Università degli Studi di Milano– Bicocca
Dipartimento di Informatica, Sistemistica e Comunicazione
Anno Accademico 2022 – 2023

# *Software Architecture*

Alexandru Nicolae Andrei 829570
Giacomo Savazzi 845372
Andrea Assirelli 820149

*November 29, 2022*

# In Depth Study - *Security*

*If you reveal your secrets to the winds, you should not blame the wind for revealing them to the trees.*

*- Kahlil Gibran*

# Security – Introduction

*Security is a measure of the system's ability to protect data and information from unauthorized access while still providing access to people and systems that are authorized.*

*An attack could be:*

- *an unauthorized attempt to access data/services;*
- *an unauthorized modification of the data;*
- *deny services to legitimate users.*

# Security – CIA

*Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization.*

# Security – CIA – Availability

- ***Availability*** *is the property that the system will be available for legitimate use.*

*For **example**, a denial-of-service attack won't prevent you from ordering this book from an online bookstore.*

# *Security – CIA – Integrity*

- ***Integrity*** *is the property that data or services are not subject to unauthorized manipulation.*

*For* ***example****, your grade has not been changed since your instructor assigned it.*

# *Security – CIA – Confidentiality*

- ***Confidentiality*** *is the property that data or services are protected from unauthorized access.*

*For* ***example****, a hacker cannot access your income tax returns on a government computer.*

# *Security – Privacy*

*An issue closely related to security is the quality of privacy. Privacy concerns have become more important in recent years and are enshrined into law in the European Union through the General Data Protection Regulation (**GDPR**).*
*Achieving privacy is about limiting access to information, which in turn is about which information should be access-limited and to whom access should be allowed.*

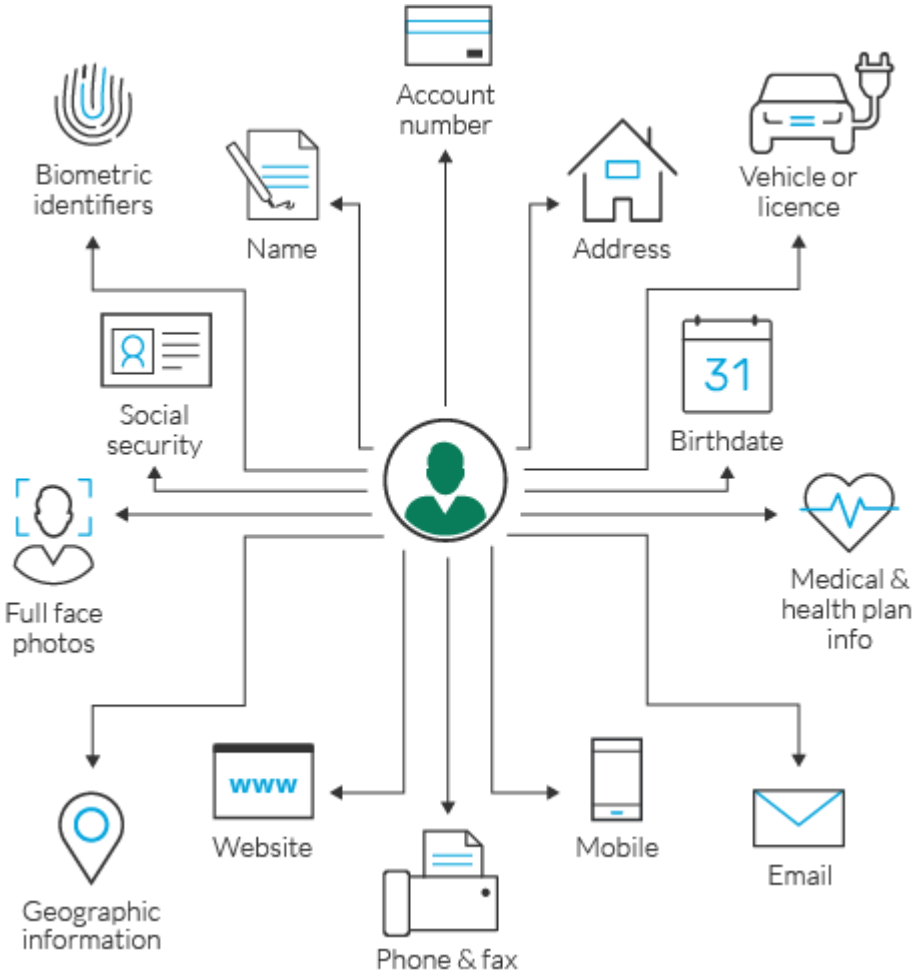
Data Privacy

≠

Data Security

# Security – Privacy – PII

*The general term for information that should be kept private is personally identifiable information (PII). The National Institute of Standards and Technology (NIST) defines PII as "any information about an individual maintained by an agency,* ***including any information that can be used to distinguish or trace an individual's identity****, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."*



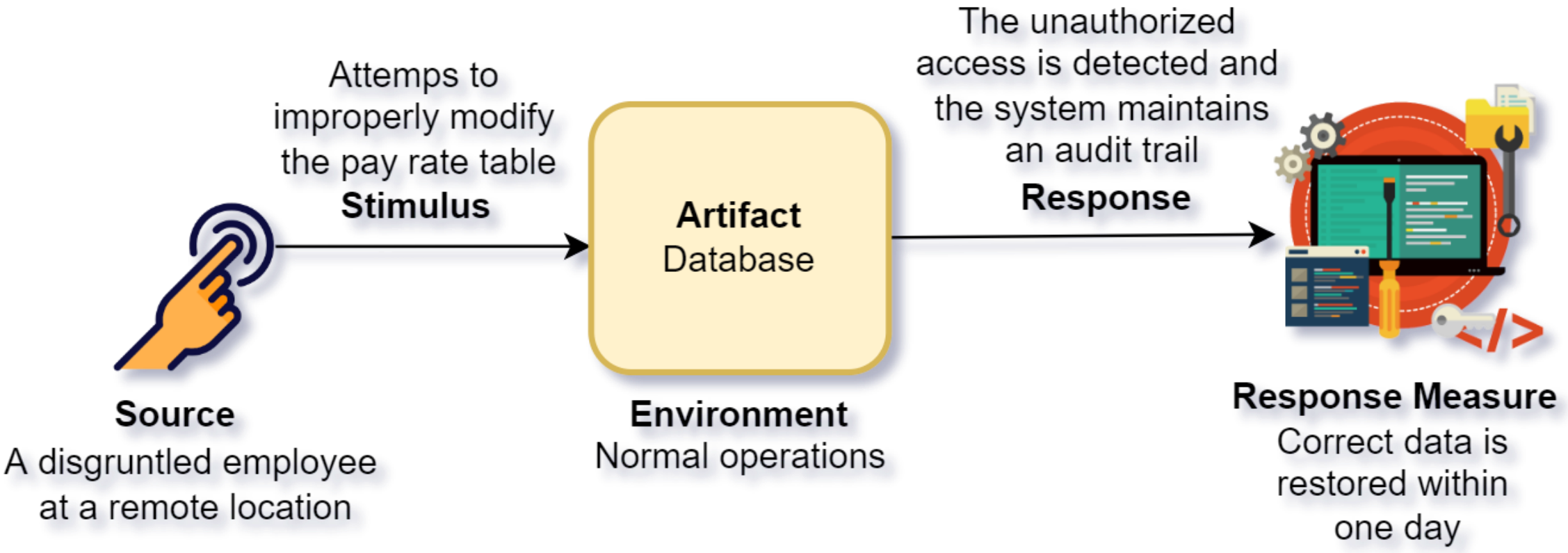
# Security – General Scenario (1/2)

| Portion of Scenario | Description | Possible Values |
|---|---|---|
| Source | The attack may be from outside the organization or from inside the organization. The source of the attack may be either a human or another system. | - Human<br>- Another system<br>Which is:<br>- Inside the organization<br>- Out ide the organization<br>- Previously identified<br>- Unknown |
| Stimulus | The stimulus is an attack. | An unauthorized attempt to:<br>- Display, Capture or Change data<br>- Access system services<br>- Change the system's behavior<br>- Reduce availability |
| Artifact | What is the target of the attack? | - System services<br>- Data within the system<br>- A component or resource of the system<br>- Data produced or consumed by the system |
| Environment | What is the state of the system when the attack occurs? | The system is:<br>-Online or offline<br>- Connected to or disconnected from a network<br>- Behind a firewall or open to a network<br>- Fully operational<br>- Partially operational<br>- Not operational |

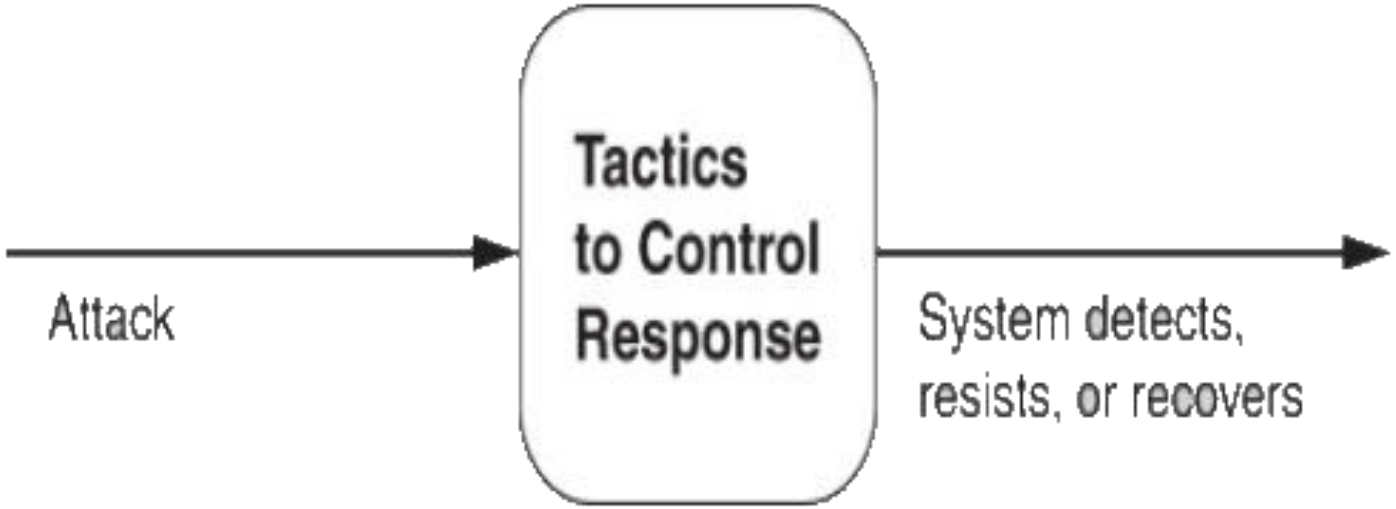
# Security – General Scenario (2/2)

| Portion of Scenario | Description | Possible Values |
|---|---|---|
| Response | The system ensures that confidentiality, integrity, and availability are maintained | Transactions are carried out in a fashion such that<br>- Data or services are protected from unauthorized access<br>- Data or services are not being manipulated without authorization<br>- Parties to a transaction are identified with assurance<br>- The parties to the transaction cannot repudiate their involvements<br>- The data, resources, and system services will be available for legitimate use<br>The system tracks activities within it by<br>- Recording access or modification<br>- Recording attempts to access data, resources, or services<br>- Notifying appropriate entities(people or systems) when an apparent attacks is occurring |
| Response measure | Measures of a system's response are related to the frequency of successful attacks, the time and cost to resist and repaid attacks, and the consequential damage of those attacks. | One or more of the following:<br>- How much of a resource is compromised or ensured<br>- Accuracy of attacks detection<br>- How much time passed before an attacks was detected<br>- How many attacks were resisted<br>- How long it takes to recover from a successful attacks<br>- How much data is vulnerable to a particular attacks |

# Security – Sample Scenario



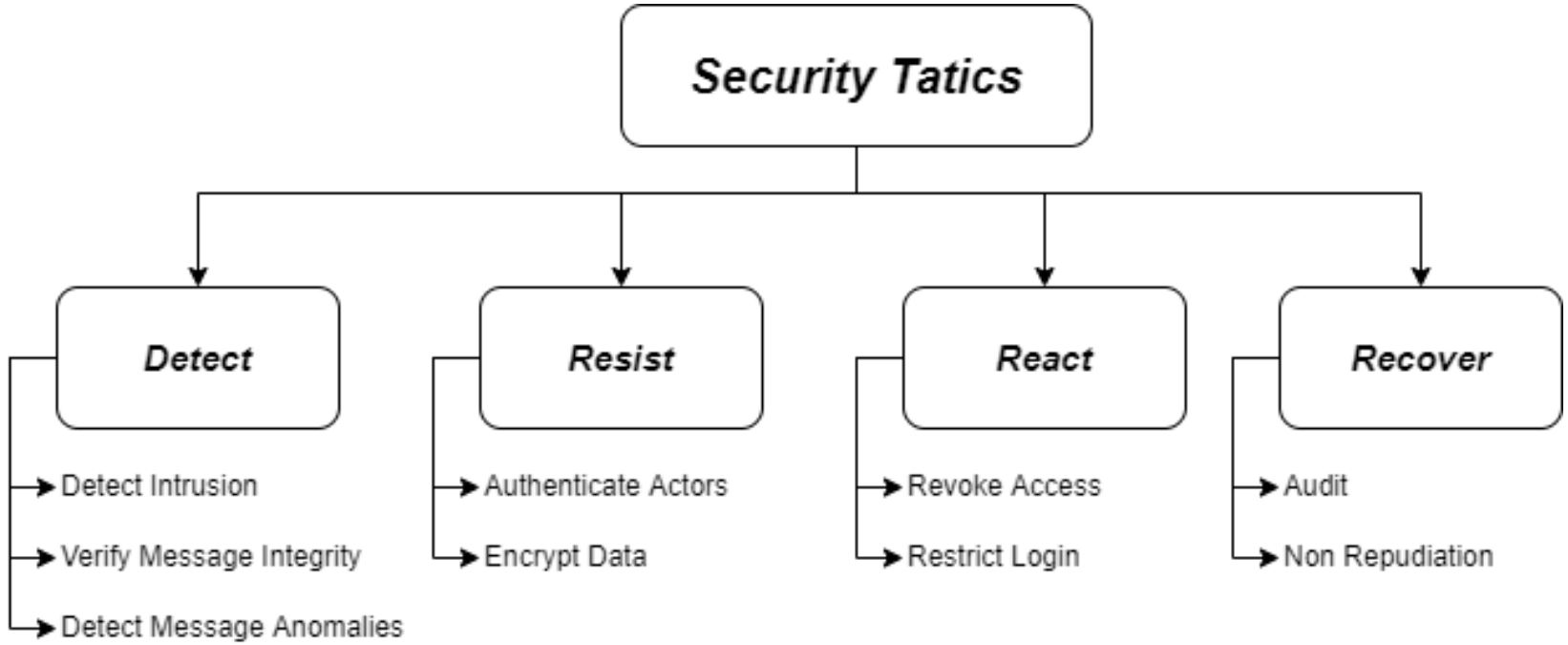
# Tactics for Security



# First Step – Physical Security

- ***Limited access*** *(e.g., fences and security checkpoint);*
- ***Detecting intruders*** *(e.g., visitors with badges);*
- ***Deterrence mechanisms*** *(e.g., armed guards);*
- ***Reaction mechanisms*** *(e.g., doors automatic lock, acoustic alarm);*
- ***Recovery mechanisms*** *(e.g., off-site backup);*

# Categories of Tactics




- ***Detect Attacks**: identify attacks before it takes effect;*
- ***Resist Attacks**: prevent possible attack;*
- ***React to Attacks**: resist to ongoing attacks;*
- ***Recover from Attacks**: restore system successful attacks;*

# Categories of Tactics – Detect Attacks

- ***Detect Intrusion****: compares network traffic with a set of known malicious patterns, based on payload size, port number, source or destination address etc.;*
- ***Verify message Integrity****: using of techniques, like checksum or hash value, to verify the integrity of messages, resource file, configuration files etc.;*
- ***Detect message delivery anomalies****: detect potential man-in-the-middle attack. Can be indicated by too long time for sending or receiving, or abnormal number of connection and disconnecting during communication;*

# Categories of Tactics – Resist Attacks

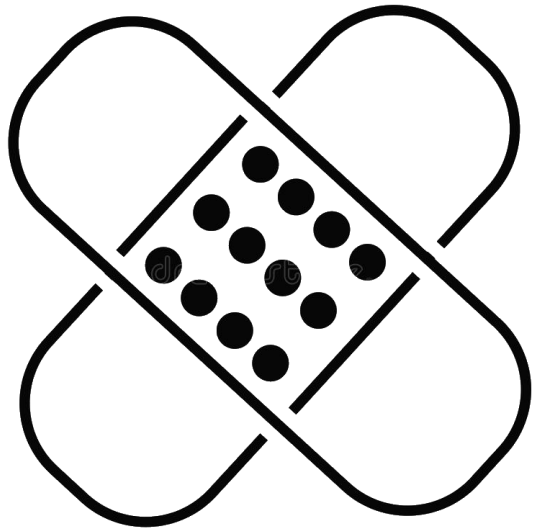
- ***Authenticate Actors**: ensuring that an actor is actually who (or what) it purports to be. Techniques to do that are password, OTP, biometric identification etc. Another example is CAPTCHA, a challenge-response test, used to verify if the user is human or not;*
- ***Encrypt Data**: provide extra protection on confidential data. This is the only useful protection for passing data over public access network;*

# Categories of Tactics – React to Attacks

- ***Revoke Access****: if the system notice that an attack is under way, access can be limited for sensitive resources, even for legitimate users, until the attack was not interrupted;*
- ***Restrict Login****: repeated failed login may indicate an attack, so we can limit access to a particular system after several failed login attempt. The lock-out period must be considered only for a certain period of time, because also legitimate users can make mistakes;*

# Categories of Tactics – Recover from Attacks

- ***Audit**: keep a record of user, system actions and their effects, to help trace all actions, and in case, identify an attacker. We can also analyze audit to see attack pattern, and create better defenses for future;*
- ***Non Repudiation**: guarantees that the sender of a message cannot deny the send of that message, and same of the receiver. This could be achieved with combination of digital signature and authentication by trusted parties;*



# Thanks for Your Attention