Sharing and Automation for Privacy Preserving Attack Neutralization

58th TF-CSIRT Meeting – Paphos, Cyprus
September 17th, 2019
SAPPAN – Sharing and Automation for Privacy Preserving Attack Neutralization

- **H2020 – Call: Dynamic countering of cyber-attacks**
  - **Scope:** Cyber-attacks management – advanced response and recovery

- **Highlights from the Call:**
  - dynamic support of human operators, CSIRTs
  - controlling **response and recovery** actions, including information **visualization**.
  - best **measures** are to withstand and recover from a threat/attack (beyond cyber)
  - utilization of both **structured** (e.g. logs) and **unstructured** data
  - handling (e.g. classification, anomaly detection) of **encrypted** network traffic
  - dynamic, evidence based security and privacy risk **assessment methodologies and management** tools targeting emerging/advanced technologies
SAPPAN Concept

**General Aim:**
- develop a platform for sharing and automation ...
- ... to enable privacy preserving and efficient response and recovery ...
- ... utilizing advanced data analysis and machine learning.

**Key Contributions**
- **privacy-preserving** aggregation and data analytics including advanced client-side abstractions
- **federated threat detection** based on sharing of anonymised data and sharing of trained machine learning models
- **standardisation of knowledge** in the context of incident response and recovery to enable reuse and sharing
- **visual, interactive support** for Security Operation Center operators.
SAPPAN Consortium

- **Coordinator:**
  - Fraunhofer FIT

- **Industrial Partners:**
  - Hewlett Packard Enterprise
  - CESNET
  - DREAMLAB TECHNOLOGIES
  - F-Secure

- **Academia:**
  - RWTH Aachen University
  - Università di Bologna
  - Masaryk University
  - Universität Stuttgart
SAPPAN Concept - Cyber Incident Response and Recovery
SAPPAN Concept

Local Response & Recovery
- Collect
  - Detection
    - Events
- Assessment
  - Incident
- Handling
  - Closed

Cybersecurity Data (Logs, Flows, Forensics data,...)

Sharing
- Raw Data for Detection
- Detection Mechanism
- Threat Detection
- Assessment Approach
- Best Practices
- Handling Model

Global Response & Recovery
- Central Analysis
  - (Global Threat Detection, Attack Propagation, Machine Learning, ...)
- Assessment
  - Best Practices
- Handling
SAPPAN Concept

Local Level

1. Local Response & Recovery
   - Collect
   - Detection
     - Events
   - Assessment
     - Incident
   - Handling
     - Closed

Global Level

1. Sharing
   - Raw Data for Detection
   - Detection Mechanism
     - Threat Detection
   - Assessment Approach
     - Best Practices
     - Handling Model

2. Global Response & Recovery
   - Central Analysis
     - (Global Threat Detection, Attack Propagation, Machine Learning, ...)
   - Assessment
     - Best Practices
     - Handling
WP: Use Cases and Requirements Analysis

- Analysis and specification of response and recovery use-cases
- Privacy requirements
- Presentation requirements
- Functional specification and architecture definition
- Evaluation methodology

WP: Massive Data Acquisition and Local Attack Detection

- Data selection and data processing design
- Fast and scalable processing of cybersecurity data
- Analysis of encrypted and anonymised cybersecurity data
- Development of cybersecurity data abstractions that allow for anonymous data transit
- Visualisation support for the design of attack and anomaly detection models
WP: Managing and Automating Threat Intelligence

- Develop a methodology for formalising and modeling response and recovery actions and their triggers
- Develop approach for capturing and expressing incident response and recovery steps with involvement of human operators
- Develop approach for automatically recommending response and recovery actions to human operators
- Develop approach to automate response and recovery actions without human operators
- Tracking of analytical provenance

WP: Sharing and Federation for Cyber Threat Detection and Response

- Distributed Learning of a global model based on shared anonymized data
- Federated learning of a global model based on shared locally trained models
- Federated learning of a global model without sharing local models
- Sharing response handling information
- Visualisation support for distributed and federated learning of models
WP: Integration, Validation, and Visualization

- Dashboard for response and recovery awareness
- SAPPAN demonstrator
- Validation of response and recovery capabilities
Your comments are welcome

Advisory board member wanted

https://sappan-project.eu

Tomas Jirsik

jirsik@ics.muni.cz

This project has received funding from the European Union’s Horizon 2020 Research and Innovation programme, under the Grant Agreement number 833418.