Security Pillars

Paolo PRINETTO

Director
CINI Cybersecurity
National Laboratory

Paolo.Prinetto@polito.it

Mob. +39 335 227529

CYBER
CHALLENGE
CyberChallenge.IT

cini
Cybersecurity
National Lab

https://cybersecnatlab.it

License & Disclaimer

License Information

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Acknowledgments

- The presentation includes material from
  - Alessandro ARMANDO
  - Riccardo FOCARDI
  - Nicolò MAUNERO
  - Gianluca ROASCIO

whose valuable contributions are here acknowledged and highly appreciated.

Prerequisites

- Lectures:
  - *CS_1.1 – Security: An Introduction*
  - *CS_1.2 – Cybersecurity: Definition & relevance*

Goal

- Presenting in details the concepts mostly considered as *Security Pillars*

Outline

- Secure Systems Basic Pillars:
  - CIA Triad
- Additional pillars

Outline

- Secure Systems Basic Pillars:
  - CIA Triad
- Additional pillars

Cybersecurity

- That practice that allows an entity (organization, citizen, nation, ...) to protect its physical assets and *confidentiality*, *integrity* and *availability* of its information from threats that come from *cyberspace*

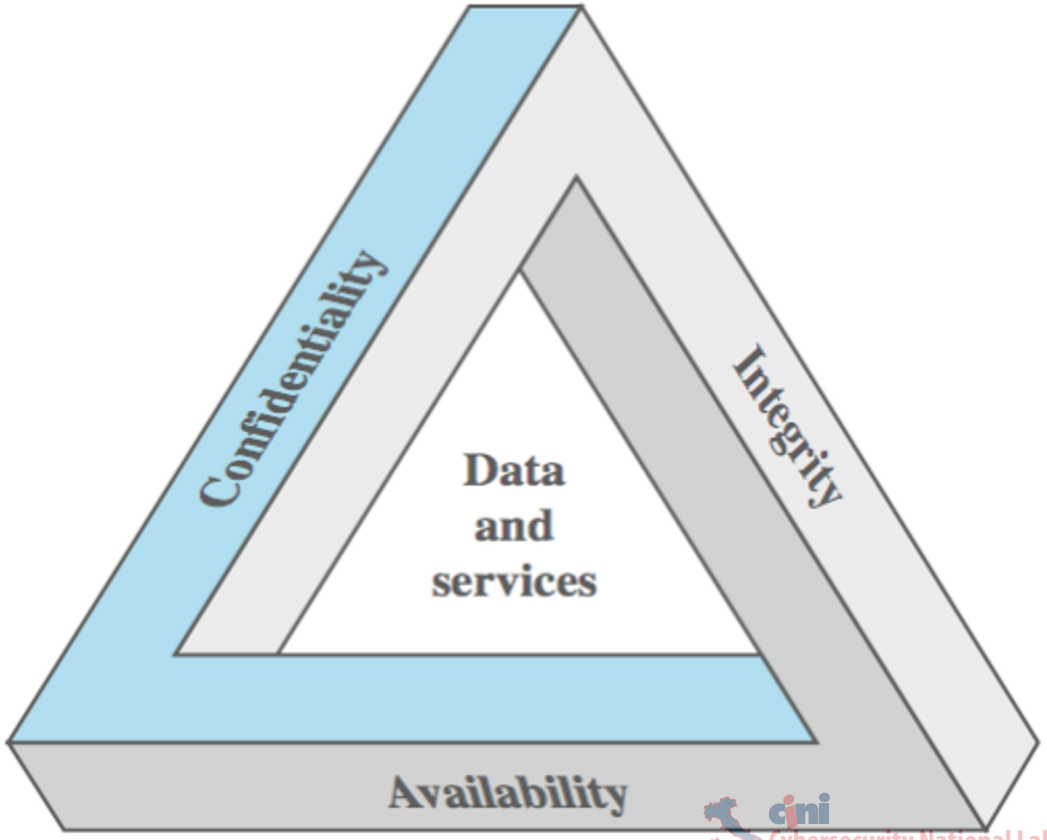
[standard ISO/IEC 27000:2014 & ISO/IEC 27032:2012]

Secure Systems Basic Pillars

- *Confidentiality*
  - Ensuring that information is accessible only to those authorized
- *Integrity*
  - Ensuring that information has not been modified
- *Availability*
  - Legitimate users have access when they need it

The CIA triad

- *Confidentiality, Integrity, Availability* form what is usually referred to as the *CIA triad*



Secure Systems Basic Pillars

- *Confidentiality*
  - Ensuring that information is accessible only to those authorized
- *Integrity*
  - Ensuring that information has not been modified
- *Availability*
  - Legitimate users have access when they need it

Confidenziality

- *Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…*

[US Federal Information Security Management Act (FISMA) - United States Code, 2006 Edition, Supplement 5, Title 44]

Confidentiality

It covers 3 related areas:

- *Data*
- *Individuals (Privacy)*
- *Organizations (Secrecy)*

Confidentiality

It covers 3 related areas:

- *Data*
- *Individuals (Privacy)*
- *Organizations (Secrecy)*

- Assures that confidential information is not disclosed to unauthorized individuals

Confidentiality

It covers 3 related areas:

- *Data*
- *Individuals (Privacy)*
- *Organizations (Secrecy)*

- Assures that individuals control or influence:
  - what information related to them may be collected and stored
  - by whom and to whom that information may be disclosed

Privacy

- Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual

[NISTIR 8053 (ISO/IEC 2382)]

Confidentiality

It covers 3 related areas:

- *Data*
- *Individuals (Privacy)*
- *Organizations (Secrecy)*

- Pertains to confidentiality for organizations, such as commercial companies or governments

Secure Systems Basic Pillars

- *Confidentiality*
  - Ensuring that information is accessible only to those authorized
- *Integrity*
  - Ensuring that information has not been modified
- *Availability*
  - Legitimate users have access when they need it

Integrity

- Guarding against improper information modification or destruction, and includes ensuring information *non-repudiation* and *authenticity.*

[US Federal Information Security Management Act (FISMA) - United States Code, 2006 Edition, Supplement 5, Title 44]

Integrity

It covers two related concepts:

- *Data integrity*: Assures that information and programs are changed only in a specified and authorized manner
- *System integrity*: Assures that a system performs its operations in unimpaired manner, free from unauthorized manipulation

Secure Systems Basic Pillars

- *Confidentiality*
  - Ensuring that information is accessible only to those authorized
- *Integrity*
  - Ensuring that information has not been modified
- *Availability*
  - Legitimate users have access when they need it

Availability

- Ensuring timely and reliable access to and use of information …

[US Federal Information Security Management Act (FISMA) - United States Code, 2006 Edition, Supplement 5, Title 44]

Availability

- Assures that systems work promptly, and service is not denied to authorized users.

Availability

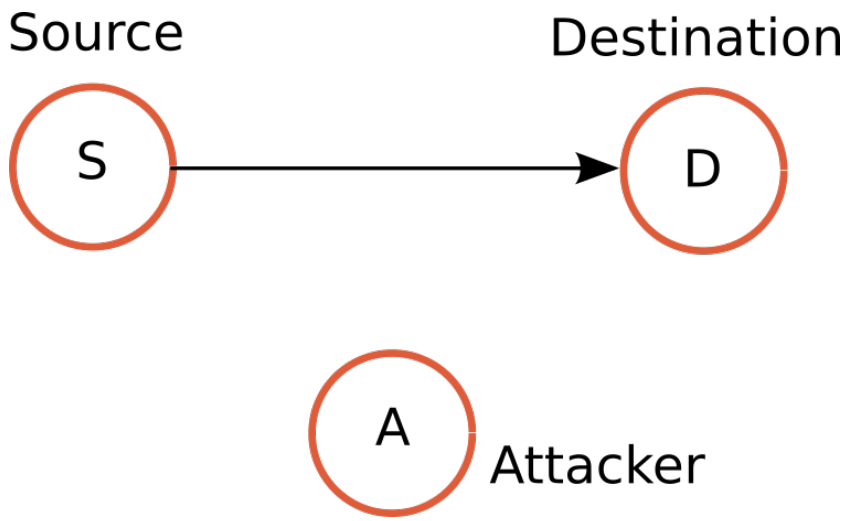
- The probability D(t) that the system will function correctly at a given instant t.

DAD vs CIA

- Attacks on the CIA are typically referred to as *DAD*:
  - **D**isclosure > **C**onfidentiality
  - **A**lteration > **I**ntegrity
  - **D**estruction > **A**vailability

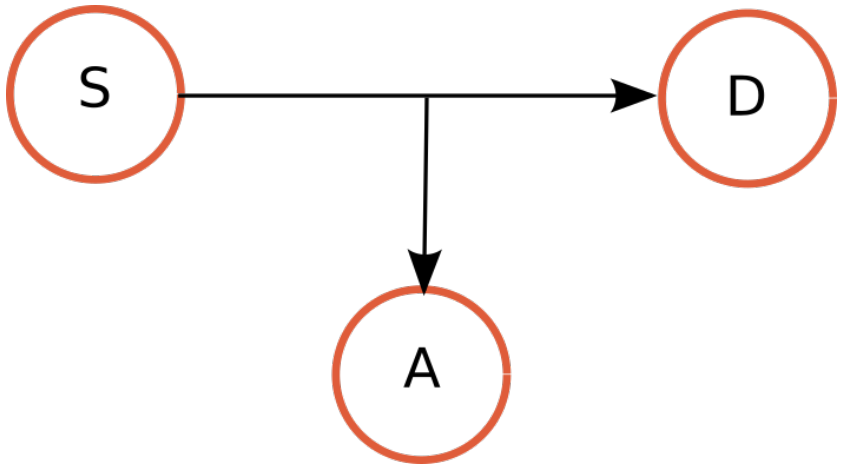
A practical example of CIA attack

- Let's assume an information (or service) move from a source to a destination
- The attacker could subvert this pattern in several ways
- Let's analyse some of them



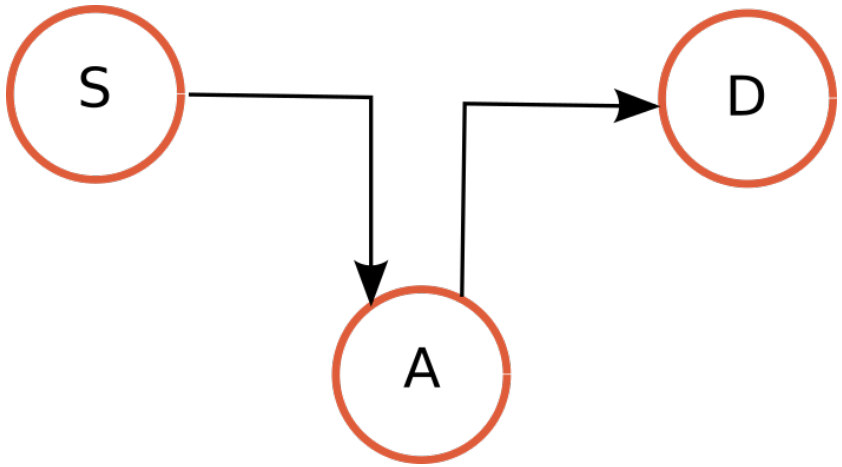
Stealing: attack to Confidentiality

- The attacker gets *unauthorized access* to information
- So, he breaks *confidentiality*
- Examples:
  - S is a vulnerable database
  - S sends a credit card number to D “in clear”



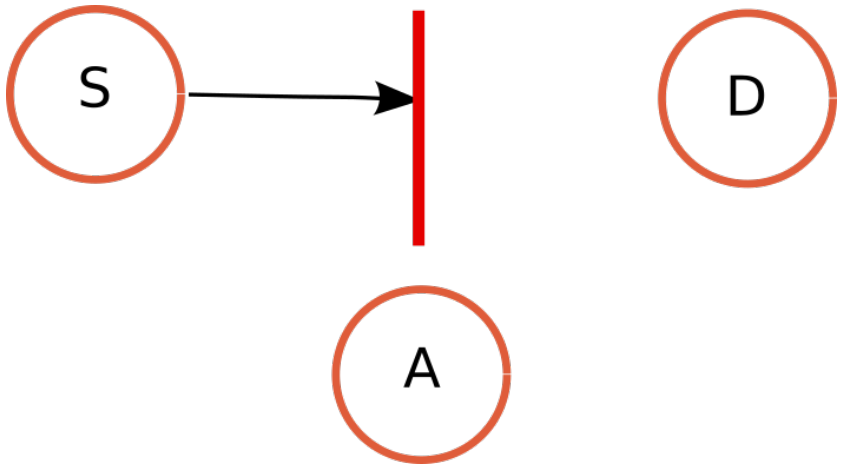
Corrupting: attack to Integrity

- The attacker *maliciously modifies* the transmitted information
- So, he breaks *integrity*
- Example:
  - A redirects S's bank transfer
  - NOTE: The attacker A can be either in the browser or on the network (*Man-in-the-middle*)



Inhibiting: attack to Availability

- The attacker *stops* the information flow
- So, he breaks *availability*
- Examples:
  - DoS on a server
  - Attack to the Ukrainian Power supply network



Countermeasures

- Attacks on the CIA can be taken to any level, from hardware to software to communications.
- To be effective, each application domain has developed and adopts its own specific countermeasures

Examples of possible countermeasures

- In the sequel we focus on just two examples of possible countermeasures in the field of protection of transmitted messages
  - *Hash functions*
  - *Encryption*

Hash Functions

- A Hash function:
  - gets in input a set of data M (of variable length)
  - returns a hash value h (of fixed length):

$$h = H(M)$$

Hash Functions usage

- Hash functions can be used to demonstrate the *integrity* of a message M.

Hash Functions usage

- Hash functions can be used to demonstrate the *integrity* of a message M.
- If M is sent together with h (i.e., the result of the hash function applied to it) and an attacker modifies M in M', the receiver, calculating the hash function on M', will get a value h' most likely different from the value h originally sent together with the message M.

Encryption

- Operation that, resorting to an *encryption algorithm* and a *key,* renders a message "blurred", so that it is not comprehensible/intelligible to persons not authorised to read it.

Encryption & Decryption

- Can be exploited to guarantee *confidentiality*.

Outline

- Secure Systems Basic Pillars:
  - CIA Triad
- Additional pillars

Secure Systems Additional Pillars

- *Resilience*
- *Non-repudiation*
- *Authenticity*
- *Access control*

[https://www.itgovernance.co.uk/cyber-resilience]

Secure Systems Additional Pillars

- *Resilience*
- *Non-repudiation*
- *Authenticity*
- *Access control*

- The ability of an information system to continue to:
  - operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities;
  - recover to an effective operational posture in a time frame consistent with mission needs.

[NIST SP 800-53 Rev. 4 under Information System Resilience
NIST SP 800-39 under Information System Resilience]

Secure Systems Additional Pillars

- *Resilience*
- *Non-repudiation*
- *Authenticity*
- *Access control*

- The ability of an information system to continue to operate while under attack, even if in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack

[NIST SP 800-30 Rev. 1 under Information System Resilience]

Secure Systems Additional Pillars

- *Resilience*
- *Non-repudiation*
- *Authenticity*
- *Access control*

- Cyber resilience is a measure of how well an organization can manage (i.e., prepare for, respond to and recover form) a cyberattack or data breach, while continuing to operate its business effectively.

Resilience effects

- It helps an organisation protect against *cyber risks*, defend against and limit the severity of attacks, and ensure its continued survival despite an attack.

[https://www.itgovernance.co.uk/cyber-resilience]

Risk

- The possibility that human actions or events lead to consequences that have an impact on *what humans value*

[O. Renn, "*The role of risk perception for risk management*," Reliability Engineering & System Safety, vol. 59, no. 1, pp. 49 – 62, 1998, http://www.sciencedirect.com/science/article/pii/S0951832097001191]

The four elements of cyber resilience

- *Manage and protect*
- *Identify and detect*
- *Respond and recover*
- *Govern and assure*

- Being able to identify, assess and manage the risks associated with network and information systems, including those across the supply chain.
- It also requires the protection of information and systems from cyber attacks, system failures, and unauthorised access.

The four elements of cyber resilience

- *Manage and protect*
- *Identify and detect*
- *Respond and recover*
- *Govern and assure*

- Continual monitoring of network and information systems to detect anomalies and potential cyber security incidents before they can cause any significant damage.

The four elements of cyber resilience

- *Manage and protect*
- *Identify and detect*
- *Respond and recover*
- *Govern and assure*

- Implementing an incident response management programme and measures to ensure business continuity will help you continue to operate even if you have been hit by a cyber attack, and get back to business as usual as quickly and efficiently as possible.

The four elements of cyber resilience

- *Manage and protect*
- *Identify and detect*
- *Respond and recover*
- *Govern and assure*

- Ensure that your programme is overseen from the top of the organisation and built into business as usual.
- Over time, it should align more and more closely with your wider business objectives.

Secure Systems Additional Pillars

- *Resilience*
- *Non-repudiation*
- *Authenticity*
- *Access control*

[CNSSI 4009-2015 (NIST SP 800-53 Rev. 4)
NIST SP 800-53 Rev. 4 under Non-repudiation]

- 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.

Secure Systems Additional Pillars

- *Resilience*
- *Non-repudiation*
- *Authenticity*
- *Access control*

- 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.

[NIST SP 800-137 under Authenticity (CNSSI 4009)
NIST SP 800-30 Rev. 1 under Authenticity (CNSSI 4009)
NIST SP 800-39 under Authenticity
NIST SP 800-53 Rev. 4 under Authenticity
NIST SP 800-53A Rev. 4 under Authenticity]

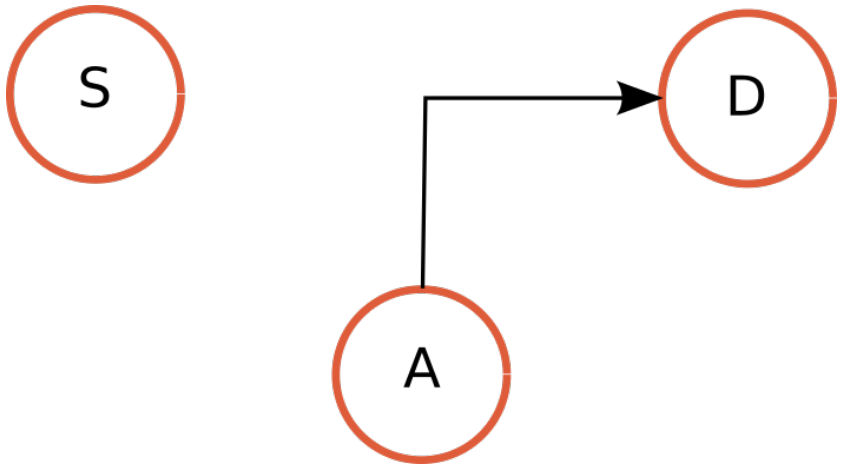
Authenticity and Trust

- “An entity can be trusted if it always behaves in the expected manner for the intended purpose.”

[D. Grawrock, Dynamics of a Trusted Platform: A building block approach. Intel Press, 2008]

Forging: attack to Authenticity

- The attacker creates a new information item
- So, he breaks *authenticity*
- Examples:
  - Falsifying a signature through a cryptographic vulnerability (e.g., the collisions present in the MD5 protocol)

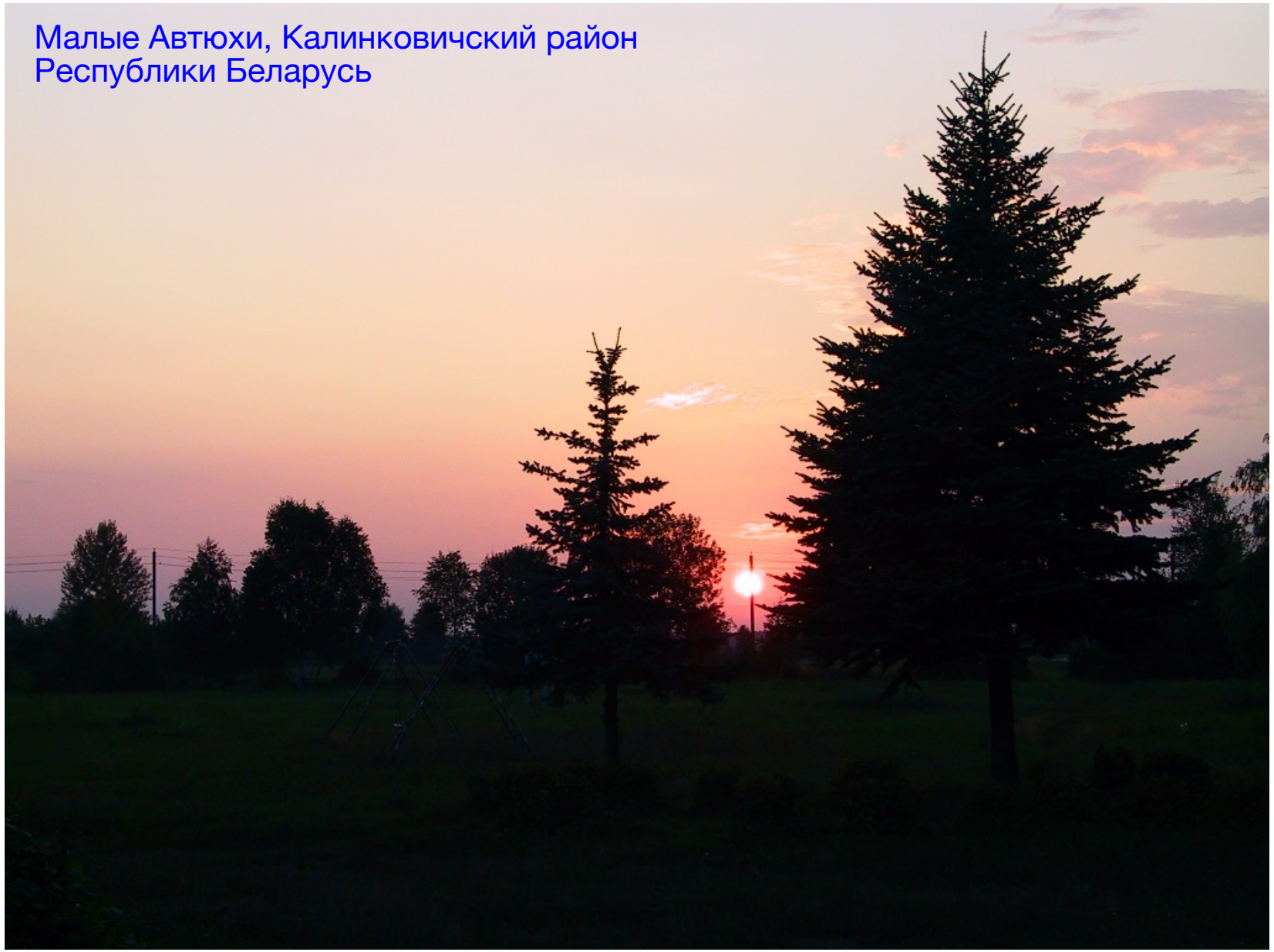


Secure Systems Additional Pillars

- *Resilience*
- *Non-repudiation*
- *Authenticity*
- *Access control*

- The process of granting or denying specific requests:
  - for obtaining and using information and related information processing services;
  - to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances)

[CNSSI 4009-2015 (FIPS 201-1 - Adapted]



Малые Автюхи, Калинковичский район
Республики Беларусь

Paolo PRINETTO

Director
CINI Cybersecurity
National Laboratory

Paolo.Prinetto@polito.it

Mob. +39 335 227529

CYBER CHALLENGE
CyberChallenge.IT

cini
Cybersecurity
National Lab

https://cybersecnatlab.it