ANASTACIA has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement N° 731558 and from the Swiss State Secretariat for Education, Research and Innovation.

ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

Emerging IoT Threats and Ethical Hacking: Anomaly-based Intrusion Detection

Stefano Bianchi & Andrea Balogh
Softeco Sismat & United Technologies Research Center

IoTWeek2018

ANASTACIA has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement N° 731558 and from the Swiss State Secretariat for Education, Research and Innovation.

ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

TYPE:	Research & Innovation Action
CALL:	H2020-DS-LEIT-2016
TOPIC:	DS-01-2016 Assurance and Certification for Trustworthy and Secure ICT systems, services and components
DURATION:	36 MONTHS (Jan 2017 → Dec 2019)
COSTS:	€ 5,420,208.75
FUNDING:	€ 3,999,208.75
G.A.:	731558

It takes (=took) only 98 seconds...

Nov 16th 2016

55$ security camera infected by malware

98 seconds after it was plugged in

Live experiment on Twitter:

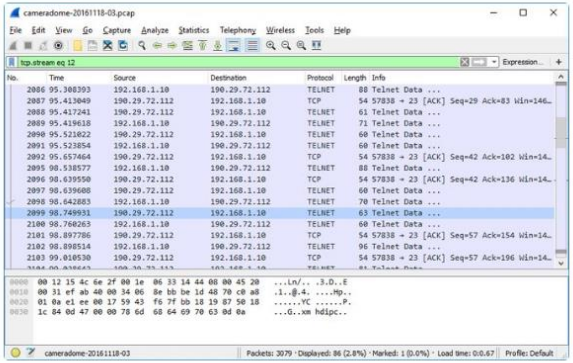
Rob Graham, Elf @ErrataRob 18 Nov

7/x: And when it's done, it runs the binary, and the box is now officially infected: pic.twitter.com/iggDPSZlri

Rob Graham, Elf @ErrataRob Follow

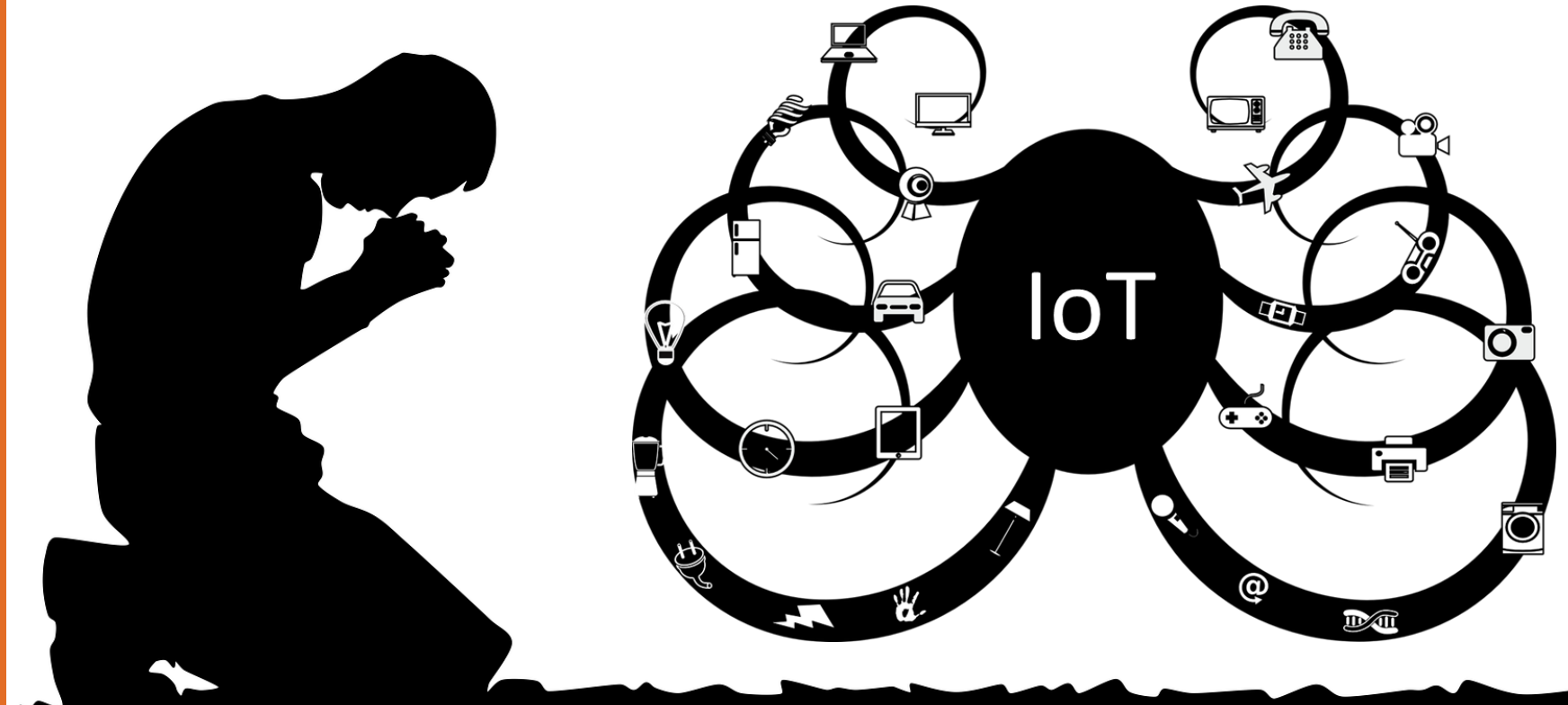
8/x: Actually, it took 98 seconds for first infection pic.twitter.com/EDdOZaEs0V

11:42 AM - 18 Nov 2016



224 210

Will it be maneagable for the common man?

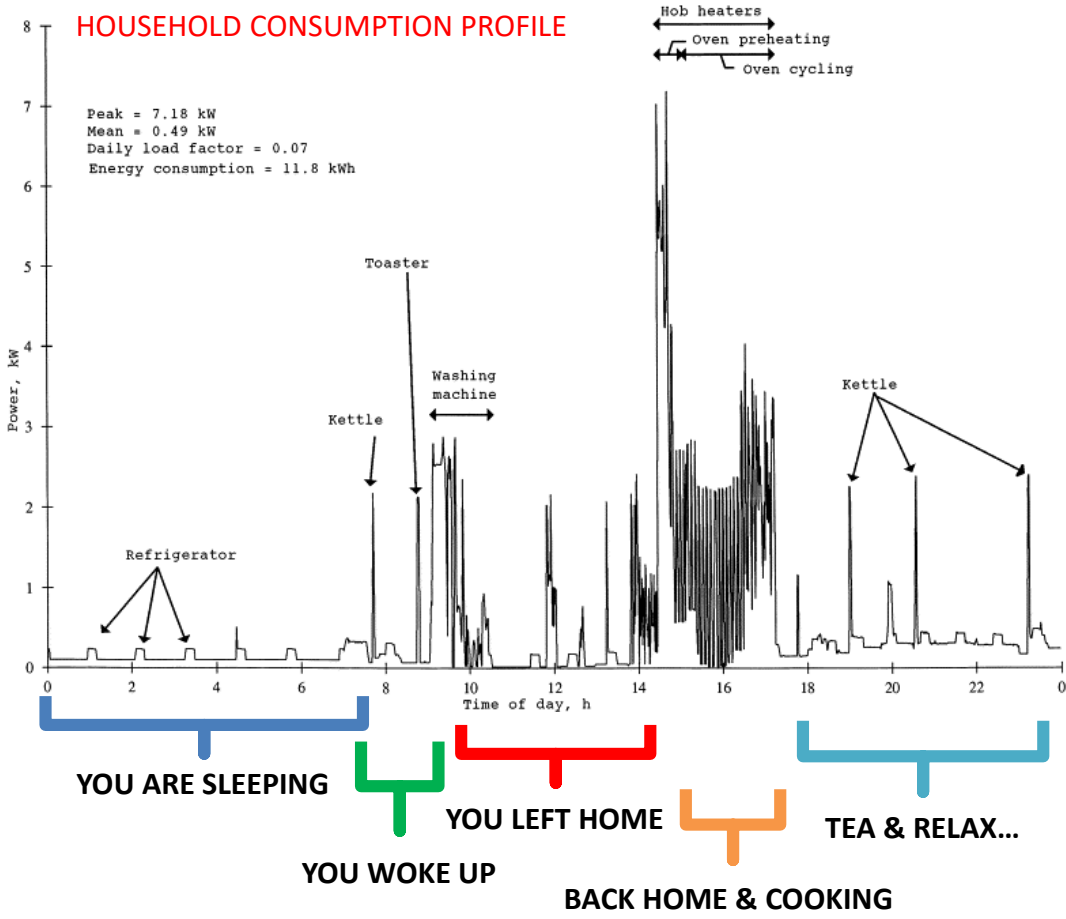


IoT pervasivity: VALUE ADDED vs (KNOWN?) RISKS

Privacy and data ownership

More detailed data are collected from a growing number of connected devices and appliances (see IoT).
For instance, data on energy use in households collected by smart meters can be used to tell when someone is home, using the shower, or making tea.

Yet, aggregated and anonymised individual energy use data can improve understanding of energy systems, such as load profiles, and help lower costs for individual consumers. Policy makers will need to balance privacy concerns with these other objectives, including promoting innovation and the operational needs of utilities.

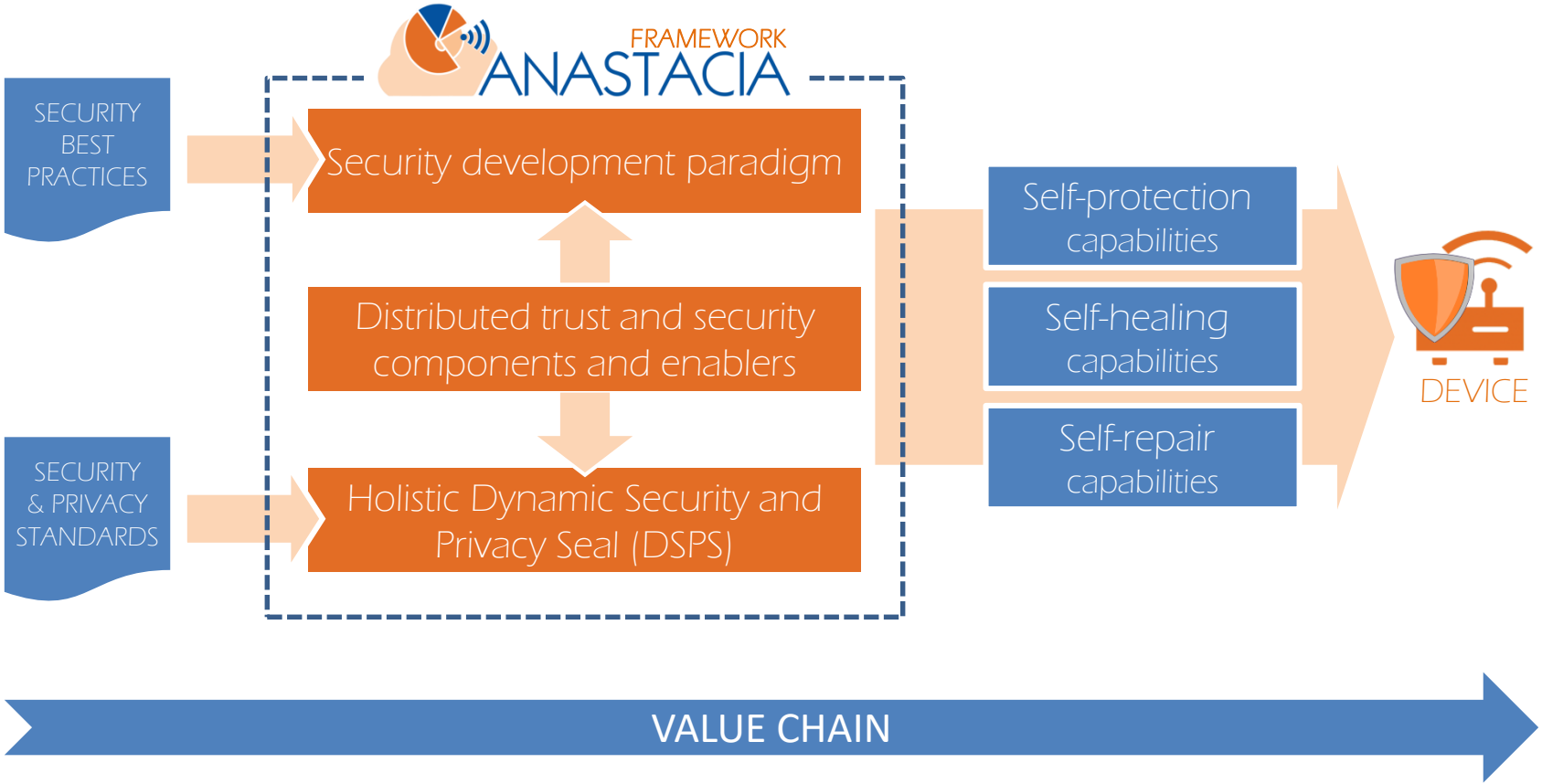


ANASTACIA's mission

- To develop a trustworthy-by-design autonomic security framework which will address all the phases of the ICT Systems Development Lifecycle (SDL) and will be able to take autonomous decisions through the use of new networking technologies such as Software Defined Networking (SDN) and Network Function Virtualisation (NFV) and intelligent and dynamic security enforcement and monitoring methodologies and tools

- holistic solution enabling trust and security by-design for Cyber Physical Systems (CPS) based on IoT and cloud architectures

ANASTACIA framework

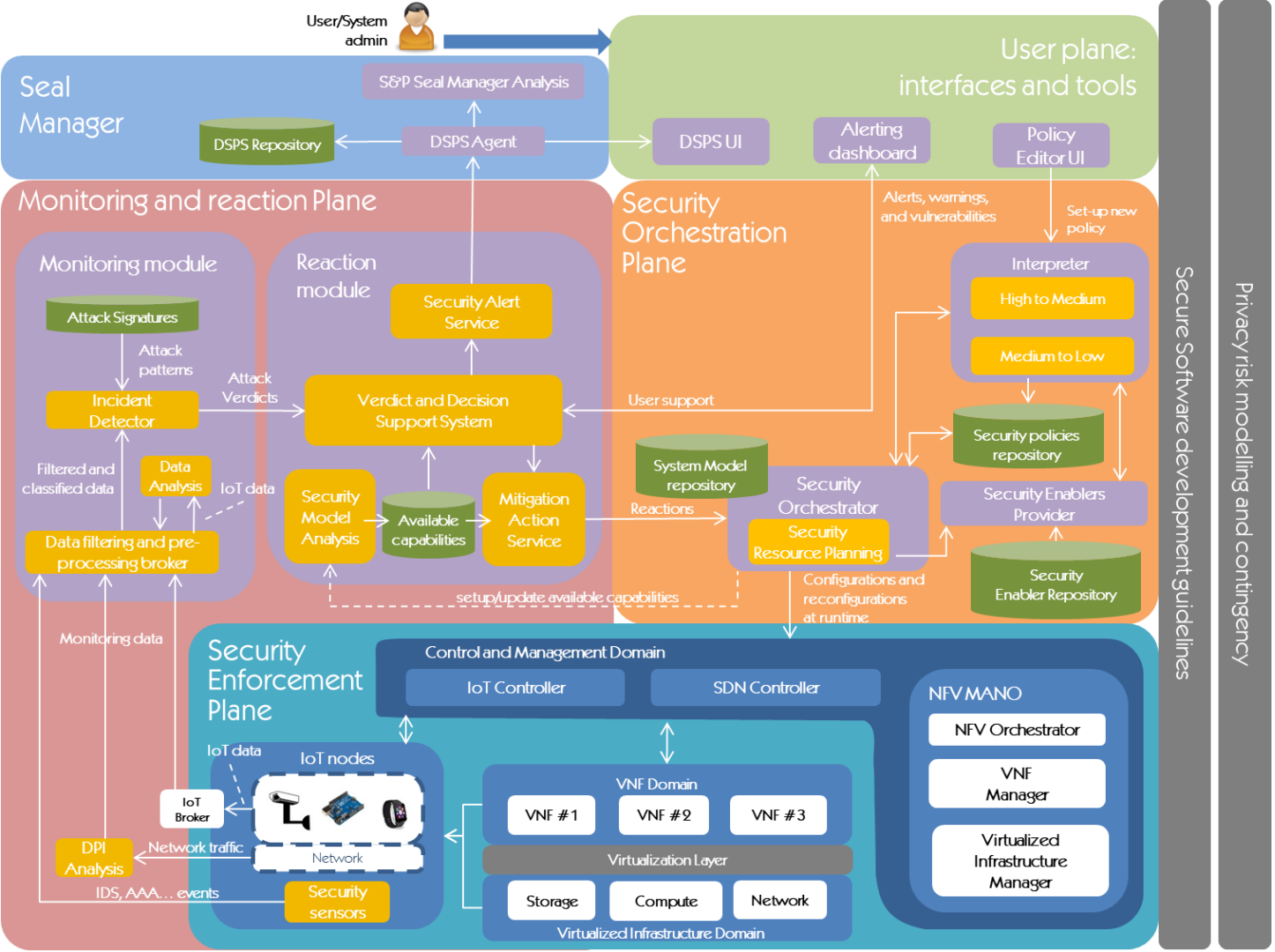


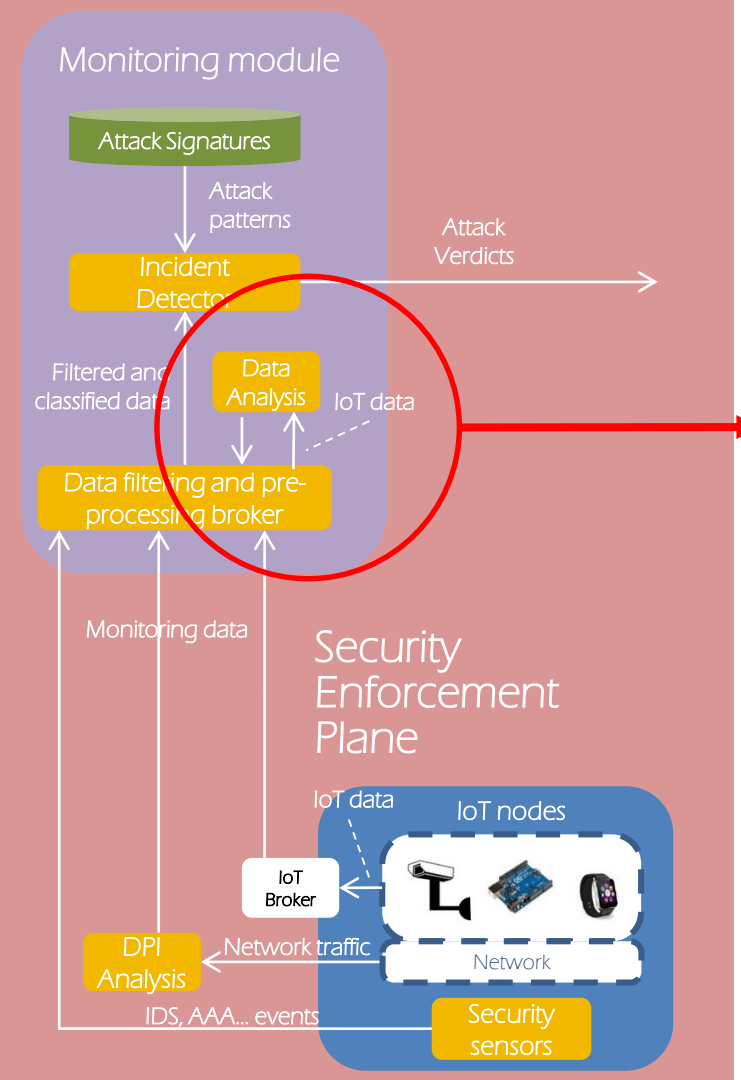
Use Cases

- Multi-access Edge Computing applications
  - **Test Case**: MEC on video cameras
  - **Scenario**: Spoofing attack on the security camera system

- Smart Building Management Systems applications
  - **Test Case**: Resilient cyber-physical systems in smart buildings
  - **Scenario**: Cyber-attack at a hospital building

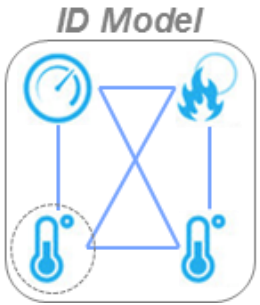
ANASTACIA framework architecture





United Technologies Research Center

Anomaly based Intrusion Detection Model



- Aggregate different types of IoT data: temperature, pressure, current flow, etc.
- Create a model for the normal behavior of the supervised system at the system level.
- Model = network of relations between sensor data

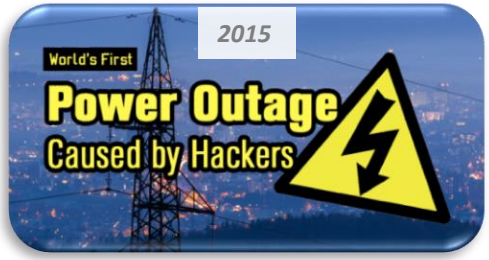
UTC Proprietary, Created at UTRC-I, This page contains EU and US technical data - ECCN(EU): NLR, ECCN(US): EAR99

United Technologies Research Center

Importance of Cyber-physical system security

German Steel-Mill
controls mill's production software leads to "massive" damage

Ukraine's power outage
first-of-its-kind cyber attack cut the lights to 225,000 people in western Ukraine



Charlie Miller
U.S. auto giant Chrysler had to recall 1.4 million vehicles

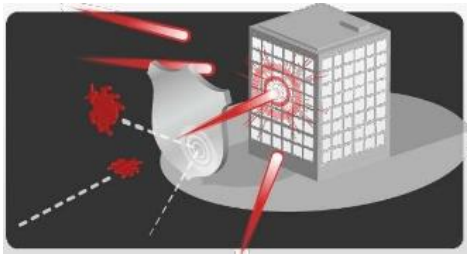
SAN Francisco Municipal Railway
Ransomware Attack

STUXNET Nuclear plant
Controls Siemens PLC for fast-spinning centrifuges

UTC Proprietary, Created at UTRC-I, This page contains EU and US technical data - ECCN(EU): NLR, ECCN(US): EAR99

Types of Intrusion Detection Systems

Knowledge-based ID: Apply the knowledge accumulated about specific attacks and system vulnerabilities. Use a database of patterns/signatures of malicious activities

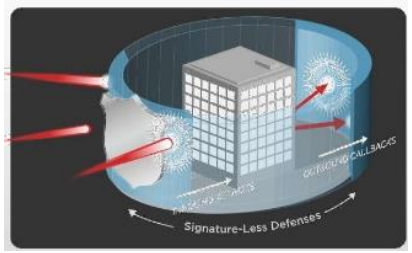


Advantages:

- Highly affective towards well known attacks
- Low false positive rates

Anomaly-based ID:

- Build a profile or data model of the "normal" behaviour (data model can be learned using machine learning).
- Use the normal profile to detect anomalies (observations whose characteristics differ significantly from the normal behaviour).



Advantages:

- Can identify new attacks

UTC Proprietary, Created at UTRC-I, This page contains EU and US technical data - ECCN(EU): NLR, ECCN(US): EAR99

Anomaly based intrusion detection

Capabilities:

- Provides a guideline explaining the attack cause
- Model is interpretable by end-user
- Different types IoT data can be captured in one model
- Model continuously learns both from online data and end-user input

Drawbacks:

- No clear separation between fault and attack

UTC Proprietary, Created at UTRC-I, This page contains EU and US technical data - ECCN(EU): NLR, ECCN(US): EAR99

Contacts

- Project Coordinator

  Stefano BIANCHI (Softeco Sismat)

  stefano.bianchi@softeco.it

- Scientific and Technical Project Manager

  Antonio SKARMETA (Universidad de Murcia)

  skarmeta@umu.es

ANASTACIA has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement N° 731558 and from the Swiss State Secretariat for Education, Research and Innovation.

ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

www.anastacia-h2020.eu

http://youtube.anastacia-h2020.eu

http://twitter.anastacia-h2020.eu

http://linkedin.anastacia-h2020.eu

http://www.anastacia-h2020.eu

http://youtube.anastacia-h2020.eu

http://twitter.anastacia-h2020.eu

http://linkedin.anastacia-h2020.eu

ANASTACIA

ANASTACIA

softeco sismat information technology

THALES

Atos

ERICSSON

United Technologies Research Center

UBITECH ubiquitous solutions

montimage

MANDAT INTERNATIONAL

OdinS

UDG UNIVERSAL DEVICE GATEWAY

Consiglio Nazionale delle Ricerche

Aalto University

UNIVERSIDAD DE MURCIA

ANASTACIA has received funding from the European Union's
Horizon 2020 Research and Innovation Programme under Grant Agreement N° 731558
and from the Swiss State Secretariat for Education, Research and Innovation.