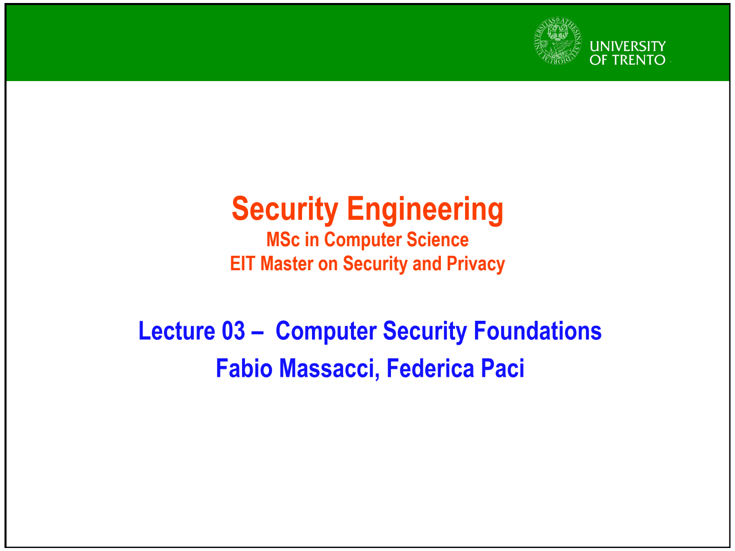


UNIVERSITY OF TRENTO

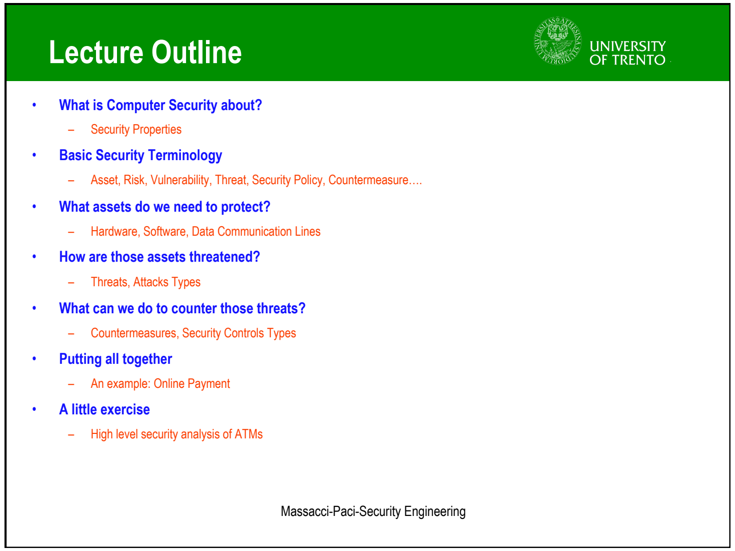
# Security Engineering

MSc in Computer Science

EIT Master on Security and Privacy

## Lecture 03 – Computer Security Foundations

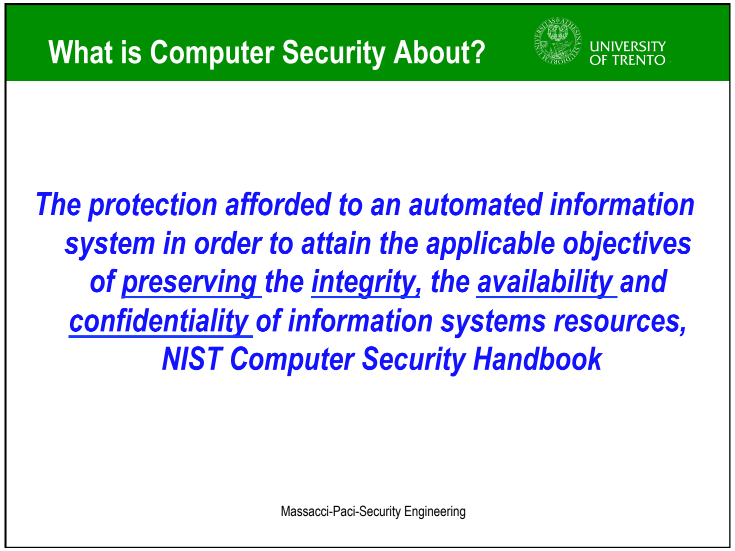
Fabio Massacci, Federica Paci



## Lecture Outline

UNIVERSITY OF TRENTO

- What is Computer Security about?
  - Security Properties
- Basic Security Terminology
  - Asset, Risk, Vulnerability, Threat, Security Policy, Countermeasure….
- What assets do we need to protect?
  - Hardware, Software, Data Communication Lines
- How are those assets threatened?
  - Threats, Attacks Types
- What can we do to counter those threats?
  - Countermeasures, Security Controls Types
- Putting all together
  - An example: Online Payment
- A little exercise
  - High level security analysis of ATMs

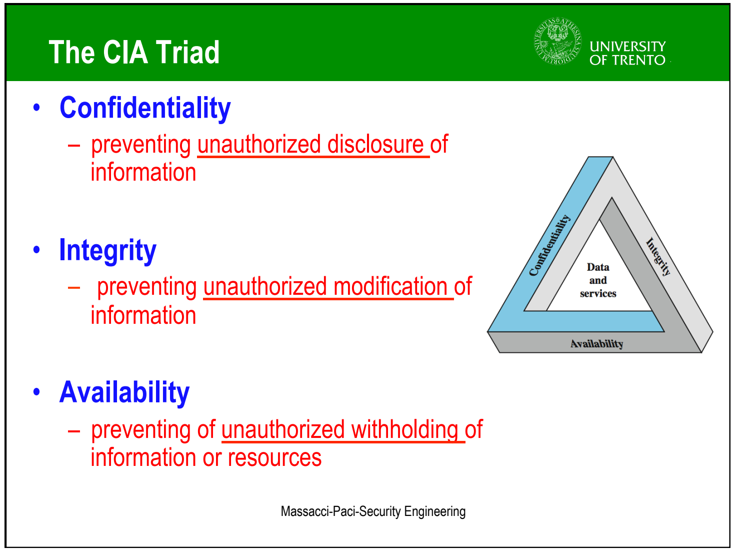


## What is Computer Security About?

UNIVERSITY OF TRENTO

*The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, the availability and confidentiality of information systems resources,*

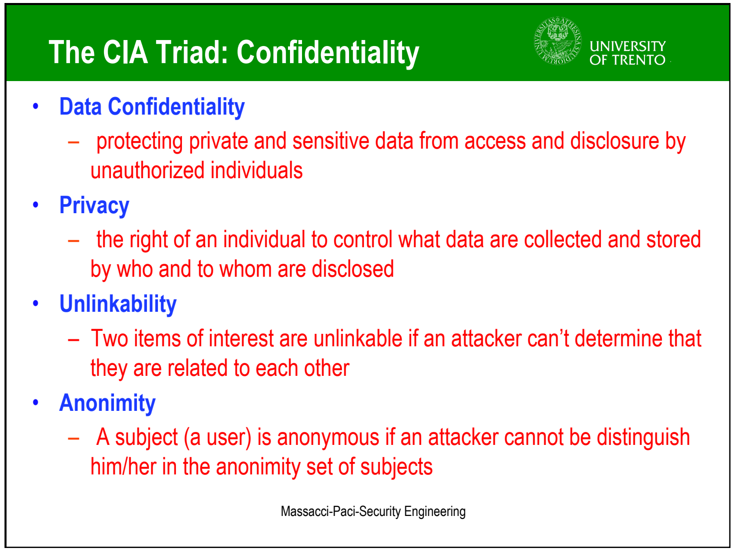
*NIST Computer Security Handbook*



## The CIA Triad

UNIVERSITY OF TRENTO

- **Confidentiality**
  - preventing unauthorized disclosure of information
- **Integrity**
  - preventing unauthorized modification of information
- **Availability**
  - preventing of unauthorized withholding of information or resources

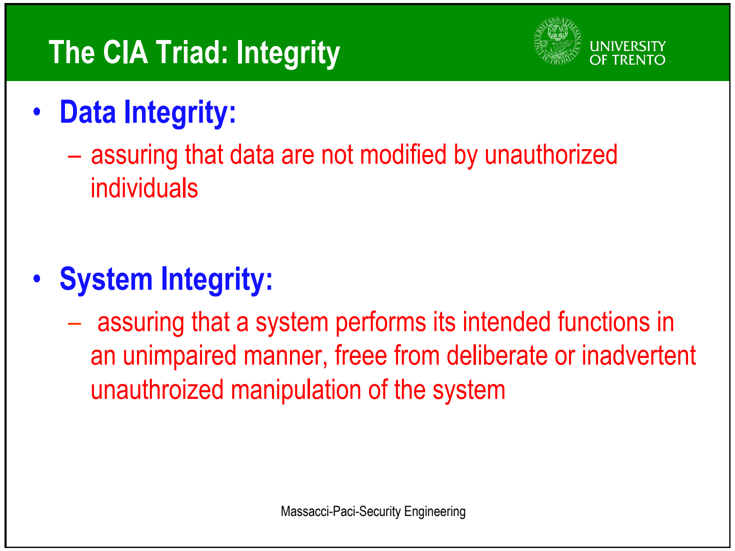


## The CIA Triad: Confidentiality

UNIVERSITY OF TRENTO

- Data Confidentiality
  - protecting private and sensitive data from access and disclosure by unauthorized individuals
- Privacy
  - the right of an individual to control what data are collected and stored by who and to whom are disclosed
- Unlinkability
  - Two items of interest are unlinkable if an attacker can't determine that they are related to each other
- Anonimity
  - A subject (a user) is anonymous if an attacker cannot be distinguish him/her in the anonimity set of subjects

Massacci-Paci-Security Engineering

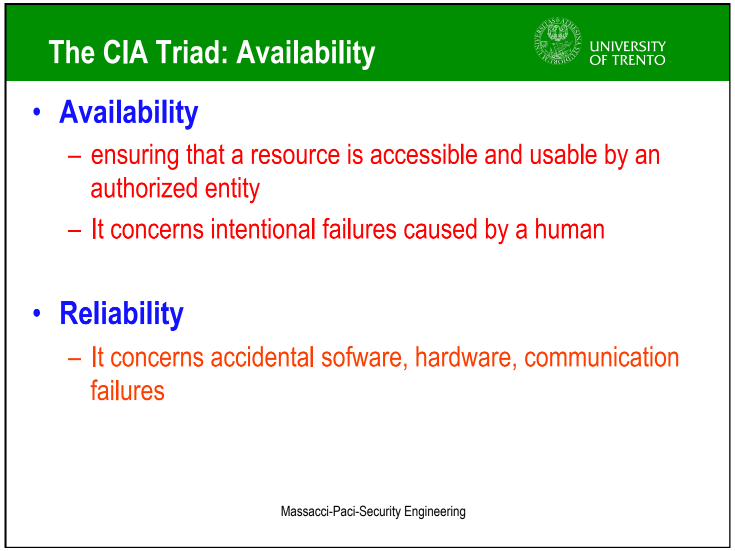


## The CIA Triad: Integrity

UNIVERSITY OF TRENTO

- Data Integrity:
  - assuring that data are not modified by unauthorized individuals
- System Integrity:
  - assuring that a system performs its intended functions in an unimpaired manner, freee from deliberate or inadvertent unauthroized manipulation of the system

Massacci-Paci-Security Engineering

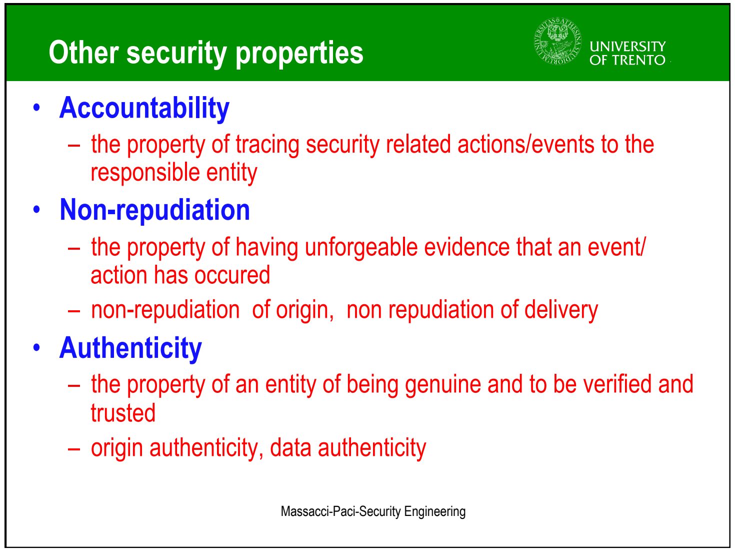


## The CIA Triad: Availability

UNIVERSITY OF TRENTO

- Availability
  - ensuring that a resource is accessible and usable by an authorized entity
  - It concerns intentional failures caused by a human
- Reliability
  - It concerns accidental sofware, hardware, communication failures

Massacci-Paci-Security Engineering

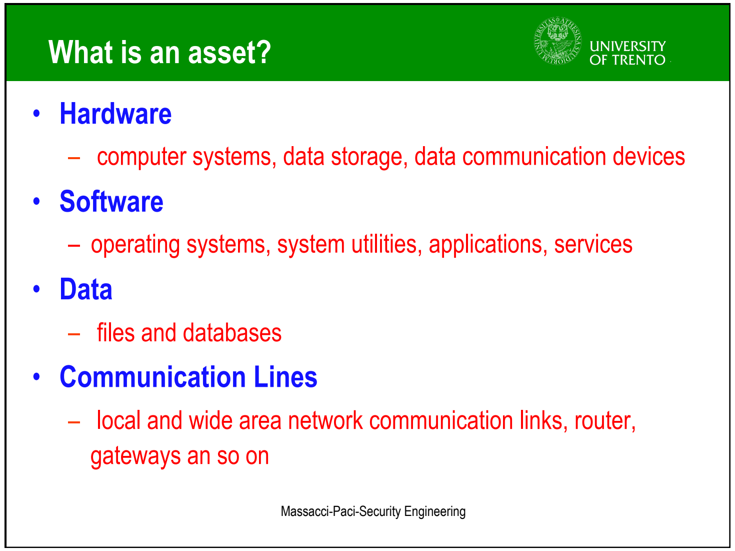


## Other security properties

UNIVERSITY OF TRENTO

- Accountability
  - the property of tracing security related actions/events to the responsible entity
- Non-repudiation
  - the property of having unforgeable evidence that an event/ action has occured
  - non-repudiation of origin, non repudiation of delivery
- Authenticity
  - the property of an entity of being genuine and to be verified and trusted
  - origin authenticity, data authenticity

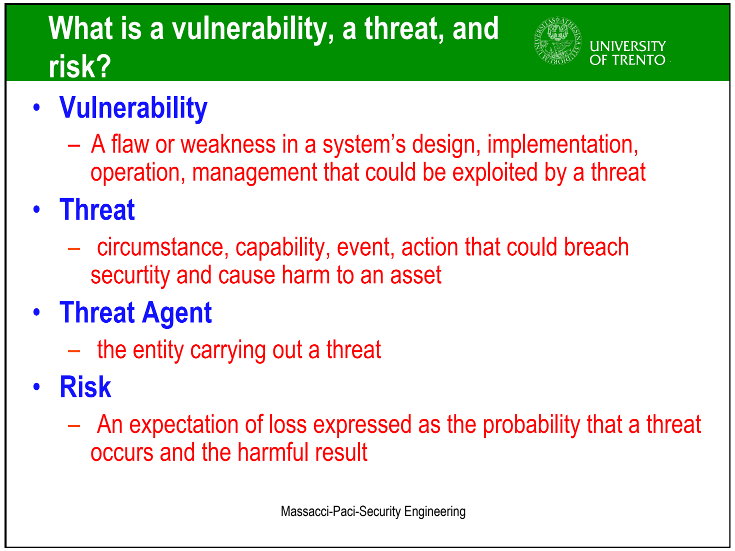
Massacci-Paci-Security Engineering



## What is an asset?

UNIVERSITY OF TRENTO

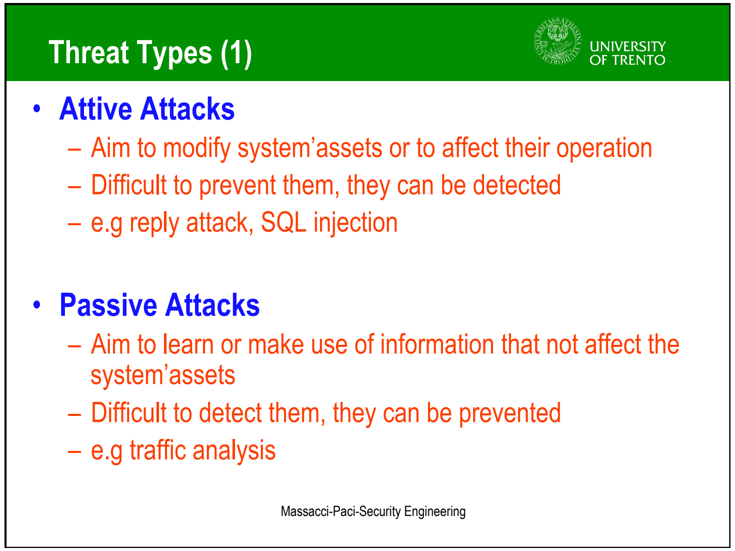
- **Hardware**
  - computer systems, data storage, data communication devices
- **Software**
  - operating systems, system utilities, applications, services
- **Data**
  - files and databases
- **Communication Lines**
  - local and wide area network communication links, router, gateways an so on



## What is a vulnerability, a threat, and risk?

UNIVERSITY OF TRENTO

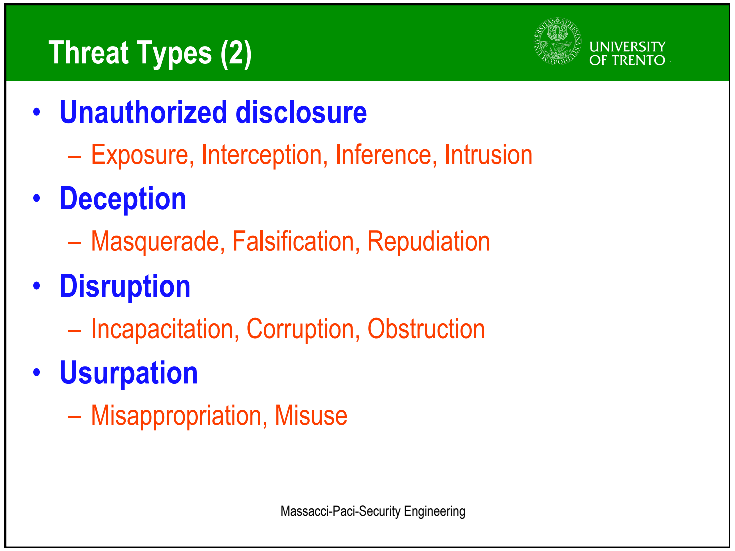
- **Vulnerability**
  - A flaw or weakness in a system's design, implementation, operation, management that could be exploited by a threat
- **Threat**
  - circumstance, capability, event, action that could breach secturity and cause harm to an asset
- **Threat Agent**
  - the entity carrying out a threat
- **Risk**
  - An expectation of loss expressed as the probability that a threat occurs and the harmful result



## Threat Types (1)

UNIVERSITY OF TRENTO

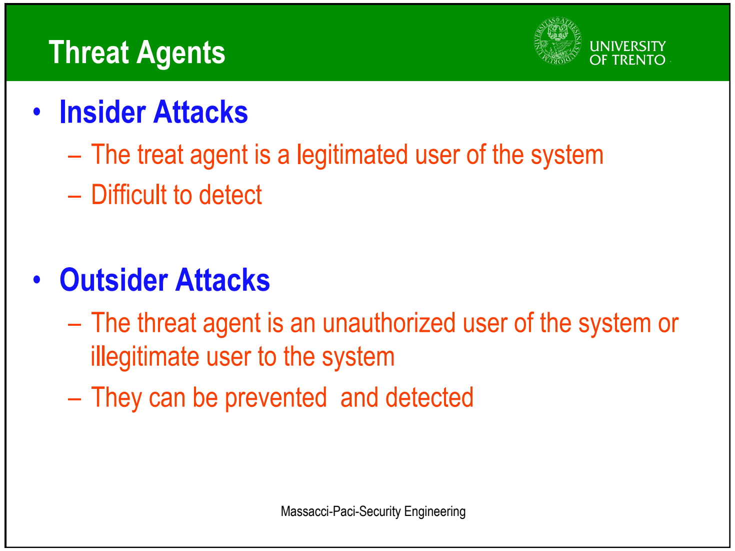
- **Attive Attacks**
  - Aim to modify system'assets or to affect their operation
  - Difficult to prevent them, they can be detected
  - e.g reply attack, SQL injection
- **Passive Attacks**
  - Aim to learn or make use of information that not affect the system'assets
  - Difficult to detect them, they can be prevented
  - e.g traffic analysis



## Threat Types (2)

UNIVERSITY OF TRENTO

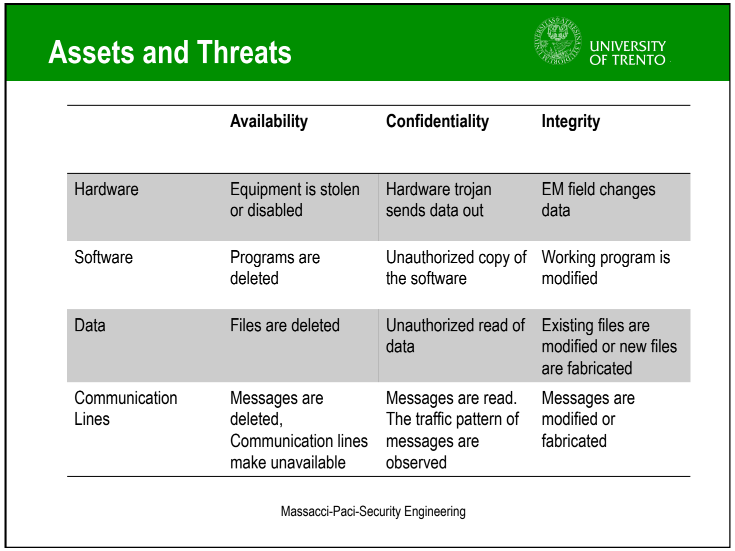
- **Unauthorized disclosure**
  - Exposure, Interception, Inference, Intrusion
- **Deception**
  - Masquerade, Falsification, Repudiation
- **Disruption**
  - Incapacitation, Corruption, Obstruction
- **Usurpation**
  - Misappropriation, Misuse



## Threat Agents

UNIVERSITY OF TRENTO

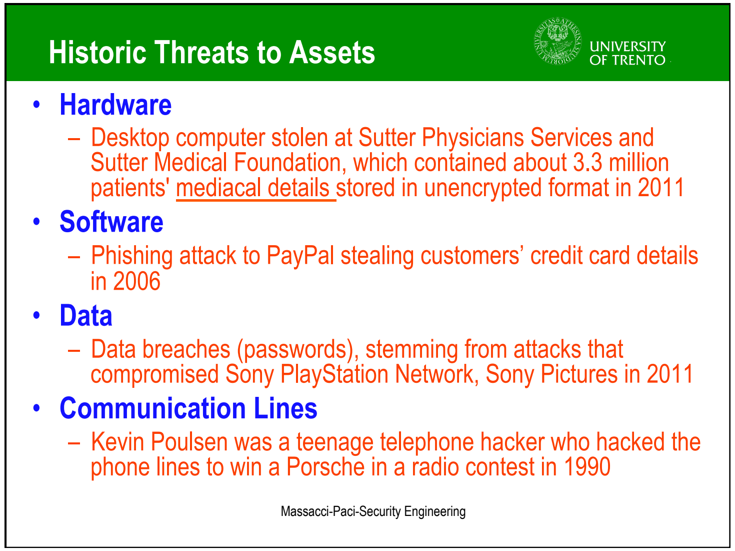
- **Insider Attacks**
  - The treat agent is a legitimated user of the system
  - Difficult to detect
- **Outsider Attacks**
  - The threat agent is an unauthorized user of the system or illegitimate user to the system
  - They can be prevented  and detected



## Assets and Threats

UNIVERSITY OF TRENTO

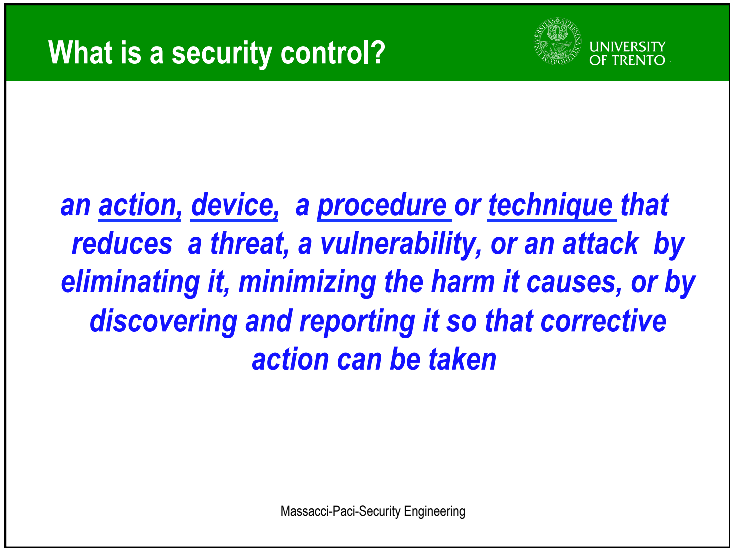
| | Availability | Confidentiality | Integrity |
|---|---|---|---|
| Hardware | Equipment is stolen or disabled | Hardware trojan sends data out | EM field changes data |
| Software | Programs are deleted | Unauthorized copy of the software | Working program is modified |
| Data | Files are deleted | Unauthorized read of data | Existing files are modified or new files are fabricated |
| Communication Lines | Messages are deleted, Communication lines make unavailable | Messages are read. The traffic pattern of messages are observed | Messages are modified or fabricated |



## Historic Threats to Assets

UNIVERSITY OF TRENTO

- **Hardware**
  - Desktop computer stolen at Sutter Physicians Services and Sutter Medical Foundation, which contained about 3.3 million patients' mediacal details stored in unencrypted format in 2011
- **Software**
  - Phishing attack to PayPal stealing customers' credit card details in 2006
- **Data**
  - Data breaches (passwords), stemming from attacks that compromised Sony PlayStation Network, Sony Pictures in 2011
- **Communication Lines**
  - Kevin Poulsen was a teenage telephone hacker who hacked the phone lines to win a Porsche in a radio contest in 1990



## What is a security control?

UNIVERSITY OF TRENTO

***an action, device,  a procedure or technique that reduces  a threat, a vulnerability, or an attack  by eliminating it, minimizing the harm it causes, or by discovering and reporting it so that corrective action can be taken***

## Types of Security Controls

- **Management Controls**
  - Awareness and Training
  - Security policy and practices
  - Audit and Accountability
  - Risk-assessment
  - Contingency Planning
- **Technical Controls**
  - Identification and authentication
  - Access and authorization
  - Encryption
  - Digital Signature
  - Privacy-enhancing technologies

## When they can be applied?

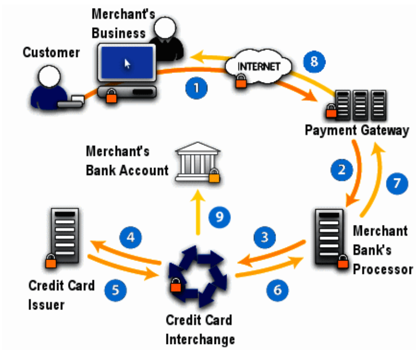
- **Preventive**
  - Measures that prevent your assets to be damaged
- **Detective**
  - Measures that allow to detect when an assets has been damaged, how it has been damaged, and by who
- **Reactive**
  - Measures that allow to recover your assets or recover from damage to your assets

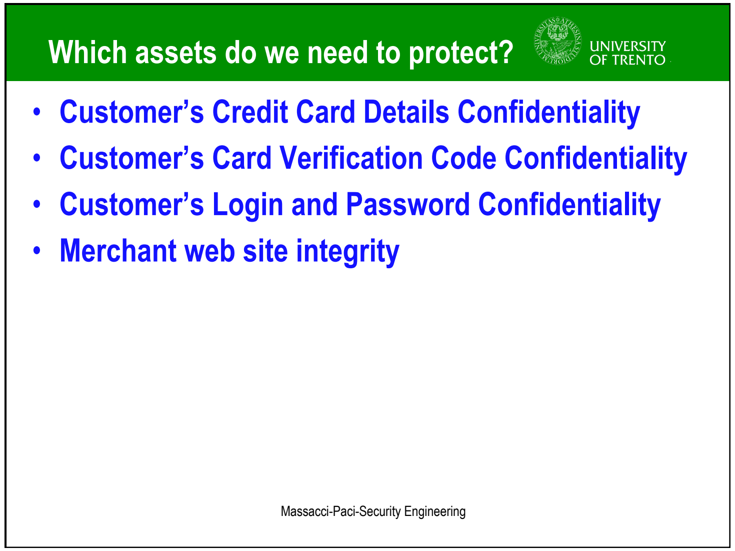
## Where security controls should be placed?

- **You need to find**
  - right layer for each security control
  - right security control for each layer
- **Usually three levels**
  - Users (Database access controls)
  - Applications
  - Infrastructure

| |
|---|
| Applications |
| Services |
| Operating System |
| OS Kernel |
| Hardware |

## Putting all together: Online Payment



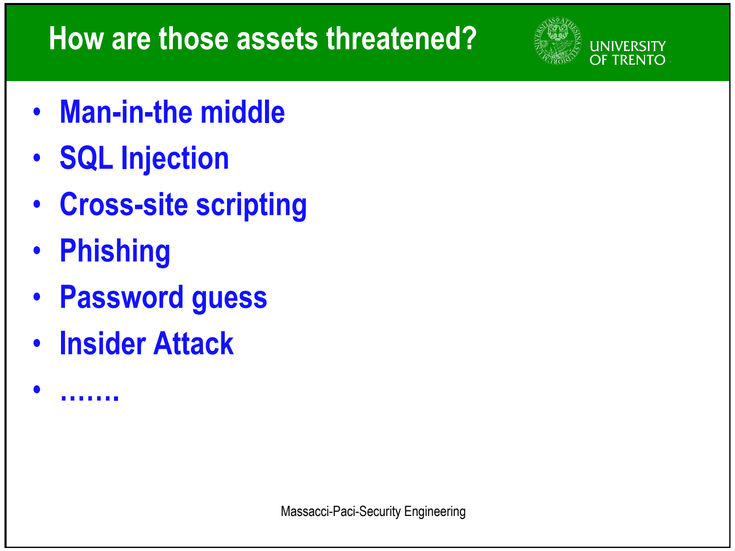


## Which assets do we need to protect?

UNIVERSITY OF TRENTO

- Customer's Credit Card Details Confidentiality
- Customer's Card Verification Code Confidentiality
- Customer's Login and Password Confidentiality
- Merchant web site integrity

Massacci-Paci-Security Engineering

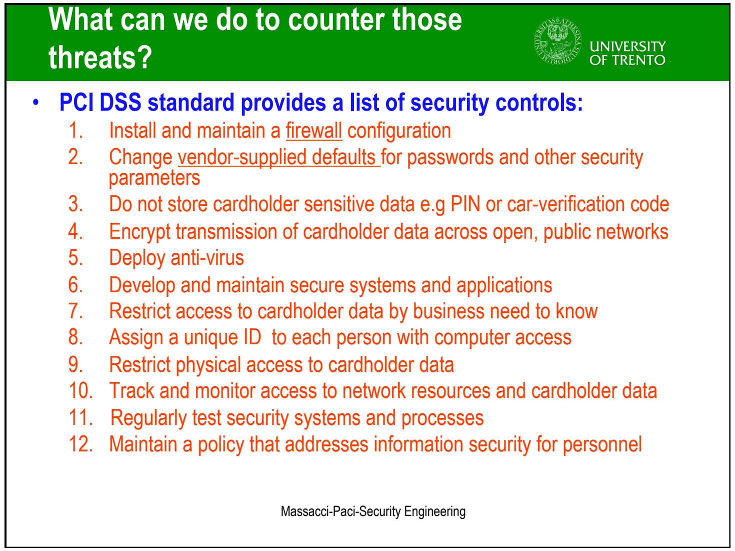


## How are those assets threatened?

UNIVERSITY OF TRENTO

- Man-in-the middle
- SQL Injection
- Cross-site scripting
- Phishing
- Password guess
- Insider Attack
- …….

Massacci-Paci-Security Engineering

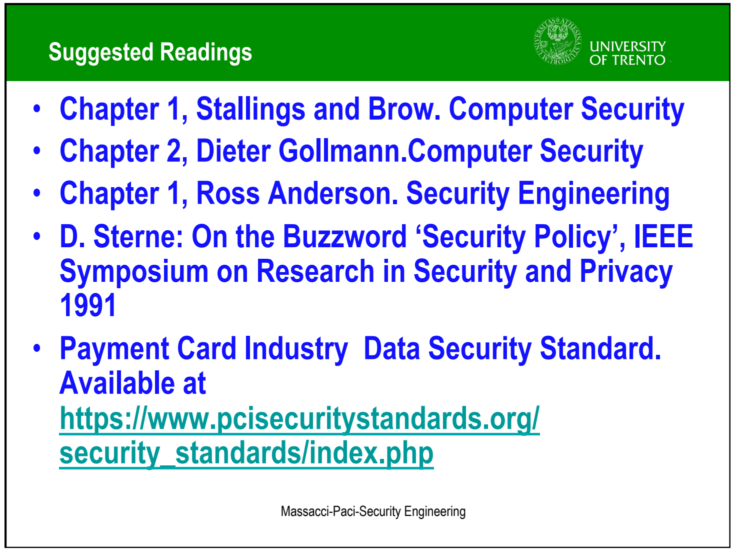


## What can we do to counter those threats?

UNIVERSITY OF TRENTO

- PCI DSS standard provides a list of security controls:
  1. Install and maintain a firewall configuration
  2. Change vendor-supplied defaults for passwords and other security parameters
  3. Do not store cardholder sensitive data e.g PIN or car-verification code
  4. Encrypt transmission of cardholder data across open, public networks
  5. Deploy anti-virus
  6. Develop and maintain secure systems and applications
  7. Restrict access to cardholder data by business need to know
  8. Assign a unique ID  to each person with computer access
  9. Restrict physical access to cardholder data
  10. Track and monitor access to network resources and cardholder data
  11. Regularly test security systems and processes
  12. Maintain a policy that addresses information security for personnel

Massacci-Paci-Security Engineering



## Suggested Readings

UNIVERSITY OF TRENTO

- Chapter 1, Stallings and Brow. Computer Security
- Chapter 2, Dieter Gollmann.Computer Security
- Chapter 1, Ross Anderson. Security Engineering
- D. Sterne: On the Buzzword 'Security Policy', IEEE Symposium on Research in Security and Privacy 1991
- Payment Card Industry  Data Security Standard. Available at https://www.pcisecuritystandards.org/security_standards/index.php

Massacci-Paci-Security Engineering