The European project CitySCAPE on cyber-security for multi-modal transport systems

Francesca Giampaolo – Engineering
Amedeo D'Arcangelo – Kaspersky
Luca Bianconi – Gruppo Sigla

EuroCyberSec 2021 Workshop – 25-26 October 2021
Project at a Glance

• **Call identifier:** H2020-SU-DS-2019

• **Topic:** SU-DS05-2018-2019 - Digital security, privacy, data protection and accountability in critical sectors

• **EC Funding:** 6 293 011,25 €

• **Duration:** 36 months – 1 Sep 2020 → 31 Aug 2023

• **Consortium:** 15 partners

• **Coordinator:** Institute of Communication and Computer Systems (ICSS), Greece – Dr. Angelos Amditis (a.amditis@iccs.gr)

Learn more: www.cityscape-project.eu

Join us: @EUCityscape CitySCAPE Project

EuroCyberSec 2021 Conference
Genova Use Case - Some details

Focus on 2 transport scenarios:

✓ **Information to passengers** (info-mobility),
✓ Electronic and mobile **ticketing**

considering electronic services (e.g., website or mobile application) provided to the public transport users

For each scenario several micro-use cases are analyzed addressing very specific situations

- **Info-mobility**
  ✓ Waiting time at the stop
  ✓ Service schedule
  ✓ Waiting time of the next train
  ✓ Metro Station info-mobility
  ✓ Notifications to passengers on service update

- **Ticketing**
  ✓ Ticket from the mobile app
  ✓ Validating a mobile ticket
  ✓ Ticketing – City-Pass subscription
  ✓ Validating a City-Pass subscription ticket
  ✓ Ticketing Using Urban Train
Kaspersky Mobile Security SDK and Genova Mobile App

- Threats of the mobile app and the mobile device
- Vulnerabilities of the mobile app and the mobile device

AMT Mobile App Backend Server

CPaaS

AIRBUS Collaborative Threat Investigation Platform (CTIP)

SIEM

CitySCAPE

Financial impact and cost-benefit assessment engine (FIMCA)

Cost-benefit analysis

Kaspersky Mobile Security SDK and Genova Mobile App

- Mobile App
- Kaspersky

Passengers
KMS – SDK for iOS & Android
Integrating security measures in the Genova mobile apps

<table>
<thead>
<tr>
<th>Assessing device</th>
<th>Protecting device</th>
<th>Securing connection</th>
<th>Securing data</th>
<th>Protecting apps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Detection</strong></td>
<td><strong>Device Protection</strong></td>
<td><strong>Web &amp; Network Protection</strong></td>
<td><strong>Data Protection</strong></td>
<td><strong>Self Defense</strong></td>
</tr>
<tr>
<td>✓ Unknown apps detector.*</td>
<td>✓ Wi-Fi Safety Analysis.</td>
<td>✓ Website reputation analysis.</td>
<td>✓ Digital signature verification*.</td>
<td>✓ Debugging</td>
</tr>
<tr>
<td>✓ Malicious apps detector.*</td>
<td>✓ Website reputation analysis.</td>
<td>✓ Website reputation analysis.</td>
<td>✓ Website reputation analysis.</td>
<td>✓ Website reputation analysis.</td>
</tr>
</tbody>
</table>

* Feature available only for Android

EuroCyberSec 2021 Conference
Kaspersky Threat Data Feeds and the CitySCAPE Collaborative Threat Investigation Platform (CTIP)
Kaspersky CyberSafety Manager Games

Target Audience
✓ Onsite edition:
  ✓ AMT administrative area employees.
  ✓ AMT operational area employees.
✓ On-line edition:
  ✓ More than 50 regular passengers (Genoa + Tallinn).
The first step is to **identify critical assets** (*tangible and intangible*) to evaluate and determine the scope of the assessment. This will allow to prioritize which assets to assess. For the evaluation of the intangible assets the system will suggest how to proceed to **define the cost** associated to the asset.

- The **Montecarlo Simulation** will support the **calculation of the medium cost** that will occur in case of an attack that compromise one or more assets.

- We have now determined the **value of the asset** in case of compromission.

Now we have to **calculate how much we could spend to protect it**.

We will refer to the CIS Controls to set up a **list of countermeasure** related to a specific asset and to a specific phase of NIST. The quantitative evaluation of the **return on investment** in safety is calculated by how much loss you have avoided thanks to your investment.

\[
\text{Rosin} = \frac{\text{ALE} - \text{mALE} - \text{Cost of the solution}}{\text{Cost of the solution}}
\]
IDS/IPS component

- The objective is to develop the **IDS/IPS module** that will support cybersecurity experts in the **analysis of all the events and anomalies on the network**, detect any potential incident, evaluate the situation and put in place the **most appropriate (risk-based) reaction**.

The IDS/IPS module will be able to **monitor constantly** the **IT (Information Technology) and OT (Operational Technology) infrastructures**.

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Description</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Passive IDS</td>
<td>The IDS is configured only to monitor constantly the IT (Information Technology) and OT (Operation Technology) infrastructure, all the traffic that goes through the network.</td>
<td>Must have</td>
</tr>
<tr>
<td>2</td>
<td>Active IDS or IPS</td>
<td>The IDS is configured to monitor and stop malicious traffic before it enters the network, as well as to alert the administrator. An active IDS now is commonly known as an Intrusion Prevention System (IPS)</td>
<td>Must have</td>
</tr>
<tr>
<td>3</td>
<td>Real-time detection</td>
<td>The IDS/IPS will notify the administrator when it comes across anything malicious.</td>
<td>Must have</td>
</tr>
<tr>
<td>4</td>
<td>Communication with SIEM</td>
<td>The IDS/IPS communicates with SIEM using the syslog protocol, using the Graylog tool.</td>
<td>Must have</td>
</tr>
<tr>
<td>5</td>
<td>Communication with CpaasS</td>
<td>The IDS/IPS capture the packets from the Cpaas platform. The format of these packets is pcap.</td>
<td>Must have</td>
</tr>
<tr>
<td>6</td>
<td>Multi-threading</td>
<td>The IDS/IPS module will be multi-threading, i.e., the support for the parallelization of the analysis on multiple cores to improve overall performance in network traffic analysis</td>
<td>Must have</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>The CitySCAPE IDS/IPS tool will advance the state of the art by moving from the binary decision (i.e., threat or not) based on the signature of an exploiting known vulnerability to an advanced level of threat detection capabilities.</td>
<td>Must/Should have?</td>
</tr>
</tbody>
</table>
Expectations

✓ Prevent attacks to critical IT infrastructures and assets via an integrated risk assessment

✓ Defend organization against novel cyber attacks by recognize them on time

✓ Improve the cybersecurity awareness of the company employees

✓ Prevent fraud on ticketing by using innovative solutions both on the IT infrastructure and on the mobile phone
<table>
<thead>
<tr>
<th>Name</th>
<th>Project Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Truth Seekers Chain</td>
<td>designs methodology to tackle spread of fake news and tampered contents</td>
</tr>
<tr>
<td>Dogana</td>
<td>framework that delivers &quot;aDvanced sOcial enGineering And vulNerability Assessment“</td>
</tr>
<tr>
<td>COMPACT</td>
<td>effective tools and services for removing security bottlenecks for Public Administrations</td>
</tr>
<tr>
<td>Hermeneut</td>
<td>methodology based on cost-benefit analysis to assess the vulnerability of their tangible and intangible assets</td>
</tr>
<tr>
<td>Cyberspace for Europe</td>
<td>testing and demonstrating potential governance structures for Network of Competence Centres</td>
</tr>
<tr>
<td>PrOTectMe</td>
<td>creates a targeted start-up offering B2B cyber-risk management services to Medium Enterprises</td>
</tr>
<tr>
<td>GEIGER</td>
<td>help SMEs and entrepreneurs to become aware of and reducing risks related to data protection, privacy, and cybersecurity</td>
</tr>
<tr>
<td>TRAPEZE</td>
<td>develop technologies to empower citizens to actively contribute to the cyber resilience of the common European data space</td>
</tr>
</tbody>
</table>
Any questions?

Thank you!

Francesca Giampaolo
Amedeo D’Arcangelo
Luca Bianconi

francesca.giampaolo@eng.it
amedeo.darcangelo@kaspersky.com
luca.bianconi@grupposigla.it

This project has received funding from the EU’s Research and Innovation programme Horizon 2020 under grant agreement No 883321. Content reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.