Online Network Traffic Security Inspection Using MMT Tool

Wissam Mallouli*, Bachar Wehbi*, Edgardo Montes de Oca*
Michel Bourdellès†, Denis Rocher† and Arnaud Baloche†

* Montimage EURL, 39 rue Bobillot, 75013 Paris – France
† THALES CS, 160 Bd de Valmy, 92704 Colombes – France

9th Workshop on System Testing and Validation (STV)
Wednesday October 24, 2012
Montimage is an innovative SME

- Creation year: 2004
- Location: 39 rue Bobillot – 75013 Paris

Services

- Reliable software design and development
- Test and validation
  - Innovative testing and monitoring tools (functional, security, QoS)

Flagship tool: Montimage Monitoring Tool (to be released 2012 as Open Source)
**Motivation**

Different methodologies:

- **Signature based analysis**: e.g. SNORT, Cisco intrusion prevention system
- **Behavior based analysis**: anomaly detection based on state-full protocol analysis:
  - Using **scripts**, e.g. BRO (scripting language enabling protocol and semantic analysis),
  - **Hard coded** security properties, proprietary tools
  - Using **Model**, e.g. MMT
Motivations

Different technologies:

- Network-based IDPS: examines network traffic and monitors multiple hosts
- Host-based IDPS: identifies intrusions by analyzing system calls, logs, file-system modifications...
- Wireless IDPS: specialized for wireless communication
- Network Behavior Analysis (NBA)
- Security Information and Event Management (SIEM): integrates and correlates different sources
Motivations

Problems:
- Too many false positives due to bad traffic (bugs, corrupted and lost packets)
- Performance and scalability: tracking of simultaneous sessions
- Denial of service attacks are not based on incorrect behaviour

Proposed solutions:
- Specialized detection and correlation of different data sources
- Distributed detection mechanisms: integrate and correlate different sources
- Combine different methods and techniques: QoS, machine learning, statistics, pattern matching...
- Transparency: open source engine, properties to analyze are known by the end user.
MMT Overview

MMT Operator
- Monitoring & reporting
- Web technology
- Manages multiple probes

MMT Probe
Analysis modules
- Traffic Monitoring
- Quality Monitoring
- Security & Functional Analysis

MMT Extract
- Deep Packet Inspection functionalities
- Traffic classification (150+ protocols)
- Protocol decoding & attributes extraction
- Extraction of metrics

Config
Traffic DB
View Plugins

User defined reports
Add analysis modules
HW/SW Probe Can be installed on dedicated HW
Software library (SDK) Can be integrated in 3rd party SW
Add plugins
MMT in a transport network Scenario
MMT: Innovation

- Use of security properties to describe both wanted and unwanted behaviour
  - Not exclusively based on pattern matching like most intrusion detection techniques
  - More abstract description of sequence of events (MMT properties)
  - Can integrate performance indicators, statistics and machine learning techniques; as well as countermeasures
- Allows combining centralised and distributed analysis to detect 0-day attacks (under development)
- Applicable in several domains (at protocol, application and business levels)
- Open-source generic core with a plug-in architecture
- Allows combining active and passive approaches
MMT-Properties (1/3)

- MMT-Security properties have two types:
  - A **Security rule** describes the expected behaviour of the application or protocol under-test.
    - The non-respect of the MMT-Security property indicates an incorrect behaviour.
  - An **Attack** describes a malicious behaviour whether it is an attack model, a vulnerability or a misbehaviour.
    - The respect of the MMT-Security property indicates the detection of an abnormal behaviour that might indicate the occurrence of an attack.
Set of properties specifying constraints on the message exchange
- e.g., the access to a specific service must always be preceded by an authentication phase

Set of properties referring to a vulnerability or to an attack
- e.g., a big number of requests from the same user in a limited period can be considered as a behavioral attack
A security property is composed of 2 parts:
- A Context
- A Final condition (trigger)

The “Context” and “Trigger” of a property are composed of:
- Events
  - Simple events
  - Complex events linked by logical operators (AFTER/BEFORE/AND/OR)
- A simple event is composed of:
  - Attributes (values of packet fields, values of sessions attributes, time of reception, length of message, statistics …)
  - Conditions on attributes (IP @ equal to 1.2.3.4)
Radio Protocol case study

- Provided by Thales: definition of ad-hoc waveform « networking » protocols and algorithms
  - High Data Radio Network Wave Form

- Technical challenges
  - Automatic network: no initial planning
  - Network continuity whatever are the stations in the network
  - “On the move” automatic network reorganization and operation
  - End-to-end heterogeneous user services transmission: voice, messages
  - Decentralized mesh network. No base stations.

19/04/12
Detection of potential attacks

- Link spoofing, Link withholding attack, Data alteration, Flooding attack, Blackhole attack, Denial of service, Replay …
Testing architecture

**SMARTTESTING**
Security test generation model and test purposes specification
Generation of test scenarios denoting attacks using Certify-it

**FSCOM**
TTCN3 test cases specification
Test execution using TT-Workbench

**MONTIMAGE**
Specification of 19 security properties
Online analysis of captured messages and detection of attacks occurrences
Thales Case study
Security rules specification

**Threat:** Deny of service by flooding of RLC_CL_UNIT_DATA_ACK messages

**Security property:** A message RLC_CL_UNIT_DATA_ACK must be preceded with a message RLC_CL_UNIT_DATA_REQ that asked for acknowledgement (R == 00010000) (correlation with the USER_TRANSACTION_ID)

BEFORE

<table>
<thead>
<tr>
<th>RLC_CL_UNIT_DATA_ACK message</th>
<th>RLC_CL_UNIT_DATA_REQ message that asked for acknowledgment</th>
</tr>
</thead>
<tbody>
<tr>
<td>BASE.PROTO == 5152 &amp;&amp; MSG_RLC_CL_UNIT_DATA_ACK.USER_TRANSACTION_ID == MSG_RLC_CL_UNIT_DATA_REQ.USER_TRANSACTION_ID.2</td>
<td>BASE.PROTO == 1056 &amp;&amp; MSG_RLC_CL_UNIT_DATA_REQ.QOS_R == 128</td>
</tr>
</tbody>
</table>
• **Security requirement:** Every node must periodically send a notification message that includes the list of its neighbors on its allocated service slot.

• **Attack scenario 1:** A malicious node sends a message on a non-allocated service slot.

• **Specified security properties:**
  • If one node receives two successive MSG_SPHY_DATA_IND messages from the same source, then these two messages must be separated by 50 slots
  • If one node receives two MSG_SPHY_DATA_IND messages from different sources, then these two messages must have two different slot ids
### Execution Results Report

**Project Name:** Advanced monitoring of ad-hoc network nodes for security checking using the MMT tool

**Project Description:**
Montimage Monitoring Tool (MMT) is a functional and security analysis tool that verifies the network traffic trace of an application or protocol against a set of properties called MMT-Security properties. MMT can be executed against a recorded packet trace file or live on a network interface for real-time analysis. In this demonstrator, MMT was applied to the radio protocol traces of Thales group provided by OMNET simulator.

### Security rules summary results

<table>
<thead>
<tr>
<th>Id</th>
<th>Description</th>
<th>Respected/Detected</th>
<th>Not respected/detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SECURITY RULE: If one node receives two successive MSG_SPHY_DATA_IND messages from the same source, then these two messages must be separated by 50 slots (in the case of slot reallocation, this property is no longer correct)</td>
<td>11</td>
<td>7</td>
</tr>
</tbody>
</table>

### Results Details

<table>
<thead>
<tr>
<th>Pid</th>
<th>Verdict</th>
<th>Property description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Respected</td>
<td>SECURITY_RULE: If one node receives two successive MSG_SPHY_DATA_IND messages from the same source, then these two messages must be separated by 50 slots (in the case of slot reallocation, this property is no longer correct)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EVENT: MSG_SPHY_DATA_IND message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- - - - - timeslot=000257</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- - - - - THALES_META.TIME_SLOT = 257</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- - - - - THALES_META.NODE_ID = 2</td>
</tr>
</tbody>
</table>

**Total for each rule**

**List of events (and data) that lead to the verdict**
Results and conclusion

- A plugin for data extraction from collected messages has been developed for layer 2 protocols and services.
  - Will be extended for Layer 3 protocols and services
- A set of 19 security properties have been specified and checked by Montimage
  - More properties (~50) are in the design phase
- Future work
  - Distributed monitoring is planned
- Supported by DIAMONDS project