FITNESS

FAULT AND INTRUSION TOLERANT NETWORKED SYSTEMS

Fondamenti di Cybersecurity

Prof. Luigi Romano
Commissione CRUI ICT e Università degli Studi di Napoli “Parthenope”

Webinar Internet Governance
01 dicembre, 2025

Objectives of this talk

1. Define the basic concepts and terminology of the security domain
2. Provide a “bird’s eye view” of main security issues
3. Put things into context, with respect to some major application domains

FITNESS

FAULT AND INTRUSION TOLERANT NETWORKED SYSTEMS

Basic concepts and terminology

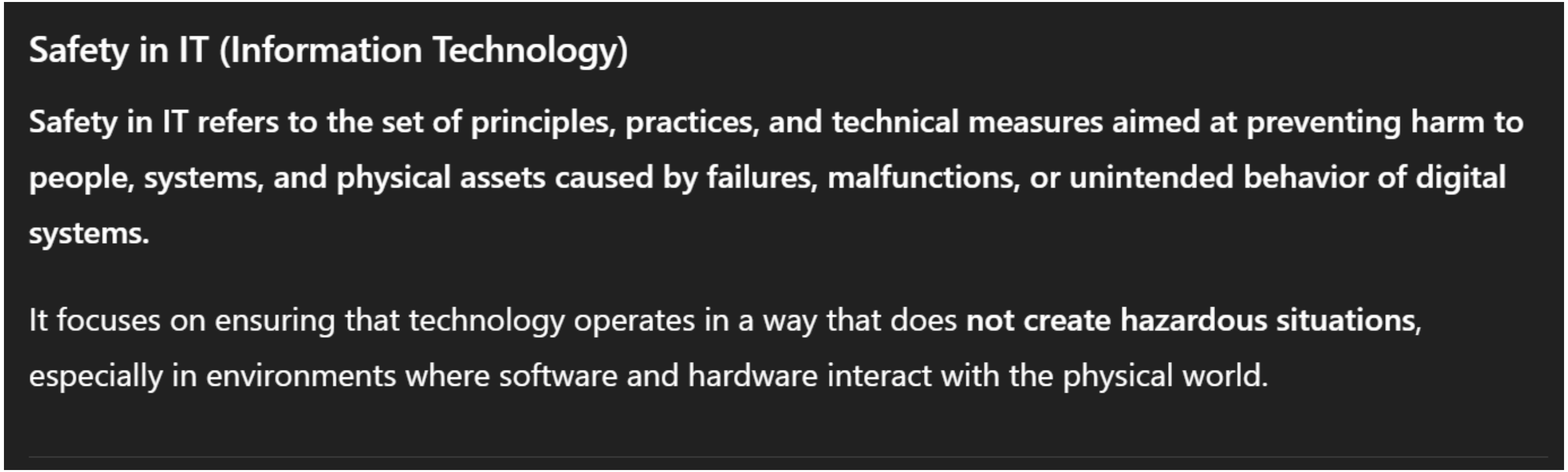
Security

- The CIA Triad:
  - C = Confidentiality
    - Ensures that data is accessible only to authorized individuals
    - Prevents the unauthorized disclosure of information
  - I = Integrity
    - Ensures that data is not altered or tampered with without authorization
    - Guarantees that information remains accurate and complete
  - A = Availability
    - Ensures that data and resources are accessible when needed
    - Guarantees the functioning of systems and timely access to information

A famous spot by Oracle

BRAND
SLOGANS
ORACLE
Can't break it, can't break-in

Safety

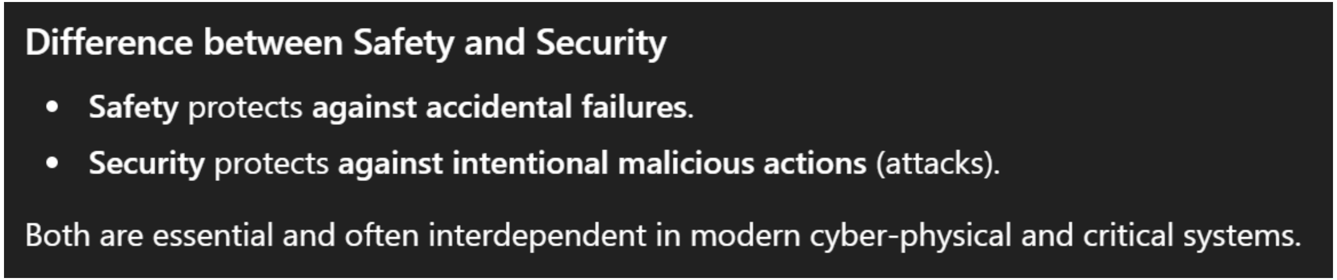


Safety in IT (Information Technology)

Safety in IT refers to the set of principles, practices, and technical measures aimed at preventing harm to people, systems, and physical assets caused by failures, malfunctions, or unintended behavior of digital systems.

It focuses on ensuring that technology operates in a way that does **not create hazardous situations**, especially in environments where software and hardware interact with the physical world.

Difference bw Safety and Security

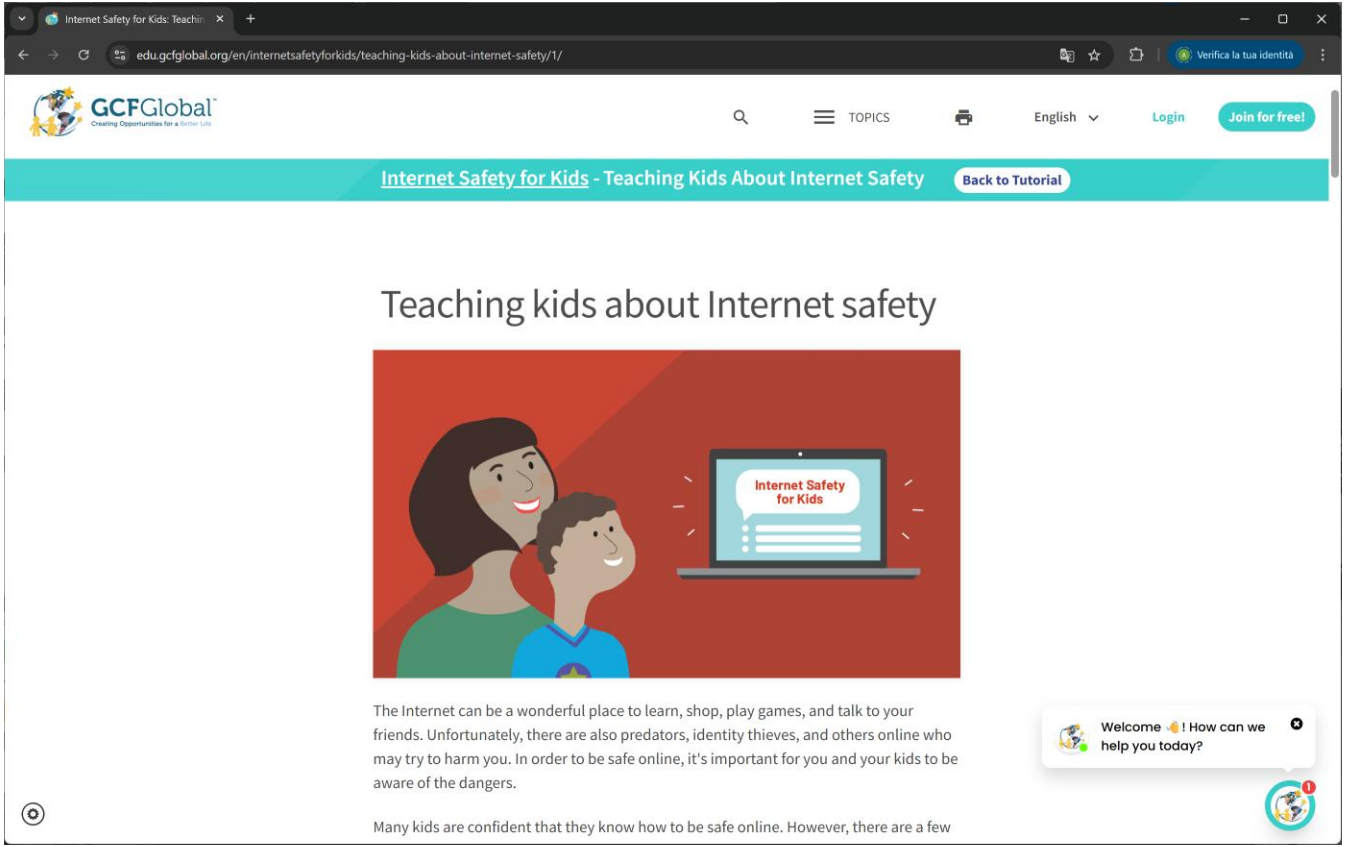


Difference between Safety and Security

- **Safety** protects **against accidental failures**.
- **Security** protects **against intentional malicious actions** (attacks).

Both are essential and often interdependent in modern cyber-physical and critical systems.

Internet Safety

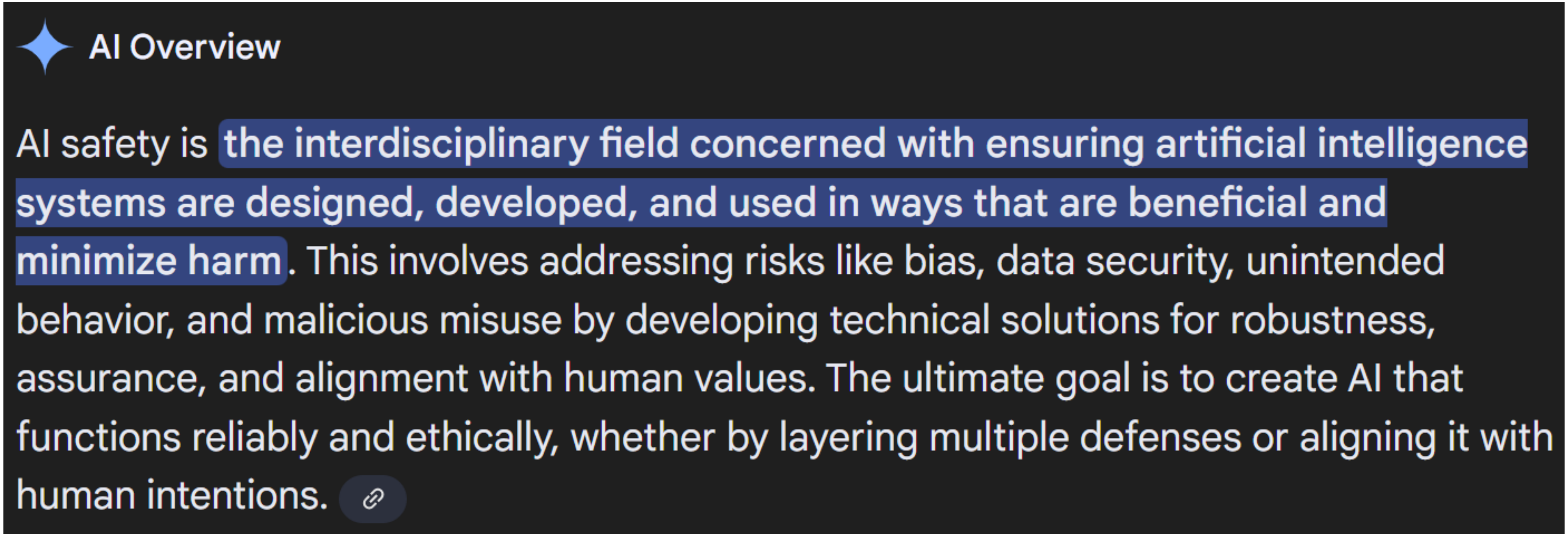

Internet Safety for Kids: Teachin
edu.gcfglobal.org/en/internetsafetyforkids/teaching-kids-about-internet-safety/1/
Verifica la tua identità
GCFGlobal
Creating Opportunities for a Better Life
TOPICS
English
Login
Join for free!
Internet Safety for Kids - Teaching Kids About Internet Safety
Back to Tutorial
Internet Safety for Kids
Welcome 👋! How can we help you today?
1

Teaching kids about Internet safety

The Internet can be a wonderful place to learn, shop, play games, and talk to your friends. Unfortunately, there are also predators, identity thieves, and others online who may try to harm you. In order to be safe online, it's important for you and your kids to be aware of the dangers.

Many kids are confident that they know how to be safe online. However, there are a few

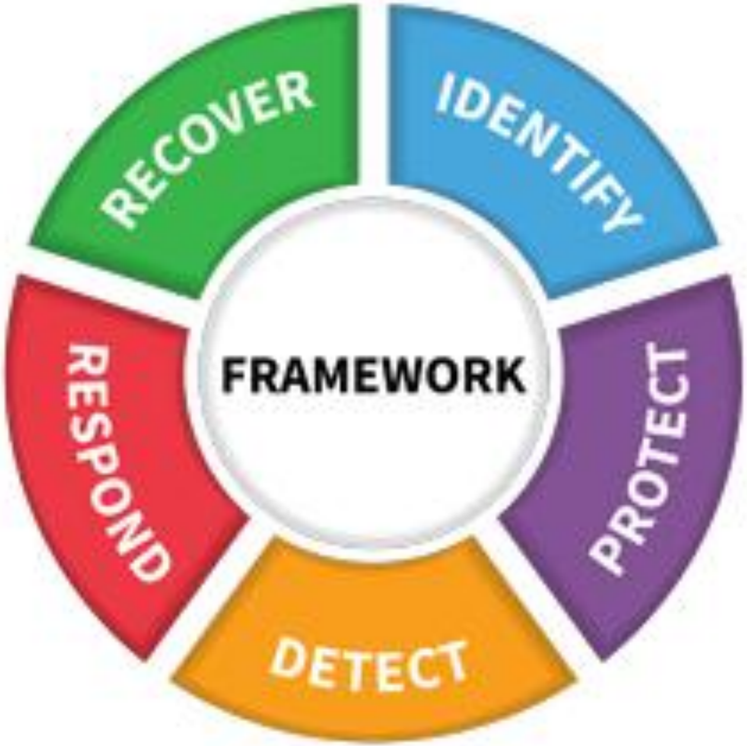
AI Safety



AI Overview

AI safety is the interdisciplinary field concerned with ensuring artificial intelligence systems are designed, developed, and used in ways that are beneficial and minimize harm. This involves addressing risks like bias, data security, unintended behavior, and malicious misuse by developing technical solutions for robustness, assurance, and alignment with human values. The ultimate goal is to create AI that functions reliably and ethically, whether by layering multiple defenses or aligning it with human intentions.

NIST Cybersecurity Cycle



Threat

- A threat is something that represents a menace to the system
  - Example: Hackers are a threat
- As such, a threat by itself does not violate security properties, since it does not make any damage to the system
- The fact that there are hackers in the environment does not – at least not immediately – imply that the ICT system will be violated

Vulnerability

- A vulnerability is a flaw in the system (or in the surrounding environment, or in the way the system interacts with the environment/users) that may enable an attacker to violate the system
- Again, a vulnerability is not by itself a violation
- Rather, its existence is the pre-condition for an attack, which is the only thing that can actually result in a violation
  - Example: if the system includes code that is vulnerable to buffer overflow attacks, that code represents a vulnerability. Unless an attacker launches a buffer overflow attack, there is still no violation to the system.

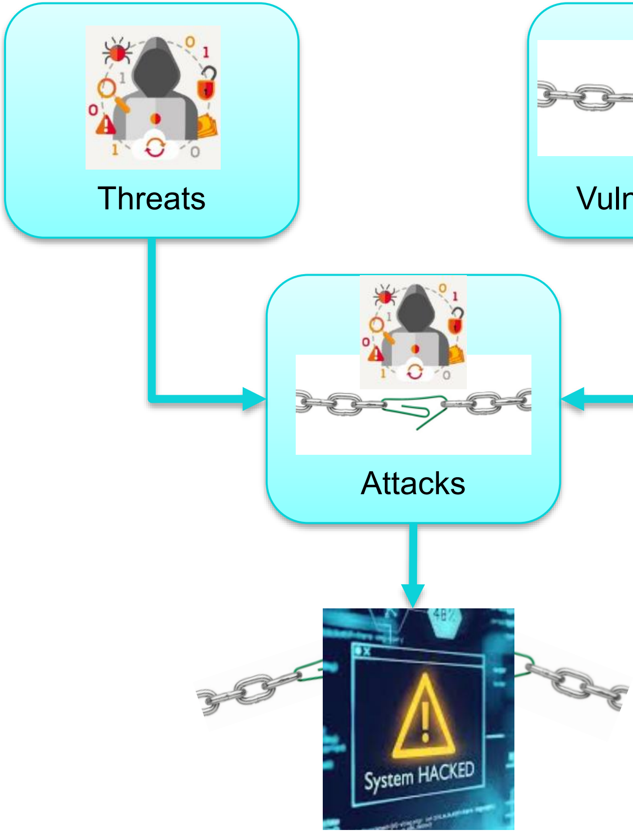
Intrusion

- An intrusion is the result of an attack
- More precisely, it is the result of a successful attack
- If an intrusion occurs, it is likely that the security of the system is violated

In practical terms

- A threat is something that represents a menace to the system
  - Example: Hackers are a threat
- As such, a threat by itself does not violate security properties, since it does not make any damage to the system
- The fact that there are hackers in the environment does not – at least not immediately – imply that the IT system will be violated

The activation process of an intrusion



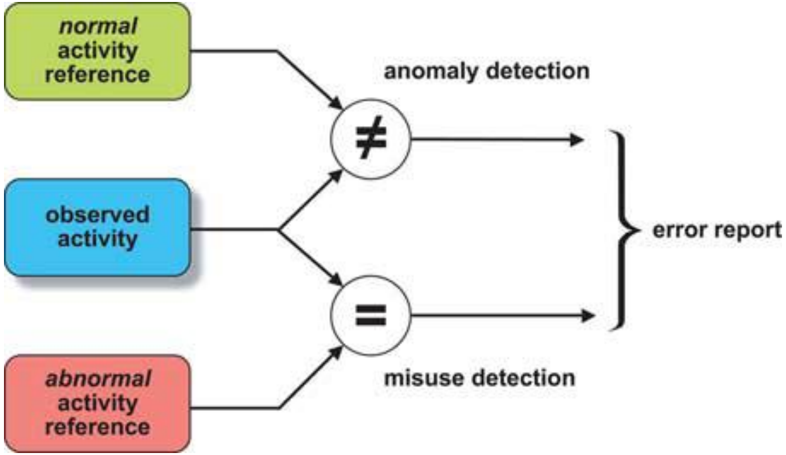
Threats

Vulnerabilities

Attacks

Improper use of words: example #1

- Currently available products only provide some (indeed limited) support in terms of Intrusion Prevention and Intrusion Detection, but they very much lack detailed and effective Intrusion Diagnosis capabilities



Intrusion =

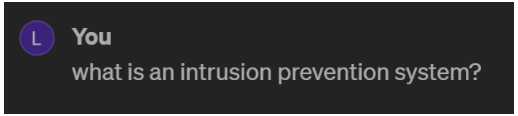
a successful **Attack**

to the system

There is quite a bit of confusion bw the two concepts in current IDS technology

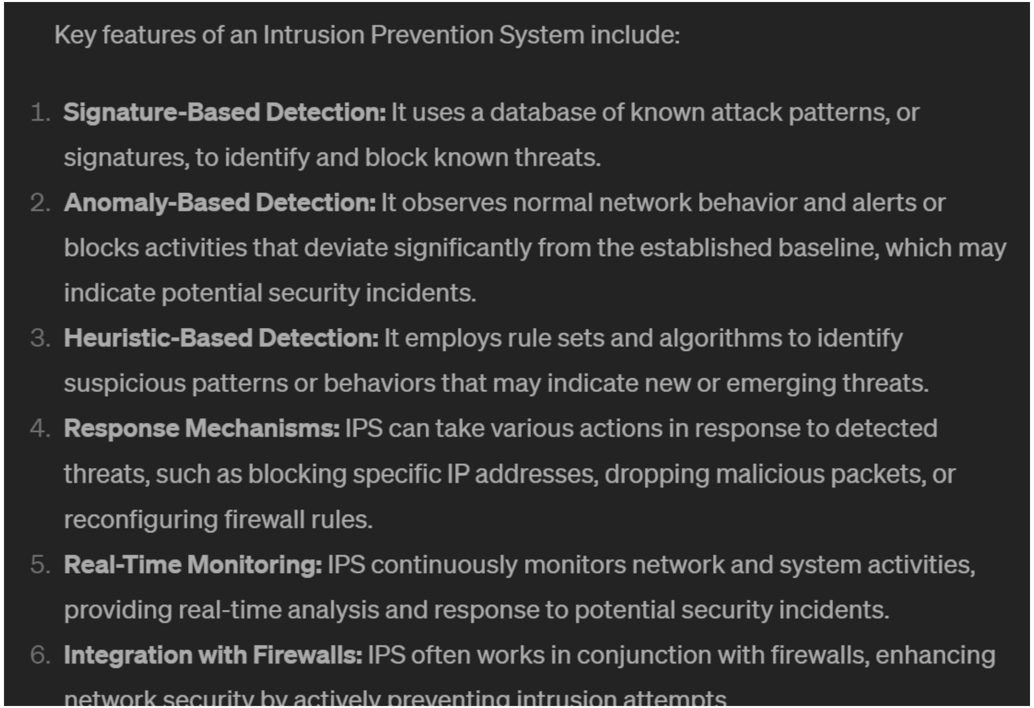
“Internet Security: An Intrusion-Tolerance Approach” , Deswarte Y., Powell D. - Proceedings of the IEEE, Volume 94, Issue 2, Feb. 2006 - Page(s):432 - 441

Improper use of words: example #2



You

what is an intrusion prevention system?



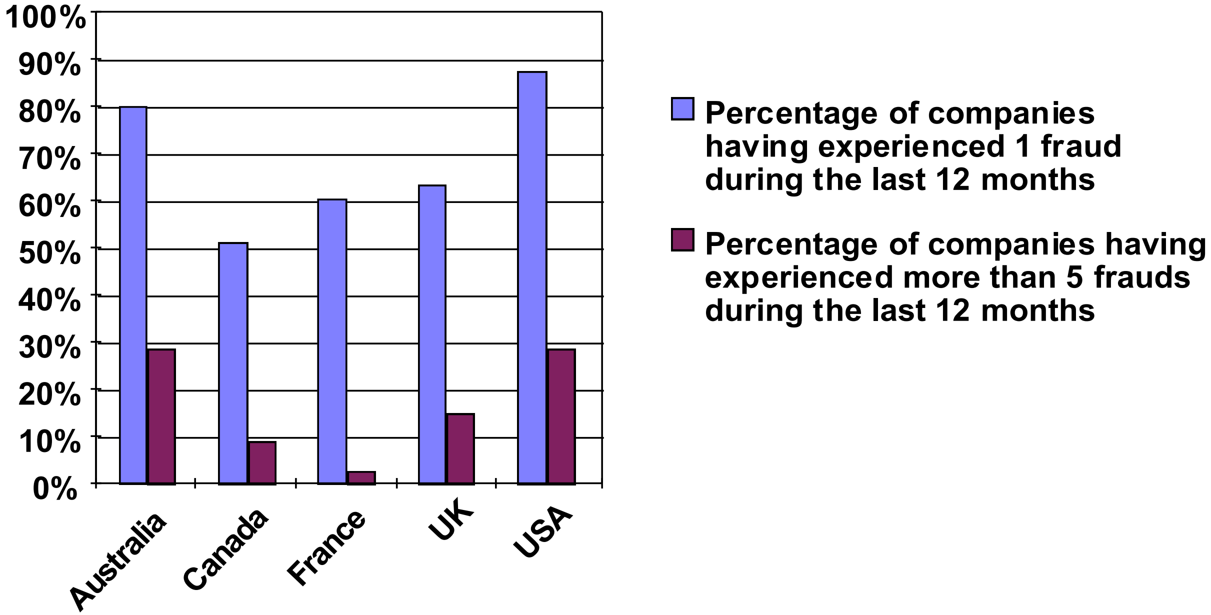
Key features of an Intrusion Prevention System include:

1. **Signature-Based Detection:** It uses a database of known attack patterns, or signatures, to identify and block known threats.
2. **Anomaly-Based Detection:** It observes normal network behavior and alerts or blocks activities that deviate significantly from the established baseline, which may indicate potential security incidents.
3. **Heuristic-Based Detection:** It employs rule sets and algorithms to identify suspicious patterns or behaviors that may indicate new or emerging threats.
4. **Response Mechanisms:** IPS can take various actions in response to detected threats, such as blocking specific IP addresses, dropping malicious packets, or reconfiguring firewall rules.
5. **Real-Time Monitoring:** IPS continuously monitors network and system activities, providing real-time analysis and response to potential security incidents.
6. **Integration with Firewalls:** IPS often works in conjunction with firewalls, enhancing network security by actively preventing intrusion attempts

The false myth of IDS

Malicious faults

[Ernst & Young, 1998 - 1200 companies surveyed in 32 countries]



- 84% of frauds are performed by employees

Cloud security

Cloud Service Models

- The type of cloud offerings (or service models) varies depending on the number of hardware and software layers managed by the provider
- Each service model targets a different user, also called tenant
- Generally, the cloud market proposes three solutions:

Software as a Service (SaaS) – Target: App Users

- e.g.: Google Docs, Office365, Dropbox, Apple iCloud

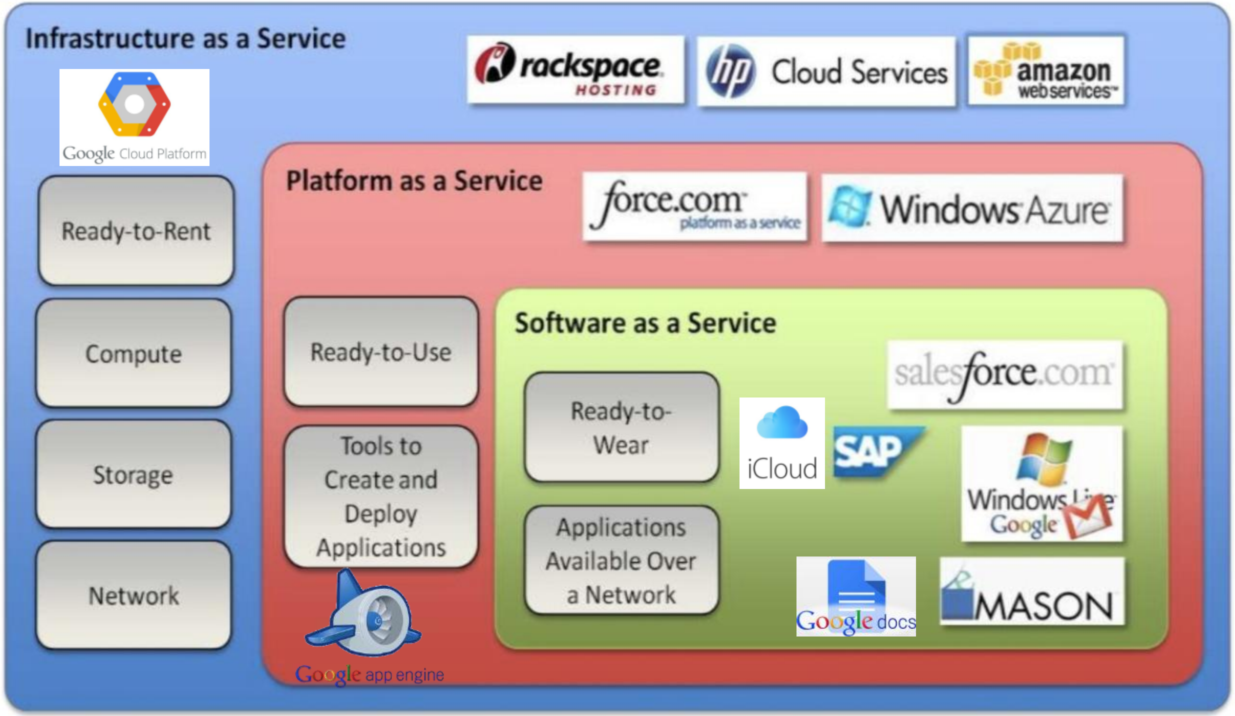
Plaform as a Service (PaaS) – Target: App Developers

- e.g.: RedHat OpenShift, Force.com, Google App engine

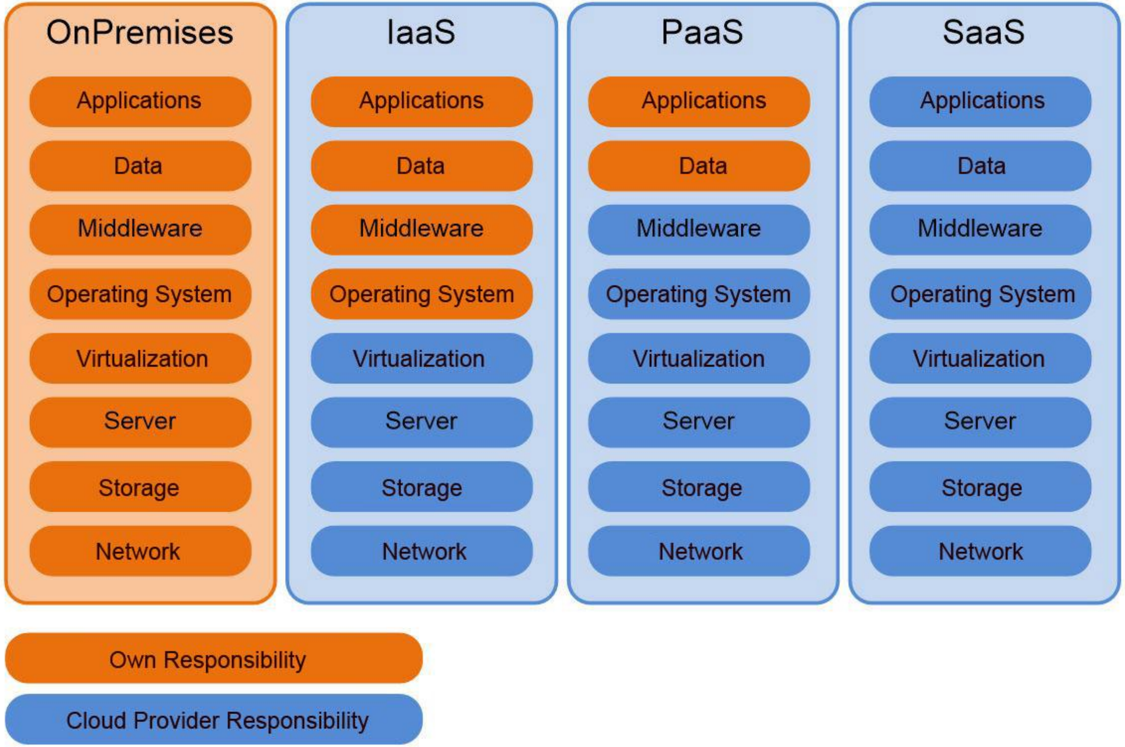
Infrastructure as a Service (IaaS) – Target: System Admin

- e.g.: Amazon AWS EC2, Microsoft Azure, Google Cloud

Examples of cloud service offerings



Liability distribution



OnPremises	IaaS	PaaS	SaaS
🟧 Applications	🟧 Applications	🟧 Applications	🟦 Applications
🟧 Data	🟧 Data	🟧 Data	🟦 Data
🟧 Middleware	🟧 Middleware	🟦 Middleware	🟦 Middleware
🟧 Operating System	🟧 Operating System	🟦 Operating System	🟦 Operating System
🟧 Virtualization	🟦 Virtualization	🟦 Virtualization	🟦 Virtualization
🟧 Server	🟦 Server	🟦 Server	🟦 Server
🟧 Storage	🟦 Storage	🟦 Storage	🟦 Storage
🟧 Network	🟦 Network	🟦 Network	🟦 Network

🟧 Own Responsibility

🟦 Cloud Provider Responsibility

Security increase brought by the Cloud

- Cloud technology provides protection from some types of attacks that are easy to realize on locally managed systems, since it ensures:
- Higher Physical Security. Cloud vendors often host their systems in facilities that have much stronger physical security controls against external intruders
- Advanced detection and prevention mechanisms for Denial of Service at the network level
- More frequent Security Patching and System Updates that prevent viruses or worms from exploiting software bugs
- Multi-factor authentication which is much more secure than the more traditional user name and password authentication

Example: Ransomware (WannaCry)

- A ransomware is a virus which infects a computer and freezes the machine and the files on it. It encrypts data and requests money
- The most recent (2017) ransomware was WannaCry, that infected more than 400k Windows machines
- Note: The patch for the exploited vulnerability was available 59 days prior to the attack
- Companies/people did not update their IT systems (i.e. the OS)
- The adoption of cloud ensures that systems are always up to date and patched
- Attacks like WannaCry - or more in general a high percentage of viruses - would not have been possible

Security decrease brought by the Cloud

- Outsourced company systems and services are exposed to a number of confidentiality and integrity risks
- Some attacks have ancient origins, others leverage typical cloud features
- The Cloud Security Alliance (CSA) identified the following top threats:
  - Account/Service Hijacking
  - Shared Technology Vulnerabilities
  - DDoS/DoS at application layer
  - Extrusion Attacks
  - **Malicious Insiders**

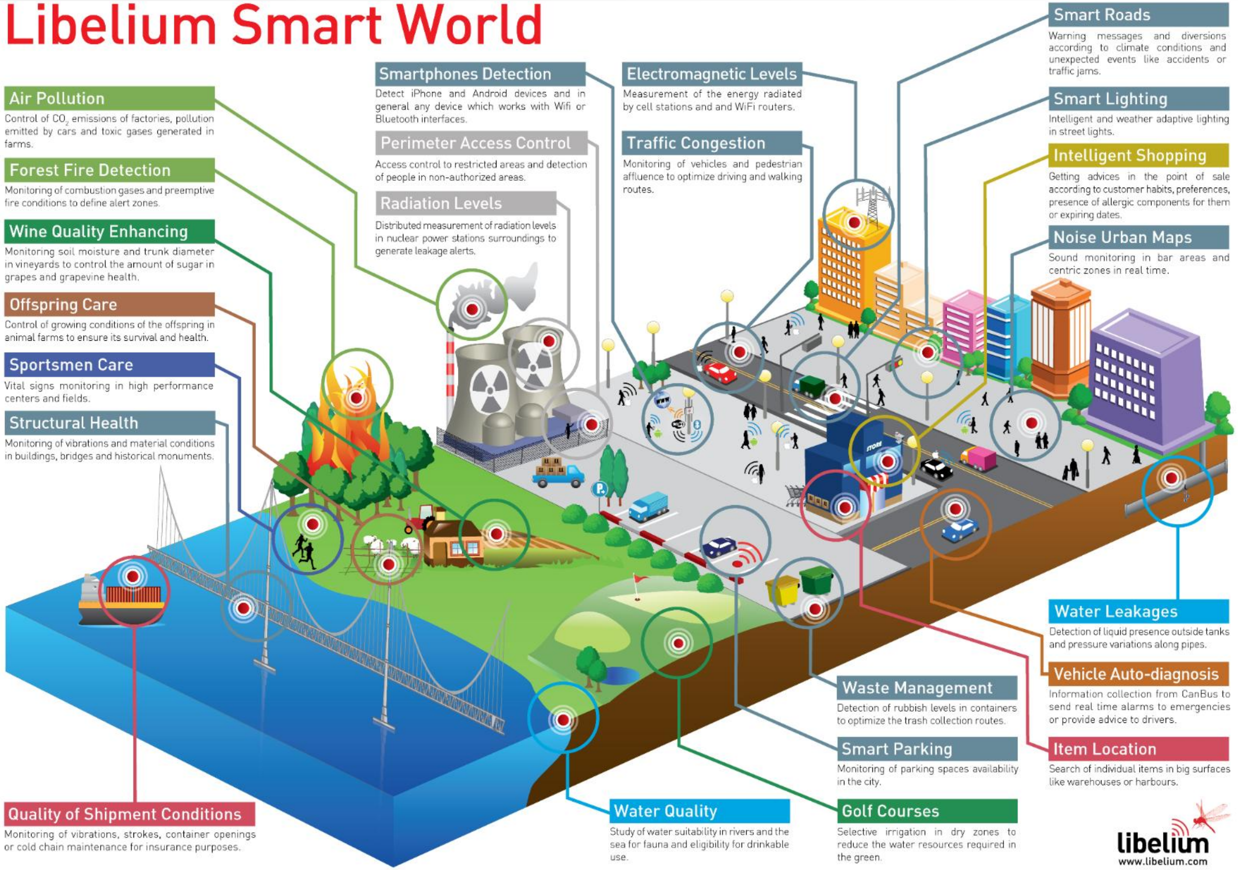
The Malicious Insider Threat

- Employees working for the cloud service provider can have complete access (both physical and logical) to company resources
- Insider threats to cloud security are underestimated
- Most employees are trustworthy, but a rogue cloud provider employee has privileges that an outside cyber attacker would have to work much harder to acquire
- The security of data at rest is not an issue, but malicious insiders can access the physical memory of servers to easily steal data of a VM without the need of performing complicated side-channel attacks
- Currently, this is considered the most worrisome threat

FITNESS
Fault and Intrusion Tolerant NEtworked SystemS

IoT security

IoT: Smart World



Libelium Smart World

Air Pollution
Control of CO_2 emissions of factories, pollution emitted by cars and toxic gases generated in farms.

Forest Fire Detection
Monitoring of combustion gases and preemptive fire conditions to define alert zones.

Wine Quality Enhancing
Monitoring soil moisture and trunk diameter in vineyards to control the amount of sugar in grapes and grapevine health.

Offspring Care
Control of growing conditions of the offspring in animal farms to ensure its survival and health.

Sportsmen Care
Vital signs monitoring in high performance centers and fields.

Structural Health
Monitoring of vibrations and material conditions in buildings, bridges and historical monuments.

Smartphones Detection
Detect iPhone and Android devices and in general any device which works with Wifi or Bluetooth interfaces.

Perimeter Access Control
Access control to restricted areas and detection of people in non-authorized areas.

Radiation Levels
Distributed measurement of radiation levels in nuclear power stations surroundings to generate leakage alerts.

Electromagnetic Levels
Measurement of the energy radiated by cell stations and WiFi routers.

Traffic Congestion
Monitoring of vehicles and pedestrian affluence to optimize driving and walking routes.

Smart Roads
Warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams.

Smart Lighting
Intelligent and weather adaptive lighting in street lights.

Intelligent Shopping
Getting advices in the point of sale according to customer habits, preferences, presence of allergic components for them or expiring dates.

Noise Urban Maps
Sound monitoring in bar areas and centric zones in real time.

Water Leakages
Detection of liquid presence outside tanks and pressure variations along pipes.

Vehicle Auto-diagnosis
Information collection from CanBus to send real time alarms to emergencies or provide advice to drivers.

Item Location
Search of individual items in big surfaces like warehouses or harbours.

Waste Management
Detection of rubbish levels in containers to optimize the trash collection routes.

Smart Parking
Monitoring of parking spaces availability in the city.

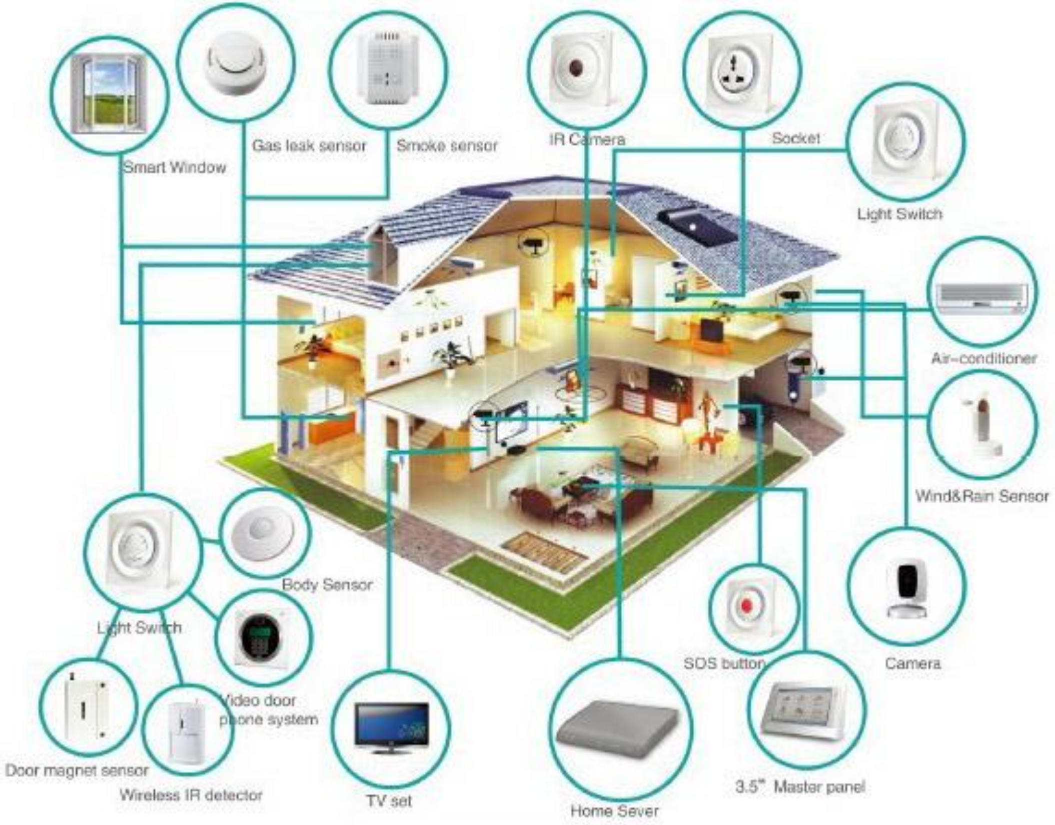
Golf Courses
Selective irrigation in dry zones to reduce the water resources required in the green.

Water Quality
Study of water suitability in rivers and the sea for fauna and eligibility for drinkable use.

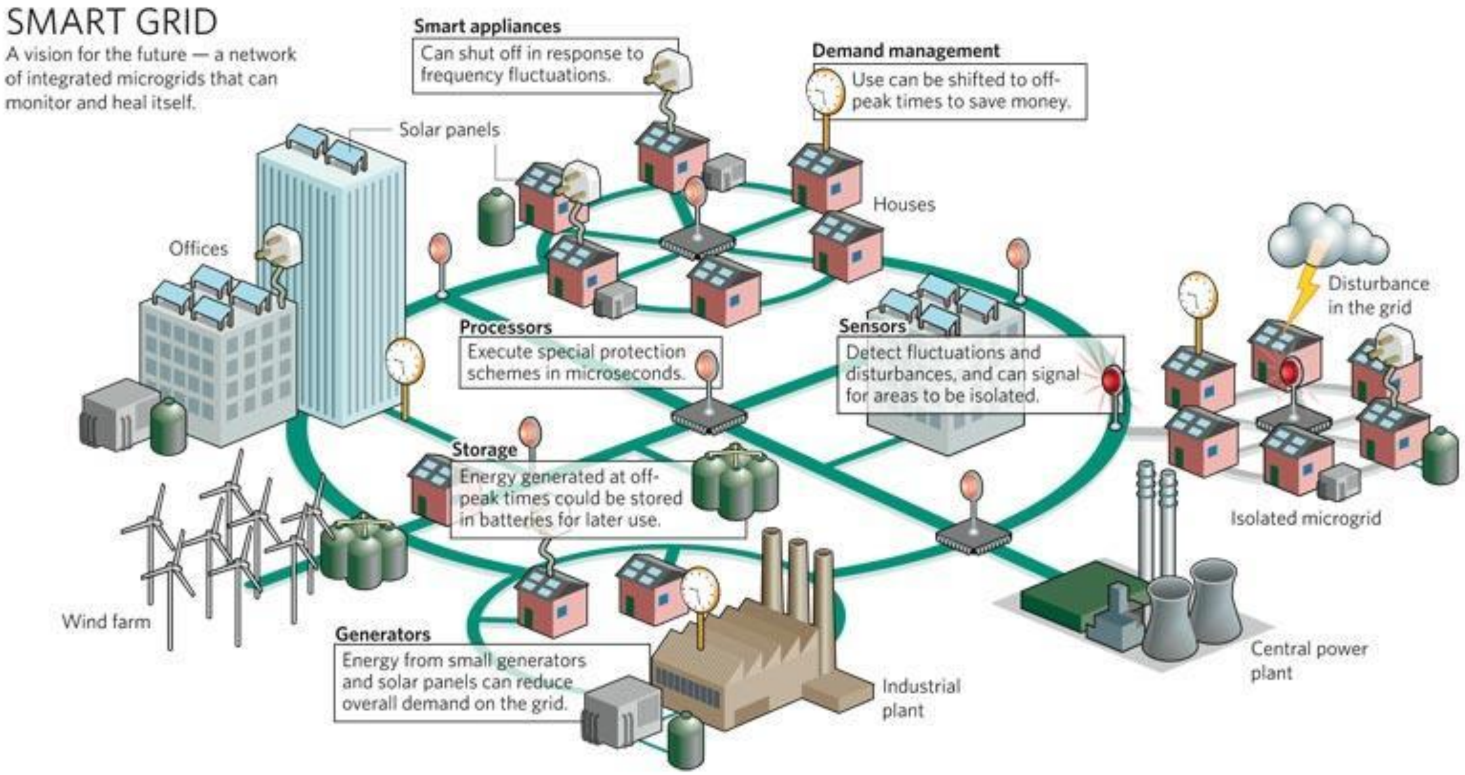
Quality of Shipment Conditions
Monitoring of vibrations, strokes, container openings or cold chain maintenance for insurance purposes.

libelium
www.libelium.com

IoT: Smart Home



Industrial IoT



SMART GRID

A vision for the future — a network of integrated microgrids that can monitor and heal itself.

Smart appliances
Can shut off in response to frequency fluctuations.

Demand management
Use can be shifted to off-peak times to save money.

Processors
Execute special protection schemes in microseconds.

Sensors
Detect fluctuations and disturbances, and can signal for areas to be isolated.

Storage
Energy generated at off-peak times could be stored in batteries for later use.

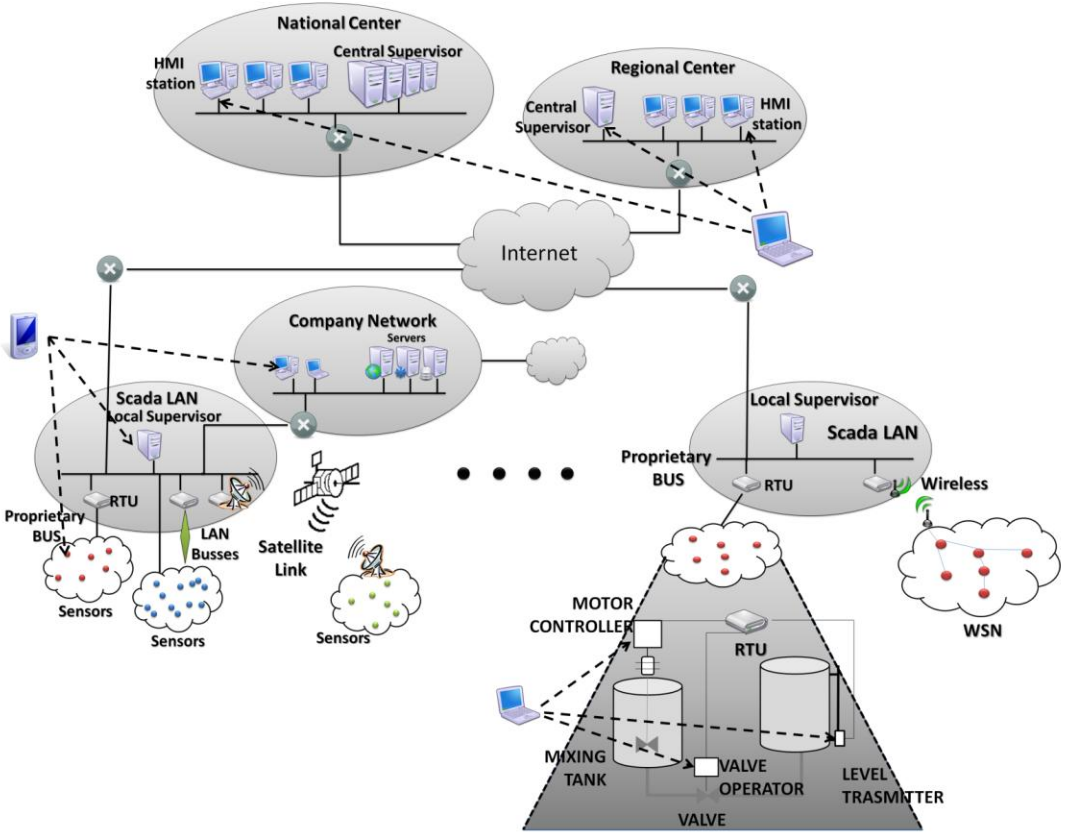
Generators
Energy from small generators and solar panels can reduce overall demand on the grid.

FITNESS

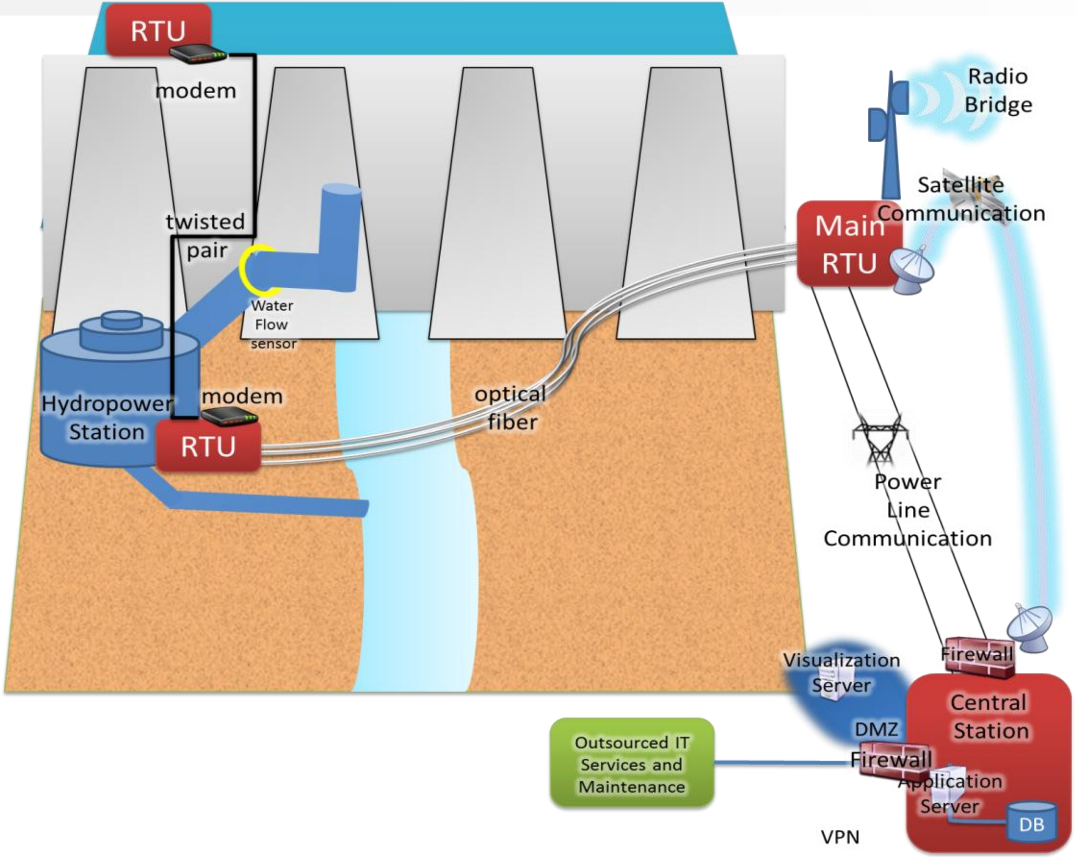
Fault and Intrusion Tolerant NEtworked SystemS

ICS security

Typical architecture of a SCADA system



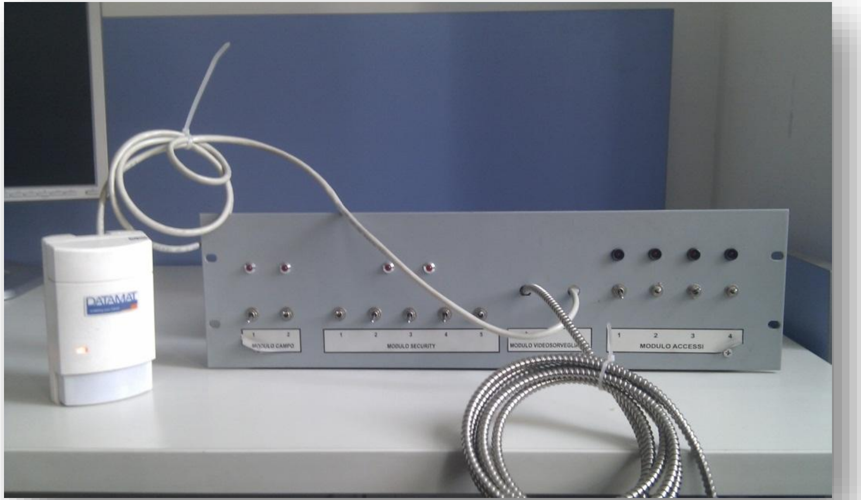
Example of a real SCADA system



Yesterday's SCADA technology

- Traditional SCADA systems:
  - Were largely based on special-purpose devices
  - Included distinct subsystems that operated almost in isolation
  - Used dedicated (non-shared) communication links
  - Implemented proprietary (non-open) communication protocols
- This led to the (false) belief that traditional SCADA systems were inherently secure

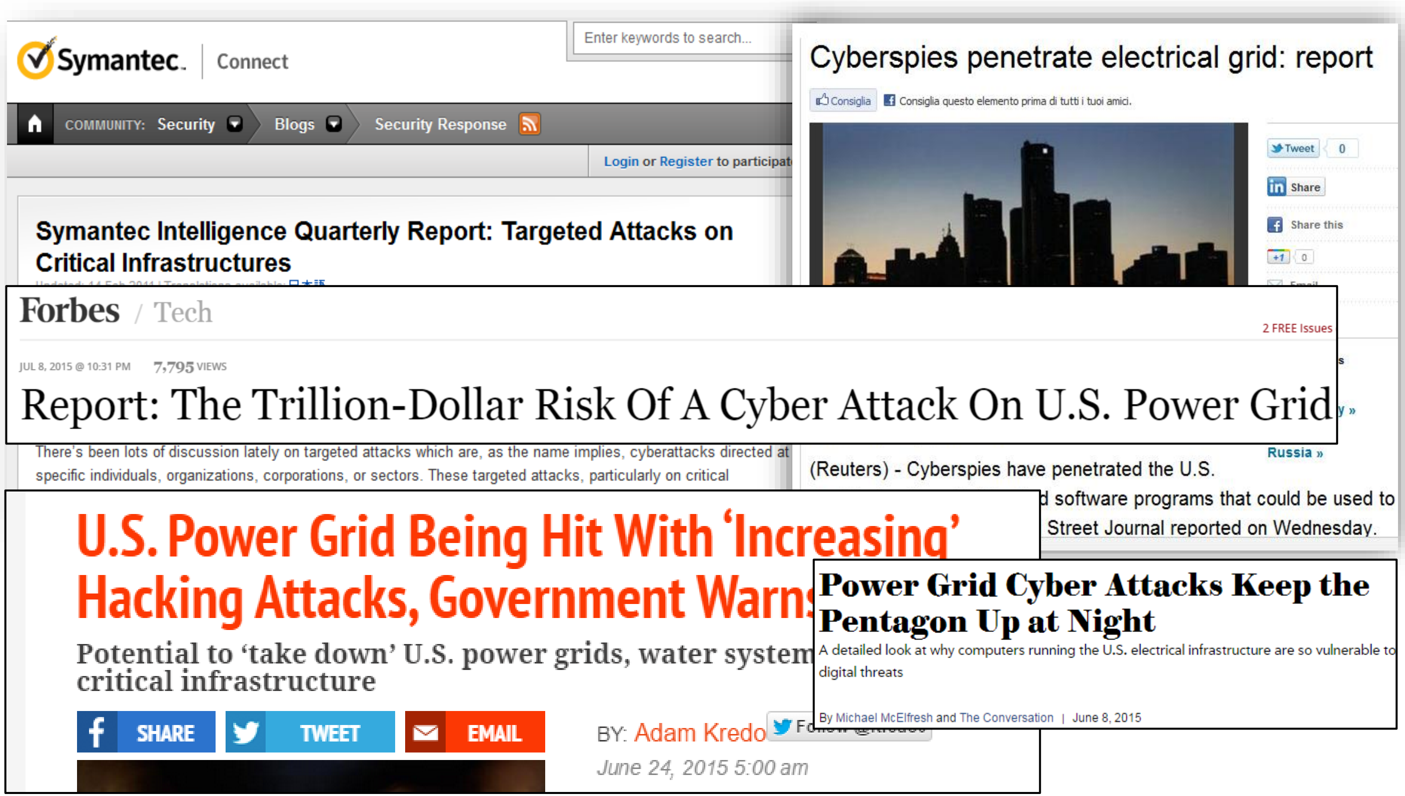
Example of legacy SCADA technology



Today's SCADA technology

- For the implementation of SCADA systems, there is an increasing reliance on COTS (Commercial-Off-The-Shelf) components
- The individual subsystems are connected through the company's LAN network infrastructure, or even via WAN segments, with the possibility of traversing the Internet as well as wireless or satellite-based links
- There is a growing use of open communication protocols, which exposes SCADA systems to the same threats that make standard IT (Information Technology) systems vulnerable
- Wireless Sensor Networks (WSNs) have now become an integral part of many SCADA systems (and this will be increasingly the case)

ICS security in the media



Symantec Intelligence Quarterly Report: Targeted Attacks on Critical Infrastructures

There's been lots of discussion lately on targeted attacks which are, as the name implies, cyberattacks directed at specific individuals, organizations, corporations, or sectors. These targeted attacks, particularly on critical

Cyberspies penetrate electrical grid: report

(Reuters) - Cyberspies have penetrated the U.S.

d software programs that could be used to

Street Journal reported on Wednesday.

JUL 8, 2015 @ 10:31 PM 7,795 VIEWS

Report: The Trillion-Dollar Risk Of A Cyber Attack On U.S. Power Grid

U.S. Power Grid Being Hit With 'Increasing' Hacking Attacks, Government Warns

Potential to 'take down' U.S. power grids, water system critical infrastructure

BY: Adam Kredo

June 24, 2015 5:00 am

Power Grid Cyber Attacks Keep the Pentagon Up at Night

A detailed look at why computers running the U.S. electrical infrastructure are so vulnerable to digital threats

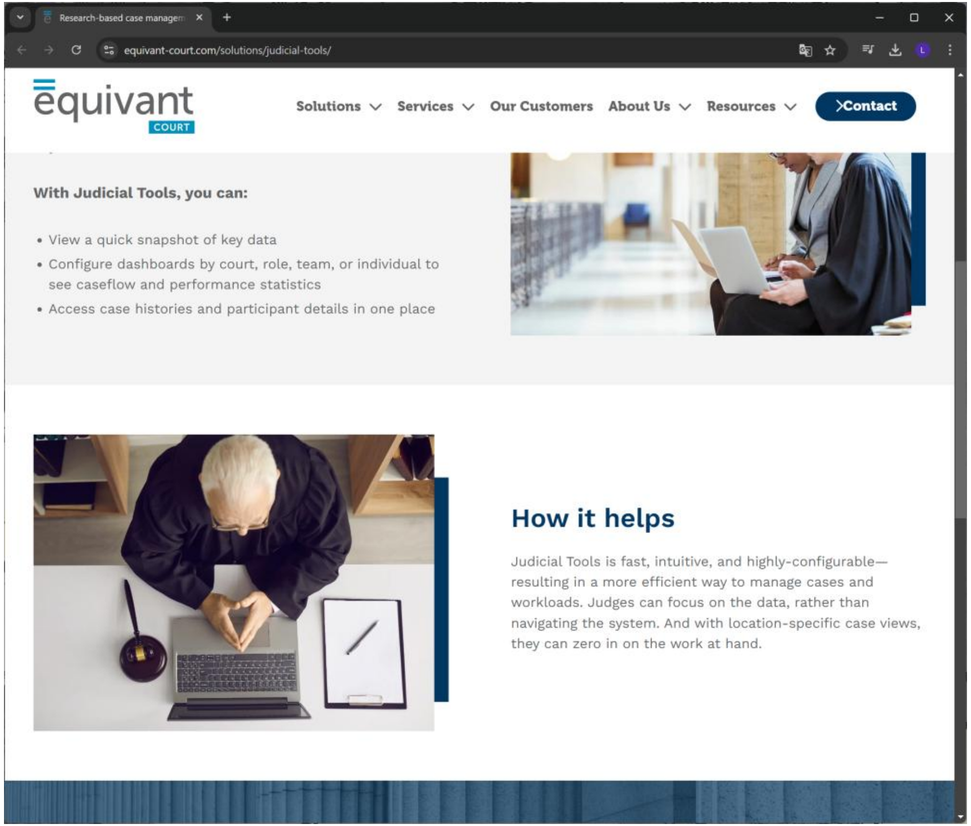
By Michael McElfresh and The Conversation | June 8, 2015

FITNESS

Fault and Intrusion Tolerant NEtworked SystemS

Supply Chain security

Just an example


Research-based case managem
equivant-court.com/solutions/judicial-tools/
equivant
COURT
Solutions
Services
Our Customers
About Us
Resources
Contact

With Judicial Tools, you can:

- View a quick snapshot of key data
- Configure dashboards by court, role, team, or individual to see caseflow and performance statistics
- Access case histories and participant details in one place

How it helps

Judicial Tools is fast, intuitive, and highly-configurable—resulting in a more efficient way to manage cases and workloads. Judges can focus on the data, rather than navigating the system. And with location-specific case views, they can zero in on the work at hand.

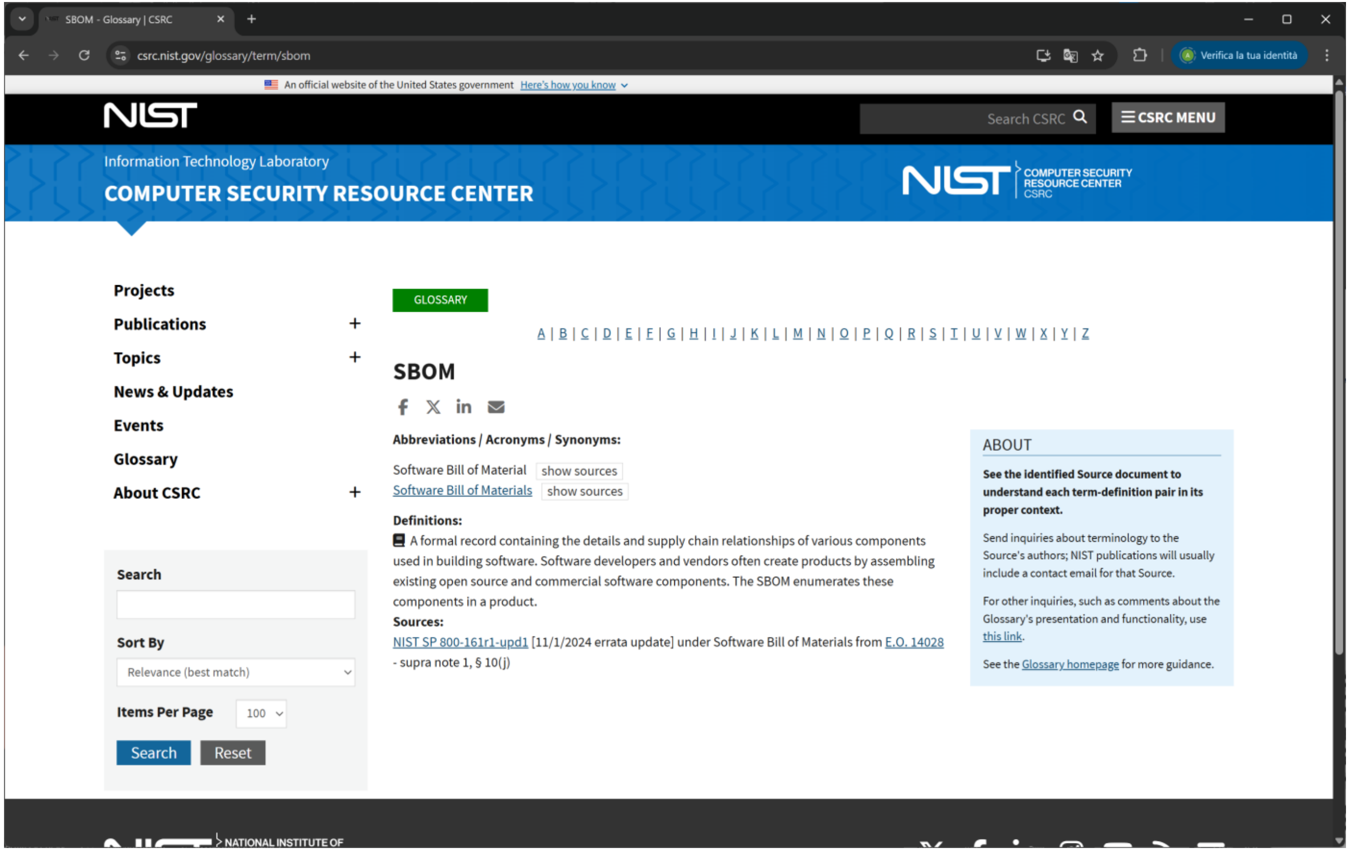
Question

Whom are you (implicitly) trusting?

Possible answers (not an exhaustive list)

- Simple (obvious) one:
  - “The application provider”
- Better one, but still with a lot of room for improvement:
  - “The application provider and the Operating System provider”
- Good one:
  - “The entire supply chain of the application”

SBOM: Software Bill Of Materials


SBOM - Glossary | CSRC
csrc.nist.gov/glossary/term/sbom
Verifica la tua identità
An official website of the United States government Here's how you know
NIST
Search CSRC
CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC
Projects
Publications
Topics
News & Updates
Events
Glossary
About CSRC
Search
Sort By
Relevance (best match)
Items Per Page
100
Search
Reset
GLOSSARY
A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z
NATIONAL INSTITUTE OF

SBOM

Abbreviations / Acronyms / Synonyms:

Software Bill of Material show sources
Software Bill of Materials show sources

Definitions:
A formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product.
Sources:
NIST SP 800-161r1-upd1 [11/1/2024 errata update] under Software Bill of Materials from E.O. 14028 - supra note 1, § 10(j)

ABOUT

See the identified Source document to understand each term-definition pair in its proper context.

Send inquiries about terminology to the Source's authors; NIST publications will usually include a contact email for that Source.

For other inquiries, such as comments about the Glossary's presentation and functionality, use this link.

See the Glossary homepage for more guidance.

Acknowledgements

- IDA (Information Disorder Awareness) Partenariato Esteso SERICS (PE00000014), nell’ambito dello Spoke 2 Misinformation and Fakes

- EMDAS (Enforcement and Monitoring of Data Sovereignty policies) SPOKE 1 “HUMAN, SOCIAL, AND LEGAL ASPECTS” DELL’INIZIATIVA “SECURITY RIGHTS IN CYBER SPACE – SERICS” PROJECT: DIGITAL SOVEREIGNTY (DISE)

- S2 (Safe and Secure Industrial Internet of Things) PRIN: PROGETTI DI RICERCA DI RILEVANTE INTERESSE NAZIONALE – Bando 2022

Contact Info:
Luigi Romano

Full Professor of Computer Engineering
Università degli Studi di Napoli Parthenope

President
Centro Regionale Information Communication Technology - CeRICT scrl

luigi.romano@uniparthenope.it
+39 333 3016817