CitySCAPE
IDS/IPS engine for CPaaS

Rosella O. Mancilla
Engineering Ingegneria Informatica SpA

Dec. 15, 2021
Agenda

- Engineering Ingegneria Informatica
- Anomaly detection
  - The process
- IDS/IPS engine in CPaaS
  - Deployment scenario
Engineering– Profile

- With around **12,000 professionals in 65 locations** (in Italy, Belgium, Germany, Norway, Republic of Serbia, Spain, Sweden, Switzerland, Argentina, Brazil and the USA), the Engineering Group **designs, develops and manages innovative solutions** for the business areas where digitalization is having the biggest impact, including Digital Finance, Smart Government & E-Health, Augmented City, Digital Industry, Smart Energy & Utilities, Digital Media & Communication.
ENGINEERING implements a highly structured innovation process, in which Research & Development represents a core pillar, both as an internal development force of more than 450 researchers across 5 R&D labs, and through partnerships with highly skilled international partners. This central department of Research & Development has a strong track record in successful participation to European and national projects. With a significant annual investment in R&D of 40 M€, ENGINEERING plays a leading role in research, by coordinating national and international projects (with more than 80 on-going projects) and a network of industrial and research partners and universities throughout Europe.
Engineering- Profile

Rosella O. Mancilla profile:

- Part of the Research & Development Department of ENG since 2014
- Part of Cybersecurity team since 2015, involved into:
  - Proposals writing
  - Design, Development, Deployment and integration of assets in national and EU funded projects (such as DOGANA and COMPACT projects)

ROLE in the Project

- Leader of T5.4: design and develop an intrusion detection system for CITYSCAPE - Intrusion detection systems (IDS) and intrusion prevention systems (IPS) constantly watch your network, identifying possible incidents and logging information about them, stopping the incidents, and reporting them to security administrators. In addition, some networks use IDS/IPS for identifying problems with security policies and deterring individuals from violating security policies. IDS/IPS have become a necessary addition to the security infrastructure of most organizations, precisely because they can stop attackers while they are gathering information about your network

21/12/2021
Anomaly detection

- Identify anomalous traffic from legitimate
- Identify malicious traffic
  - Add rule to alert anomalous traffic
Anomaly detection: idea

- We do not have a labelled dataset from the Pilot to train the ML algorithms (usually classification)
- anomalous traffic = outlier

Datasets
- KDD CUP99
- HCRL
- IoT 23
- Tallin
Anomaly detection: predict

CLUSTERING

Pilot dataset

Train

k

Predict

New traffic

k clusters

Outlier Detection

CLASSIFICATION

Binary dataset

Train Classification

Predict Classification

Classified Dataset
Outlier detection

Assumptions
- Distance based techniques
- No normal distribution
- Multivariate dataset (two or more attributes)
### Classification Accuracy:

<table>
<thead>
<tr>
<th>CLUSTERING + OULIER DETECTION</th>
<th>NORMAL</th>
<th>X</th>
<th>~0</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANORMAL</td>
<td>~0</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NORMAL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ANORMAL</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CLASSIFICATION**
Anomaly detection: implementation

**CLUSTERING**
- Train
- Predict
- k clusters

**Bisecting K-means**
- DBSCAN

**CLASSIFICATION**
- Train
- Predict
- 70%
- 30%

**Decision tree**
- SVM
- Random forest
- MLPC
- LR

**Outlier Detection**
- DBSCAN
- Quartile
- LOF

**Binary dataset**

KDD CUP 99, HCRL, TALLINN
IDS/IPS engine Vs CPaaS and SIEM

• Forward events to the public IDS/IPS engine
• Forward events to the SIEM
• Update Anomaly detection model
Any questions?

Thank you!

Rosella Omana Mancilla
Engineering Ingegneria Informatica SpA

✉️ rosellaomana.mancilla@eng.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.