Project at a Glance

- **Call identifier**: H2020-SU-DS-2019
- **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
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
2 macro-scenarios combining all the micro-use cases

1. All the steps for the transport of a passenger from their home in Genoa to Casella using public transportation

2. Re-plan scenario – during her trip, an event of a “technical problem” disrupts the provided service, so the passenger has to reschedule and re-arrange paths
Use case infrastructure
High-level Architecture
Kaspersky Mobile Security SDK and the AMT Genova Mobile App

Passengers

kaspersky

Mobile App

Vulnerabilities of the mobile app and the mobile device

Threats of the mobile app and the mobile device

CPaaS

AMT Mobile App Backend Server

AIRBUS

SIEM

ENGINEERING

Financial impact and cost-benefit assessment engine (FIMCA)

Cost-benefit analysis

Kaspersky Mobile Security SDK and the AMT Genova Mobile App
KMS – SDK for iOS & Android
Integrating security measures in the AMT mobile apps

Assessing device

<table>
<thead>
<tr>
<th>Risk Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Root detector.</td>
</tr>
<tr>
<td>✓ Insecure settings detector.</td>
</tr>
<tr>
<td>✓ Unknown apps detector.*</td>
</tr>
<tr>
<td>✓ Malicious apps detector.*</td>
</tr>
</tbody>
</table>

Protecting device

<table>
<thead>
<tr>
<th>Device Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ On-Access scanner*.</td>
</tr>
</tbody>
</table>

Securing connection

<table>
<thead>
<tr>
<th>Web &amp; Network Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ DNS spoofing checker.</td>
</tr>
<tr>
<td>✓ Certificate Validation.</td>
</tr>
<tr>
<td>✓ Wi-Fi Safety Analysis.</td>
</tr>
<tr>
<td>✓ Website reputation analysis.</td>
</tr>
</tbody>
</table>

Securing data

<table>
<thead>
<tr>
<th>Data Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Secure Input technology vs Keyloggers.</td>
</tr>
<tr>
<td>✓ Secure storage for sensitive data.</td>
</tr>
</tbody>
</table>

Protecting apps

<table>
<thead>
<tr>
<th>Self Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Protection from 3rd party exploitation*.</td>
</tr>
<tr>
<td>✓ Method implementation replacement detector*.</td>
</tr>
<tr>
<td>✓ Digital signature verification*.</td>
</tr>
<tr>
<td>✓ Debugging detection*.</td>
</tr>
</tbody>
</table>

* Feature available only for Android
Kaspersky Threat Data Feeds and the CitySCAPE Collaborative Threat Investigation Platform (CTIP)
Kaspersky CyberSafety Management Games

Target Audience
- Onsite edition:
  - AMT administrative area employees.
  - AMT operational area employees.
- On-line edition:
  - More than 50 regular passengers (Genoa + Tallinn).
Training for Genova Use Case

Training employees to:

- Prevent success of attackers because one click is all it takes to overcome hardware and software defenses

- Shape an organization into one where employees are part of the defense strategies

- Protect business (brand image and services)
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
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.