CNR-IEIIT – Network Security Group

Enrico Cambiaso
enrico.cambiaso@ge.ieiit.cnr.it

Consiglio Nazionale delle Ricerche - Istituto IEIIT
Via De Marini, 6 - Genova, Italy

NetSec Group Presentation

Genoa, Februray 9th, 2018

The NetSec Group

Maurizio Aiello

Maurizio Mongelli

Enrico Cambiaso

Ivan Vaccari

Sandro Ballestrasse

Giovanni Chiola

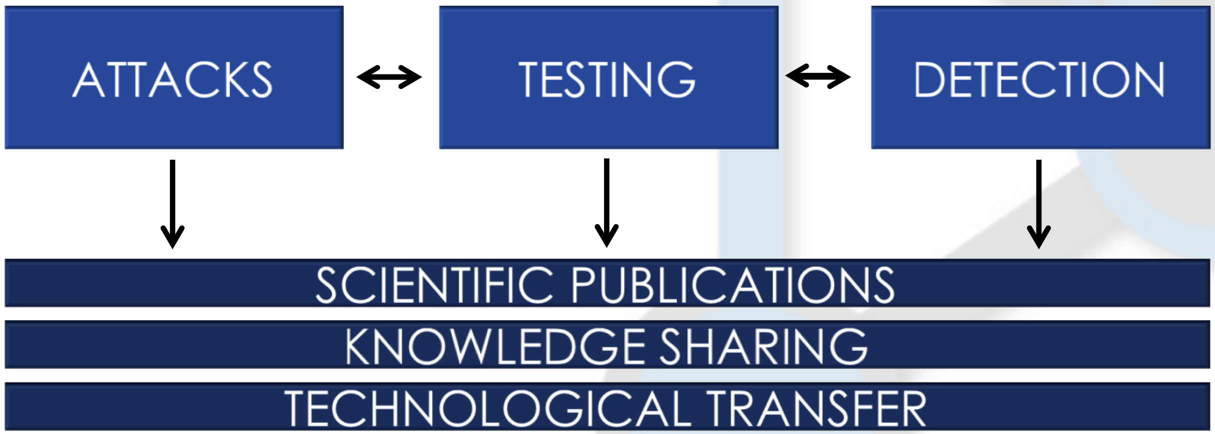
Alessandro Armando

Silvia Scaglione

Silvia Giuliano

Research activities of the group

RESEARCH ACTIVITIES



ATTACKS ↔ TESTING ↔ DETECTION

SCIENTIFIC PUBLICATIONS

KNOWLEDGE SHARING

TECHNOLOGICAL TRANSFER

Acquired knowledge

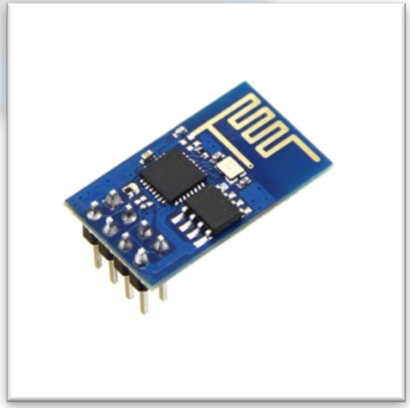
- **Network management**
  design, configuration and maintenance

- **Attacks development**
  protocol analysis, threats modeling, designing, and implementation

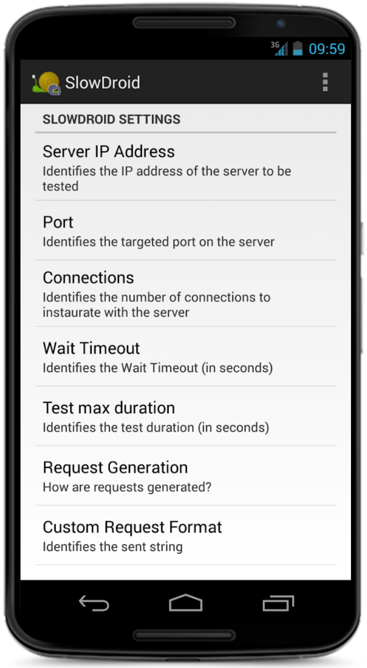
- **Network traffic and data analysis**
  statistics, machine learning, neural networks, spectral/Fourier analysis
  - **Attacks recognition**
    features extrapolation, situations characterization, on-line classification

Attacks study and development

- **Denial of Service**
  with particular focus on emerging slow DoS and Amplification/Reflection DoS attacks and DDoS
- **Data exfiltration**
  i.e. tunneling techniques, TOR and anonymizing networks, malware implementation
- **Mobile security**
  BYOD, security assessment, botnets, apps development
- **IoT security**
  security of IoT networks and sensors
- **Just discovered threats**
  tempestive study of recent large impact threats (i.e. Heartbleed, Shellshock, LogJam, etc.)



Some examples
SlowDroid



09:59

SlowDroid

SLOWDROID SETTINGS

Server IP Address
Identifies the IP address of the server to be tested

Port
Identifies the targeted port on the server

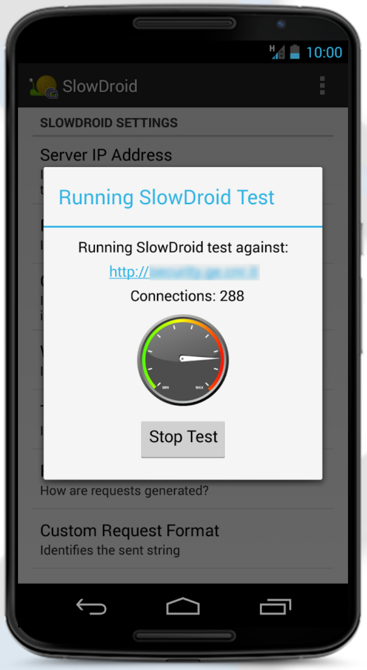
Connections
Identifies the number of connections to instaurate with the server

Wait Timeout
Identifies the Wait Timeout (in seconds)

Test max duration
Identifies the test duration (in seconds)

Request Generation
How are requests generated?

Custom Request Format
Identifies the sent string



10:00

SlowDroid

SLOWDROID SETTINGS

Server IP Address

Running SlowDroid Test

Running SlowDroid test against:
http://[redacted]
Connections: 288

Stop Test

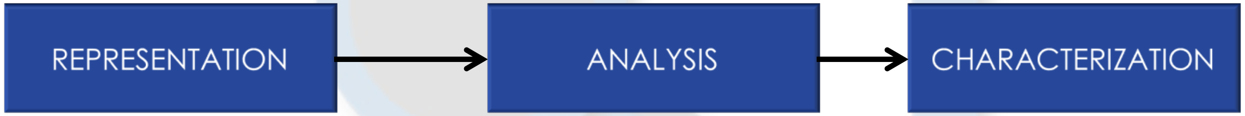
How are requests generated?

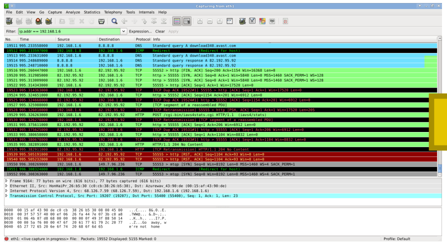
Custom Request Format
Identifies the sent string

http://security.ge.cnr.it/projects/slowdroid/

NetSec Group

Network traffic and data analysis


REPRESENTATION → ANALYSIS → CHARACTERIZATION



Capturing from eth1
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply

Filter: ip.addr == 192.168.1.6

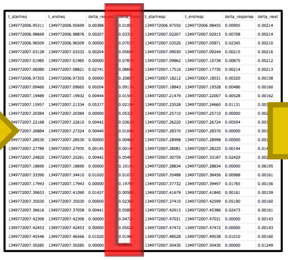
```
No.   Time          Source          Destination     Protocol Info
19511 995.233558000 192.168.1.6     8.8.8.8         DNS      Standard query A download340.avast.com
19512 995.233597000 192.168.1.8     192.168.1.6     ICMP     Redirect            (Redirect for host)
19513 995.233631000 192.168.1.6     8.8.8.8         DNS      Standard query A download340.avast.com
19514 995.248689000 8.8.8.8         192.168.1.6     DNS      Standard query response A 82.192.95.92
19515 995.248710000 8.8.8.8         192.168.1.6     DNS      Standard query response A 82.192.95.92
19516 995.260447000 192.168.1.6     82.192.95.92    TCP      55552 > http [FIN, ACK] Seq=200 Ack=1154 Win=16368 Len=0
19520 995.312985000 82.192.95.92    192.168.1.6     TCP      http > 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
19521 995.313009000 82.192.95.92    192.168.1.6     TCP      http > 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
19522 995.314343000 192.168.1.6     82.192.95.92    TCP      55555 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
19523 995.314363000 192.168.1.6     82.192.95.92    TCP      [TCP Dup ACK 19522#1] 55555 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
19524 995.324651000 82.192.95.92    192.168.1.6     TCP      http > 55552 [ACK] Seq=1154 Ack=201 Win=6912 Len=0
19525 995.324668000 82.192.95.92    192.168.1.6     TCP      [TCP Dup ACK 19524#1] http > 55552 [ACK] Seq=1154 Ack=201 Win=6912 Len=0
19527 995.325988000 192.168.1.6     82.192.95.92    TCP      [TCP segment of a reassembled PDU]
19528 995.326010000 192.168.1.6     82.192.95.92    TCP      [TCP Retransmission] 55555 > http [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=205
19529 995.326263000 192.168.1.6     82.192.95.92    HTTP     POST /cgi-bin/iavs4stats.cgi HTTP/1.1  (iavs4/stats)
19530 995.326278000 192.168.1.6     82.192.95.92    TCP      [TCP Retransmission] [TCP segment of a reassembled PDU]
19531 995.375611000 82.192.95.92    192.168.1.6     TCP      http > 55555 [ACK] Seq=1 Ack=206 Win=6912 Len=0
19532 995.375625000 82.192.95.92    192.168.1.6     TCP      [TCP Dup ACK 19531#1] http > 55555 [ACK] Seq=1 Ack=206 Win=6912 Len=0
19533 995.380658000 82.192.95.92    192.168.1.6     TCP      http > 55555 [ACK] Seq=1 Ack=1104 Win=8832 Len=0
19534 995.380678000 82.192.95.92    192.168.1.6     TCP      [TCP Dup ACK 19533#1] http > 55555 [ACK] Seq=1 Ack=1104 Win=8832 Len=0
19535 995.382891000 82.192.95.92    192.168.1.6     HTTP     HTTP/1.1 204 No Content
19536 995.382911000 82.192.95.92    192.168.1.6     HTTP     [TCP Retransmission] HTTP/1.1 204 No Content
19539 995.505191000 192.168.1.6     82.192.95.92    TCP      55555 > http [RST, ACK] Seq=1104 Ack=93 Win=0 Len=0
19540 995.505232000 192.168.1.6     82.192.95.92    TCP      55555 > http [RST, ACK] Seq=1104 Ack=93 Win=0 Len=0
19550 996.308269000 192.168.1.6     149.7.96.236    TCP      55553 > mtqp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
19551 996.308324000 192.168.1.8     192.168.1.6     ICMP     Redirect            (Redirect for host)
19552 996.308363000 192.168.1.6     149.7.96.236    TCP      55553 > mtqp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

▷ Frame 9164: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
▷ Ethernet II, Src: HonHaiPr_26:b5:30 (c0:cb:38:26:b5:30), Dst: Azurewav_43:90:de (00:15:af:43:90:de)
▷ Internet Protocol Version 4, Src: 68.126.7.59 (68.126.7.59), Dst: 192.168.1.6 (192.168.1.6)
▷ Transmission Control Protocol, Src Port: 19207 (19207), Dst Port: 55400 (55400), Seq: 1, Ack: 1, Len: 23

0000  00 15 af 43 90 de c0 cb  38 26 b5 30 08 00 45 00   ...C.... 8&.0..E.
0010  00 3f 57 57 40 00 ef 06  26 fa 44 7e 07 3b c0 a8   .?WW@... &.D~.;..
0020  01 06 4b 07 d8 68 00 08  80 80 0f 49 3f 88 50 14   ..K..h.. ...I?.P.
0030  00 08 5a f6 00 00 47 6f  20 61 77 61 79 2c 20 77   ..Z...Go  away, w
0040  65 27 72 65 20 6e 6f 74  20 68 6f 6d 65            e're not  home
```

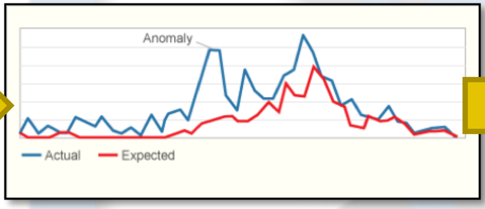
eth1: <live capture in progress> File: Packets: 19552 Displayed: 5155 Marked: 0 Profile: Default

TRAFFIC DUMP



t_startreq	t_endreq	delta_request	delta_delay	t_startresp	t_endresp	delta_response	delta_next
1349772006.95311	1349772006.95699	0.00388	0.01851	1349772006.97550	1349772006.98455	0.00905	0.00214
1349772006.98669	1349772006.98876	0.00207	0.03331	1349772007.02207	1349772007.02915	0.00708	0.00214
1349772006.96509	1349772006.96509	0.00000	0.07017	1349772007.03526	1349772007.05871	0.02345	0.00210
1349772007.03128	1349772007.03332	0.00204	0.05698	1349772007.09030	1349772007.09244	0.00215	0.00216
1349772007.01985	1349772007.01985	0.00000	0.07876	1349772007.09862	1349772007.10736	0.00875	0.00212
1349772007.06080	1349772007.08821	0.02741	0.08695	1349772007.17516	1349772007.17730	0.00214	0.00213
1349772006.97355	1349772006.97355	0.00000	0.20857	1349772007.18212	1349772007.18531	0.00320	0.00158
1349772007.09460	1349772007.09665	0.00204	0.09178	1349772007.18843	1349772007.19328	0.00486	0.00160
1349772007.19489	1349772007.19932	0.00444	0.01547	1349772007.21479	1349772007.22007	0.00528	0.00162
1349772007.15957	1349772007.21334	0.05377	0.02194	1349772007.23528	1349772007.24660	0.01131	0.001
1349772007.20384	1349772007.20384	0.00000	0.05325	1349772007.25710	1349772007.25710	0.00000	0.002
1349772007.22168	1349772007.22610	0.00442	0.03610	1349772007.26220	1349772007.26724	0.00504	0.001
1349772007.26884	1349772007.27324	0.00440	0.01046	1349772007.28370	1349772007.28370	0.00000	0.001
1349772007.28530	1349772007.28530	0.00000	0.00468	1349772007.28998	1349772007.28998	0.00000	0.001
1349772007.27789	1349772007.27935	0.00145	0.00147	1349772007.28081	1349772007.28225	0.00144	0.014
1349772007.24820	1349772007.25261	0.00442	0.05497	1349772007.30759	1349772007.33187	0.02429	0.002
1349772007.18690	1349772007.18690	0.00000	0.10145	1349772007.28834	1349772007.28834	0.00000	0.06195
1349772007.33390	1349772007.34410	0.01020	0.01077	1349772007.35488	1349772007.36456	0.00968	0.00161
1349772007.17943	1349772007.17943	0.00000	0.19789	1349772007.37732	1349772007.39497	0.01765	0.00156
1349772007.39653	1349772007.41090	0.01437	0.00589	1349772007.41679	1349772007.41840	0.00161	0.00159
1349772007.35030	1349772007.35030	0.00000	0.02380	1349772007.37410	1349772007.42599	0.05190	0.00160
1349772007.36616	1349772007.37058	0.00441	0.05855	1349772007.42913	1349772007.45386	0.02473	0.00161
1349772007.42306	1349772007.42306	0.00000	0.04724	1349772007.47031	1349772007.47031	0.00000	0.00143
1349772007.42453	1349772007.42453	0.00000	0.05020	1349772007.47472	1349772007.47472	0.00000	0.00143
1349772007.45546	1349772007.46566	0.01020	0.01962	1349772007.48528	1349772007.49538	0.01010	0.00160
1349772007.50285	1349772007.50285	0.00000	0.00145	1349772007.50430	1349772007.50430	0.00000	0.01249

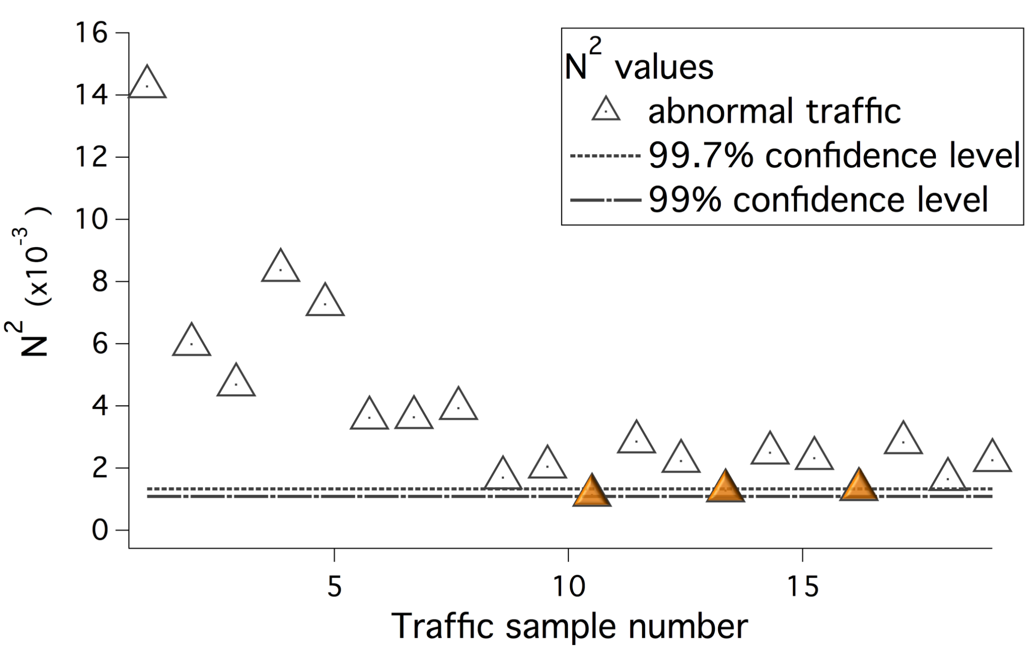
FEATURES SELECTION AND EXTRAPOLATION



DETECTION ALGORITHM

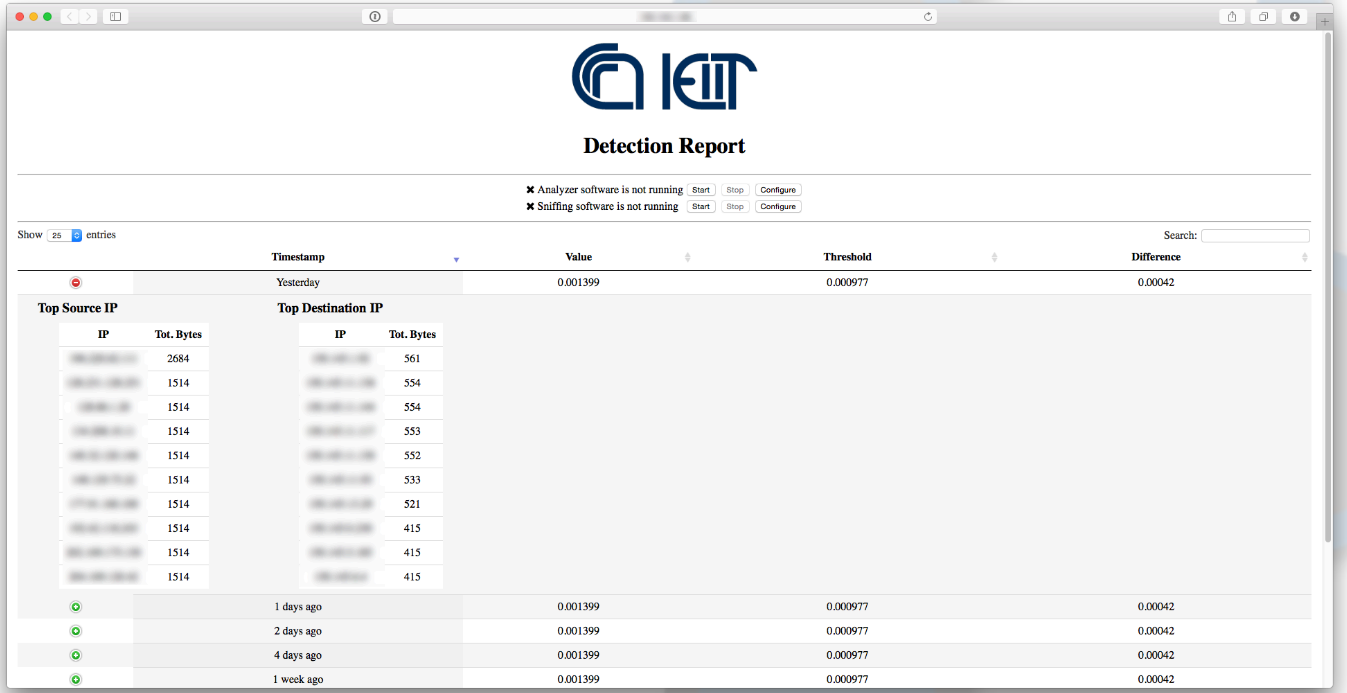
DETECTION RESULT

An Example: Anomaly based IDS algorithms



Aiello, Maurizio, et al. "A similarity based approach for application DoS attacks detection." Computers and Communications (ISCC), 2013 IEEE Symposium on. IEEE, 2013.

An Example: Tunneling Detection



Detection Report

✖ Analyzer software is not running Start Stop Configure
✖ Sniffing software is not running Start Stop Configure

Show 25 entries Search:

	Timestamp	Value	Threshold	Difference
⊖	Yesterday	0.001399	0.000977	0.00042

Top Source IP

IP	Tot. Bytes
[redacted]	2684
[redacted]	1514
[redacted]	1514
[redacted]	1514
[redacted]	1514
[redacted]	1514
[redacted]	1514
[redacted]	1514
[redacted]	1514
[redacted]	1514

Top Destination IP

IP	Tot. Bytes
[redacted]	561
[redacted]	554
[redacted]	554
[redacted]	553
[redacted]	552
[redacted]	533
[redacted]	521
[redacted]	415
[redacted]	415
[redacted]	415

	Timestamp	Value	Threshold	Difference
⊕	1 days ago	0.001399	0.000977	0.00042
⊕	2 days ago	0.001399	0.000977	0.00042
⊕	4 days ago	0.001399	0.000977	0.00042
⊕	1 week ago	0.001399	0.000977	0.00042

Aiello, Maurizio, et al. "Profiling DNS tunneling attacks with PCA and mutual information." Logic Journal of IGPL (2016): jzw056.

Current research

- IoT Security
  - Protection algorithms and methodologies for IoT networks
  - Activity supported by the ANASTACIA H2020-DS-01-2016 project

ANASTACIA

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

- Blockchain Security
  - Vulnerability assessment and penetration testing against blockchain networks
  - Activity supported by the MHMD H2020-ICT-18-2016 + FINSEC H2020-CIP-01-2017 projects

MY HEALTH MY DATA

FINSEC

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 **N**etworked **A**gents for **S**ecurity and **T**rust **A**ssessment in **CPS**/**I**oT **A**rchitectures

Project overview

Enrico Cambiaso

CNR-IEIIT

Genoa, February 9th, 2018

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**

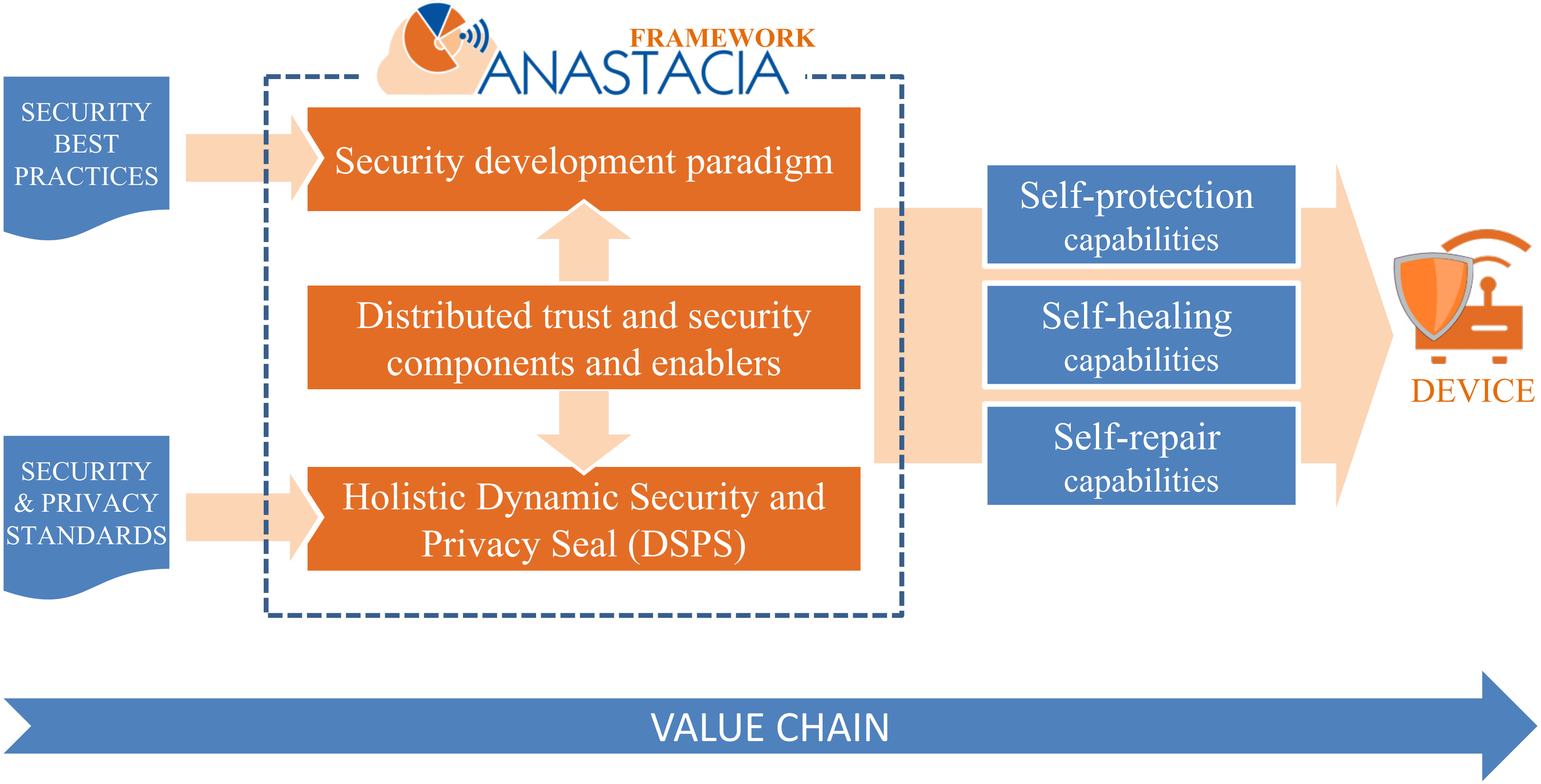
Rationale

- ANASTACIA will deliver paradigms and methods that
  - build security into the system at the outset;
  - adapt to changing conditions;
  - reduce the need of finding flaws and repairing them when the system is already deployed;
  - provide the assurance that ICT systems are secure and trustworthy at all times.

The ANASTACIA framework provides

1. Self-protection capabilities
2. Self-healing capabilities
3. Self-repair capabilities

Summarizing…


SECURITY BEST PRACTICES

SECURITY & PRIVACY STANDARDS

ANASTACIA FRAMEWORK

Security development paradigm

Distributed trust and security components and enablers

Holistic Dynamic Security and Privacy Seal (DSPS)

Self-protection capabilities

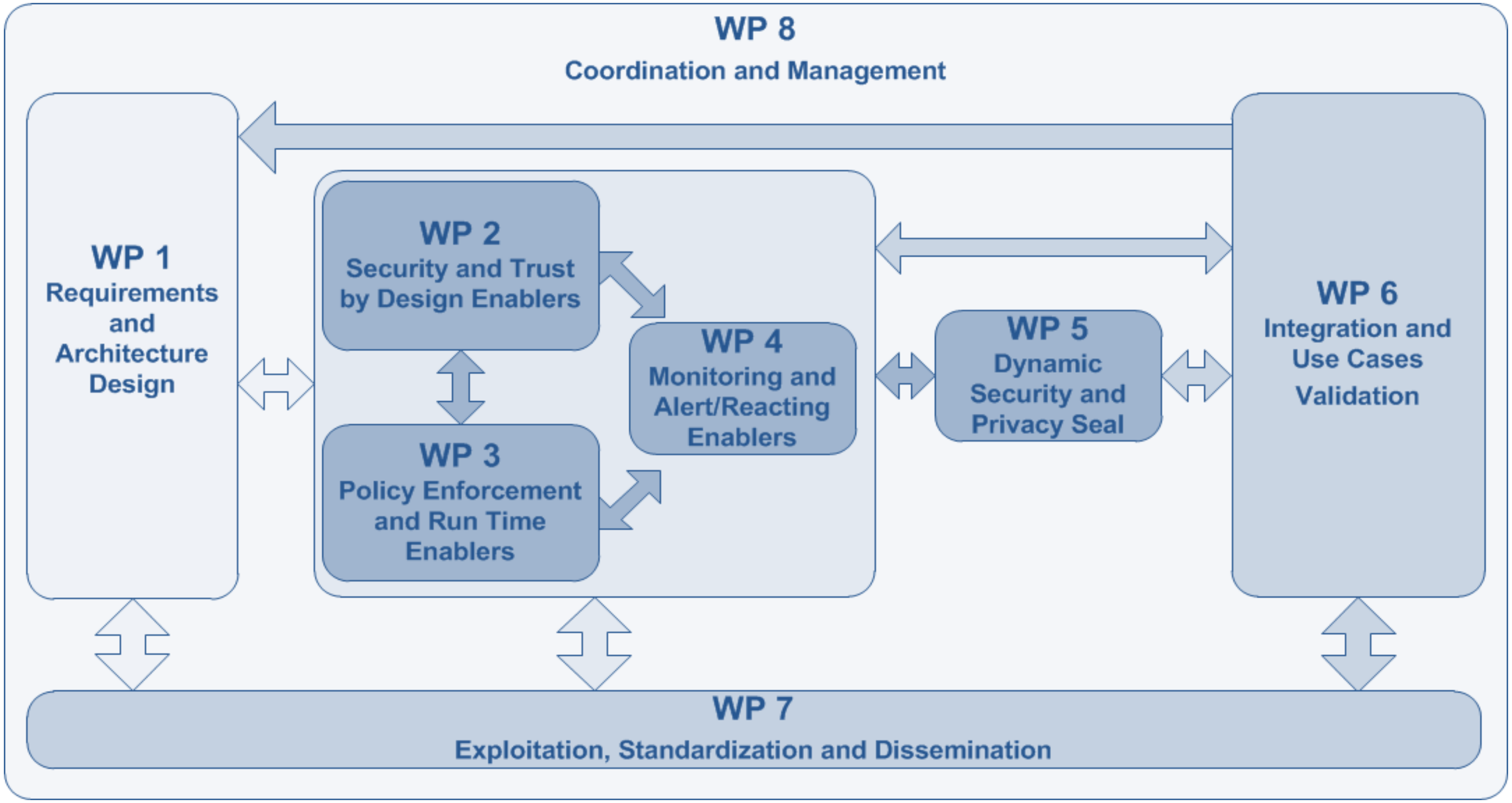
Self-healing capabilities

Self-repair capabilities

DEVICE

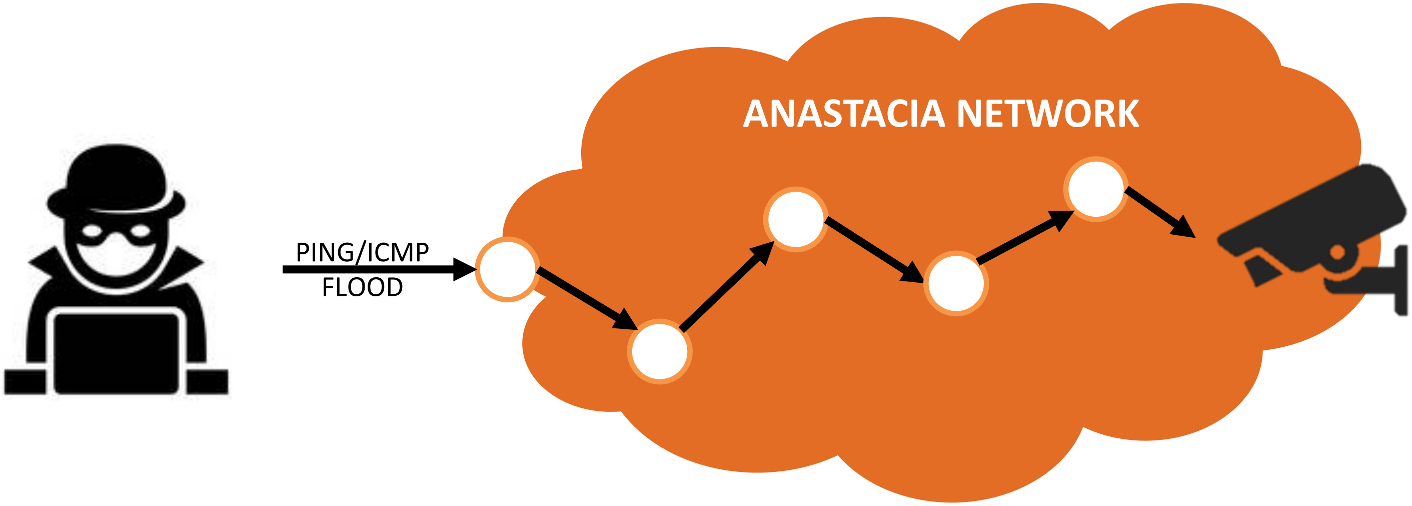
VALUE CHAIN

WP structure


WP 8
Coordination and Management
WP 1
Requirements and Architecture Design
WP 2
Security and Trust by Design Enablers
WP 3
Policy Enforcement and Run Time Enablers
WP 4
Monitoring and Alert/Reacting Enablers
WP 5
Dynamic Security and Privacy Seal
WP 6
Integration and Use Cases Validation
WP 7
Exploitation, Standardization and Dissemination

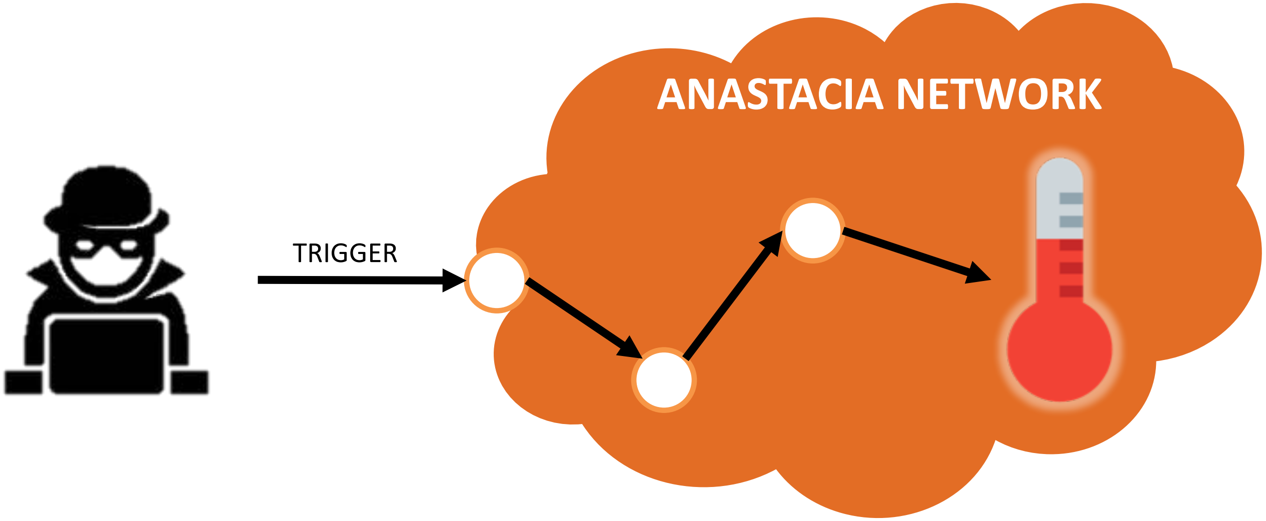
UseCase_MEC.3

- DoS and DDoS attack against smart cameras and IoT devices



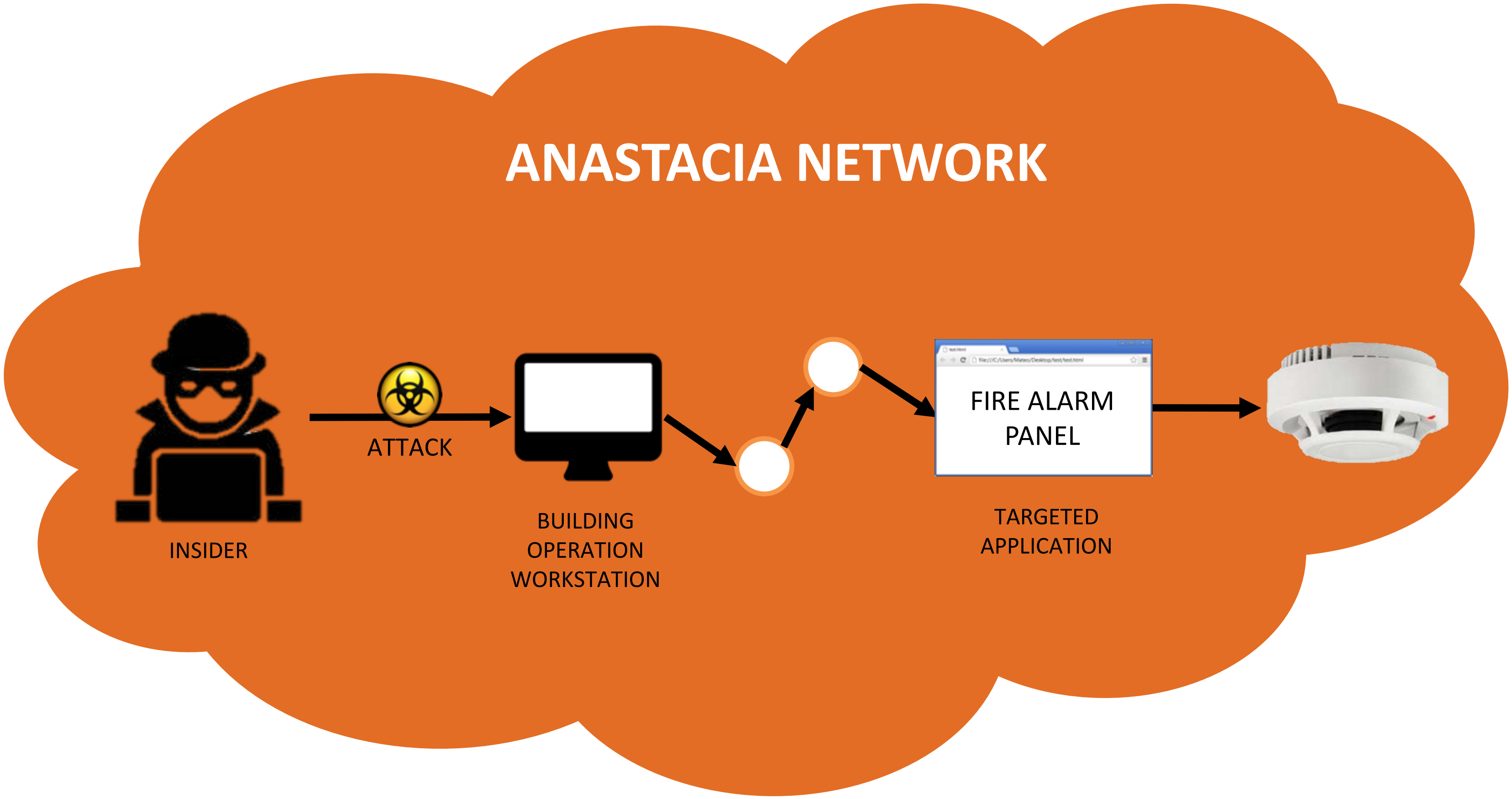
UseCase_BMS.4

- Manipulation of critical IoT temperature sensor to trigger a fire and evacuation alarm

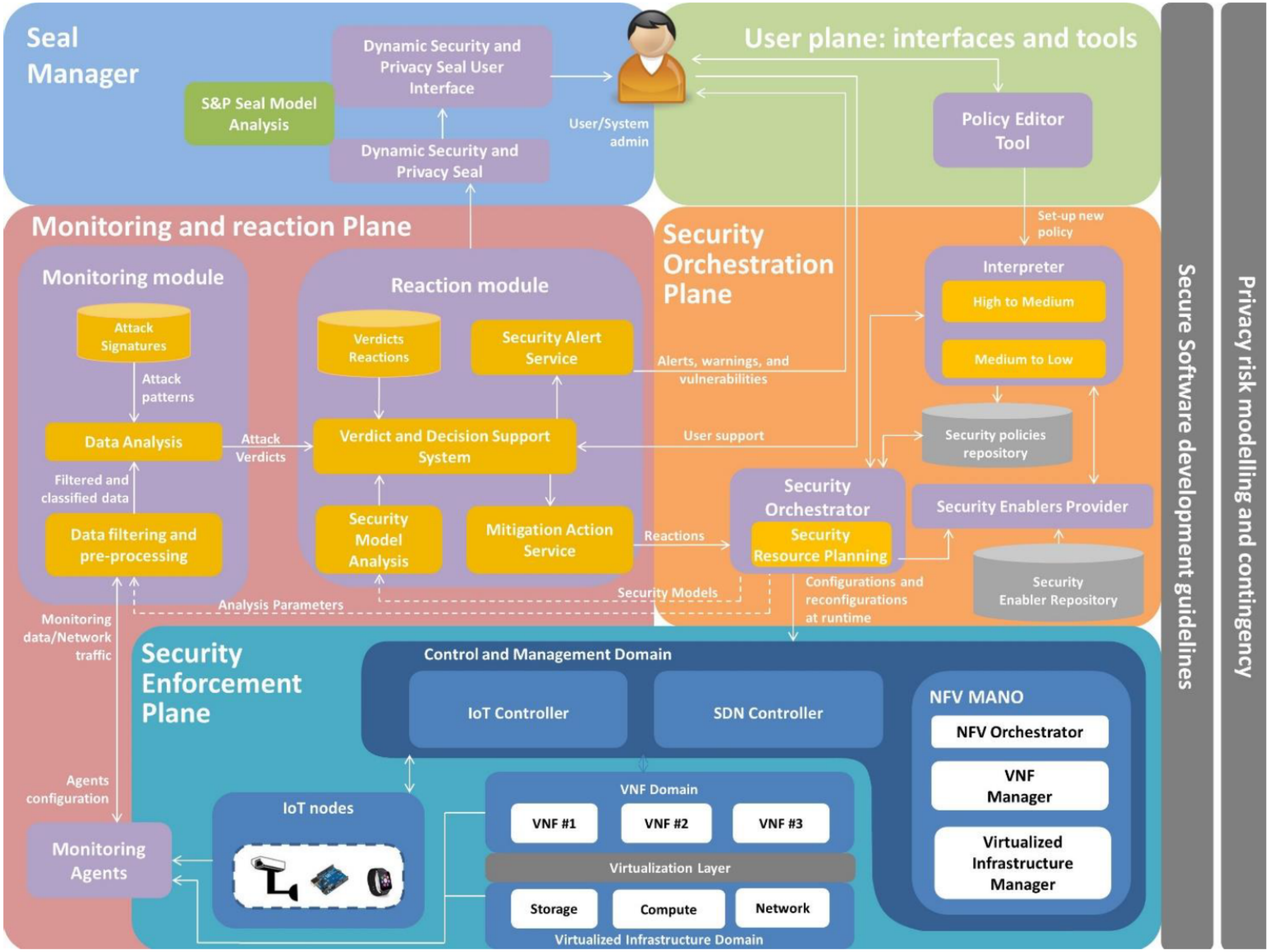


UseCase_BMS.2

- Insider attack to a fire suppression system



ANASTACIA framework architecture



Seal Manager

Dynamic Security and Privacy Seal User Interface

S&P Seal Model Analysis

Dynamic Security and Privacy Seal

User/System admin

User plane: interfaces and tools

Policy Editor Tool

Set-up new policy

Monitoring and reaction Plane

Monitoring module

Attack Signatures

Attack patterns

Data Analysis

Filtered and classified data

Data filtering and pre-processing

Attack Verdicts

Reaction module

Verdicts Reactions

Security Alert Service

Verdict and Decision Support System

Security Model Analysis

Mitigation Action Service

Security Orchestration Plane

Alerts, warnings, and vulnerabilities

User support

Interpreter

High to Medium

Medium to Low

Security policies repository

Security Orchestrator

Security Resource Planning

Security Enablers Provider

Security Enabler Repository

Reactions

Security Models

Analysis Parameters

Configurations and reconfigurations at runtime

Monitoring data/Network traffic

Agents configuration

Monitoring Agents

Security Enforcement Plane

Control and Management Domain

IoT Controller

SDN Controller

NFV MANO

NFV Orchestrator

VNF Manager

Virtualized Infrastructure Manager

IoT nodes

VNF Domain

VNF #1

VNF #2

VNF #3

Virtualization Layer

Storage

Compute

Network

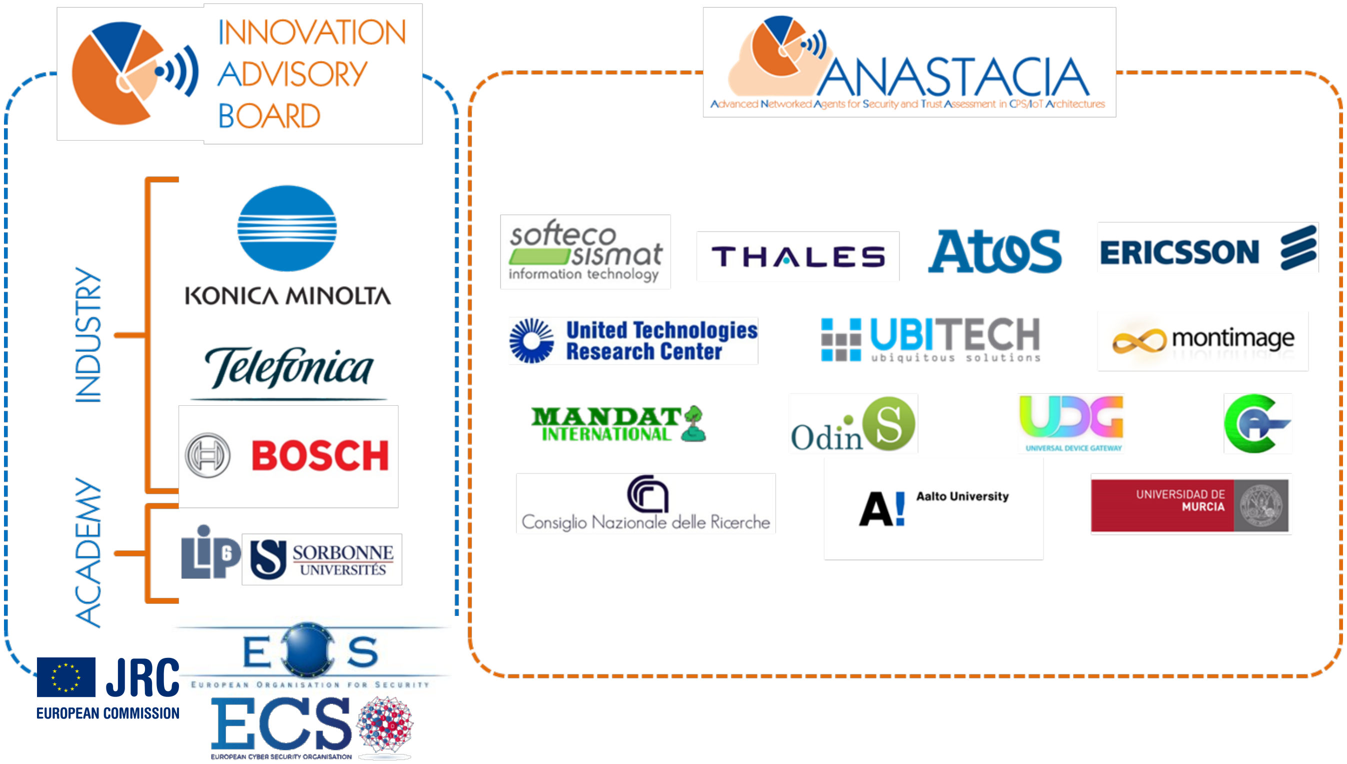
Virtualized Infrastructure Domain

Secure Software development guidelines

Privacy risk modelling and contingency

Innovation Advisory Board (IAB)

To support the Consortium in the identification and implementation of the strategy to maximize the impact of results, overviewing and aligning the released outcomes with the industry's and standardization bodies' requirements

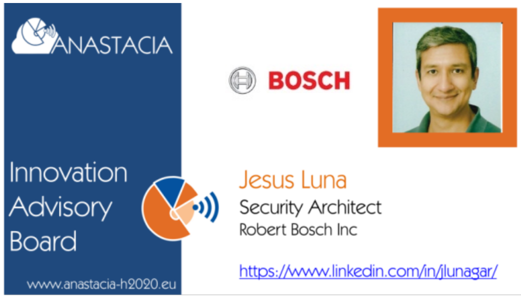

INNOVATION ADVISORY BOARD
INDUSTRY
KONICA MINOLTA
Telefonica
BOSCH
ACADEMY
LIP6
SORBONNE UNIVERSITÉS
JRC EUROPEAN COMMISSION
EOS EUROPEAN ORGANISATION FOR SECURITY
ECS EUROPEAN CYBER SECURITY ORGANISATION
ANASTACIA
Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures
softeco 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
A! Aalto University
UNIVERSIDAD DE MURCIA

IAB members

Christian Mastrodonato
Chief Technologist
Konica Minolta Inc
https://www.linkedin.com/in/cmastrodonato/

Diego R. Lopez
Senior Technology Expert
Telefonica I+D
https://es.linkedin.com/in/dr2lopez

Gianmarco Baldini
Scientific Officer
EC, Joint Research Centre
https://www.linkedin.com/in/gianmarco-baldini-61558216/



Jesus Luna
Security Architect
Robert Bosch Inc
https://www.linkedin.com/in/jlunagar/

Stefano Secci
Associate Professor
Pierre and Marie Curie University (UPMC)
Paris VI - LIP6
https://www.linkedin.com/in/stefanosecci/

Mark Miller
CEO of CONCEPTIVITY
Vice Chairman of EOS
Member of the Board of Directors at European Cyber Security OrganisationScientific Officer
https://www.linkedin.com/in/markrobertmiller/

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 **N**etworked **A**gents for **S**ecurity and **T**rust **A**ssessment in **C**PS/**I**oT **A**rchitectures

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

Summarizing CNR-IEIIT activities

- Research entity operating in the ICT field
- Focus on the implementation of both innovative cyber-threats and protection systems, on different contexts
- Involved in several research projects
- Available for further collaborations

Thanks

security@ieiit.cnr.it
http://www.netsec.ieiit.cnr.it