Secure and Private Smart Grid: The SPEAR Architecture

Panagiotis Radoglou-Grammatikis

University of Western Macedonia

pradoglou@uowm.gr

Under SPEAR Project

Authors

UOWM

Panagiotis Radoglou Grammatikis

Panagiotis Sarigiannidis

TECNALIA

Eider Iturbe

Erkuden Rios

SIDROCO

Antonios Sarigiannidis

CERTH

Odusseas Nikolis

Dimosthenis Ioannidis

8BELLS

Vasileios Machamint

Michalis Tzifas

EUROPEAN DYNAMICS

Alkiviadis Giannakoulias

PPC

Michail Angelopoulos

Anastasios Papadopoulos

SCHNEIDER ELECTRIC

Francisco Ramos

- **Legacy Systems**: SCADA/ICS
- **Smart Technologies**: IoT, AMI
- **Cybersecurity Challenges**: DDoS, privacy breaches, Unauthorised Access, Vulnerable Protocols, APTs
- **Cascading Effects**: Power outage, brownouts, CIs disasters
- **SPEAR Solutions**: Intrusion Detection, Privacy Protection, Cybersecurity Training

SPEAR Layers

3-Layer Architecture

SPEAR SIEM

AlienVault OSSIM

SPEAR SIEM Basis

BDAC

VIDS

GTM,

Message Bus

SPEAR FRF

SPEAR Forensic Repository

AMI Honeypots

Honeypot Manager

SPEAR CHF

SPEAR RI

SPEAR Architecture

3-Layer Architecture

SPEAR SIEM

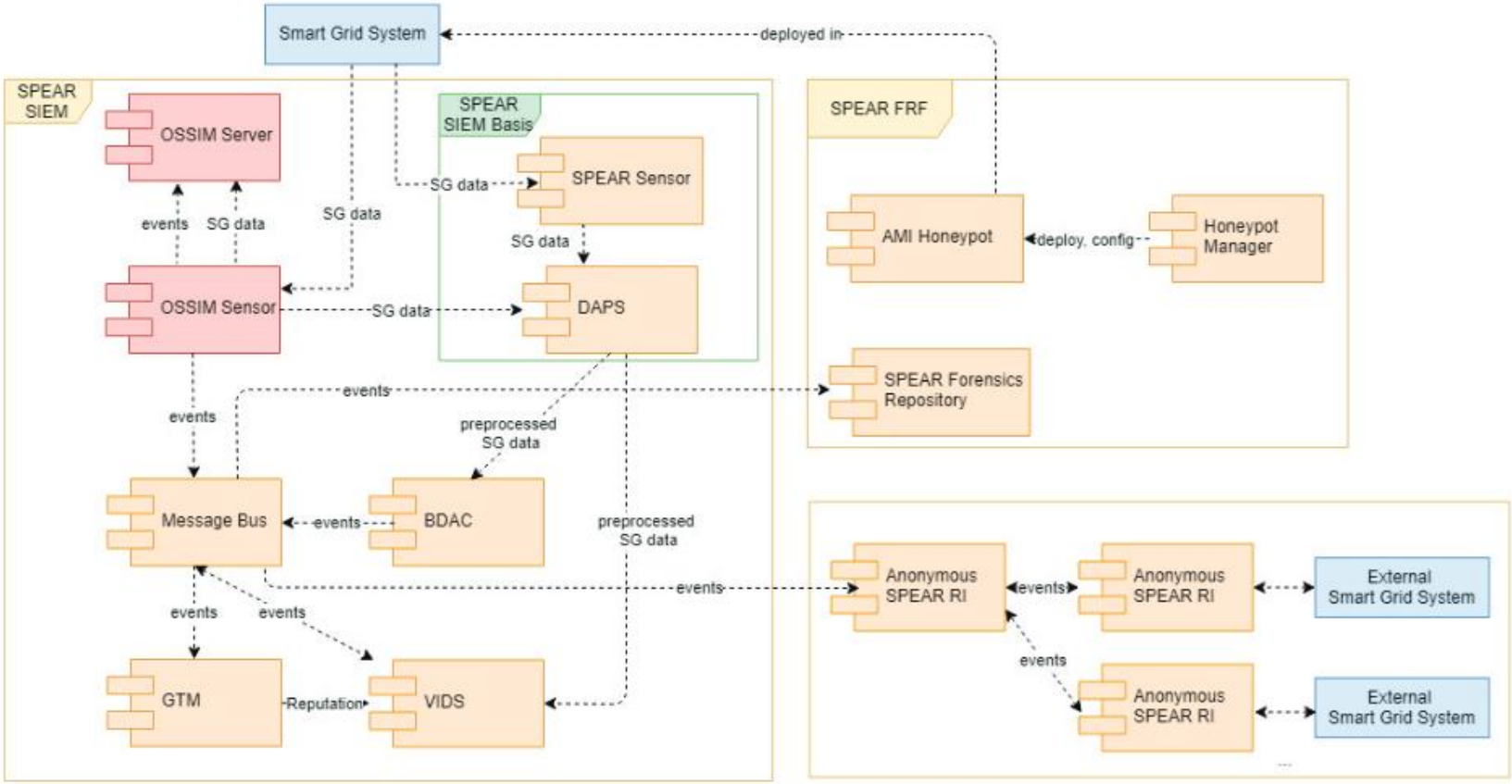
OSSIM Server, OSSIM Sensor, SPEAR Sensor, SPEAR DAPS, BDAC, VIDS, GTM Message Bus

SPEAR FRF

AMI Honeypots, Honeypot Manager, SPEAR Forensic Repository

SPEAR CHF

SPEAR RI



1st Layer: SPEAR SIEM

- ✓ **AlienVault OSSIM**: Signature-based detection; SPEAR complements AlienVault OSSIM with anomaly based detection, visual analytics, reputation/trust calculation mechanisms.
- ✓ **SPEAR SIEM Basis**: SPEAR SIEM Basis feeds the other SPEAR SIEM components with the necessary data for detecting intrusions/anomalies and computing the reputation value of each asset.
- ✓ **Message Bus**: Communication system of SPEAR SIEM.
- ✓ **BDAC**: Anomaly-based detection system using ML/DL techniques.
- ✓ **VIDS**: Main dashboard of SPEAR SIEM; visual analytics for detecting anomalies.
- ✓ **GTM**: Calculates the reputation/trust value of each asset based on the relevant security events.

SPEAR SIEM Basis & Message Bus

First Layer of SPEAR SIEM

SPEAR SIEM Basis – SPEAR Sensor

Responsible for collecting and preprocesses smart grid data and transmit it to DAPS in near real time.

SPEAR SIEM Basis - DAPS

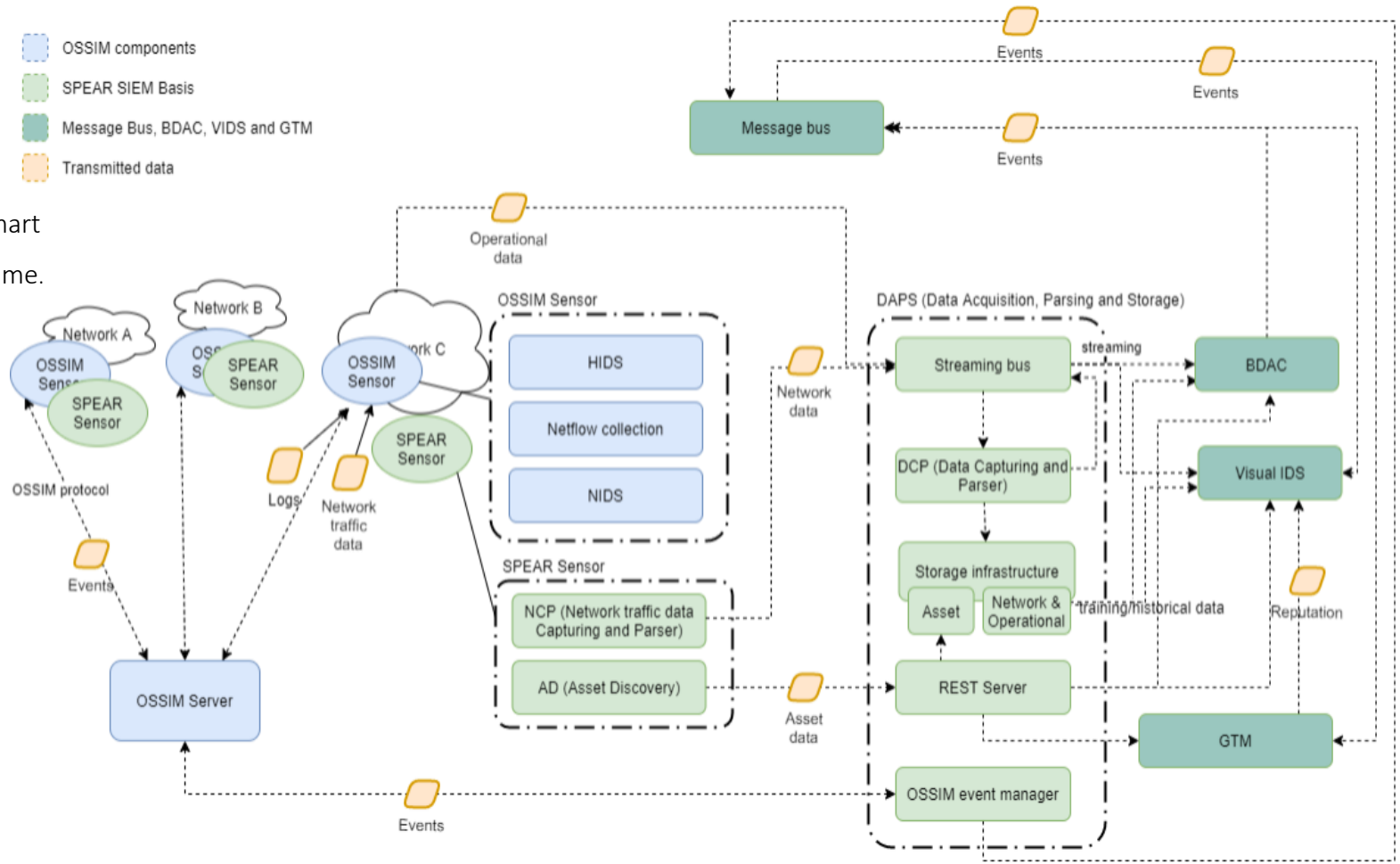
Data streaming, data storage, REST Server, OSSIM Event Manager

Message Bus

A communication system among all SPEAR components that exchange security events

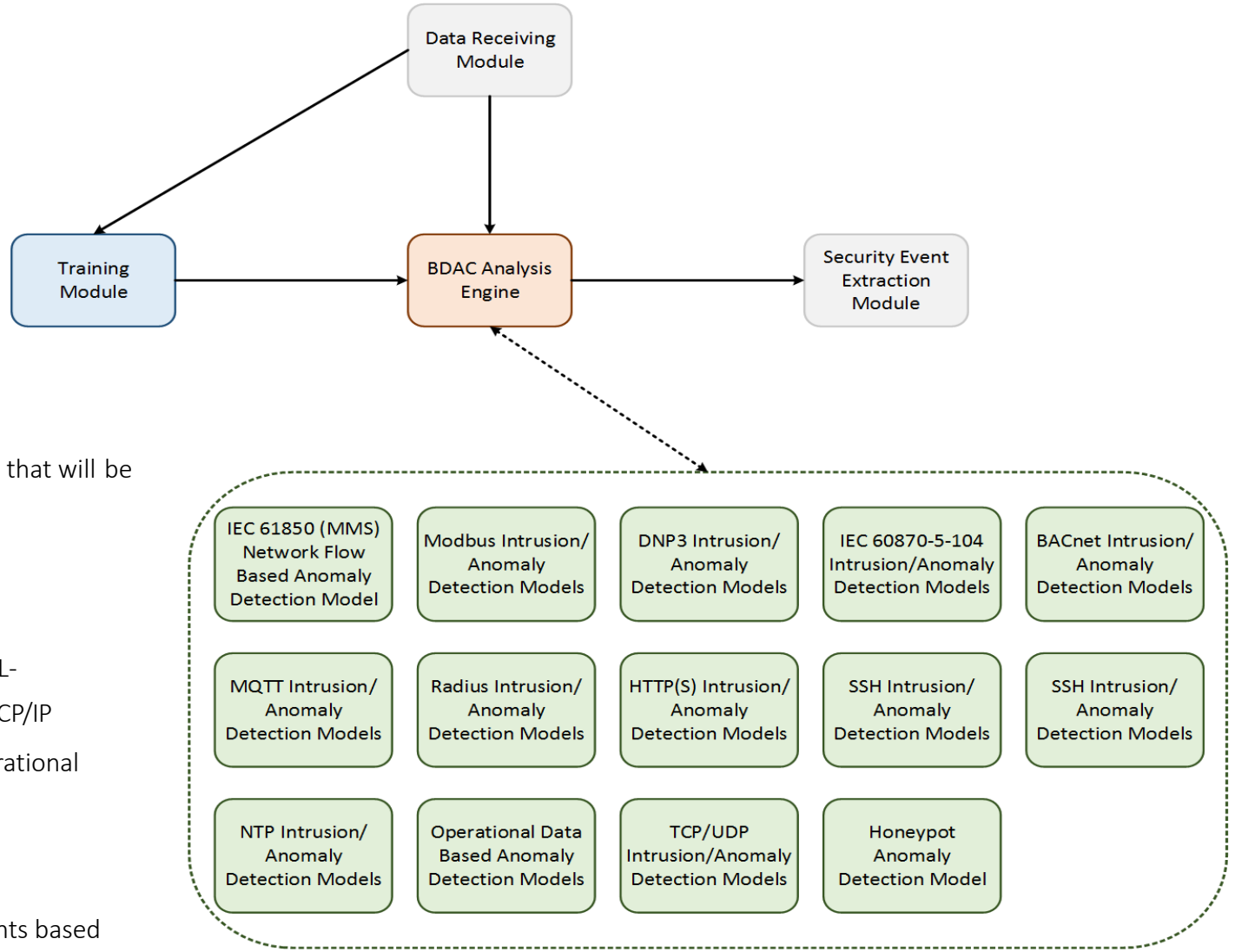
OSSIM Server and Sensor

Existing opensource SIEM; asset discovery; vulnerability assessment; intrusion detection; event correlation; OSSIM has been developed by AlienVault.



BDAC

Second Layer of SPEAR SIEM



Data Receiving Module

Receives from DAPS the preprocessed smart grid data that will be used for the detection processes.

Self-Training Module

Implements the training processes and extracts ML/DL-based models that detect possible attacks based on TCP/IP network flows, Application-Layer protocols data, operational data and honeypot data.

BDAC Analysis Engine

It takes the decisions about the possible security events based on the ML/DL-models extracted by the Training Module.

Security Event Extraction Module

Extracts and pushes the security Events to the Message Bus component

- **Intrusion Detection Models**: They detect specific types of cyberattacks
- **Anomaly Detection Models**: They detect only anomalies, they cannot detect specific type of anomalies

VIDS

Third Layer of SPEAR SIEM

Visual Analytics

Receives from DAPS the preprocessed smart grid data and perform Visual Analytics.

Security Events

Presents all Security Events received by the Message Bus (BDAC, VIDS, SIEM Basis)

Network Assets

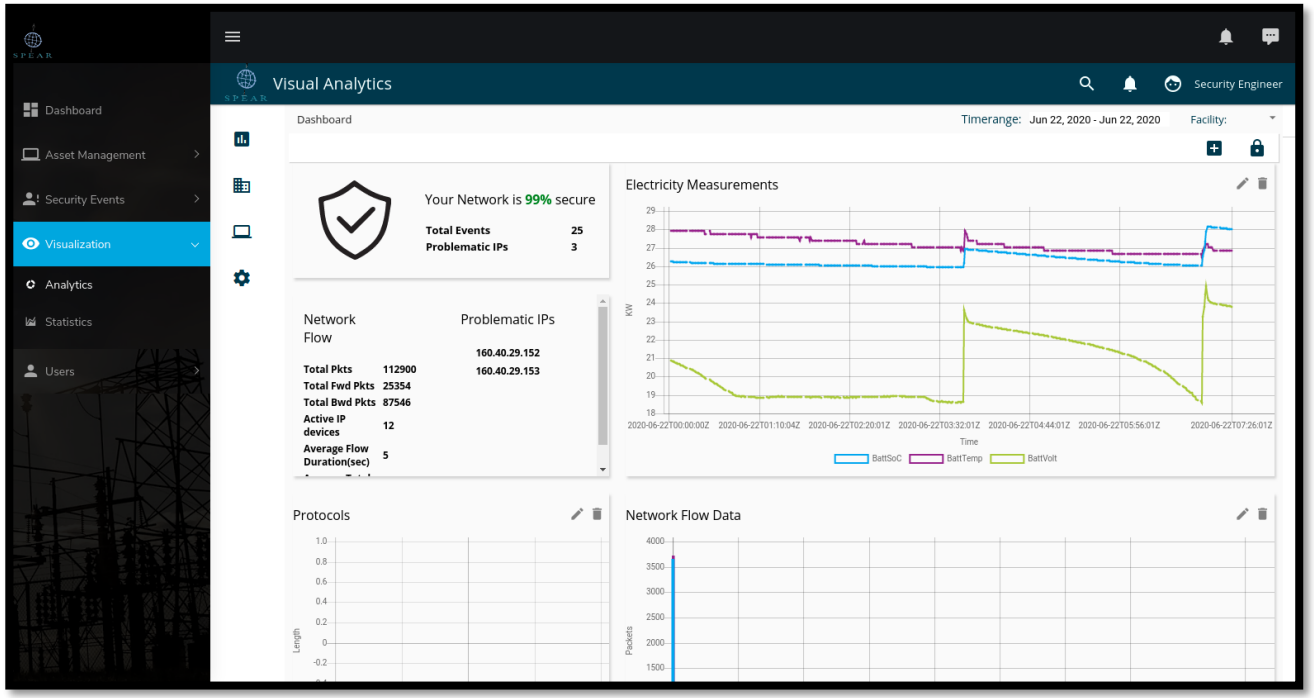
Presents and visualize the network assets and their reputation scores

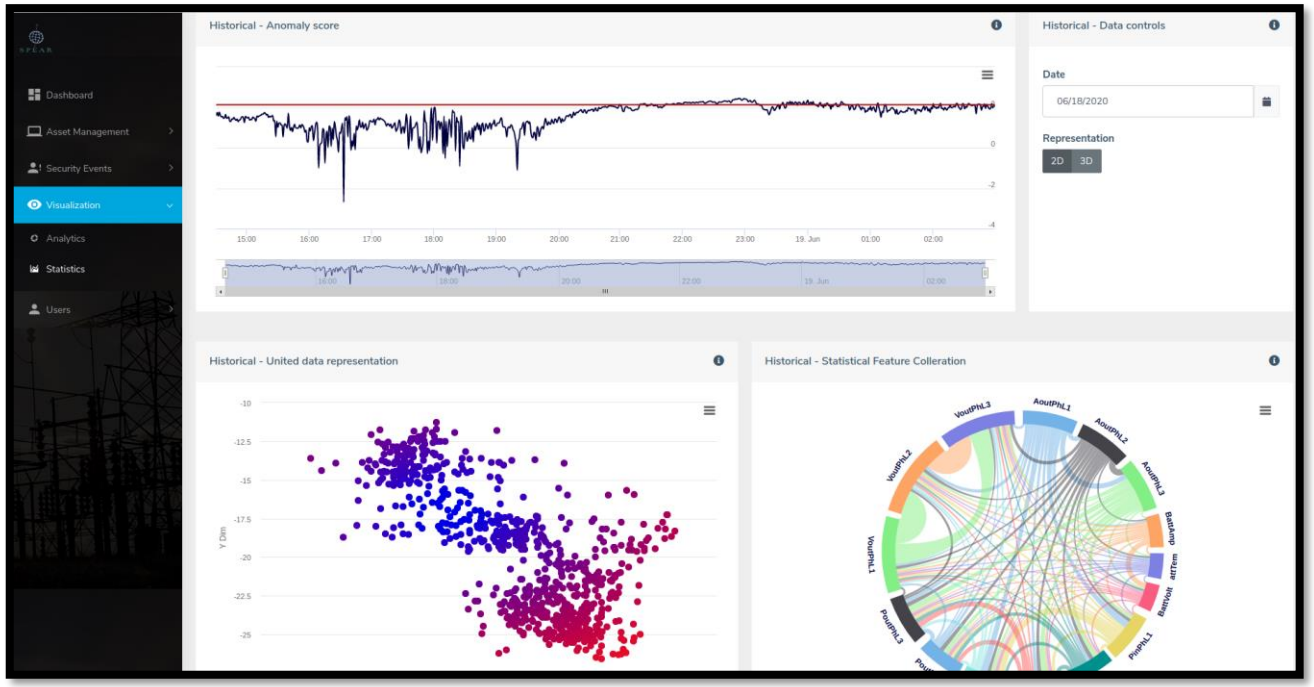
RBAC – Role Based Access Control

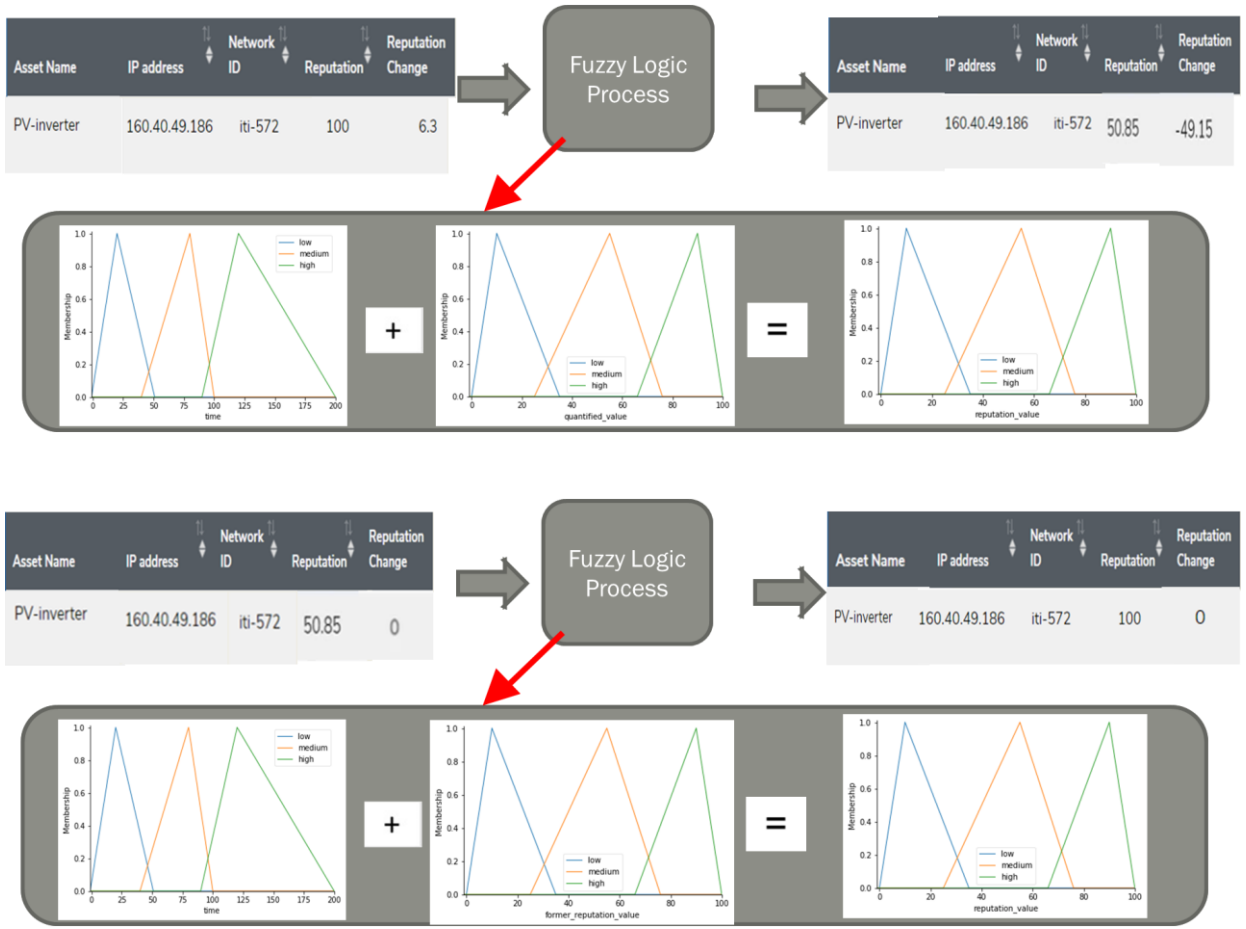
V-IDS support different views for different V-IDS user roles

User Notification

V-IDS notifies the V-IDS users for new Security Events, Network Management Alerts and Daily Report







GTM

Fourth Layer of SPEAR SIEM

Fuzzy Logic Core

Quantifies the incoming anomalous event using Fuzzy Logic and by taking into consideration five different variables: (e.g., asset value, event risk, priority and reliability).

Fuzzy Logic Reputation Reduction System

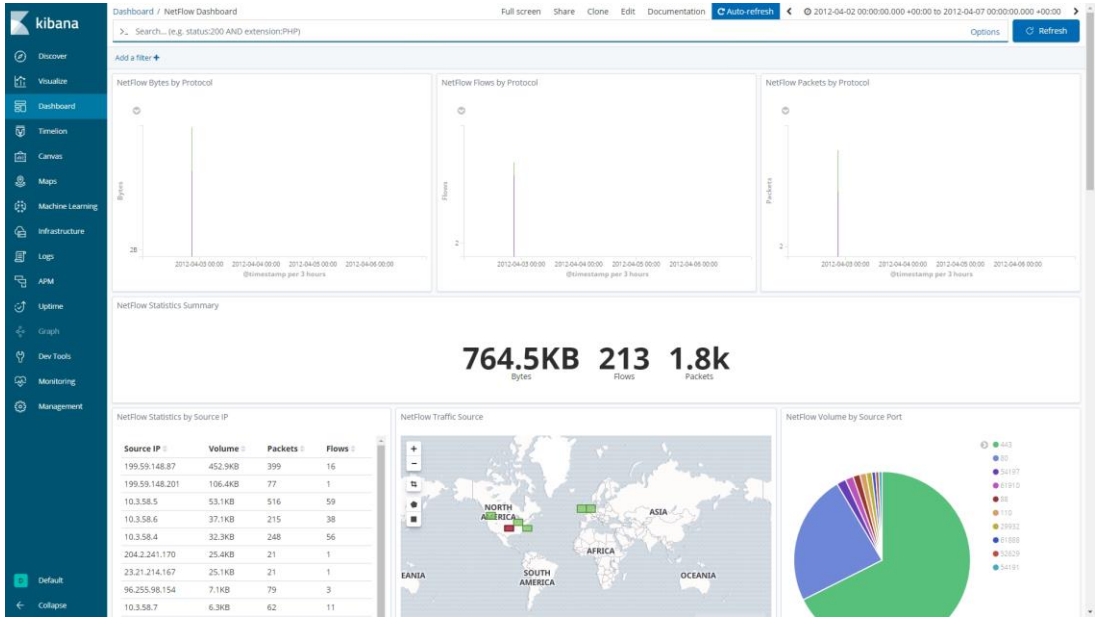
Decreases the reputation value for every asset by taking into consideration the quantified value and the time interval from the previous reputation degradation until the production of the updated reputation value.

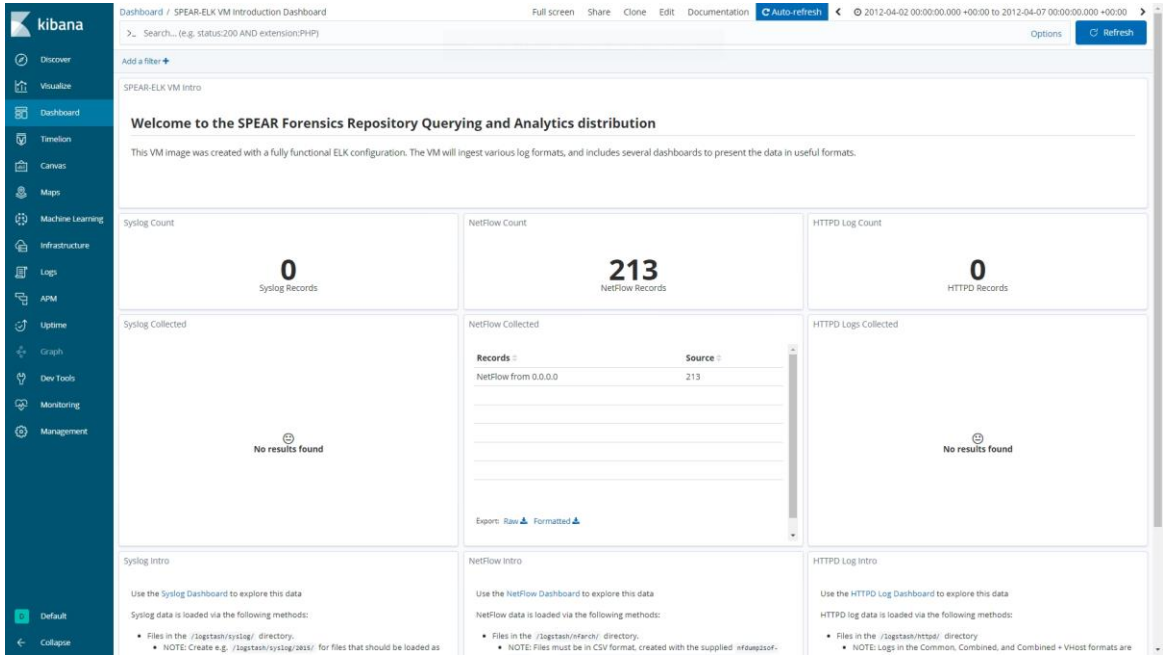
Fuzzy Logic Reputation Update System

Updates the reputation value for every asset by taking into consideration the previous reputation value and the time interval from the previous reputation degradation until the production of the updated reputation value.

2nd Layer: SPEAR FRF

- ✓ **SPEAR FR**: Aggregates the necessary forensic evidence data.
- ✓ **Honeypot Manager**: Calculates and deploy the appropriate number of honeypots based on a game theory-based strategy.
- ✓ **RTU Honeypot**: Master-Client Honeypot supporting multiple honeypots.
- ✓ **NeuralPot**: A DNN Modbus Honeypot.





SPEAR FR

Aggregation of Forensic Evidence Data

Data Sources

Session data, log file, security events

Data Analytics

Elasticsearch, Logstash, Kibana, Beats

Post-Incident Forensics

Built on top of open-source components such as cryptsetup, syslog-ng, softflowd, nfdump and nfsen toolsets.

Honeypot Manager -Game Theory Intelligence (GTI)

Calculation of the Appropriate Number of Honeypots

Input

N_r: Number of real connected devices, **N_max**: Maximum number of connected devices and honeypots that can be deployed in an infrastructure in terms of computing resources, **a**: attacker's weights, **d**: defender's weights

Output

a) Number of honeypots to be deployed, b) Number of real devices to be disconnected

When NA does not exist

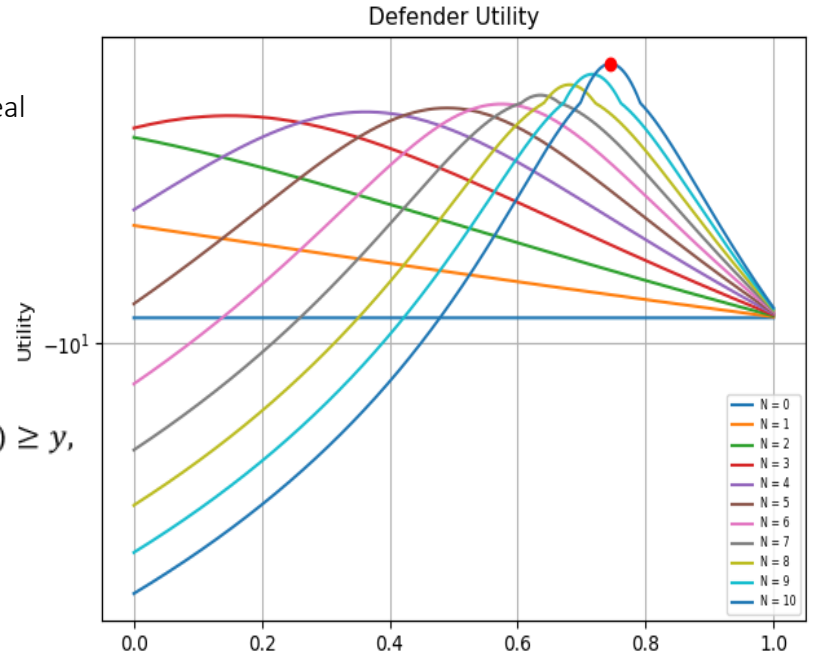
$$\max_{N_1,N_2} \quad y$$

$$\text{s.t.} \quad C_1: N_1 + N_2 \le N_{\max},$$
$$C_2: d_1 N_1 - d_2 N_2 - d_3 (N_2 - N_r)^2 - d_4 (N_1 + N_2) \ge y,$$
$$C_3: -d_3 (N_2 - N_r)^2 - d_4 (N_1 + N_2) \ge y,$$
$$C_4: N_1, N_2 \ge 0.$$

Where: $N_1 = \theta N$

$N_2 = (1-\theta) N$

$$(\theta^*, N^*, \varphi^*) = \begin{cases} (0, \frac{2d_3N_r - d_4}{2d_3}, 0), \text{if } 0 \le \frac{2d_3N_r - d_4}{2d_3} \le N_{\max} \text{ and } a_1 \le a_3 \\ (0,0,0), \text{if } \frac{2d_3N_r - d_4}{2d_3} < 0 \\ \left(\frac{d_1 + d_2 + 2d_3N_{\max} - 2d_3N_r}{2d_3N_{\max}}, N_{\max}, 1\right), \text{if } 0 \le \frac{d_1 + d_2 + 2d_3N_{\max} - 2d_3N_r}{2d_3} \le N_{\max} \\ \text{and } d_1 > d_4 \text{ and } (a_1 + a_2)N_r \ge (a_2 + a_3)N_{\max} + \frac{(a_1 + a_2)(d_1 + d_2)}{2d_3} \\ \left(0, N_r - \frac{d_2 + d_4}{2d_3}, 1\right), \text{if } \frac{d_1 + d_2 + 2d_3N_{\max} - 2d_3N_r}{2d_3} < 0 \text{ and } a_1 > a_3, \\ \nexists, \text{elsewhere} \end{cases}$$



Simulation Parameters:

- Nr = 3, Nmax = 10
  20000 random solutions
- a1 = 0.366, a2 = 0.103, a3 = 0.001
- d1 = 0.1, d2 = 0.744, d3 = 0.941, d4 = 0.04

Results:

N = 10, θ = 0.744

Honeypot Manager - Deployer

Management of Honeypots' lifecycle

Honeypots as Virtual Machines

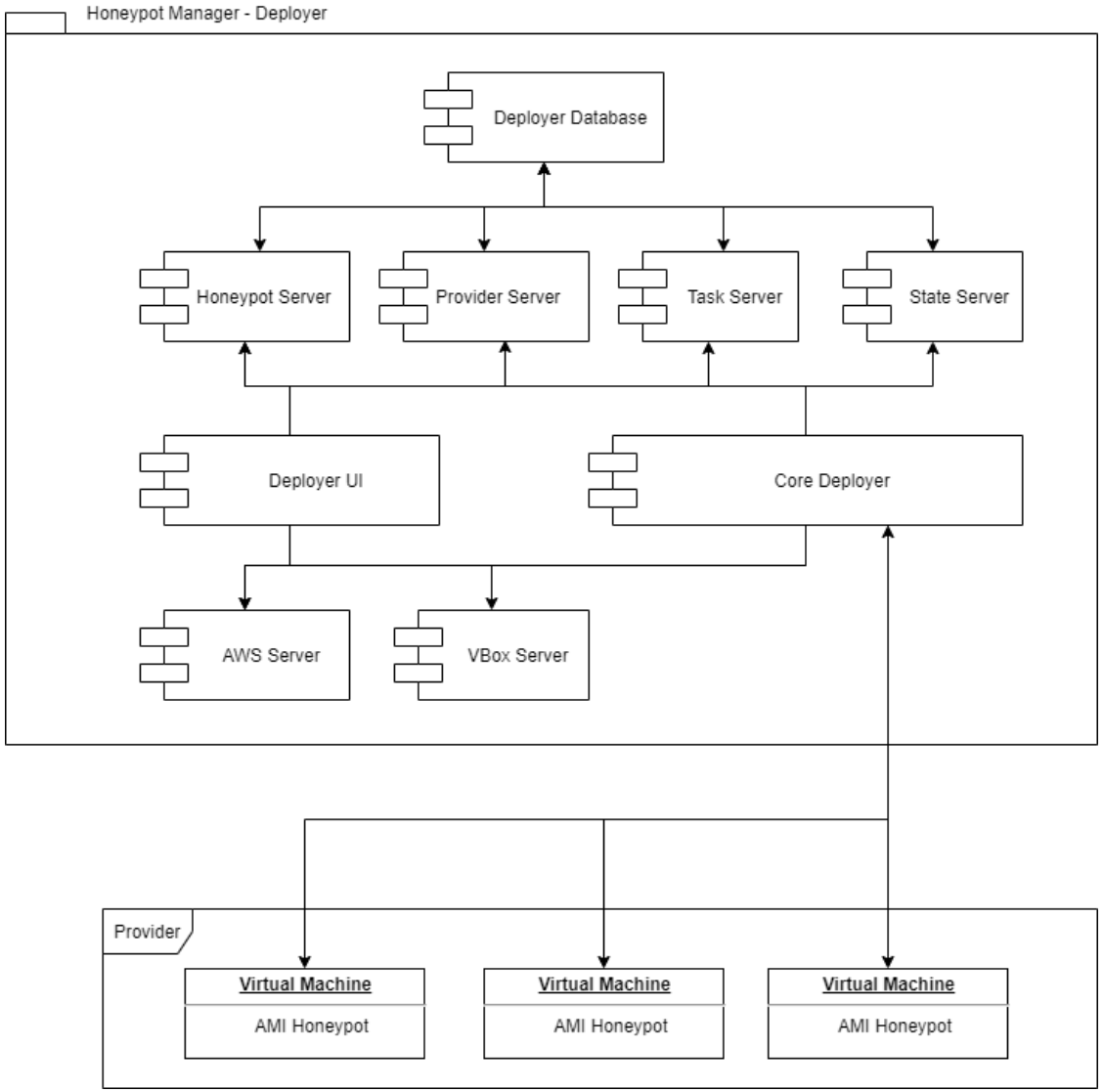
It handles the lifecycle of the virtual machines in which the honeypots will be deployed. (Each AMI honeypot deployed in separate VM).

Honeypot Lifecycle

It handles the lifecycle of the honeypots to be deployed as security mechanism in the smart grid infrastructure.

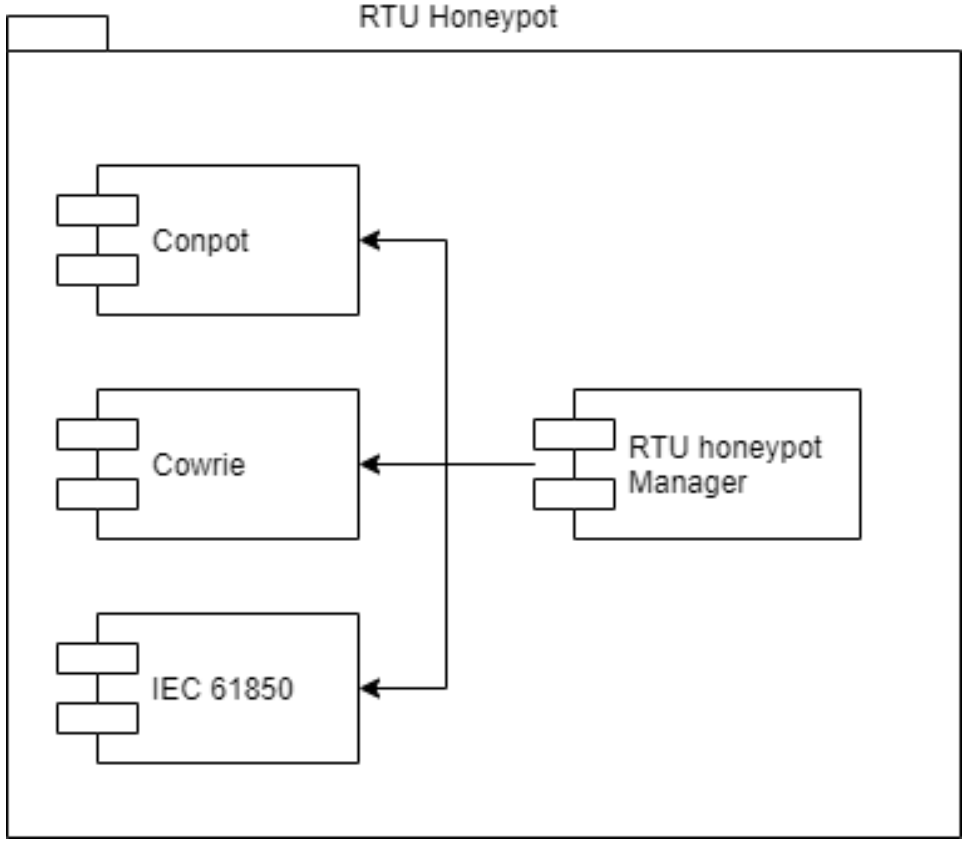
Gateway between SPEAR SIEM and Honeypots

It acts as a gateway between the SPEAR SIEM and the honeypots, by enabling the exchange of log data from the honeypots to the SPEAR SIEM.



RTU Honeypot

Master-Client Honeypot supporting multiple honeypots



Integration of Existing Honeypots

Conpot, Cowrie, IEC 61850 Server

RTU Emulation

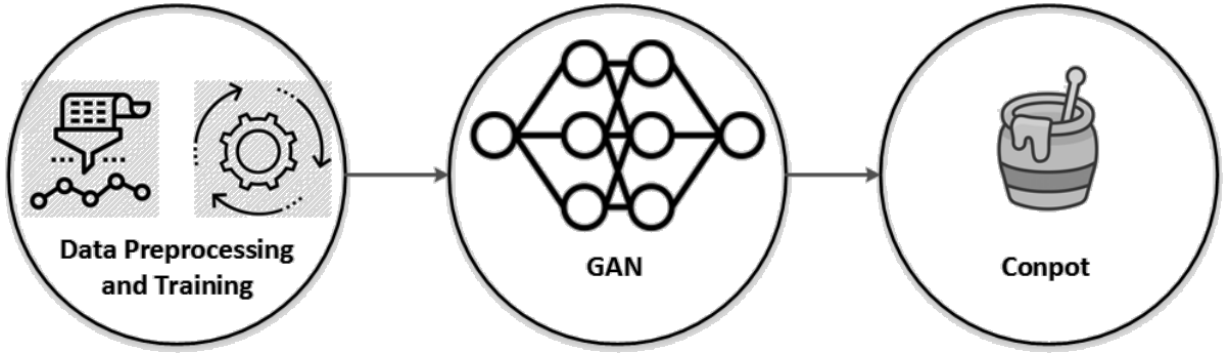
It can operate as master and slave such as a real RTU

Multiple Protocols

Modbus, IEC 61850, IEC 60870-5-104, DNP3

NeuralPot

A DNN Modbus Honeypot



Data Preprocessing

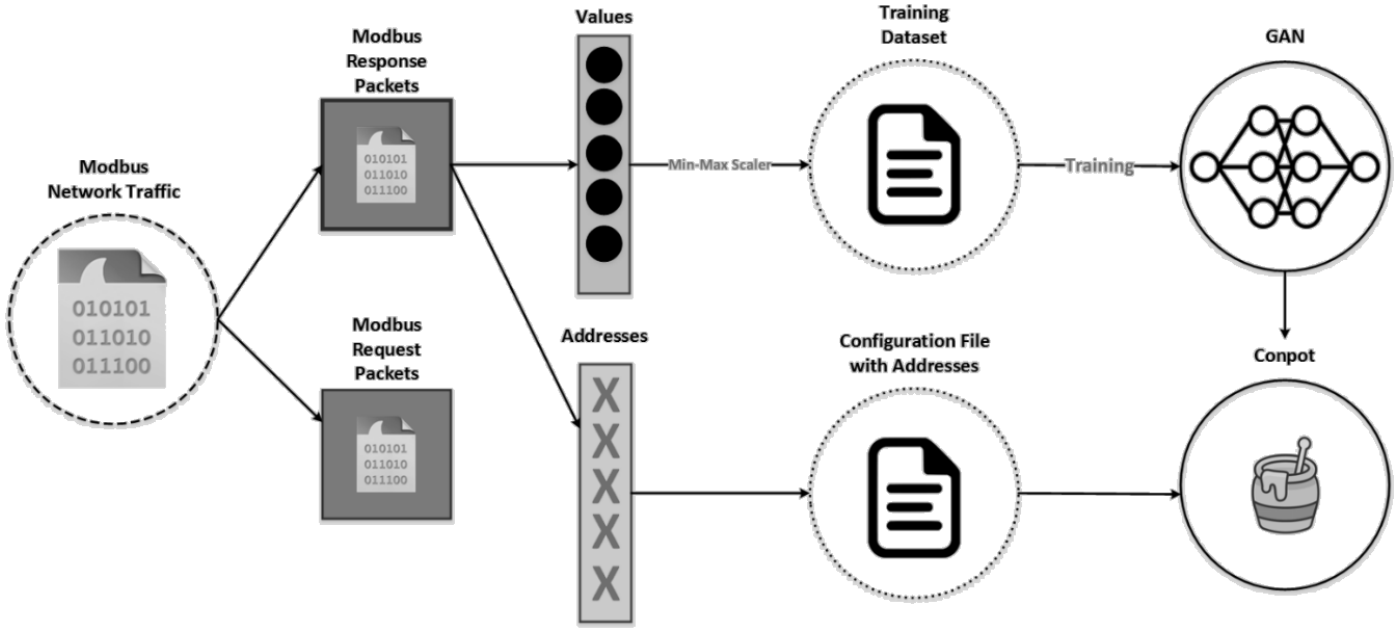
Responsible for analyzing the Modbus/TCP network traffic (PCAP) and training GAN

GAN

Responsible for generating values (Modbus Payload) based on the training process (PCAP).

Conpot

GAN is incorporated into Conpot. The values generated by GAN are enclosed into Modbus packets transmitted by Conpot.



NeuralPot GAN

A DNN Modbus Honeypot

Input Module

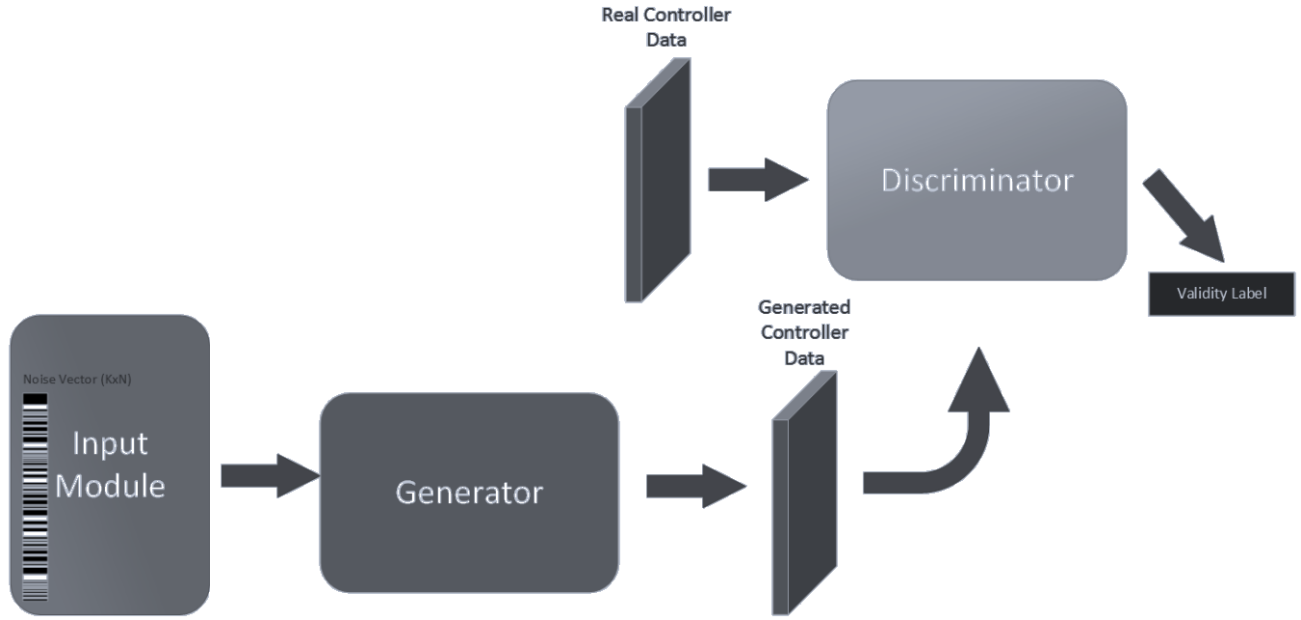
Input noise given to the Generator to produce the emulated data. The random noise is created using the normal distribution with mean μ = 0 and a standard deviation of σ = 1.

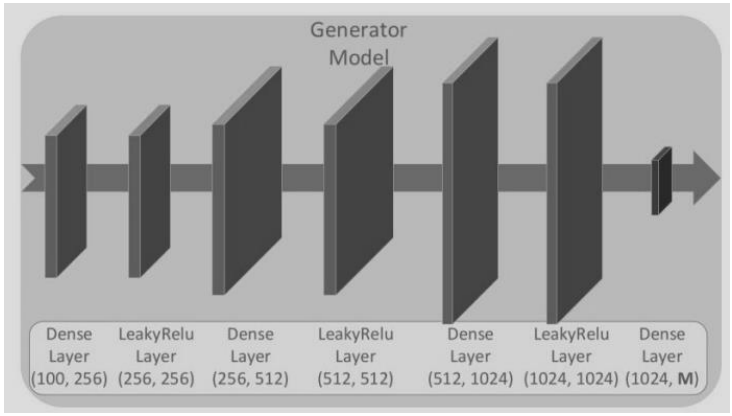
Generator

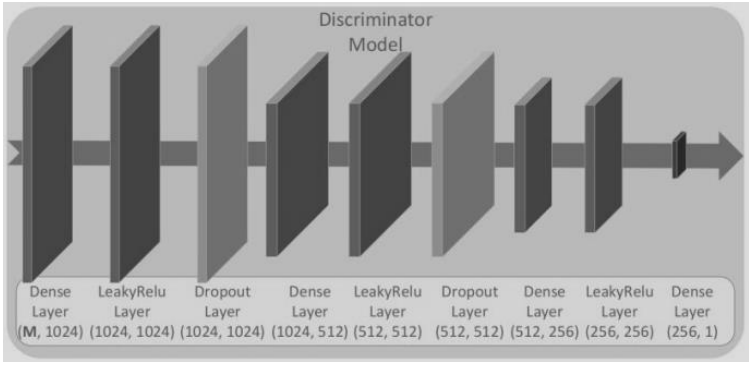
Produce an output that identical to the real data. Seven layers; Binary cross-entropy loss function; Adam Optimizer

Discriminator

Classifying real data, originating from the input dataset and the generated data originating from Generator





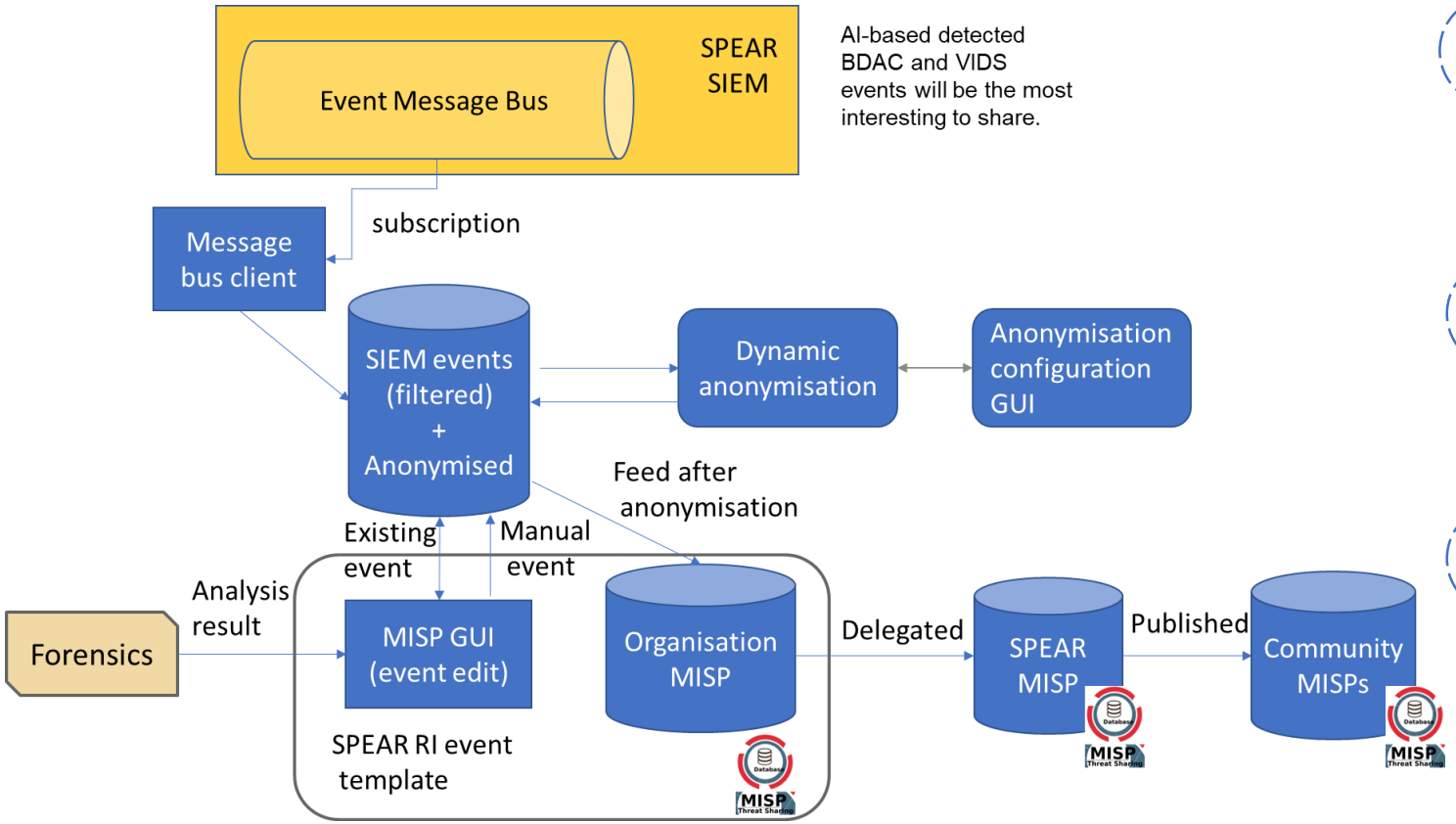


3rd Layer: SPEAR CHF

- ✓ **SPEAR RI**: SPEAR intends to contribute to improving the situational awareness by creating and maintaining a repository of SG incidents. The rationale behind the creation of this repository is to broadcast, inform and exchange critical information about cyberattack incidents in SGs across Europe. The SPEAR Repository of Incidents (SPEAR-RI) will develop the idea of utilising a network of trust where sensitive information is exchanged between institutes. It will form an anonymous repository using group signature and k-anonymity technology in sharing information. SG organisations across Europe will able to broadcast sensitive information in an anonymous way without exposing the reputation of the organisation. The advantages of the SPEAR-RI are the exchange of real-time security data and analysis, the circulation of best countermeasures practices, the comparison of various security solutions both from a technical and operational viewpoint and the ability to establish an open dialogue amongst anonymous peers who represent SG organisations (e.g., power plants) across Europe.

SPEAR RI

Anonymous Repository of Incidents



Use of Delegation feature of MISP Tool: Organisation delegates to SPEAR the publication of incidents. Incidents published only to Community of trust.

Control the iterative disclosure of anonymised events -> Need to define dynamic anonymisation technique (K-anonymity, t-closeness, etc. combination).

Balance privacy/secrecy (victim identity) with security (usefulness of information sharing).

Thank You & Q/A

Contact us

pradoglou@uowm.gr

https://www.spear2020.eu/

https://gr.linkedin.com/in/panagiotisrg

Thank You

Questions ?