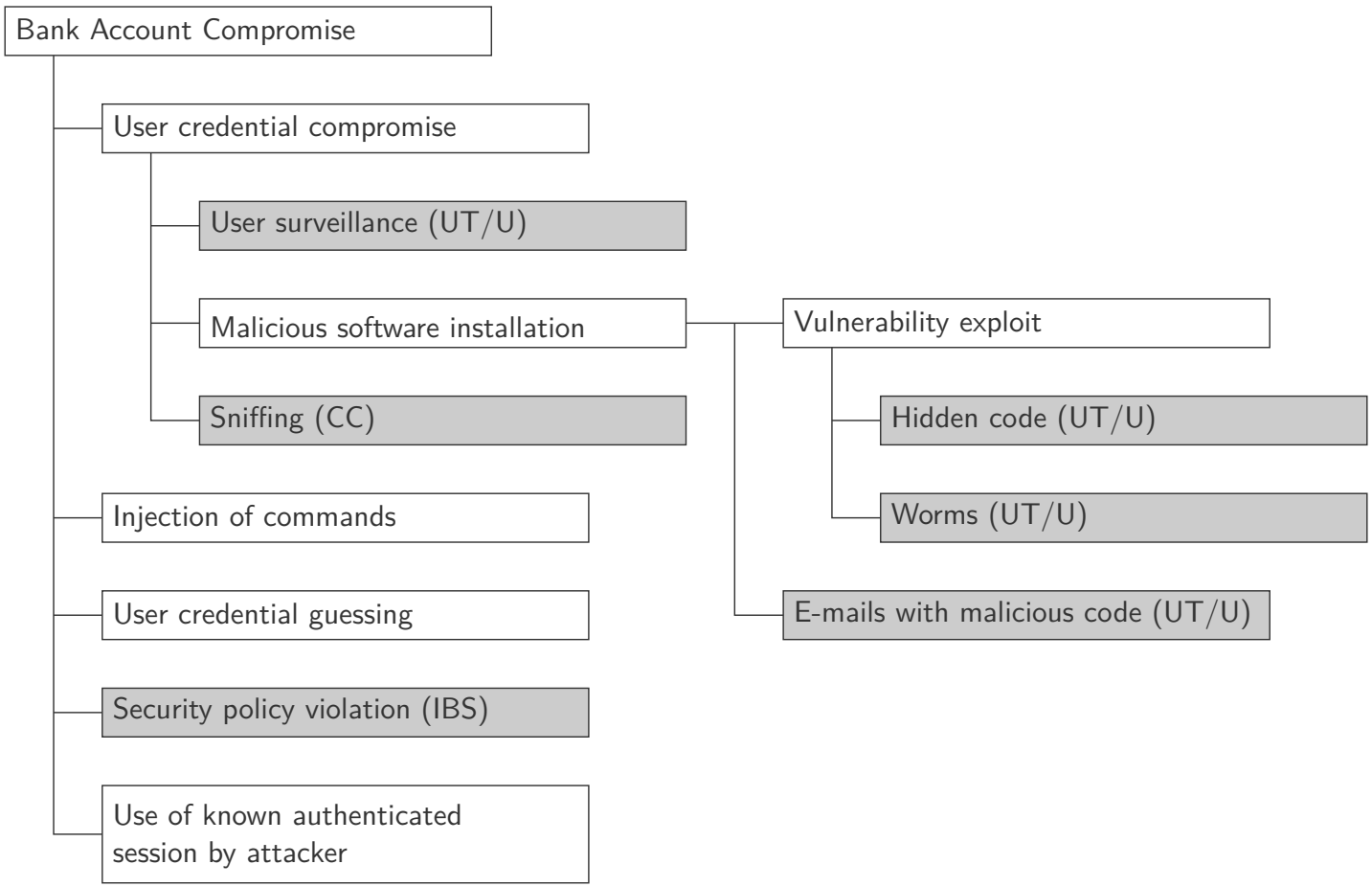
- Attack tree with set of techniques for exploiting vulnerabilities

  Branching and hierarchical data structure

- Root of the tree represents security incident goal of the attack
  - Branches represent ways an attacker can reach this goal
  - Leaves represent a mean to initiate an attack
  - Internal nodes represent subgoals (AND/OR) to achieve
- Effectively exploit information from attack patterns
  - Document security attacks in a structured form
  - Identify the key vulnerabilities of the system
  - Guide application design and choice of countermeasures

Attack Tree Example

UT/U User Terminal and User, **CC** Communication Channel, **IBS** Internet Banking Server



Components to Secure

Asset

- Users/owners want to protect the assets (system resources)

  Threats on assets increase the risk

- Four categories of assets
  - **Hardware**: data processing, storage, communication devices...
  - **Software**: operating systems, system utilities, applications...
  - **Data**: files, databases, passwords files...
  - **Network**: LAN/WAN communication links, bridges, routeurs...

Threat on Asset

- Some examples of threats on assets categorised with CIA triad

Asset	Confidentiality	Integrity	Availability
Hardware	Unencrypted USB stick stolen	Keyboard compromised with a keylogger	Equipment stolen or disabled
Software	Unauthorised copy of a program is made	Working program altered to cause it do unintended task	Program deleted
Data	Unauthorised read of data performed	New files fabricated	Files deleted
Network	Traffic pattern of messages observed	Messages modified, reordered, duplicated	Messages destroyed or deleted, communication lines destroyed

Vulnerability

- A system can suffer from vulnerabilities

  Can be exploited by threats resulting in an attack

- Three categories of vulnerabilities of an asset
  - **Corrupted**: does the wrong thing, gives wrong answers
  - **Leaky**: some information obtained without authorisation
  - **Unavailable**: makes system impossible or impractical
- Vulnerability categories correspond to the CIA triad

Attack

- Two types of attacks can be distinguished
  - **Active**: attempt to alter system resources

    Or affect the operation of those resources
  - **Passive**: attempt to learn information from the system

    Or use information without affecting any system resource
- Two origins of attacks can be identified
  - **Inside**: the security perimeter with authorised access

    System resources used in way not approved by authorisation
  - **Outside**: the perimeter by unauthorised/illegitimate user

    Amateur prankster, organised criminals, terrorist, government...

Countermeasure

- Dealing with a security attack using countermeasures
  - Preventing a particular type of attack to succeed
  - Detect the attack and then recover from its effects
- New vulnerabilities can be introduced by a countermeasure

  Residual risk introduced by countermeasures must be minimised

Risk

- Very important to have a good estimation of risks

  To propose adequate and well dimensioned countermeasure

- Main risks remain very basic

  Snatched cable, disk crash, power failure,
  expired license/certificate, wrong user profile...

- Collect information about assets and company business
  - Values of all the assets
  - Costs and delays of replacement
  - Impact on the customers to be informed about intrusions

Data

- Important to protect and secure all the data
  - Data from databases and their cache memories
  - Data coming from the outside or encoded by users
  - Authentication data provided to users
- **Solutions**
  - Complete encryption of all the data
  - Regular and secured backups
  - Duplication/replication at different geographical locations

Code and Program

- Protect and secure the programs and the software
  - Memory leaks, buffer overflow, code injection
  - Security vulnerabilities, deprecated dependencies
- **Solutions**
  - Secure programming and good practices
  - Verification of all the input user data
  - Update, security patch application

Operating System

- Protect and secure the operating system
  - Deprecated version, security vulnerabilities
  - User, permissions and installed programs management
  - Protections with respect to the environment
- **Solutions**
  - Update, security patch application
  - Creation of strong passwords, changed regularly
  - Anti-virus, firewalls... installation

User

- Protect and secure the users
  - Misuse of softwares or unauthorised use
  - Leaks and data disclosure
  - Malware introduction (BYOD)
- **Solutions**
  - Training and security awareness
  - Secured and controlled access to data and network
  - Authentication with strong password, changed regularly

Machine

- Protect and secure the machines
  - Malicious use of a machine and exploitation
  - Crash and hardware failure
- **Solutions**
  - Protect physical and remote access to machines
  - Provide physical redundancy
  - Watchdog and monitoring of the computer park

Network

- Protect and secure the network
  - Use of the internal network and internet access
  - Remote access to the internal network
  - Data and information exchanged in the network
- **Solutions**
  - Protect the network from the outside (firewall, IDS...)
  - Hardware and firmware update


Security Analysis

Security Functional Requirements

- Countermeasures seen as security functional requirements

  To be integrated in the specifications in analysis phase

- FIPS 200 classification enumerates 17 security-related areas

  To protect CIA of information systems

1. Access Control
2. Awareness and Training
3. Audit and Accountability
4. Certification, Accreditation, and Security Assessments
5. Configuration Management
6. Contingency Planning
7. Identification and Authentication
8. Incident Report
9. Maintenance
10. Media Protection
11. Physical and Environmental Protection
12. Planning
13. Personnel Security
14. Risk Assessment
15. Systems and Services Acquisition
16. System and Communications Protection
17. System and Information Integrity

Security Design Principles (1)

- Widely agreed design principles guiding development

  To have the best possible protection mechanisms

- Impossible to systematically exclude security flaws

  Nor to prevent unauthorised actions/access to a system

- Eight design principles for protection mechanisms

  1. **Economy of mechanism**

     Simple and small designs for security measures

  2. **Fail-Safe defaults**

     Access decision based on permission rather than exclusion

  3. **Complete mediation**

     Every access checked against access control mechanism

Security Design Principles (2)

- Eight design principles for protection mechanisms

4. **Open design**

   Design of security mechanism open rather than secret

5. **Separation of privilege**

   Multiple privilege attributes required to access resource

6. **Least privilege**

   Every process/user operate with least set of necessary privileges

7. **Least common mechanism**

   Minimise functions shared by different users

8. **Psychological acceptability**

   Security mechanism should not interfere with work of users

Security Design Principles (3)

- Five design principles closer to the code

1. **Isolation**
   - Public access system isolated from critical resources
   - Separate processes and files of different users
   - Security mechanisms must be isolated from other parts
2. **Encapsulation**

   Procedure and data encapsulated in a domain of its own
3. **Modularity**

   Security functions developed as separate, protected modules
4. **Layering**

   Multiple, overlapping protection approaches (defense in depth)
5. **Least astonishment**

   Program should always respond to not astonish the user

Risk Analysis

- High cost to ensure the security of a computer system

  Very important to carry out a risk analysis

- Establishing a coherent security policy

  Set of solutions to mitigate the risks

- Accepting some risk tolerance

  Relative to the risks and the acceptable costs

Impact Levels

- Measuring the impact of the presence of a security breach

  Can be useful to determine the means to implement

- FIPS 199 defines three levels of impact

  Effect on organisational operations, assets or individuals

Level of impact	**Low**	**Moderate**	**High**
Adverse effect	Limited	Serious	Severe or catastrophic
Primary function reduction	Noticeably	Significantly	Completely
Assets damage	Minor	Significant	Major
Financial loss	Minor	Significant	Major
Harm	Minor	Significant	Severe or catastrophic
Injuries	–	Small	Serious life-threatening
Loss of life	No	No	Yes

Security Policy (1)

- Security is like a chain, with a weak link

  Need to maximise the security of the weakest link

- Strong requirement to train and educate the users

- Several parts to define a security policy

  - **Hardware failure**: due to wear, aging, defect...

    Purchase with guarantees, technical support, renewal

  - **Software failure**: due to bugs, security vulnerabilities...

    Copy information, update, security patch

  - **Accidents**: breakdown, flood, fire...

    Data backup, redundancy, backup site

Security Policy (2)

- Several parts to define a security policy
  - **Human error**: wrong manipulation, configuration...

    Security copy, training
  - **Theft**: physical, burglary...

    Access control to equipments
  - **Hacking**: intrusion on the network...

    Firewall, access control, closed network
- Measures to be taken in accordance with the law

  For filtering and network data analysis, for example

Security Policy Development

- Can be as simple as an informal description

  Defining the desired behaviour of the system

- Or a formal statement of rules and practices to follow

  Specify/regulate how the system provide security services

- Two trade-offs to take into account
  - Compromise between ease of use versus security
  - Ratio between cost of security and cost of failure and recovery

- Security policy is a business decision, at the end

Security Implementation

- Chosen security policy must be implemented in the company
- Four complementary courses of action
  - **Prevention** to avoid any attack to succeed
  - **Detection** that something bad happened or is happening
  - **Response** to an attack to halt it and limit damages
  - **Recovery** to go back to a prior correct state
- Evaluate security implementation regarding the policy

  To check whether if really work and fulfils the requirements

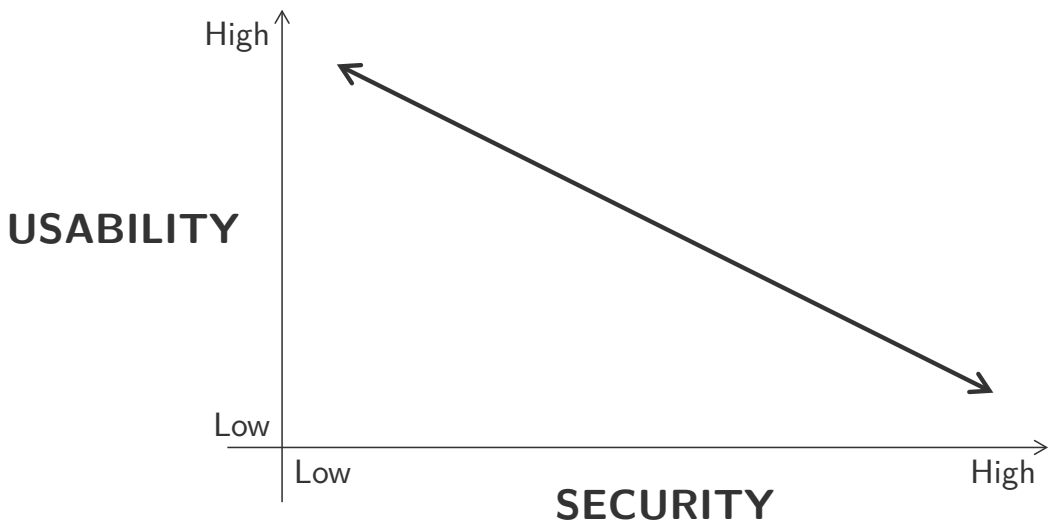
Security versus Usability

- Security and usability tend to be inversely related

  Generally not possible to achieve high level for both

- Good compromise to find depending on the application

  Mainly based on risks, risk tolerance and expected users



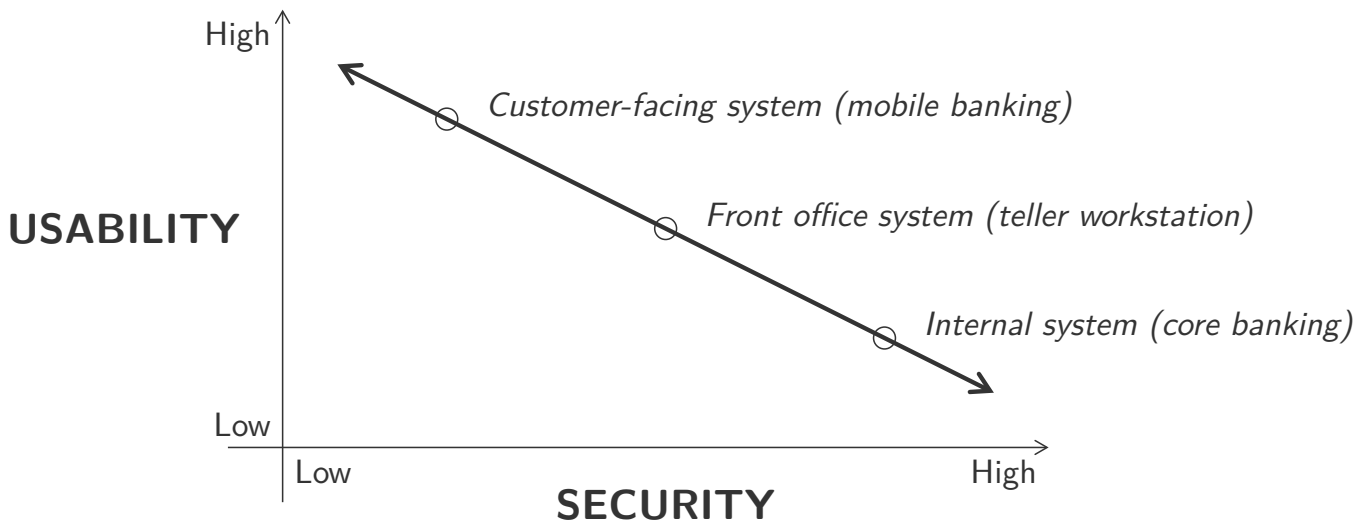
Security versus Usability

- Security and usability tend to be inversely related

  Generally not possible to achieve high level for both

- Good compromise to find depending on the application

  Mainly based on risks, risk tolerance and expected users



Security by Design

- Need to include security in all the development processes

  Best practices now built-in to organisation processes and culture

- Security by design for software and hardware development
  - Make systems free of vulnerabilities and impervious to attack
  - Measures as continuous testing and authentication safeguards

- Possible to achieve effective and usable security
  - Security by design and not designed as add-on procedures
  - Security that integrates with how the users work
  - Encourage users to make better security choices

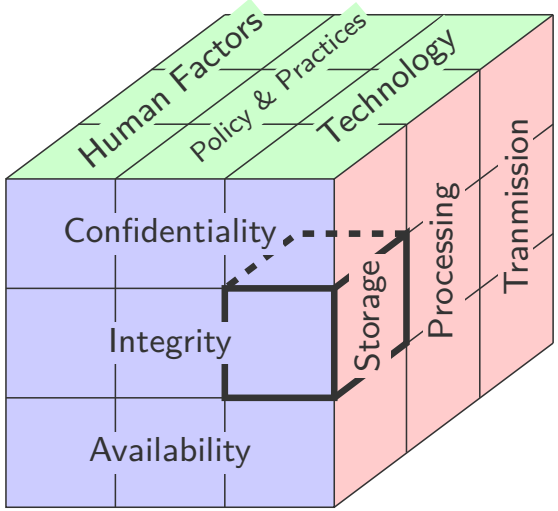
McCumber Cube

- McCumber cube framework for information assurance systems

  Establishing and evaluating information security programs

- Covers 27 areas that must be addressed

  Organised along three different axes



Use technology to protect the integrity of information while in storage.

References

- Michael Nieles, Kelley L. Dempsey, & Victoria Y. Pillitteri, *An Introduction to Information Security*, 2017, NIST Special Publication: 800-12 Rev. 1.
- NIST, *Standards for Security Categorization of Federal Information and Information Systems*, 2004, FIPS PUB 199.
- Thor Pedersen, *CISSP ? the CIA Triad and its opposites*, August 12, 2017. https://thorteaches.com/cissp-the-cia-triad-and-its-opposites
- Carsten Reffgen, *Protection Goals: CIA and CIAA*, July 25, 2018. https://www.eosgmbh.de/en/protection-goals-cia-and-ciaa
- bharat prasai, *Parkerian Hexad- Alternate perspectives of properties of Information security*, June 27, 2019. https://medium.com/@bharat.skyinfotech/parkerian-hexad-alternate-perspectives-of-properties-of-information-security-3d60fc93725d
- R. Shirey, *Internet Security Glossary, Version 2*, 2007, RFC 4949.
- Dan Schoenbaum, *What?s in a Modern Attack Surface?*, February 20, 2019. https://medium.com/@danschoenbaum/whats-in-a-modern-attack-surface-3b275be80101
- C. K. Dimitriadis, *Analyzing the Security of Internet Banking Authentication Mechanisms*, 2007, Information Systems Control Journal, 3:34–41.
- NIST, *Minimum Security Requirements for Federal Information and Information Systems*, 2006, FIPS PUB 200.
- Monique Magalhaes, *Security vs. Usability: Does there have to be a compromise?*, December 20, 2018. http://techgenix.com/security-vs-usability
- Nicole Kobie, *Balancing security and usability: it doesn?t have to be a trade-off*, July 28, 2016. https://www.telegraph.co.uk/connect/better-business/security-versus-usability-ux-debate
- Brian Jackson, *Security versus usability: overcoming the security dilemma in financial services*, October 19, 2017. https://cloudblogs.microsoft.com/industry-blog/financial-services/2017/10/19/security-versus-usability-overcoming-the-security-dilemma-in-financial-services
- Illya Golovatenko, *The Three Dimensions of the Cybersecurity Cube*, December 13, 2018. https://swansoftwaresolutions.com/the-three-dimensions-of-the-cybersecurity-cube

Credits

- Blue Coat Photos, November 21, 2014, https://www.flickr.com/photos/111692634@N04/15327725543.
- Eyrian~commonswiki, August 23, 2007, https://en.wikipedia.org/wiki/File:NIST_logo.svg.
- [Intense Potato], October 19, 2014, https://www.flickr.com/photos/73042395@N07/15579739722.
- Liz Ixer, April 14, 2012, https://www.flickr.com/photos/mrs_eds/7076795125.