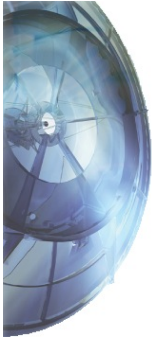


Specification-based intrusion detection

Effectively detecting intrusions using business logic specification

J. Lima, N. Escravana

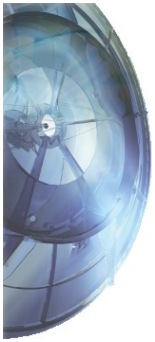




Abstract

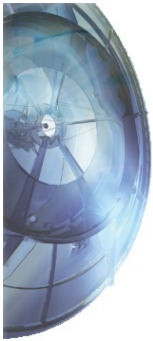
In the recent years, the advent large-scale, highly targeted cyber-attacks raised the concern on the protection of IT systems in general, and particularly the systems used to command, support and control critical infrastructures, where public transportation networks are inserted. Intrusion detection systems (IDS) have been used as a tool to detect attempted, or already accomplished, intrusions on IT systems, providing support to security administrators in the monitoring of their networks, in order to discover actual, and avoid future, intrusions. However the extensively acknowledged effectiveness problems these systems suffer have been hampering their broad usage.

In the context of the SECUR-ED FP7 project, an intrusion detection tool using an innovative, business-process specification-based approach, that may be effective in increasing the protection of critical infrastructures and, at the same time, is able to solve some of the typical IDS problems, while working at an high semantic abstraction level.



Presentation outline

- INOV and SECUR-ED presentation
- Intrusion detection systems
 - Current strategies and technologies
 - Limitation and challenges
- Business logic intrusion detection system
 - System architecture
 - Business logic specification-based model
- Laboratory validation



INOV - INESC Inovação



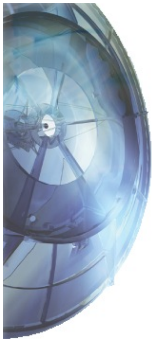
INOV - INESC Inovação is a leading private non-profit Research & Technology Organization in Portugal.

It provides Consultancy, Innovation and Technological Development in collaboration with governments, companies and universities worldwide.

INOV has strong technical expertise in:

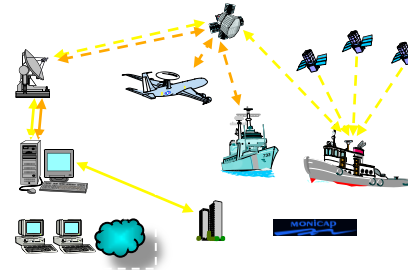
- **Monitoring and Surveillance Solutions**
- **Electronics Product Development**
- **Cyber Security & Defense**
- **Communication Networks & Services**
- **IT & Open Source Solutions**
- **Enterprise Engineering & IT Governance**



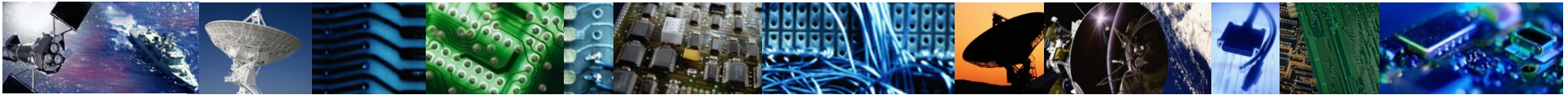


Activity Areas

- Sensors and Remote Monitoring
- Command and Control Centres
- Automatic Incident Detection
- Embedded Systems
- LASER / LIDAR
- Signal Processing



Monitoring, Navigation and Control



- IP networks
- Cybersecurity
- Fixed and Mobile Comms Equipment
- Telecom Platforms and Services
- IVRs & Voice Portals

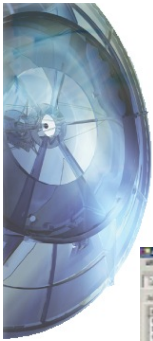


- Organisational Engineering
- Systems Integration
- Technological Consulting
- Software Quality Assurance
- Open Source

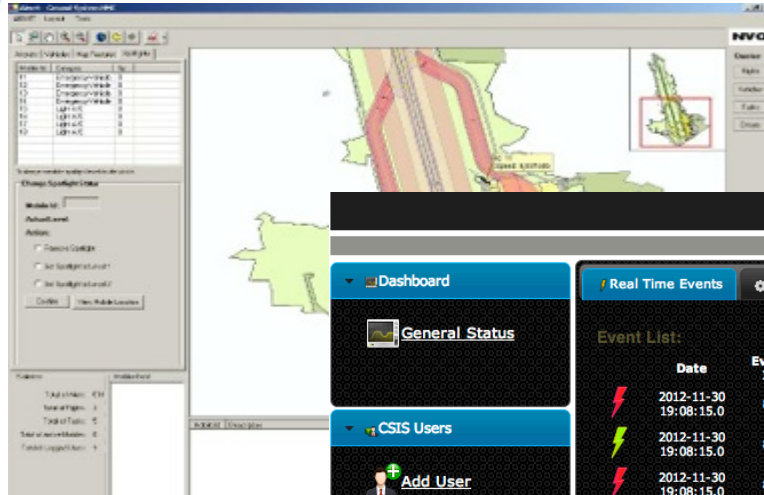
Communications

Information Technologies

Presented at Lisbon 2013 FIRST/TF-CSIRT Technical Colloquium
SECUR-ED partly funded by EU FP7 under CA n° 261605



INOV



Dashboard | **Real Time Events** | Running Processes | Sensor Notifications | System Statistics | System Health

General Status

CSIS Users

[Add User](#)

[List Users](#)

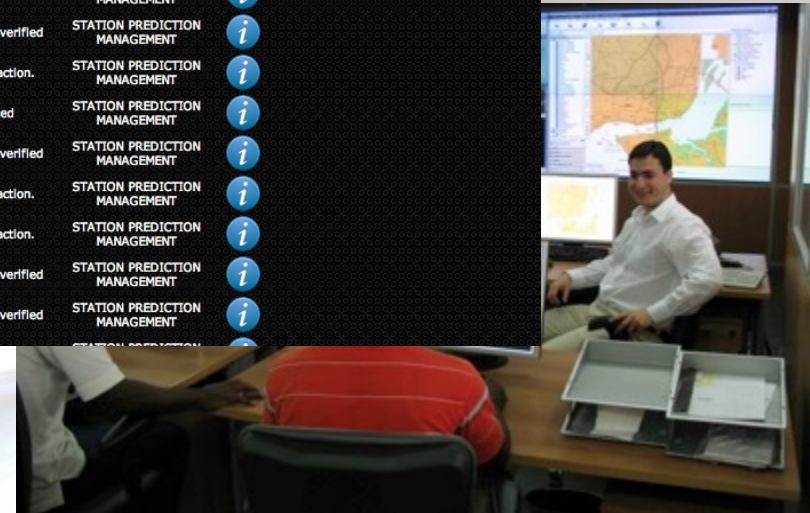
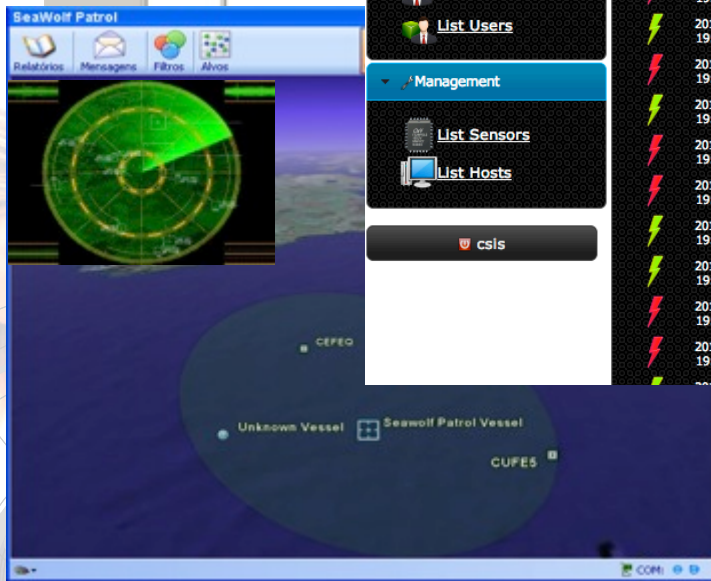
Management

[List Sensors](#)

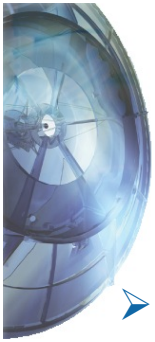
[List Hosts](#)

[csis](#)

Event List:						Filter:	
Date	Event Id	Name	Process Name			Time Constraints:	
2012-11-30 19:08:15.0	87	Application action verified	STATION PREDICTION MANAGEMENT			Start Date:	<input type="text"/>
2012-11-30 19:08:15.0	86	New application action.	STATION PREDICTION MANAGEMENT			End Date:	<input type="text"/>
2012-11-30 19:08:15.0	85	Application action verified	STATION PREDICTION MANAGEMENT			<input checked="" type="checkbox"/> Real Time	
2012-11-30 19:08:15.0	84	New application action.	STATION PREDICTION MANAGEMENT			Severity:	<input type="button" value="All"/> <input type="button" value="Info"/> <input type="button" value="Normal"/> <input type="button" value="Alarm"/>
2012-11-30 19:08:02.0	82	Application action verified	STATION PREDICTION MANAGEMENT				
2012-11-30 19:08:02.0	81	New application action.	STATION PREDICTION MANAGEMENT				
2012-11-30 19:08:02.0	83	Process Verified	STATION PREDICTION MANAGEMENT				
2012-11-30 19:07:45.0	80	Application action verified	STATION PREDICTION MANAGEMENT				
2012-11-30 19:07:45.0	79	New application action.	STATION PREDICTION MANAGEMENT				
2012-11-30 19:07:15.0	77	New application action.	STATION PREDICTION MANAGEMENT				
2012-11-30 19:07:15.0	78	Application action verified	STATION PREDICTION MANAGEMENT				
2012-11-30 19:07:15.0	76	Application action verified	STATION PREDICTION MANAGEMENT				



Presented at Lisbon 2013 FIRST/TF-CSIRT Technical Colloquium
 SECUR-ED partly funded by EU FP7 under CA n° 261605



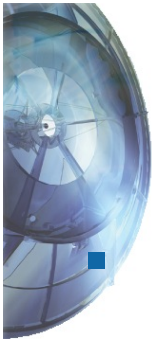
SECUR-ED in short

- Call FP7-SEC-2010-1, Security in Mass transportation

- SECured URban transportation – European Demonstration
 - Budget = 40M€, EC Funding = 25 M€, the biggest FP7 Security project
 - Starting date: 1st April 2011
 - Duration: 42 months

- The main objective of the SECUR-ED project is to give **transport operators** of large and medium **European cities** the **means to enhance urban transport security**

- The second main objective is to **enlarge the mass transport security market** for the European industry



A consistent and balanced consortium

■ 40 partners:



Operators

ATM	Italy
DEUTSCHE BAHN	Germany
RATB (Bucharest)	Romania
EMEF	Portugal
RATP	France
EMT MADRID	Spain
SNCF	France
FNM MILANO	Italy
STIB	Belgium
TCDD	Turkey

Authorities, Organisations

EOS	Belgium
STSI	France
CRTM	Spain
UITP	Belgium
UNIFE	Belgium

Industries

THALES TCS (coordinator)	France
ALSTOM TRANSPORT	France
ANSALDO STS	Italy
BOMBARDIER TRANSPORTATION	Germany
NICE	Israel
MORPHO	France
AXIS	Sweden
SELEX ELSAG	Italy

Research

CEA	France
FOI	Sweden
FRAUNHOFER	Germany
JRC	Europe
PADERBORN UNIV.	Germany
STAVANGER UNIV.	Norway
TNO	Netherlands
TU DRESDEN	Germany
VTT	Finland
WUERZBURG UNIV.	Germany
INOV	Portugal

SME

EDISOFT	Portugal
HAMBURG CONSULT	Germany
ICCA	Spain
MTRS3	Israel
INECO	Spain
G. TEAM	Israel

Presented at Lisbon 2013 FIRST/TF-CSIRT Technical Colloquium
SECUR-ED partly funded by EU FP7 under CA n° 261605

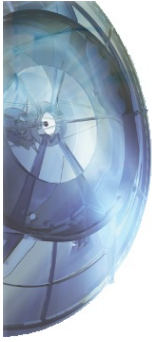




Security Capacities

- By security capacities, we mean all measures enhancing the security of passengers, staff and assets in a multimodal transport node
- This implies:
 - Specific tools for deeper analysis of the security risks & solutions
 - Smart and generic security operating procedures
 - Improve interoperability of technical security solutions
 - Video surveillance (CCTV)
 - Infrastructure protection and/or resilience
 - Protection against CBRN-E
 - Information management and communication
 - Preventive & early analysis
 - Cyber Security
 - Training programmes for various stakeholders:
 - Passengers, employees (PTO or shops)
 - Operators of control centre, security manager, decision maker

A mix of technologies and procedures
A mix of best practices and training programmes



SECUR-ED presentation



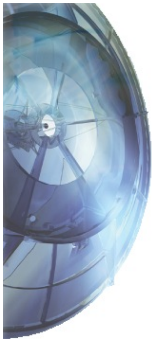
INOV role in SECUR-ED:

- Perform security risk assessments on 5 cities public transport operators (Lisbon, Bilbao, Krakow, Bucharest & Flensburg)
- Create a intrusion detection solution targeted for usage in urban public transportation



10
Presented at Lisbon 2013 FIRST/TF-CSIRT Technical Colloquium
SECUR-ED partly funded by EU FP7 under CA n° 261605



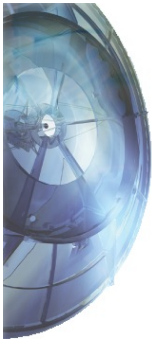


Intrusion detection systems

Overview



- Have been studied and used for more than 30 years
 - Need for IDSs was first justified by Anderson
 - Primitive IDS proposed by the same author years later
 - First IDS called IDES was proposed by Dorothy Denning
 - First proposals developed to protect small and seldom-changed systems with a restricted and well defined number of users



Intrusion detection systems

Current Technologies and strategies



- Data Collection

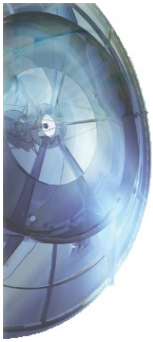
- Host-based
- Network-based

- System architecture and processing strategy

- Single instance
- Centralised
- Distributed

- Processing method

- Misuse detection
- Anomaly detection
- Specification-based



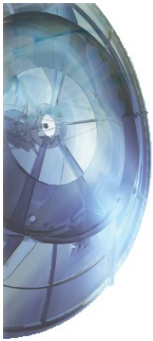
Intrusion detection systems

Limitations and challenges

- DARPA 1998 and 1999 evaluations
 - IDSs of several research teams were set to be tested
 - Comprehensive set of attacks were conducted against several test hosts
 - Significant number of false positives and false negatives generated by the systems at test

- Werlinger et al. usability assessment
 - Personal interview of 35 participants from 16 organizations with background in IT management and security
 - IDSs are said to be expensive, hard to deploy and maintain, unreliable and apparently useless

- Vigna et al.
 - Main challenge is yet to expand IDS's scope in order *“to take into account the surrounding context, in terms (...) of missions, tasks, and stakeholders, when analysing data in an effort to identify malicious intent.”*



Business logic IDS

System architecture

■ Data Collection

➤ Network-based

- “Core” sensors of the solution
- Used solution based on rules to detect misuse and specification-based => Snort

➤ Host-based

- Used when is not possible to obtain information from the network, or the information obtained is rather inconclusive
- Used to monitor the integrity in critical systems that are expected to be seldom changed

■ System architecture and processing strategy

➤ Centralised

- Intrusion detection sensors spread along the target system

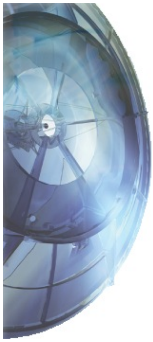
■ Processing method

➤ Misuse detection

- Used to find attacks already known

➤ Specification-based

- Used to find deviations from the application processes

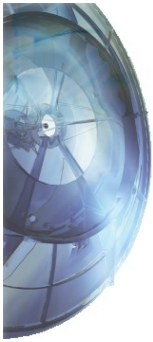


Business logic specification model



- Focused in business and application architectural layers
 - Specification of the interactions between systems in order to accomplish a certain objective => Business processes
 - BPMN as a graphical notation
 - Specification of rules that must be valid across the organization / execution of business processes => Business rules

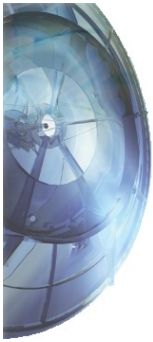
- Technically this model was divided in two sub-models
 - Types model -> supports the definition of the business logic
 - Instances model -> supports the verification of the business logic



Business logic specification model

Business processes

- Defined using concepts of BPMN
 - Pools -> Bound to hosts or groups of hosts in the monitored environment
 - Activities -> Atomic behaviour unit performed by a host or group of hosts
 - Gateways
- Extension is made to include state-tracking mechanisms based on informational entities
 - Validation class is created for each activity, expressing the conditions it must met, and the entity's attributes must be set as the result of a positive validation
- Similarly, gateways use guard conditions to condition the process flow expressed as external validators

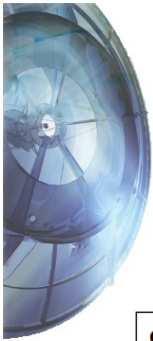


Business logic specification model



Business rules

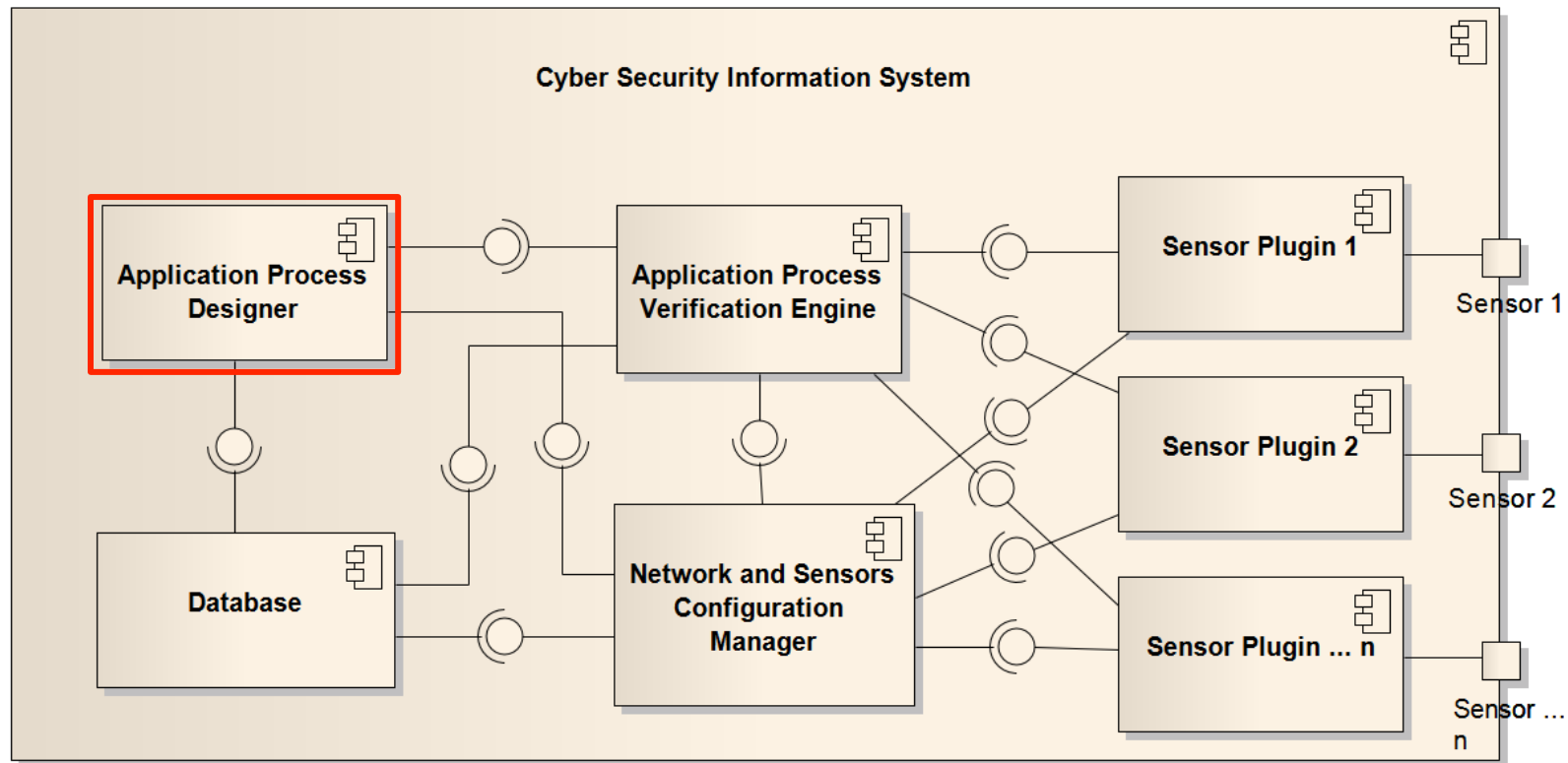
- Some relations are possible to be captured using business processes
 - It wouldn't even make sense to
- Business rules express conditions that must be met across the system
 - External validator used as in gateways and activities
 - Evaluated when a referenced informational entity is changed
 - Evaluation of the business rule can involve information external to the environment

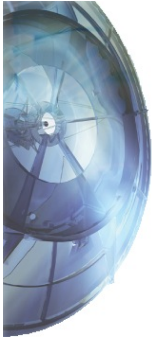


Business logic IDS

Central system

cmp Cyber Security Information System Logical M...



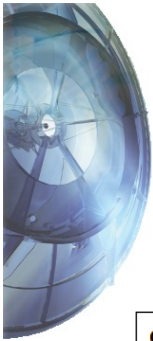


Business logic IDS

Business logic designer

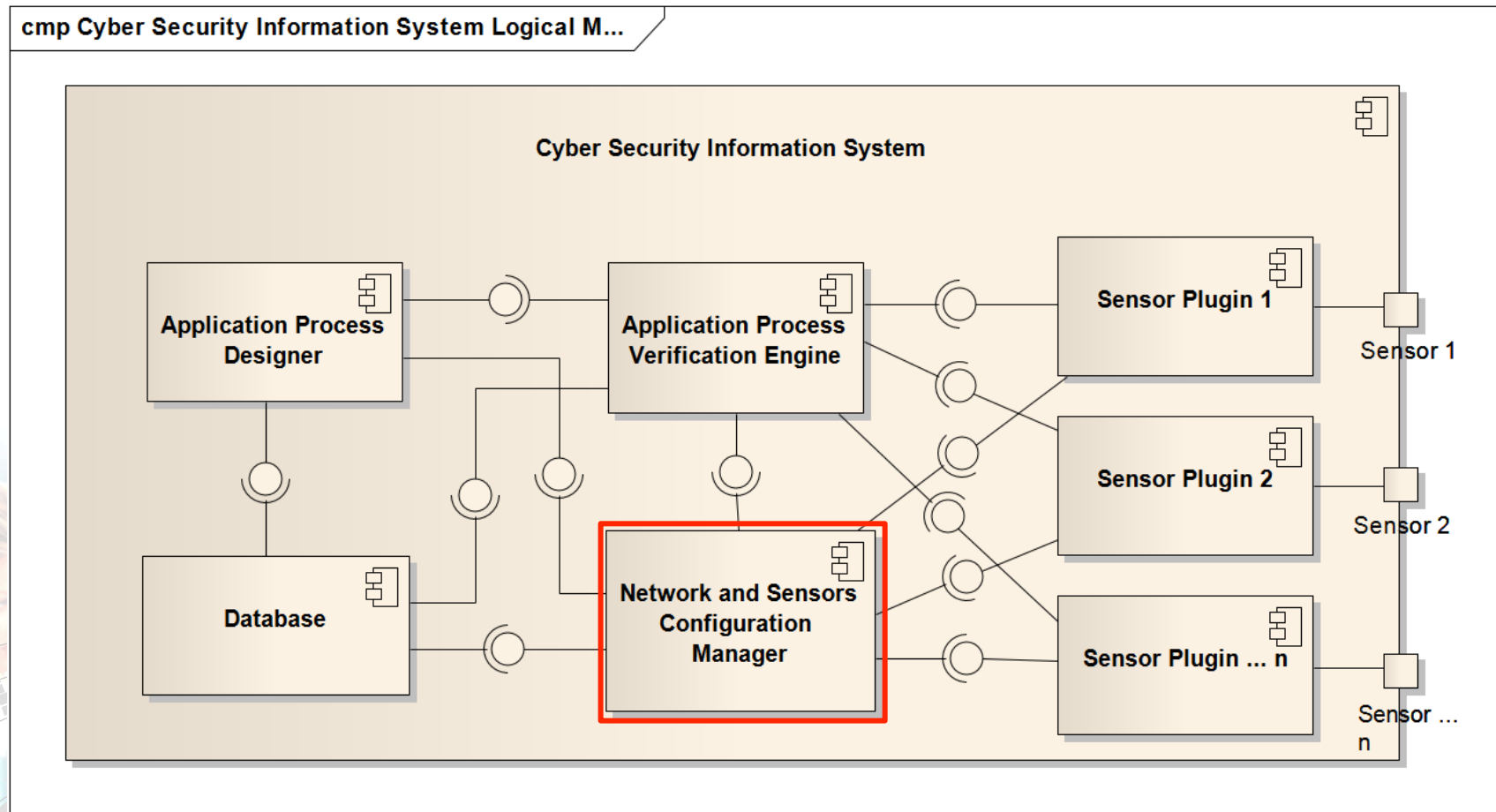


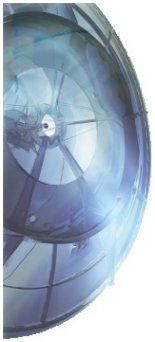
- Configuration utility
- Used to specify new, and change existent, business processes and business rules
- Also used to define the monitored environment (hosts and intrusion detection sensors)



Business logic IDS

cmp Cyber Security Information System Logical M...





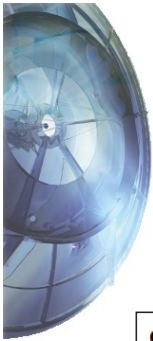
Business logic IDS

Network and sensors configuration manager



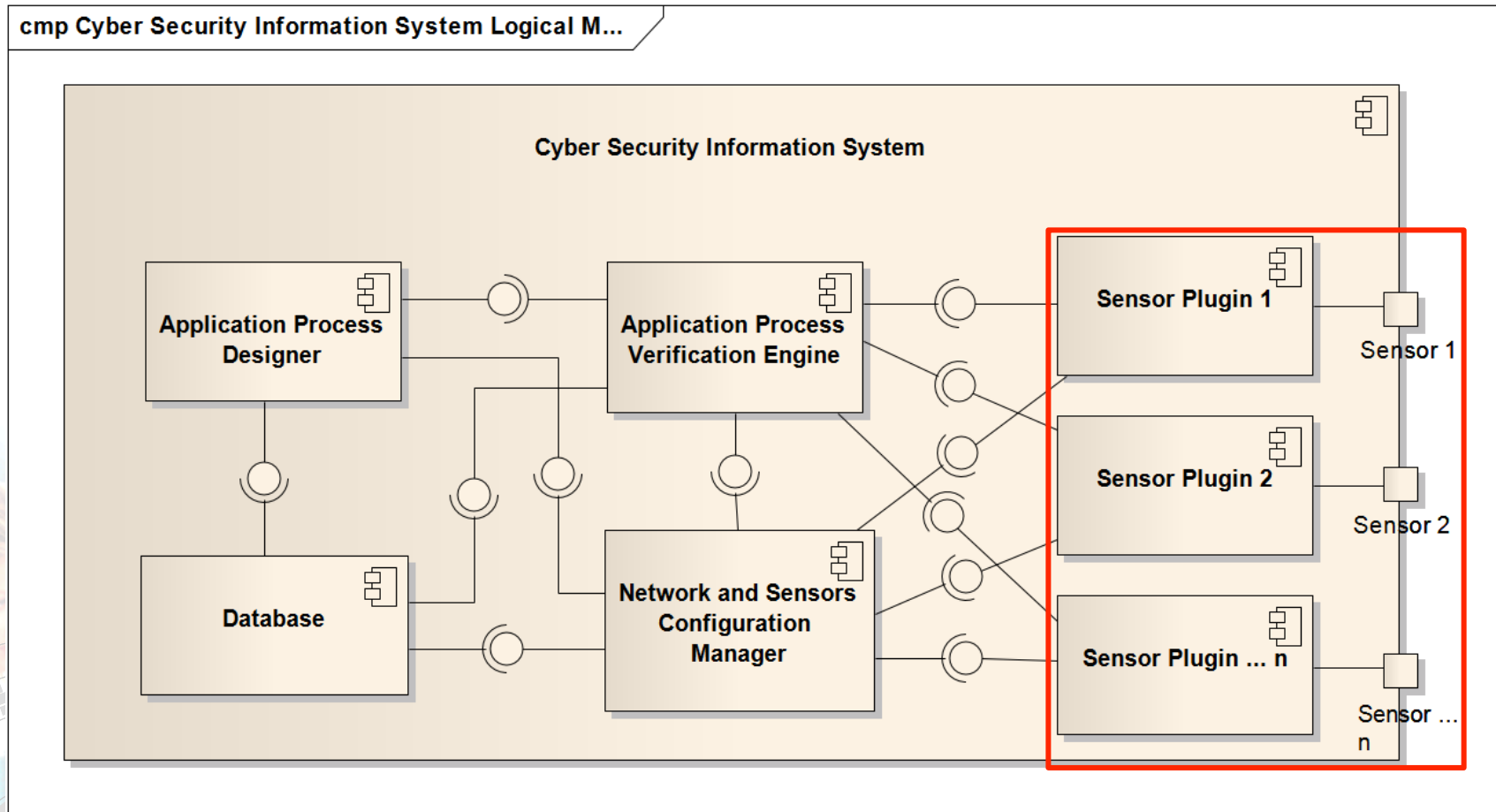
- Update the configuration of the intrusion detection sensors on specification-based model changes
- Load the configuration of the intrusion detection sensors at system startup

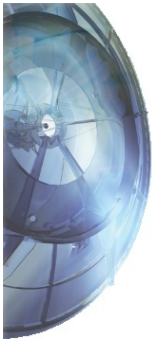




Business logic IDS

cmp Cyber Security Information System Logical M...





Business logic IDS

Sensor plugins

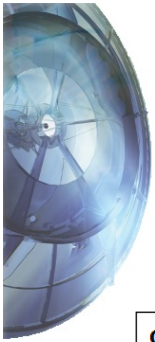
- Does the interface between the central system and each intrusion detection sensor

- Two “core” operations
 - Translation of specification-based rules to the sensor’s rule language
 - Conversion of the detected specification-based events to the system’s internal representation

- Short sensor plugin implemented

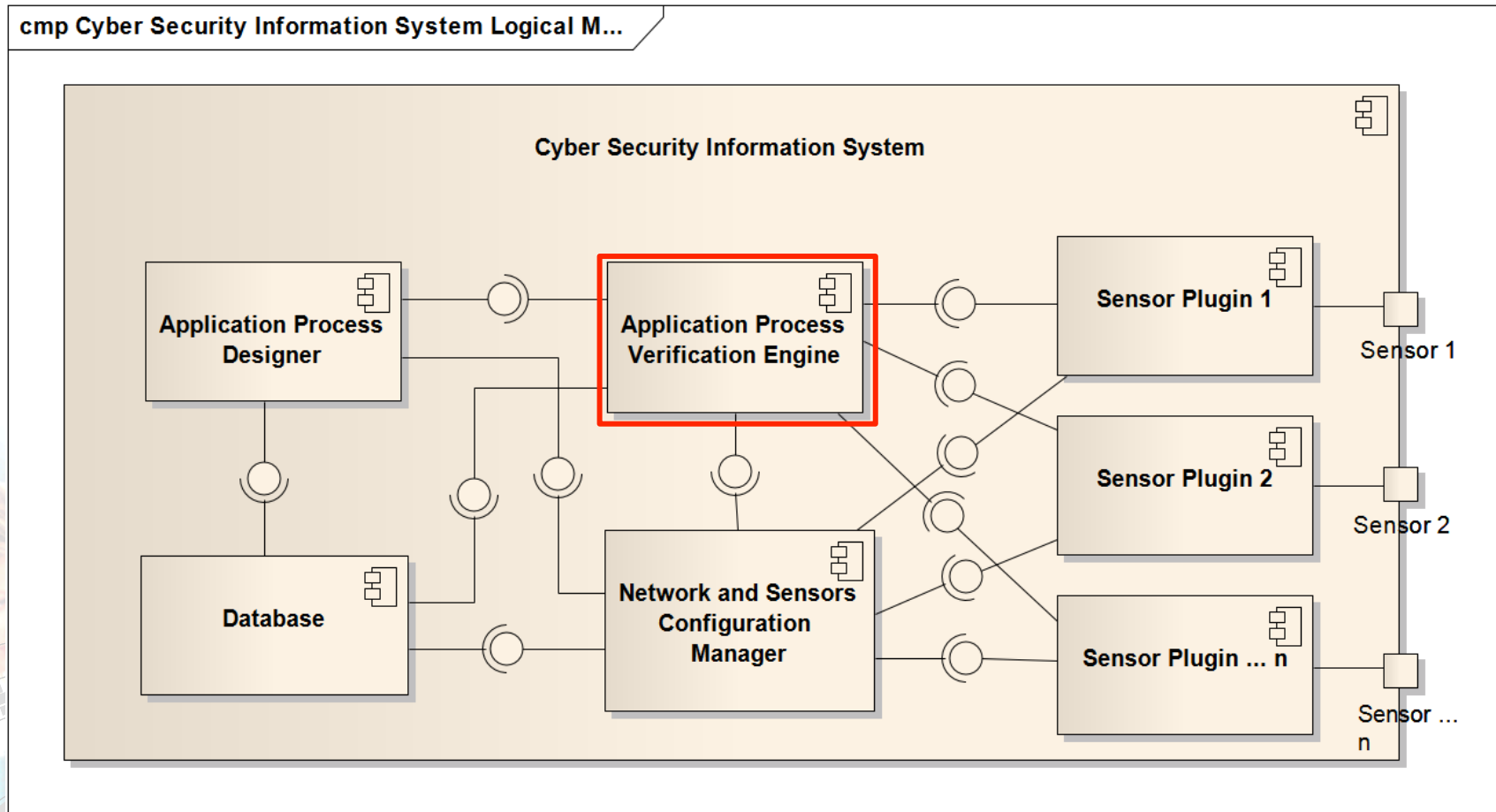
23

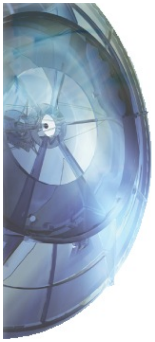
Presented at Lisbon 2013 FIRST/TF-CSIRT Technical Colloquium
SECUR-ED partly funded by EU FP7 under CA n° 261605



Business logic IDS

cmp Cyber Security Information System Logical M...



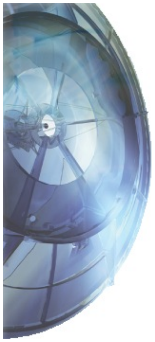


Business logic IDS

Business logic verification engine



- Main component of the system
- Responsible for verifying the execution of business processes and business rules
- Generates alerts when a deviation between the specification and the verification happens



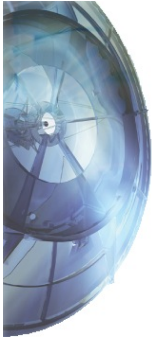
Business logic IDS

Verification algorithm

- **Event arrives at the verification engine**
 - If within time limit is set to be verified

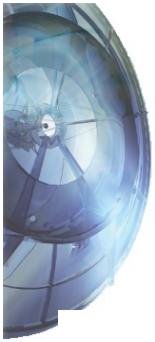
- **Obtained or created the business process the event belongs to**
 - If no process is referenced an alert is thrown
 - If the referenced process is not expecting the received event an alert is thrown

- **Received activity verified in the context of the referenced process**
 - If failed an alert is thrown

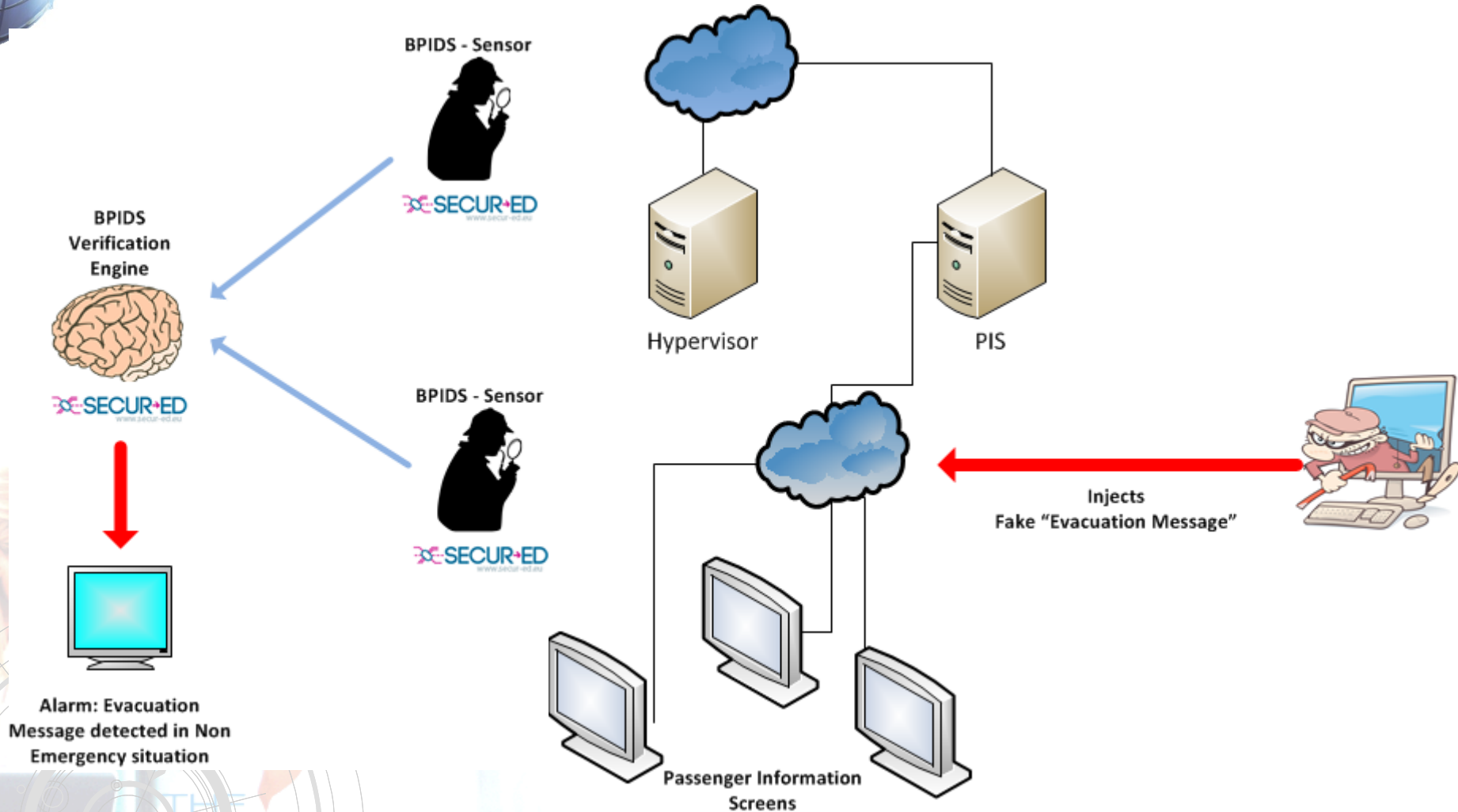


Test environment

- Based on network captures of a public transport network IT architecture laboratory simulation
- Three business process specified
 - Platform emergency management
 - Platform information management
 - Train movement management
- Four informational entity types and one business rule created

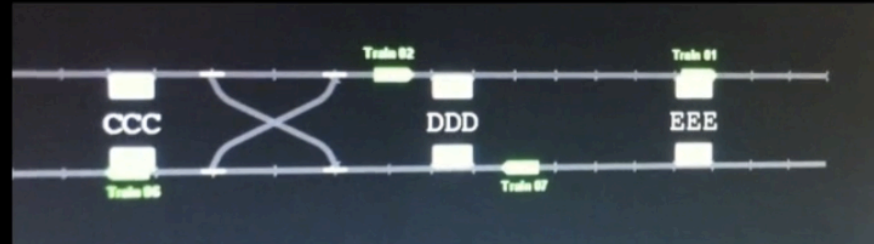


Demo possible scenario



Demo possible scenario

00:00:52 / 00:01:30
Station EEE



Platform 1 17:45

02		
Station JJJ	17:47	02 min. remaining...
03		
Station JJJ	17:49	04 min. remaining...

Platform 2 17:45

08		
Station AAA	17:46	01 min. remaining...
09		
Station AAA	17:49	03 min. remaining...

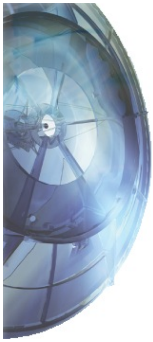
Business Process IDS
Management and Configuration Console

Dashboard | General Status | CSIS Users | Add User | List Users | Management | List Sensors | List Hosts | csis

Real Time Events | Running Processes | Sensor Notifications | System Statistics | System Health

Date	Event Id	Name	Process Name
2012-12-01 22:08:07.0	36	Application action "Display arrival prediction message" was verified in the process with id 86	STATION PREDICTION MANAGEMENT
2012-12-01 22:08:07.0	35	New application action validator to the action "Display arrival prediction message" of the process validator 86 was created with id 95	STATION PREDICTION MANAGEMENT
2012-12-01 22:08:07.0	34	New application process validator for the application process STATION PREDICTION MANAGEMENT was created with id 86	STATION PREDICTION MANAGEMENT
2012-12-01 22:08:06.0	33	Application action "Display arrival prediction message" was verified in the process with id 45	STATION PREDICTION MANAGEMENT
2012-12-01 22:08:06.0	32	New application action validator to the action "Display arrival prediction message" of the process validator 45 was created with id 84	STATION PREDICTION MANAGEMENT
2012-12-01 22:07:53.0	30	New application action validator to the action "Display arrival prediction message" of the process validator 58 was created with id 82	STATION PREDICTION MANAGEMENT
2012-12-01 22:07:53.0	31	Application action "Display arrival prediction message" was verified in the process with id 58	STATION PREDICTION MANAGEMENT
2012-12-01 22:07:52.0	29	Application action "Display arrival prediction message" was verified in the process with id 12	STATION PREDICTION MANAGEMENT
2012-12-01 22:07:52.0	28	New application action validator to the action "Display arrival prediction message" of the process validator 12 was created with id 80	STATION PREDICTION MANAGEMENT
2012-12-01 22:07:44.0	25	New application action validator to the action "Display in-station message" of the process validator 34 was created with id 79	STATION PREDICTION MANAGEMENT
2012-12-01 22:07:44.0	26	Application action "Display in-station message" was verified in the process with id 34	STATION PREDICTION MANAGEMENT

Filter: Time Constraints: Start Date: End Date: Real Time Severity: All Info Normal Alarm



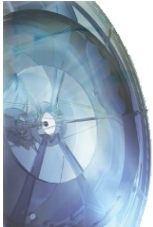
Demo possible scenario



The screenshot displays two main interface components. On the left is the 'Station EEE' control panel, which includes two platform status sections, 'Platform 1' and 'Platform 2'. Each platform section shows a yellow header with the platform name and a digital clock displaying '17:47'. Below the platform names are several horizontal bars representing train arrival and departure times. At the bottom of each platform section, a white alert box contains the text 'Alert! Please evacuate the station'. On the right is the 'Business Process IDS' Management and Configuration Console. This console features a navigation menu on the left with options like 'Dashboard', 'General Status', 'CSIS Users', 'Add User', 'List Users', 'Management', 'List Sensors', and 'List Hosts'. The main area is divided into tabs: 'Real Time Events', 'Running Processes', 'Sensor Notifications', 'System Statistics', and 'System Health'. The 'Real Time Events' tab is active, showing a table of events with columns for Date, Event Id, Name, and Process Name. The table contains multiple entries with timestamps and descriptions of application actions and validators. A 'Filter' section on the right allows for filtering events by 'Time Constraints' (Start Date, End Date, Real Time) and 'Severity' (All, Info, Normal, Alarm).

30


Presented at Lisbon 2013 FIRST/TF-CSIRT Technical Colloquium
SECUR-ED partly funded by EU FP7 under CA n° 261605




Demo possible scenario


Management and Configuration Console

Dashboard


 [General Status](#)


CSIS Users

 [Add User](#)

 [List Users](#)

Management

 [List Sensors](#)

 [List Hosts](#)

 csis

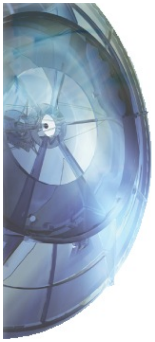
Event Details



Date: 2012-12-01 22:08:21.0
Id: 42
Name: The application action "Display evacuation message" was not expected by any process
Process Name: STATION PREDICTION MANAGEMENT

Description:

There is no process waiting for the specified entity with the given key values.
Process Type Id: 3
Action Type Id: 18
Verification Info details: Application Action Type: 18
Source Address: /192.168.8.152:1484
Destination Address: /192.168.8.151:50058
Detected Flow:
0800279aa1aa0050b609a588080045000084a03540008006c7bec0a80898c0a8089705ccc38af879bf4de1273
31b5018fe796cf200000154584d534702302c31303030352c312c393035312c332c312c207c207c207c2c322c2
07c207c207c2c332c416c6572742120506c65617365206576616375617465207468652073746174696f6e2069
6d6d6564696174656c790304
ID Sensor Timestamp: 1354399510224
Reception Timestamp: 1354399700602
Detected Attribute: Attribute ID- 21 Value: 9051
Detected Attribute: Attribute ID- 39 Value: 9051

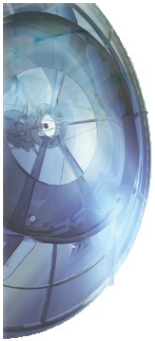


Experimentation results

- Normal operation tests
 - One false alarm produced in the first test iteration
 - No false alarms produced thereafter

- Random injection tests
 - Several alarms produced
 - No false positive or false negative alarm

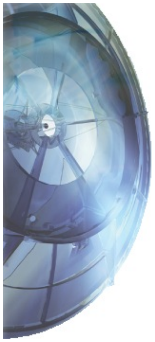




Features

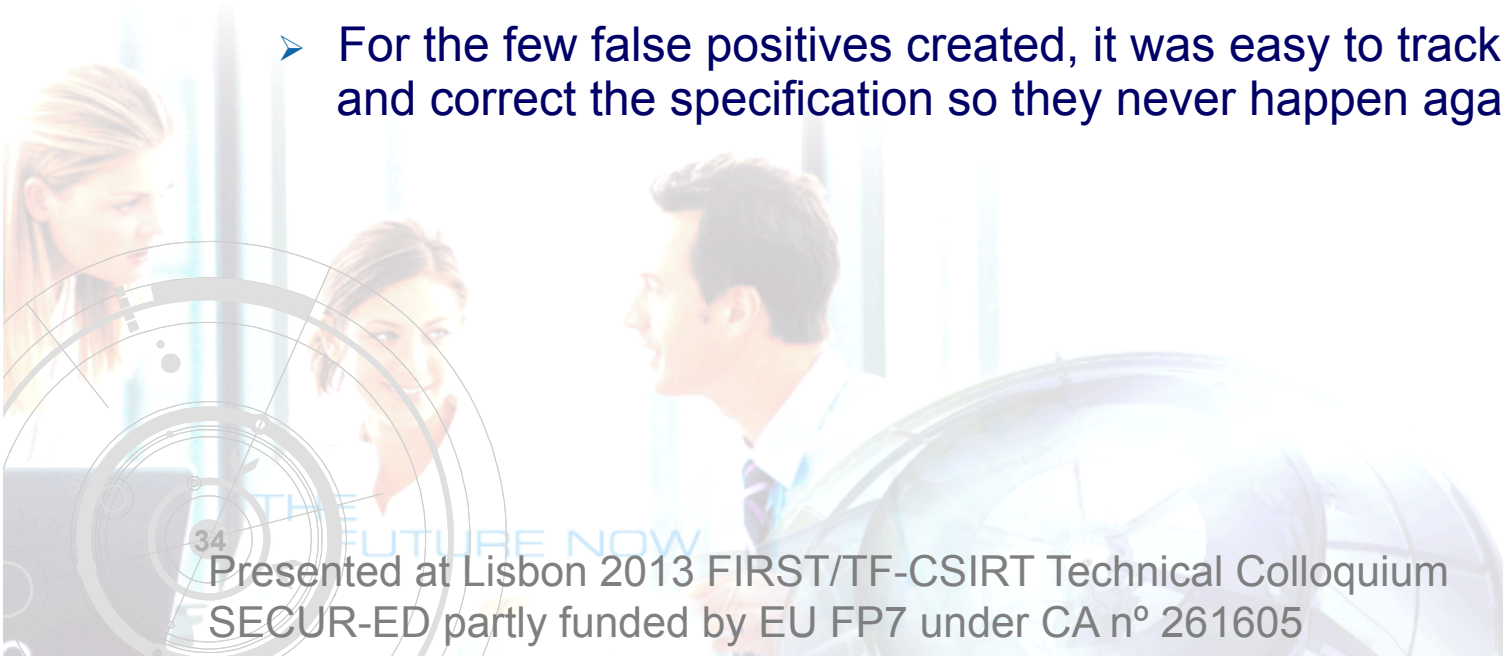
- **Detection and monitoring**
 - Detect cyber, physical and organizational attacks
 - Detect well-known cyber attacks to ICT infrastructure
 - Detect new types of attacks
 - Monitor business processes quality and performance
 - Provides a real-time overview of critical business process status

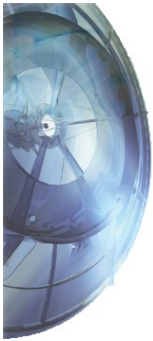




Conclusions

- Approach might provide best results when applied to environments where is possible to create a behaviour model broadly covering the environment to protect
 - Critical infrastructures are the main candidate
 - However, it may also be applied to a widest range of organizations
- Experimentation results
 - Negligible false alarm rate
 - For the few false positives created, it was easy to track them down, and correct the specification so they never happen again





www.inov.pt

SECUR-ED
SECured URban transportation - European Demonstration

**Thank you for
your attention!**

INOV - Inesc Inovação - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://www.inov.pt/>

inov
inesc • inovação

Quem somos Áreas de Actividade Sistemas Sucessos Parceiros Notícias Desenvolvimento e consultoria

Sexta-feira, 23 de Janeiro de 2004

inov
inesc • inovação

Ao longo de 20 anos, no grupo INESC, o INOV desenvolveu competências tecnológicas juntamente com grande capacidade de gestão de projectos de grande dimensão, em regime de consórcio ou em parcerias internacionais. [Mais...](#)

ciclope

➤ O INOV apresenta várias soluções e plataformas para a distribuição de áudio/vídeo sobre redes IP, permitindo responder ao largo espectro de problemas e paradigmas inerentes a esta tecnologia. [Mais...](#)

In-TRV

➤ O Sistema CICLOPE™ é um sistema de televigilância remota que possibilita a comunicação entre os diversos pontos da rede que constituem a rede de câmaras de vídeo, entre si e entre o centro de controlo e de vigilância. [Mais...](#)

MONICAP

➤ A plataforma In-TRV™ surge como uma aplicação natural do know-how acumulado pelos colaboradores do INOV nos últimos 10 anos. Trata-se de uma plataforma multi-serviço, modular, escalável, robusta, e versátil, "telecom-grade". [Mais...](#)

➤ O MONICAP™ é um sistema tipo "caixa negra" que permite a monitorização a partir de terra, da posição e velocidade dos navios em que a caixa MONICAP está instalada. [Mais...](#)

in english

© INOV marca registada de INESC INOVAÇÃO - Instituto de Novas Tecnologias
Rua Alves Redol, 9 - 1000-029 Lisboa - Portugal Tel.: +351. 213 100 450 Fax: +351. 213 100 499 Email: inov@inov.pt

[Legal] [Privacy] [Webmaster]

INOV
Rua Alves Redol, 9
1000-029 Lisboa
Portugal

Tel.: +351. 213 100 444
Fax: +351. 213 100 445
Email: inov@inov.pt
Web: www.inov.pt

Presented at Lisbon 2013 FIRST/TF-CSIRT Technical Colloquium
SECUR-ED partly funded by EU FP7 under CA nº 261605

inov
inesc • inovação