BASIC NOTIONS

Introduction to Computer and Network Security

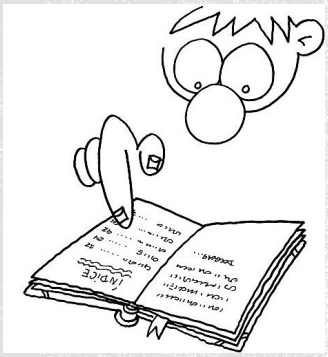
Silvio Ranise [silvio.ranise@unitn.it or *ranise@fbk.eu*]

UNIVERSITÀ DI TRENTO

FONDAZIONE BRUNO KESSLER

CONTENTS

- What is security?
  - The CIA triad
- Security policies and mechanisms / services
- Risk
  - Vulnerabilities, threats, attacks, and mitigations (security controls)
  - Likelihood and impact (w.r.t. stakeholders)
- A glimpse on security and the human factors
- Wrap-up
- Final remarks on security



1

2

THE CIA TRIAD

Characterizing security or guiding the selection and use of security controls

SECURITY PROPERTIES

- Confidentiality
  - prevent un-authorised disclosure of information
  - permit authorized sharing of information
- Integrity
  - prevent un-authorised modification of information
  - permit authorized modification of information
- Availability
  - prevent un-authorised withholding of information or services
  - readily permit authorized access to information or services

The CIA triad

3

CONFIDENTIALITY: SOME DEFS FROM NIST

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.
- The security goal that generates the requirements for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and while in transit.
- The property that sensitive information is not disclosed to unauthorized entities. In a general information security context: preserving authorized restrictions on information access and disclosure, including means for preserving personal privacy and proprietary information.

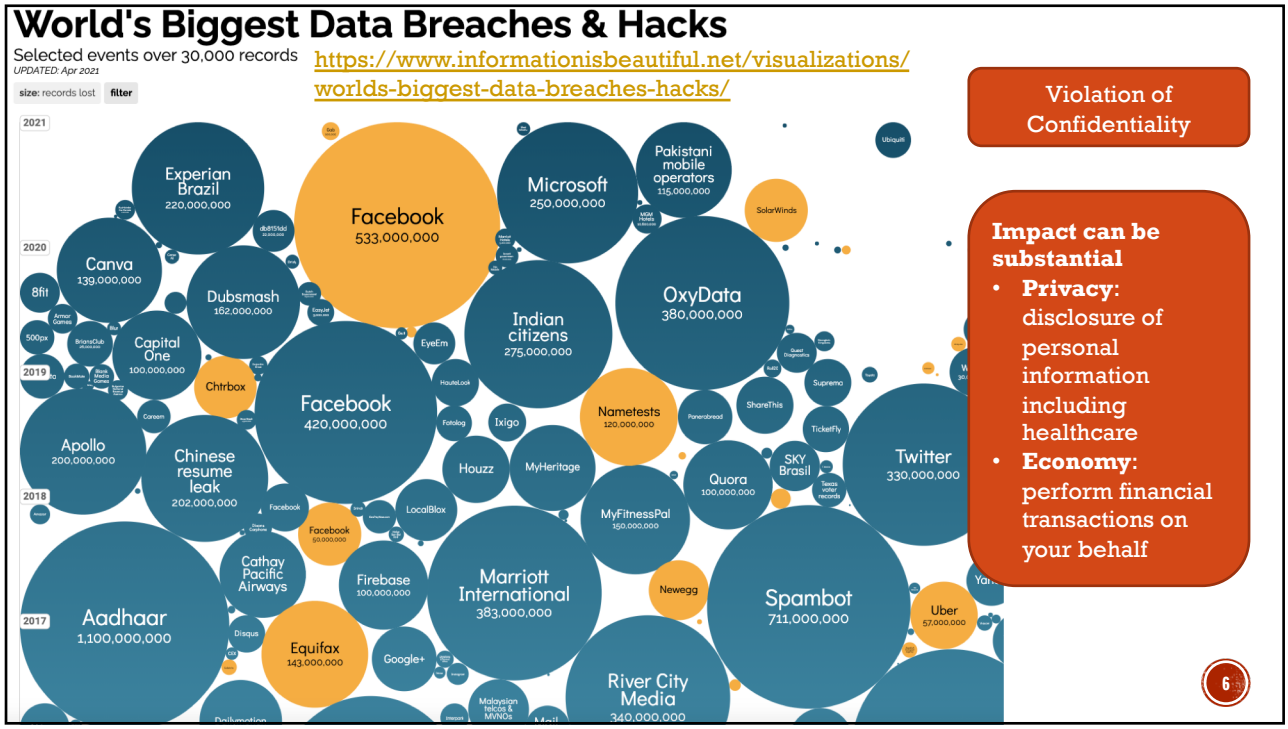
https://csrc.nist.gov/Glossary/?term=3591

4

CONFIDENTIALITY IN PRACTICE

- Unauthorized access to sensitive information could be
  - **intentional**, such as an intruder breaking into the network and reading the information
  - **unintentional**, due to the carelessness / incompetence of individuals handling the data
- How to guarantee confidentiality
  - Data **encryption** is one way to ensure confidentiality and that unauthorized users cannot retrieve data for which they do not have access
  - **Access control** is an integral part of maintaining confidentiality by managing which users have permissions for accessing data

5



INTEGRITY: SOME DEFS FROM NIST

- Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- The ability to detect even minute changes in the data.
- Ensuring the authenticity of information—that information is not altered, and that the source of the information is genuine.
- The security objective that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).

https://csrc.nist.gov/Glossary/?term=4875#AlphaIndexDiv

INTEGRITY: SOME DEFS FROM NIST

- Guarding against improper
  ensuring information non-r
- The property that sensitiv
  unauthorized and undetect
- The ability to detect even
- Ensuring the authenticity
  the source of the informati
- The security objective that
  intentional or accidental at
  has not been altered in an
  that a system has when it pe
  free from unauthorized manip

- Authenticity
  - The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
- Non-repudiation (for auditability)
  - Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

https://csrc.nist.gov/Glossary/?term=4875#AlphaIndexDiv

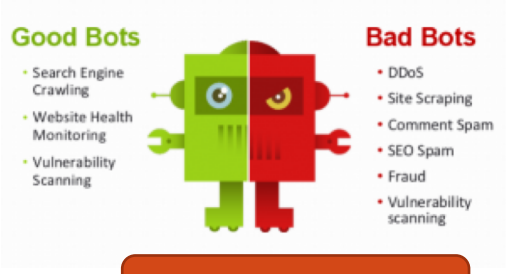
8

INTEGRITY IN PRACTICE

- Data integrity can be compromised both through
  - human errors and
  - attacks like destructive malware and ransomware
- How to guarantee integrity
  - Implementing **version control and audit trails** into an IT program will allow an organization to guarantee that its data is accurate and authentic
  - Integrity is an essential component for organizations with **compliance requirements**. For example, a condition of the compliance requirements for financial services organizations requires providing accurate and complete information to regulators

9

- Information integrity attack
  - December 2017: Federal Communication Commission's net neutrality comment form witnessed a miracle… **the dead returning to life**
  - 2 millions identical comments under the name and address of real people… were generated by bots
  - This activity was spotted because users reported that some of the names belonged to their deceased family members and friends!



Violation of Integrity

Impact is on **trustworthiness** of resources and services available online… bots can influence social media by massive posting of messages carrying manipulated information with a negative impact on social/democratic life

https://www.darkreading.com/vulnerabilities---threats/why-information-integrity-attacks-pose-new-security-challenges/a/d-id/1331562

AVAILABILITY: SOME DEFS FROM NIST

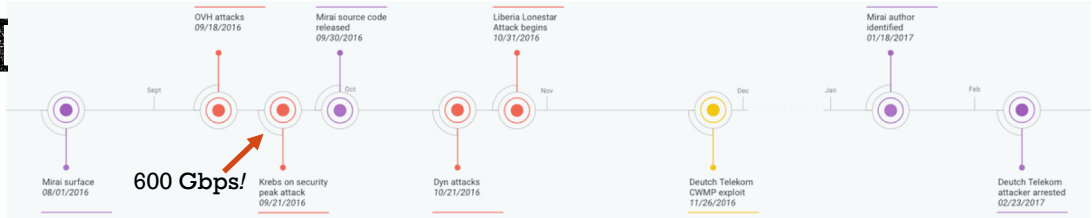
- Ensuring timely and reliable access to and use of information.
- Timely, reliable access to data and information services for authorized users.
- The ability for authorized users to access systems as needed.
- A requirement intended to assure that systems work promptly and service is not denied to authorized users.
- The security goal that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data.

https://csrc.nist.gov/Glossary/?term=3103#AlphaIndexDiv

AVAILABILITY IN PRACTICE

- Violations of availability include
  - infrastructure failures like network or hardware issues
  - infrastructure overload
  - power outages
  - attacks such as Distributed Denial of Services (DDoS) or ransomware
- How to guarantee availability
  - Employing a **backup system and a disaster recovery plan** is essential for maintaining data availability should a disaster, cyber-attack, or another threat disrupt operations
  - Utilizing **cloud** solutions for data storage is one way in which an organization can increase the availability of data for its users

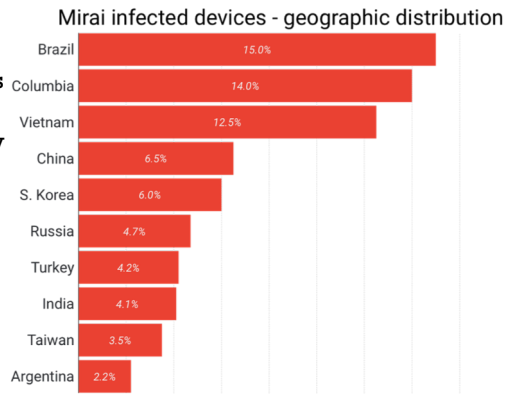
MIRAI



- Impact of attacks
  - Krebs on security: "**The Democratization of Censorship**"
  - DYN (DNS provider): impossible to access popular web sites such as Amazon, Twitter, Paypal, …
  - Lonestar (telco): shutting down Internet for an entire country (Liberia)

Violation of Availability

Impact is many fold
- **Economy**: the longer the downtime, the larger the loss of money for companies or even entire (national) eco-system
- **Fundamental rights**: censorship is obviously bad for normal democratic life



REMARKS ON CIA

- The CIA triad is essential because it allows for achieving **security**
- Its generality is, at the same time, a positive and a negative feature
  - positive since it decomposes the notion of security into simpler (**although interdependent**) notions and applies to a wide range of situations and use cases
  - negative since it must be instantiated to every situation and use case; such instantiations are called **security policies** that require **security mechanisms** or **services** to be enforced
    - Defining security policies is far from being an obvious task
- Example use case: **confidentiality of bank account data**
  - Employees of a bank shall access only selected data from each bank account, enough to perform their job
  - A teller of a bank shall access the balance of a bank account to perform withdrawal
  - A manager shall access the history of the transactions of a bank account to decide to grant or deny a loan application

14

15

SECURITY POLICIES AND MECHANISMS

SECURITY POLICY, SERVICE & MECHANISM

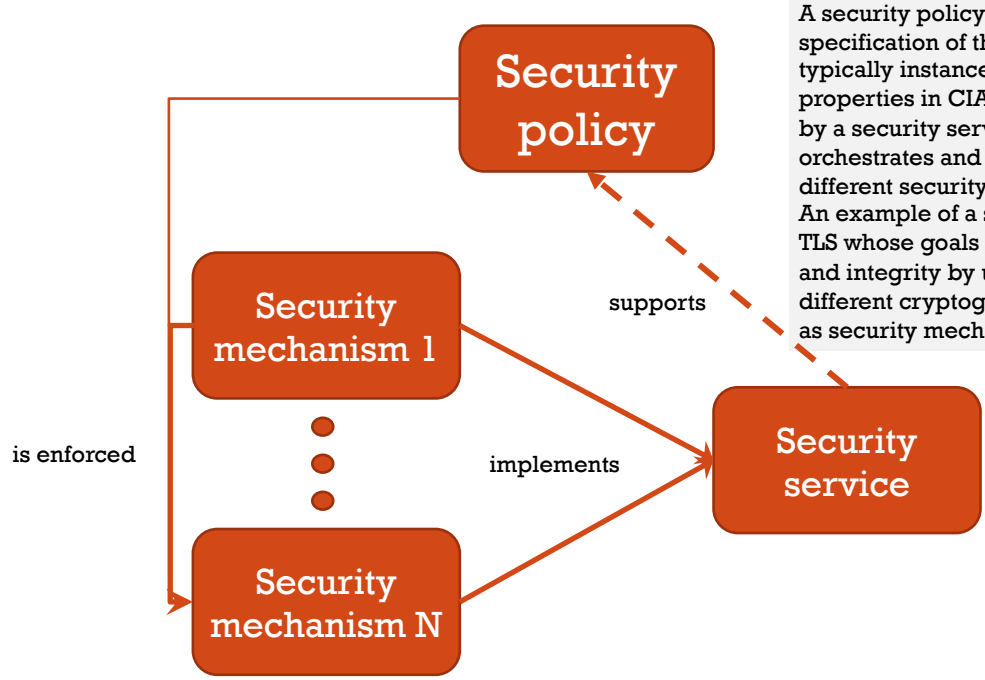
- Security **policy**
  - The rules and requirements established by an organization that governs the acceptable use of its information and services, and the level and means for protecting the confidentiality, integrity, and availability of its information

    https://csrc.nist.gov/Glossary/?term=1268#AlphaIndexDiv
- Security **mechanism**
  - A device or function designed to provide one or more security services usually rated in terms of strength of service and assurance of the design.
  - Implementation of a security policy

    https://csrc.nist.gov/Glossary/?term=1262#AlphaIndexDiv
- Security **service**
  - A capability that supports one, or more, of the security requirements (Confidentiality, Integrity, Availability). Examples of security services are key management, access control, and authentication.

    https://csrc.nist.gov/Glossary/?term=1268#AlphaIndexDiv

16



A security policy is a declarative specification of the security goals, typically instances of the high level properties in CIA, that is enforced by a security service which orchestrates and configures several different security mechanisms.
An example of a security service is TLS whose goals are confidentiality and integrity by using several different cryptographic primitives as security mechanisms.

17

EXAMPLE OF SECURITY POLICY

- Purpose
  - <Company X> must protect restricted, **confidential or sensitive data from loss** to avoid reputation damage and to avoid adversely **impacting** customers. The primary objective is user awareness and to avoid accidental loss scenarios (data leakage prevention)

- Scope
  - Any employee, contractor or individual with access to <Company X> systems or data.
  - Definition of data to be protected
    - Personal data
    - Financial
    - Intellectual Property

Try to answer the question: What does it mean for Company X "confidential/sensitive data"?

Adapted from https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en

18

EXAMPLE OF SECURITY POLICY (CONT'D)

- Policy rules
  1. Employees need to complete <Company X>'s security awareness training and agree to uphold the acceptable use policy.
  2. Visitors to <Company X> must be escorted by an authorized employee at all times. If an employee is responsible for escorting visitors, he/she must restrict them to appropriate areas.
  3. Employees must keep a clean desk. To maintain information security, employees need to ensure that all printed in scope data is not left unattended.
  4. Employees need to use a secure password on all <Company X> systems as per the password policy. These credentials must be unique and must not be used on other external systems or services.
  5. Terminated employees will be required to return all records, in any format, containing personal information.

Adapted from https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en

19

FEW EXAMPLES OF SECURITY MECHANISMS

- Authentication
  - Verifying the identity of a user, process, or device, often as a **prerequisite to allowing access** to resources in an information system.

https://csrc.nist.gov/Glossary/?term=3052#AlphaIndexDiv

- Authorization
  - The granting or denying of access rights to a user, program, or process.

https://csrc.nist.gov/Glossary/?term=3081#AlphaIndexDiv

- Access control
  - The process of granting or denying specific requests: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).

https://csrc.nist.gov/Glossary/?term=2785#AlphaIndexDiv

20

SECURITY SERVICES

- Typically, **security services are composed of security mechanisms**
- Also, **security services are easier to use than security mechanisms** as the way they can be integrated in available systems is designed to be frictionless
- This means that while security mechanisms may be difficult to configure, security services are easier to set up and deploy
- A prominent **example** of **security services** can be found **in the cloud**
  - Authentication and authorization mechanisms are available to be used with services deployed in the cloud in a more straightforward way than when deployed on premises
  - However, notice that the responsibility of configuring the security services is entirely on the shoulder of the user of the cloud platform
    - This is referred to as the **shared responsibility model**

21

22

TWO EXAMPLES OF SECURITY SERVICES

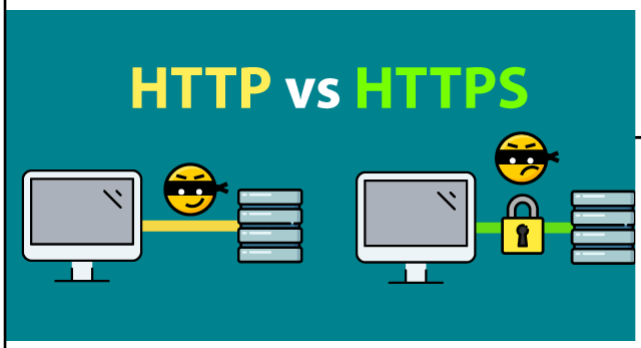
QUESTION: How can we mitigate attacks and reduce impact or, in other words, minimize risks?

ANSWER: Use security services…

Recall that a **security service** is a capability that supports one, or more, of the security requirements (CIA)

SECURITY SERVICE: EXAMPLE (1)

The Transport Layer Security (TLS) protocol is used to guarantee confidentiality and integrity of data (in transit) and it is the cornerstone of web security

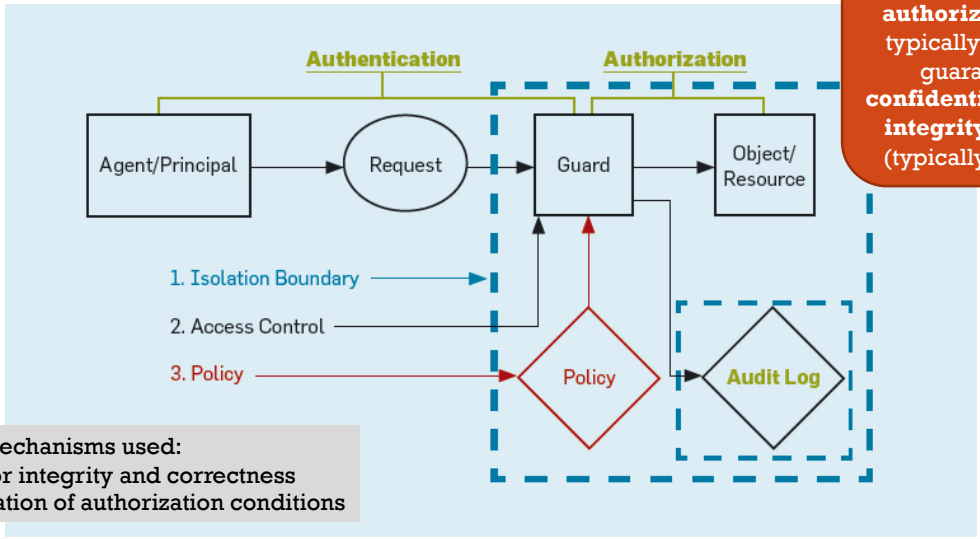


Security mechanisms used:
range of cryptographic primitives
to guarantee confidentiality and integrity

https://seopressor.com/blog/http-vs-https/

SECURITY SERVICE: EXAMPLE (2)

Access control, seen as the combination of **authentication and authorization**, is typically used to guarantee **confidentiality** and **integrity** of data (typically at rest)



Security mechanisms used:
isolation for integrity and correctness
with evaluation of authorization conditions

CIA, SECURITY VIOLATIONS, AND MITIGATIONS

- The CIA triad is not only essential for achieving **security** but also helps understanding **security violations** (i.e. what went wrong)

- Example: **ransomware attacks**
  - Ransomware is a type of malware that threatens to **publish the victim's personal data** or **permanently block access to it** unless a ransom is paid
  - It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them
  - Recovering the files without the decryption key is an intractable problem and difficult to trace digital (crypto-)currencies making tracing and prosecuting the perpetrators difficult

- Which security properties of the CIA triad can be violated in a ransomware attack?

25

CIA, SECURITY VIOLATIONS, AND MITIGATIONS (CONT'D)

- The CIA triad also helps understanding **security violations** (i.e. what went wrong)

- Example: **ransomware attacks**
  - Ransomware is a type of malware that threatens to **publish the victim's personal data** or **permanently block access to it** unless a ransom is paid
  - It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them
  - Recovering the files without the decryption key is an intractable problem and difficult to trace digital (crypto-)currencies making tracing and prosecuting the perpetrators difficult

- Which security properties of the CIA triad can be violated in a ransomware attack?
  - **Availability** as access is blocked but also **confidentiality** if the victim's data is exfiltrated… and even **integrity** as files are encrypted and can be modified by the attacker

CIA, SECURITY VIOLATIONS, AND MITIGATIONS (CONT'D)

- The CIA triad also helps understanding **security violations** (i.e. what went wrong)

- Example: **ransomware attacks**
- Which security properties of the CIA triad can be violated in a ransomware attack?
  - **Availability** as access is blocked but also **confidentiality** if the victim's data is exfiltrated… and even **integrity** as files are encrypted and can be modified by the attacker

- Mitigation: **Zero Trust**
  - Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be **authenticated**, **authorized**, and **continuously validated** for security configuration and posture before being granted or keeping access to applications and data

- This is an example of **risk management**…

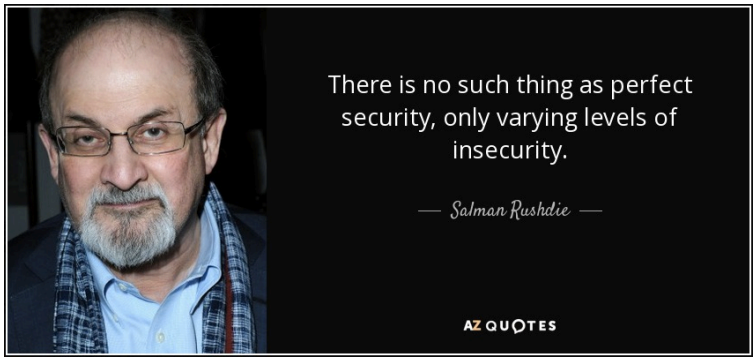
CIA, SECURITY VIOLATIONS, AND MITIGATIONS (CONT'D)

- The CIA triad also helps understanding **security violations** (i.e. what went wrong) and suggests how to avoid such problems by defining **security policies and mechanisms** (the latter enforce the former)
- More precisely, the CIA triad is crucial for **risk management** that involves identifying, assessing, and treating risks to the confidentiality, integrity, and availability of an organization data and systems
  - The end goal of risk management is to treat risks in accordance with an organization's overall risk tolerance
  - Organizations should not expect to eliminate all risks rather to identify and achieve an acceptable risk level
- **Risk management main phases**
  - Identification of assets, vulnerabilities, threats and controls (i.e. policies and enforcement mechanisms)
  - Assessment as likelihood and impact of a threat exploiting a vulnerability
  - Treatement to reduce risks by selecting appropriated controls

28

29

RISK



"Things are not quite so simple always as Black and White" – Doris Lessing

VULNERABILITY

- Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
- A weakness in a system, application, or network that is subject to exploitation or misuse.
- A flaw or weakness in a computer system, its security procedures, internal controls, or design and implementation, which could be exploited to violate the system security policy.

https://csrc.nist.gov/Glossary/?term=2436#AlphaIndexDiv

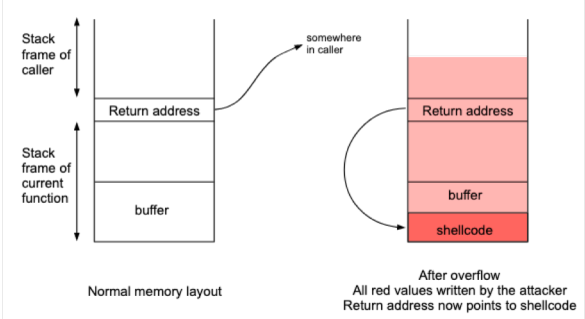
30

SOME EXAMPLES OF VULNERABILITIES

- Hidden backdoors
  - Example: Huawei equipment (https://www.bloomberg.com/news/articles/2019-04-30/vodafone-found-hidden-backdoors-in-huawei-equipment)
- Unknown software bugs
  - Example: buffer overflow/overrun
- Weak passwords

https://koofr.eu/blog/posts/worst-passwords-of-2020

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615



http://intronetworks.cs.luc.edu/current1/uhtml/security.html

31

THREAT

- Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully **exploit** a particular information system vulnerability.
- An activity, **deliberate or unintentional**, with the potential for causing harm to an automated information system or activity.
- The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

https://csrc.nist.gov/Glossary/?term=2156#AlphaIndexDiv

32

SOME EXAMPLES OF THREATS

- Hackers
  - Break a password or sniff it off the network
  - Use social engineering to get a password
  - Taking up resources with irrelevant messages
    - **Denial-of-service** attacks aim aims to disrupt a service by either exploiting a vulnerability or by sending a lot of bogus messages to a computer offering a service
- Viruses and some worms
  - A **virus** is a self-replicating program that requires user action to activate such as clicking on Email, downloading an infected file or inserting an infected floppy, CD, etc ..
  - A **worm** is a self-replicating program that does not require user action to activate. It propagates itself over the network, infects any vulnerable machine it finds and then spreads from it further.

33

ATTACK

- Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself
- An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality
- The realization of some specific threat that impacts the confidentiality, integrity, accountability, or availability of a computational resource.

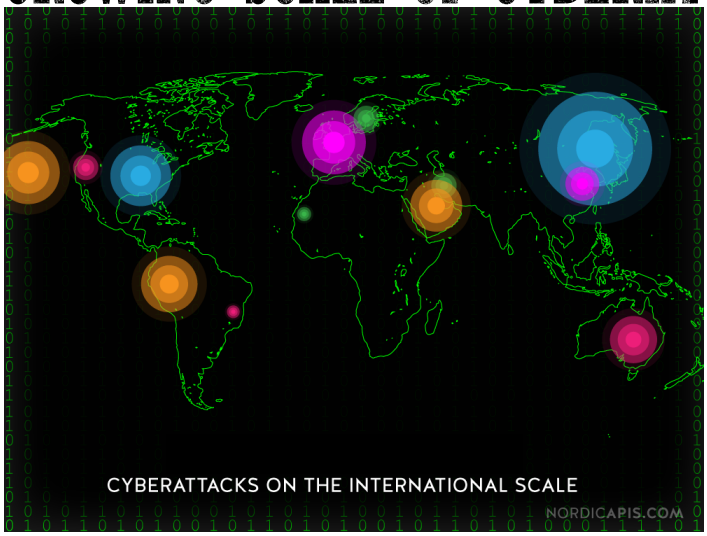
https://csrc.nist.gov/glossary/term/attack

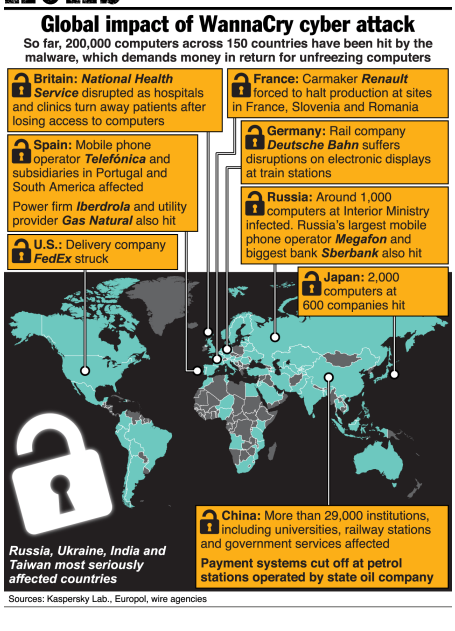
34

35

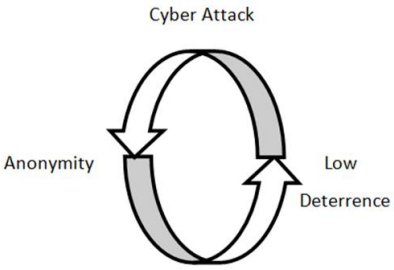
DIGRESSION ON ATTACKS

GROWING SCALE OF CYBERATTACKS





Cyber attacks are borderless and to be effective try to reach as many victims as possible!



The attribution problem

CYBERSECURITY

TECH | MOBILE | SOCIAL MEDIA | ENTERPRISE | CYBERSECURITY | TECH GUIDE

Most hacks take minutes to do — and weeks to discover

Anita Balakrishnan | @MsABalakrishnan

Published 11:24 AM ET Wed, 27 April 2016

CNBC

"[…] without the fear of being caught, convicted and punished, individuals and organizations will continue to use the Internet to conduct malicious activities."

Hunker, J., Hutchinson, B., & Margulies, J. (2008). "*Role and Challenges for Sufficient Cyber-Attack Attribution*." Dartmouth College, United States

37

"Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. [...] Cyber-attacks know no borders and no one is immune. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks."

European Commission President Jean-Claude Juncker, State of the Union Address, 13 September 2017

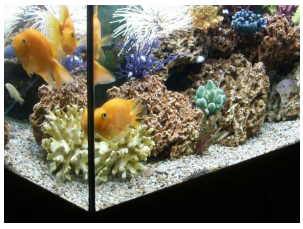
enisa European Union Agency for Network and Information Security

https://www.enisa.europa.eu

38

FURTHER DIFFICULTIES

How a fish tank helped hack a casino
https://thehackernews.com/2018/04/iot-hacking-thermometer.html



- Growing attack surface
  - How to evaluate the risks from 3rd party sw*?*
  - How to evaluate the interdependencies from the infrastructure*?*
  - How to evaluate the dependencies from the physical world*?*

- Difficulties in getting **cyber-intelligence information**
  - How to exploit information from other stakeholders to counter threats*?*
  - How to contribute (in a trusted way) to help other stakeholders*?*

40

END OF DIGRESSION ON ATTACKS

IN A NUTSHELL

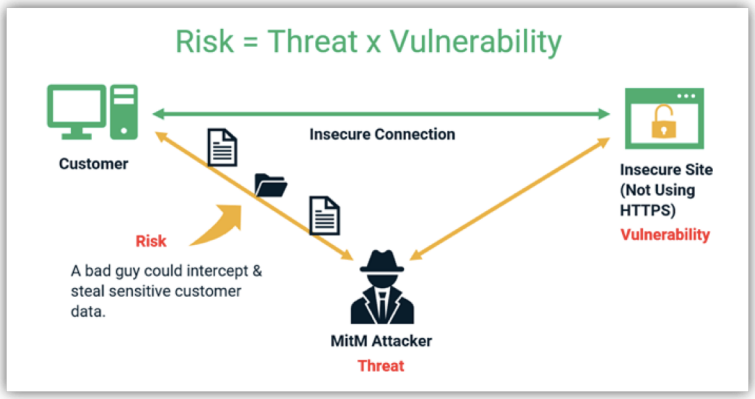
An activity potentially causing harm to a system or data

A weakness of a system that attackers can exploit

Likelihood and potential amplitude of the damage when threat exploits vulnerability by mounting an attack

41

AN EXAMPLE OF RISK

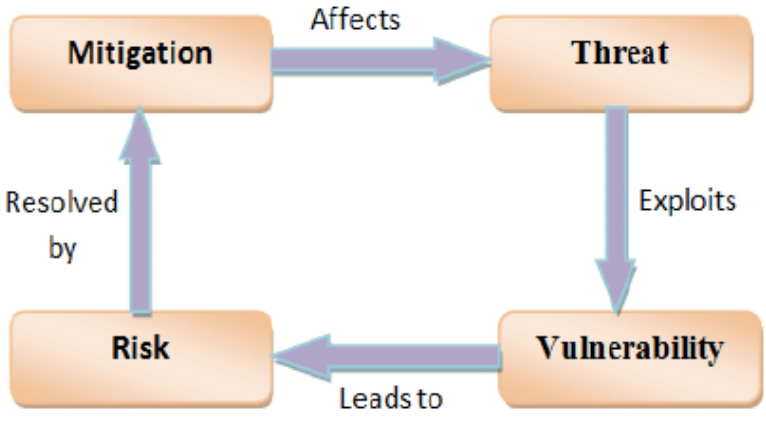


HTTPS is the secure protocol over HTTP that uses Transport Layer Security (TLS)

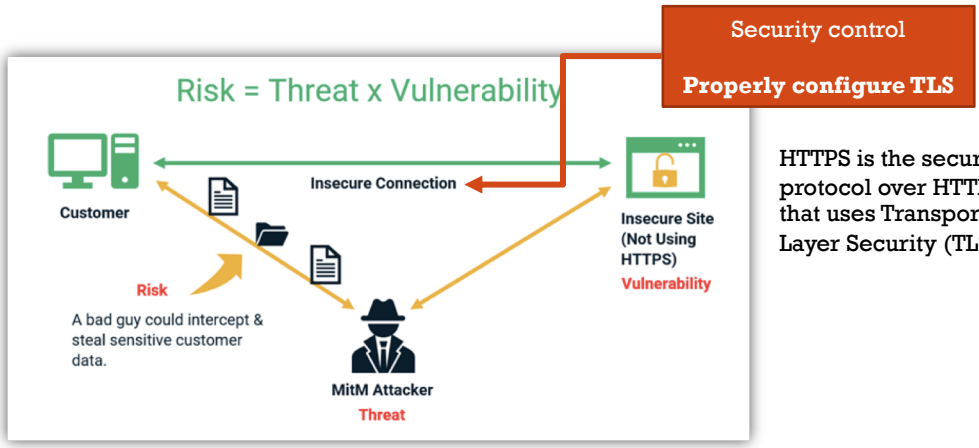
MitM stands for Man in the Middle

IN A NUTSHELL (2)

Security controls as specified by security policies and enforced by enforcement mechanisms



AN EXAMPLE OF RISK AGAIN (CONTD)



HTTPS is the secure protocol over HTTP that uses Transport Layer Security (TLS)

MitM stands for Man in the Middle

44

RISK

- The probability that a particular security threat will exploit a system vulnerability.
- A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

  Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.

https://csrc.nist.gov/Glossary/?term=1013#AlphaIndexDiv

45

REMARKS ON RISK

- Risk is the result of **threats exploiting vulnerabilities to obtain, damage, or destroy resources** together with their **impact on** the properties in the **CIA triad**
- **Threats** can be characterized as a combination of
  - **intent** = propensity to attack
  - **capability** = ability to successfully attack
- **Vulnerabilities** are characterized by how easy it is to
  - **identify** them
  - **exploit** them
- Threats and vulnerabilities give the **likelihood** that an adverse event may happen
- Impact should be evaluated with respect to each **stakeholder** that has an interest in the system under consideration
  - *Example*: unauthorised disclosure of personal information may have catastrophic consequence for the patients involved in the data breach but can be negligible for the organization offering the healthcare service if the number of patients involved is low

46

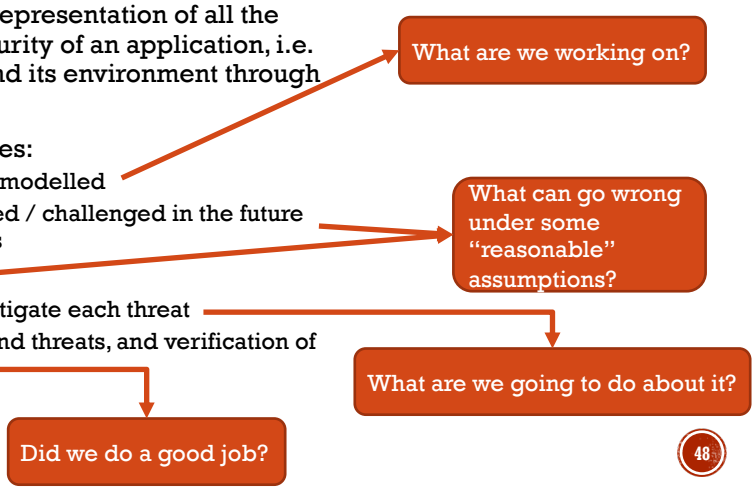
REMARKS ON RISK

- Risk is the result of **threats exploiting vulnerabilities to obtain, damage, or destroy resources** together with their **impact on** the properties in the **CIA triad**
- **Threats** can be characterized as a combination of
  - **intent** = propensity to attack
  - **capability** = ability to successfully attack
- **Vulnerabilities** are characterized by how easy it is to
  - **identify** them
  - **exploit** them
- Threats and vulnerabilities give the **likelihood** that an adverse event may happen
- Impact should be evaluated with respect to each **stakeholder** that has an interest in the system under consideration
  - *Example*: unauthorised disclosure of personal information may have catastrophic consequence for the patients involved in the data breach but can be negligible for the organization offering the healthcare service if the number of patients involved is low

47

LIKELIHOOD REQUIRES A THREAT MODEL

- A threat model is a structured representation of all the information that affects the security of an application, i.e. it is a view of the application and its environment through the lens of security
- A threat model typically includes:
  - Description of the system to be modelled
  - Assumptions that can be checked / challenged in the future as the threat landscape changes
  - Potential threats to the system
  - Controls that can be taken to mitigate each threat
  - A way of validating the model and threats, and verification of success of controls taken



48

AN EXAMPLE OF THREAT MODEL

- Description of the system to be modelled
  - Password storage in an application
- Assumptions that can be checked / challenged in the future as the threat landscape changes
  - offline attacks to passwords are the only security concerns
- Potential threats to the system
  - decryption of hashed passwords using brute force possible since weak hashing algorithm (MD5) is used
- Controls that can be taken to mitigate each threat
  - update hashing algorithm to known secure one
- A way of validating the model and threats, and verification of success of controls taken

49

REMARKS ON RISK

- Risk is the result of **threats exploiting vulnerabilities to obtain, damage, or destroy resources** together with their **impact on** the properties in the **CIA triad**
- **Threats** can be characterized as a combination of
  - **intent** = propensity to attack
  - **capability** = ability to successfully attack
- **Vulnerabilities** are characterized by how easy it is to
  - **identify** them
  - **exploit** them
- Threats and vulnerabilities give the **likelihood** that an adverse event may happen
- Impact should be evaluated with respect to each **stakeholder** that has an interest in the system under consideration
  - *Example*: unauthorised disclosure of personal information may have catastrophic consequence for the patients involved in the data breach but can be negligible for the organization offering the healthcare service if the number of patients involved is low

50

A REMARK ON IMPACT

- Nowadays, computers are everywhere and the impact of attacks can be substantial
- Example
  - Automotive attacks can lead to important consequences both on the vehicles and the passengers
  - For the 2015 attack on a FCA jeep, impact was substantial for all stakeholders
    - Manufacturer obliged to recall 1.4 millions vehicles
    - Drivers and passengers safety put at risk

https://money.cnn.com/2015/07/24/technology/chrysler-hack-recall/index.html?sr=twmoney072415chrysler900story

51

RISK MATRIX

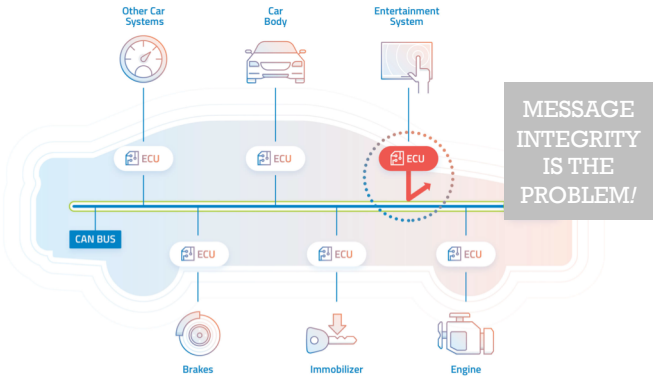
risk → likelihood, impact

risk = likelihood x impact

	1	2	3	4	5
			Severity of Impact		
Likelihood	Negligible	Marginal	Serious	Critical	Catastrophic
5 Highly Probable	1x5= 5	2x5= 10	3x5= 15	4x5= 20	5x5= 25
4 Probable	1x4= 4	2x4= 8	3x4= 12	4x4= 16	5x4= 20
3 Occasional	1x3= 3	2x3= 6	3x3= 9	4x3= 12	5x3= 15
2 Remote	1x2= 2	2x2= 4	3x2= 6	4x2= 8	5x2= 10
1 Improbable	1x1= 1	2x1= 2	3x1= 3	4x1= 4	5x1= 5

52

RISK IN AUTOMOTIVE: AGAIN (1)

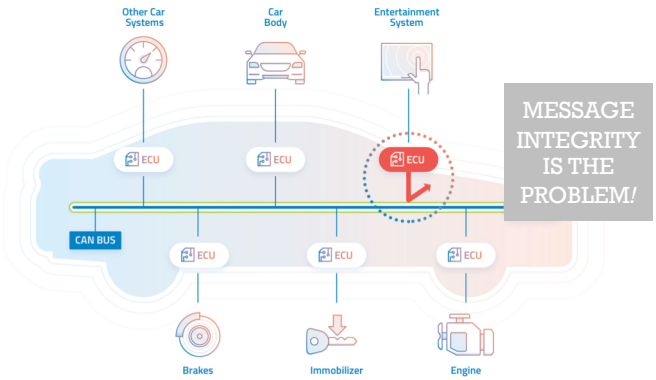


MESSAGE INTEGRITY IS THE PROBLEM!

No hope that automotive industry will replace the CAN bus for better security

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

RISK IN AUTOMOTIVE: AGAIN (2)



MESSAGE INTEGRITY IS THE PROBLEM!

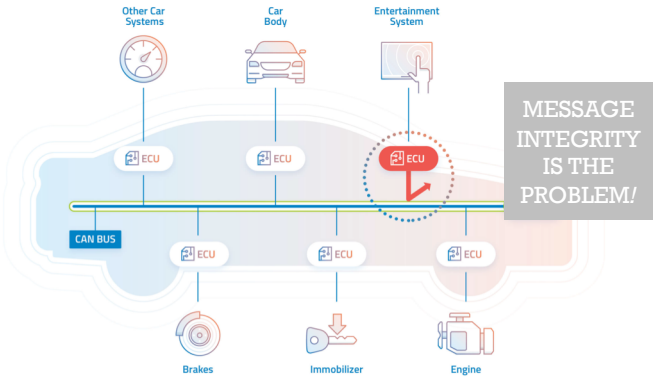
Likelihood

Wireless carjacking of a Jeep (2015)

No hope that automotive industry will replace the CAN bus for better security

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

RISK IN AUTOMOTIVE: AGAIN (3)



MESSAGE INTEGRITY IS THE PROBLEM!

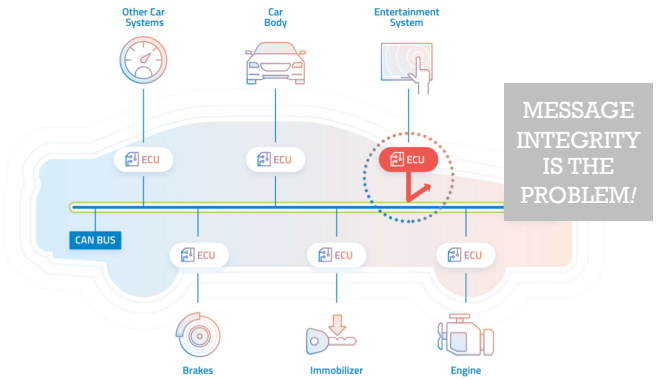
Impact

Wireless carjacking of a Jeep (2015)

No hope that automotive industry will replace the CAN bus for better security

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

RISK IN AUTOMOTIVE: AGAIN (4)



MESSAGE INTEGRITY IS THE PROBLEM!

Impact

Wireless carjacking of a Jeep (2015)

No hope that automotive industry will replace the CAN bus for better security

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

SECURITY AND HUMAN FACTORS

Make it Easy to Do the Right Thing
Hard to Do the Wrong Thing
And Easy to Recover When the Wrong Thing Happens

USABLE SECURITY

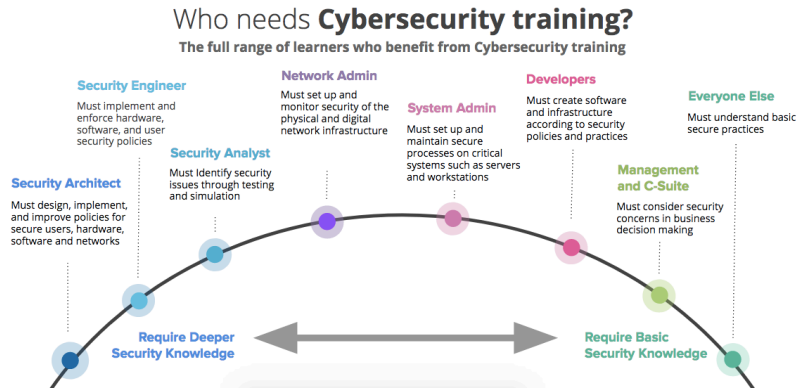
https://csrc.nist.gov/projects/usable-cybersecurity

Position	Worst passwords of 2020	Password
1. ↑ (2)		123456
2. ↑ (3)		123456789
3. (new)		picture1
4. ↑ (5)		password
5. ↑ (6)		12345678
6. ↑ (17)		111111
7. ↑ (18)		123123
8. ↓ (1)		12345
9. ↑ (11)		1234567890
10. (new)		senha

https://www.zdnet.com/article/the-worst-passwords-of-2020-show-we-are-as-lazy-about-security-as-ever/

AWARENESS: AN EXAMPLE

https://readgroup.co.uk/news/data-protection-why-passwords-are-like-pants/



SECURITY TRAINING IS INCREASINGLY NEEDED FOR MORE AND MORE IT PROFESSIONALS

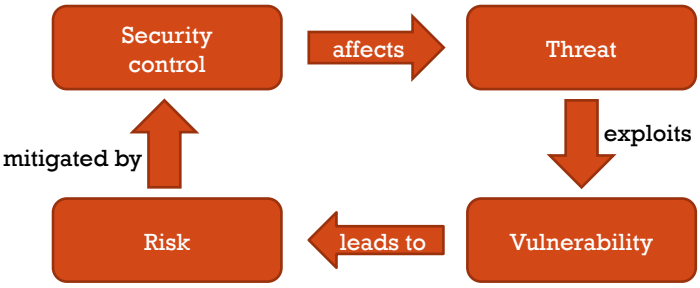
- IT professionals are increasingly taking decisions with security (and privacy) consequences
- On average, they are not trained to do so and this results in a weak security posture that offer an "easy lunch" to attackers

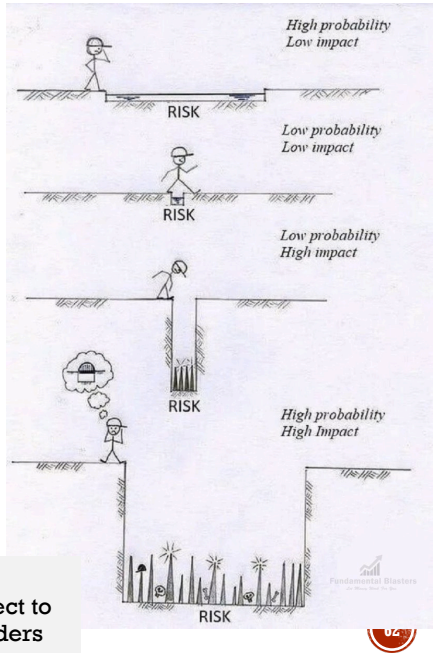
WRAP-UP (1)

- For every use case scenario, the CIA should be carefully instantiated
- Security policies can be used to specify CIA properties
- Security mechanisms and services can be used to enforce security policies (i.e. ultimately to enforce CIA)

61

WRAP-UP (2)

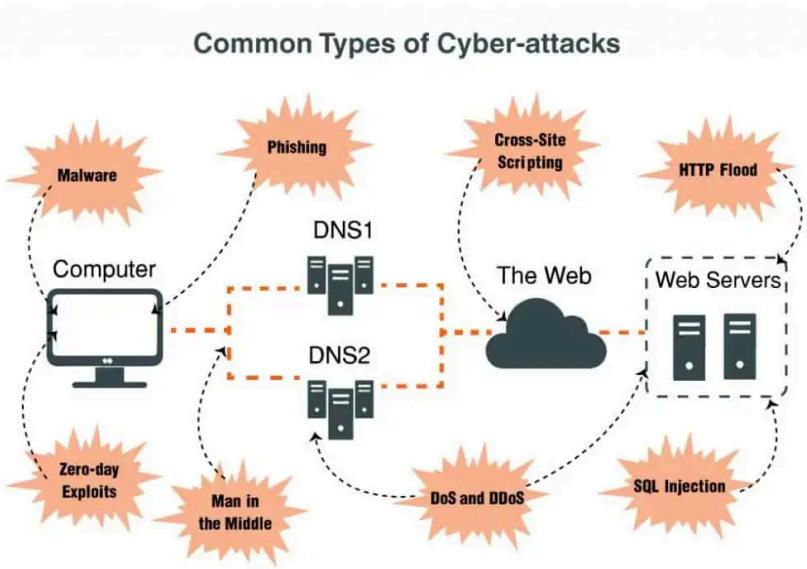




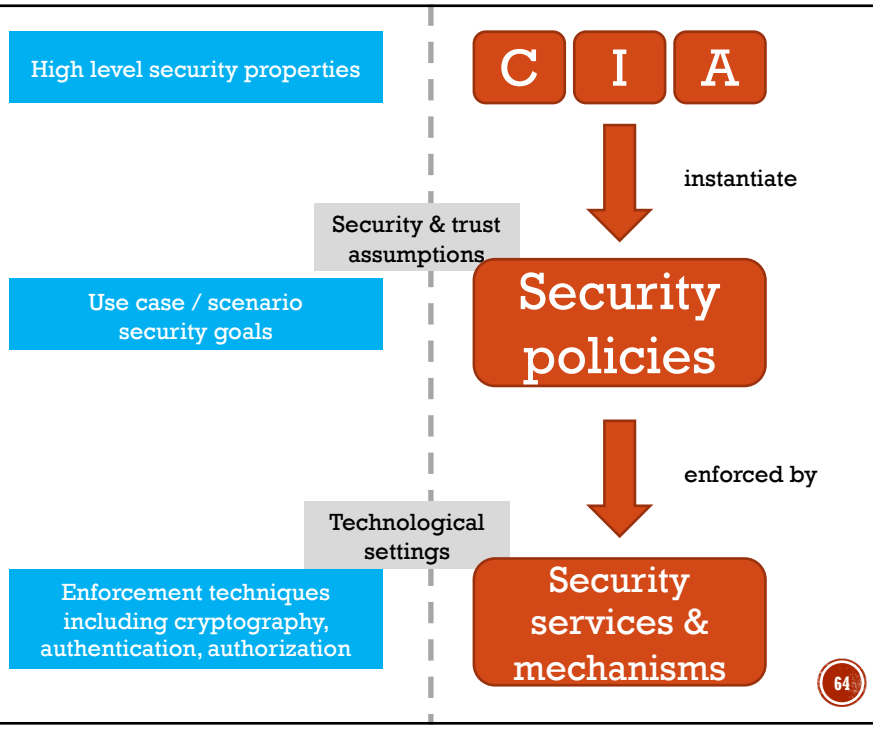
The impact should be considered with respect to the different stakeholders

WRAP-UP (3)

Security should consider the capabilities of attackers or threats to defend against



WRAP-UP IN A PICTURE



65

FINAL REMARKS ON SECURITY

THREAT MODELING IS CRUCIAL

- Security is characterized by protection **against an adversary** or, possibly, against some other physical or random process
- Security typically focuses on **malicious adversaries**
- Core to any consideration of security is the **modelling** of malicious adversaries
  - motivations (in the past… glory, nowadays… money)
  - capabilities (intercept messages, modify messages, read keys pressed, …)
  - threats (roughly, negative impact on systems, operations, organization, business, …)
- **Arguing that a system is secure without referring to an attacker model does not make much sense**
  - Example: a 0-day attack that exploits a previously unknown hardware, firmware, or software vulnerability (https://csrc.nist.gov/glossary/term/zero_day_attack)
- Indeed, absolute security does not exist even for so-called air-gapped system
  - Example: https://spectrum.ieee.org/the-real-story-of-stuxnet

DEPLOYING SECURITY CONTROLS REQUIRES TO CONSIDER SEVERAL DIFFERENT ASPECTS

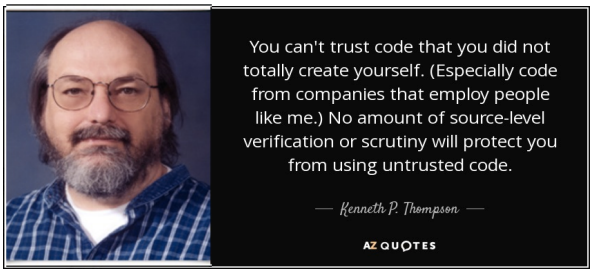
- In order to mitigate threats, security proposes **controls/mitigation strategies** affecting
  - people (e.g., rules for setting passwords)
  - process (e.g., regularly update software)
  - technology (e.g., authentication and access control)
- Controls can be classified in
  - **preventive**, i.e. before the bad event (e.g., locking out unauthorized intruders)
  - **detective**, i.e. during the bad event (e.g., turning an intruder alert on a dashboard)
  - **corrective**, i.e. after the bad event (e.g., recovering deleted data from a backup)
- Selection of controls is based on
  - **risk management**: the process of identifying vulnerabilities and threats to the information resources used by an organization and deciding what countermeasures, if any, to take in reducing risk to an acceptable level
  - considering the **human factor**: controls must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules

SECURITY AND TRUST ASSUMPTIONS ARE ALSO CRUCIAL

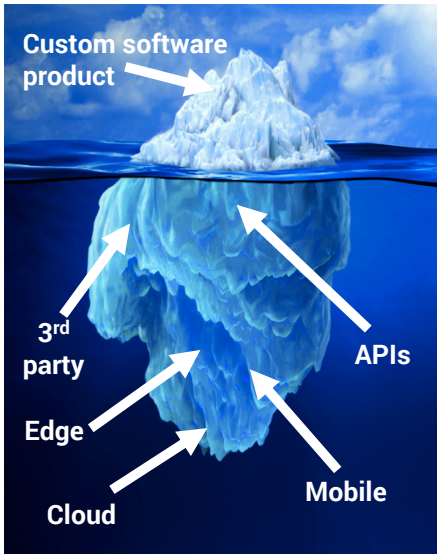
- The role of **trust** in software
  - **Dependability** = ability to avoid failures that are more frequent and severe than is acceptable
    - **Failure =** an event that occurs when the delivered service deviates from correct service
  - **Trust =** accepted dependence
  - For a complete discussion on dependability, trust, and security see
    https://drum.lib.umd.edu/bitstream/handle/1903/6459/TR_2004-47.pdf
- Example: *SolarWinds attack*
  - The attack compromises the infrastructure of SolarWinds, a company that produces a network and applications monitoring platform called Orion, and then uses that access to produce and distribute **trojanized updates** to the software's users (an instance of a supply chain attack)
    - A trojan is any malware (i.e. a software intentionally designed to cause damage) that misleads users of its true intent
  - Impact on 425 of the US Fortune 500, the top ten US telecommunications companies, the top five US accounting firms, all branches of the US Military, the Pentagon, the State Department, and hundreds of universities and colleges worldwide

https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html

ABOUT THE IMPORTANCE OF TRUST



Thompson's Turing Award Lecture in 1984 entitled "Reflections on Trusting Trust":
To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.



BE CAREFUL WITH SECURITY CONTROLS

- Security controls are human artifacts that
  - can mitigate the impact of an attack but in many cases **do not avoid it completely**
  - **can contain vulnerabilities** that can be exploited to mount attacks
- In other words, we are left with a (non-null) **residual risk**, i.e. the amount of danger associated with an attack after risks have been mitigated by security controls
- Example: automotive seat-belts
  - Use of seat-belts reduces the risk of injury although it does not cancel it as
    - accidents may be quite serious and seat-belts can only mitigate consequences
    - installation of set-belts may be defective and mitigation of risk is reduced

SECURITY VIOLATIONS CAN BE TRACED BACK TO VIOLATIONS OF THE CIA TRIAD

"Exploiting vulnerabilities allows attackers to violate security"

- At first reading, this may seem obvious but is it really so?
- What does it mean exactly to "violate security"?
- There many possibly answers to the question above including
  - A security violation can be the unauthorized sharing of sensitive information such as personal data of patients in a healthcare system
  - A security violation can be the unauthorized modification of the content of a resource such as modifying the balance of bank account
  - A security violation can be the unauthorized withholding of the content of a resource or service such as the unavailability of network services
- The three answers correspond to three crucial properties characterizing three possible dimensions of security
  - They are collectively known as …