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 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

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

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

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

**Research**

- CEA (France)
- FOI (Sweden)
- FRAUNHOFER (Germany)
- JRC (Europe)
- PADENBORN UNIVERSITAT (Germany)
- STAVANGER UNIVERSITET (Norway)
- TNO (Netherlands)
- TU DRESDEN (Germany)
- VTT (Finland)
- WUERZBURG UNIVERSITAT (Germany)
- INOV (Portugal)

**Industries**

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

**SME**

- EDISOFT (Portugal)
- HAMBURG CONSULT (Germany)
- ICCTA (Spain)
- MTRS3 (Israel)
- INECON (Spain)
- G. TEAM (Israel)

Presented at Lisbon 2013 FIRST/TF-CSIRT Technical Colloquium
SECUR-ED partly funded by EU FP7 under CA nº 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**
INOV role in SECUR-ED:

- Perform security risk assessments on 5 cities public transport operators (Lisbon, Bilbao, Krakow, Bucharest & Flensburg)

- Create an intrusion detection solution targeted for usage in urban public transportation
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 attack 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 meet, 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
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
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

Cyber Security Information System

Application Process Designer
Application Process Verification Engine
Network and Sensors Configuration Manager
Database

Sensor Plugin 1
Sensor Plugin 2
Sensor Plugin ... n

Sensor 1
Sensor 2
Sensor ... n

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

- Snort sensor plugin implemented
Business logic IDS
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
Demo possible scenario
Demo possible scenario
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 it 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
Thank you for your attention!