A Joint Venture of TÜV Austria and TU Wien

Safety and Security in Industry Research Lab „SafeSecLab“

#SafeSecLab

Project 3: Multi-Dimensional Intrusion Detection for Industrial Control Systems

The aim of this work is to detect attack preparations and ongoing attacks as well as their effects on industrial control system (ICS) networks. To this end, anomalies in network traffic will be detected and, with the network-based detection, linked to other data sources (e.g., system information, environmental sensors, context information) to support security experts aligned with operations responsible staff in assessing the situation to ensure continuous safe and secure operations and data integrity/confidentiality. Challenges here are: The new communication patterns in industrial networks, the extraction of suitable features for detection and the quality of the detection methods.

Bernhard Brenner

Education: TU Wien, DTU Copenhagen

Experience: TU Wien, N.E.S. California

Interests:

Neural Network based Classification and Machine Learning, Applied Cryptography, Protocol Security

Plans for the Future:

Publish insights and results gained from ICS traffic analysis and anomaly detection research, develop anomaly based IDS prototype for elastic stack.

From Network Data …

This experiment was conducted at the TU Wien pilot factory. We simulated a botnet in a factory cell that launches an orchestrated attack against the controller of the turning machine. The communication between the infected hosts and the C&C is hidden within HTTP and HTTPS traffic, and the C&C is split into several hosts to hide this communication even more. Another objective of the Botnet was to covertly exfiltrate information to outside of the factory. For this purpose, exfiltrated data was split into small chunks that were sent covertly as HTTPS post requests to an attacker-controlled storage.

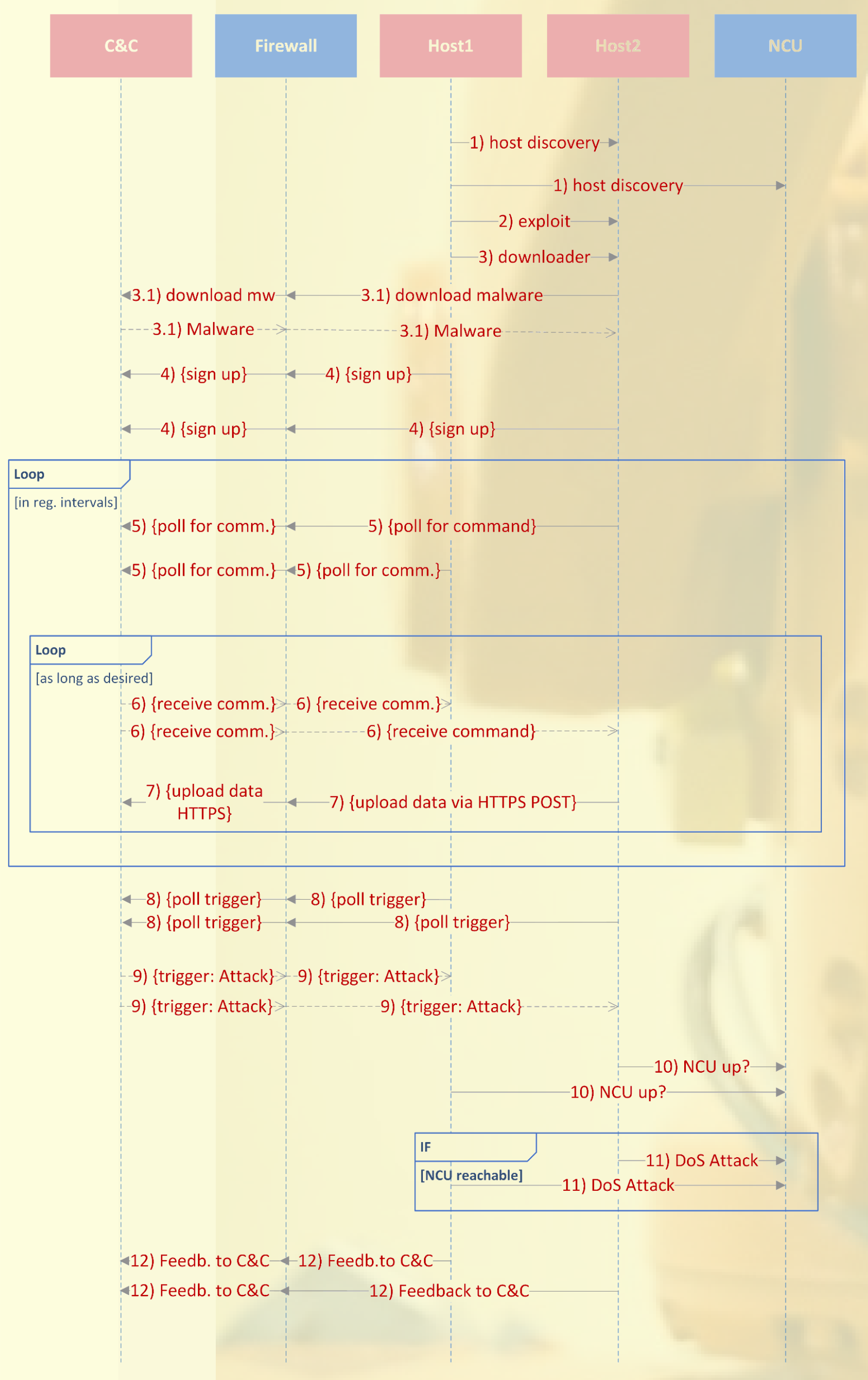

Fig. 1: Botnet attack simulation at TU pilot factory

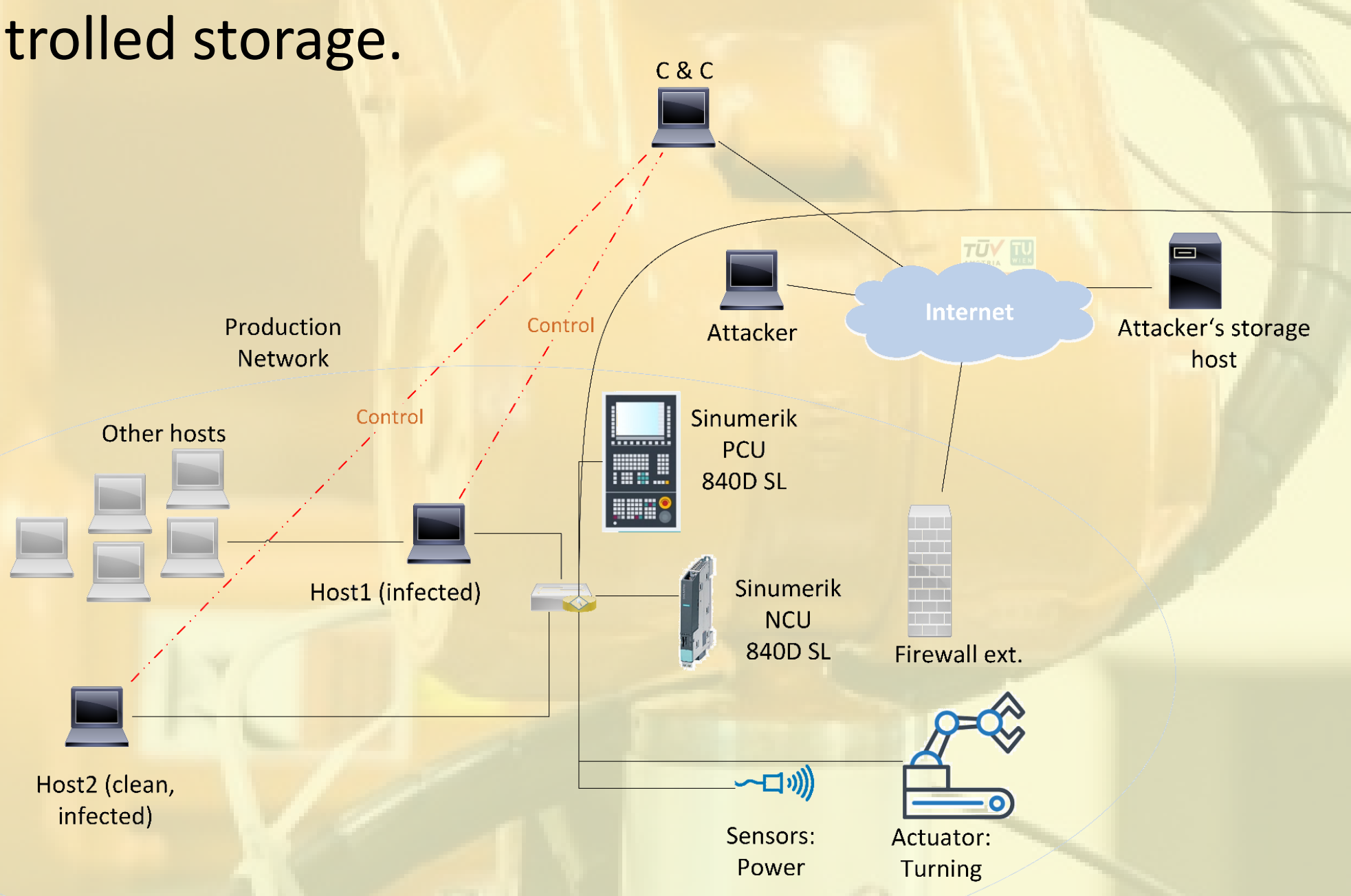

Fig. 2: From raw network traffic to machine learning based traffic/attack classification

… to IDS Model

With this and other (smaller) experiments, together with our large collection of benign traffic, we now have several terabytes of network data examples. Meanwhile, we found candidates for machine learning based traffic classifiers and implemented a working Prototype after the scheme shown in Fig. 3.

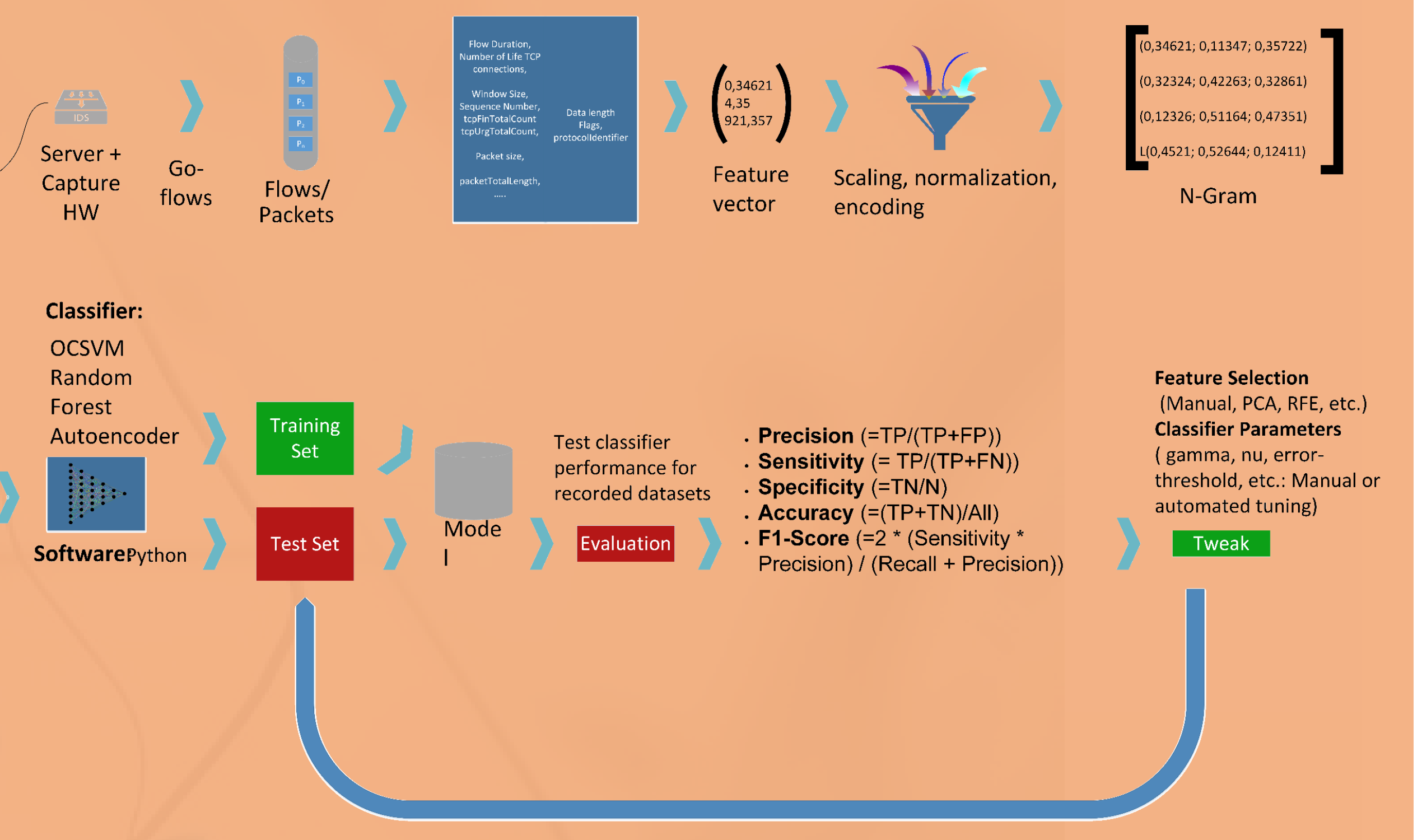

Fig. 3: Stepwise Data collection to classifier Training. Loop

Picture by Michal Jarmoluk

Machine Learning Module

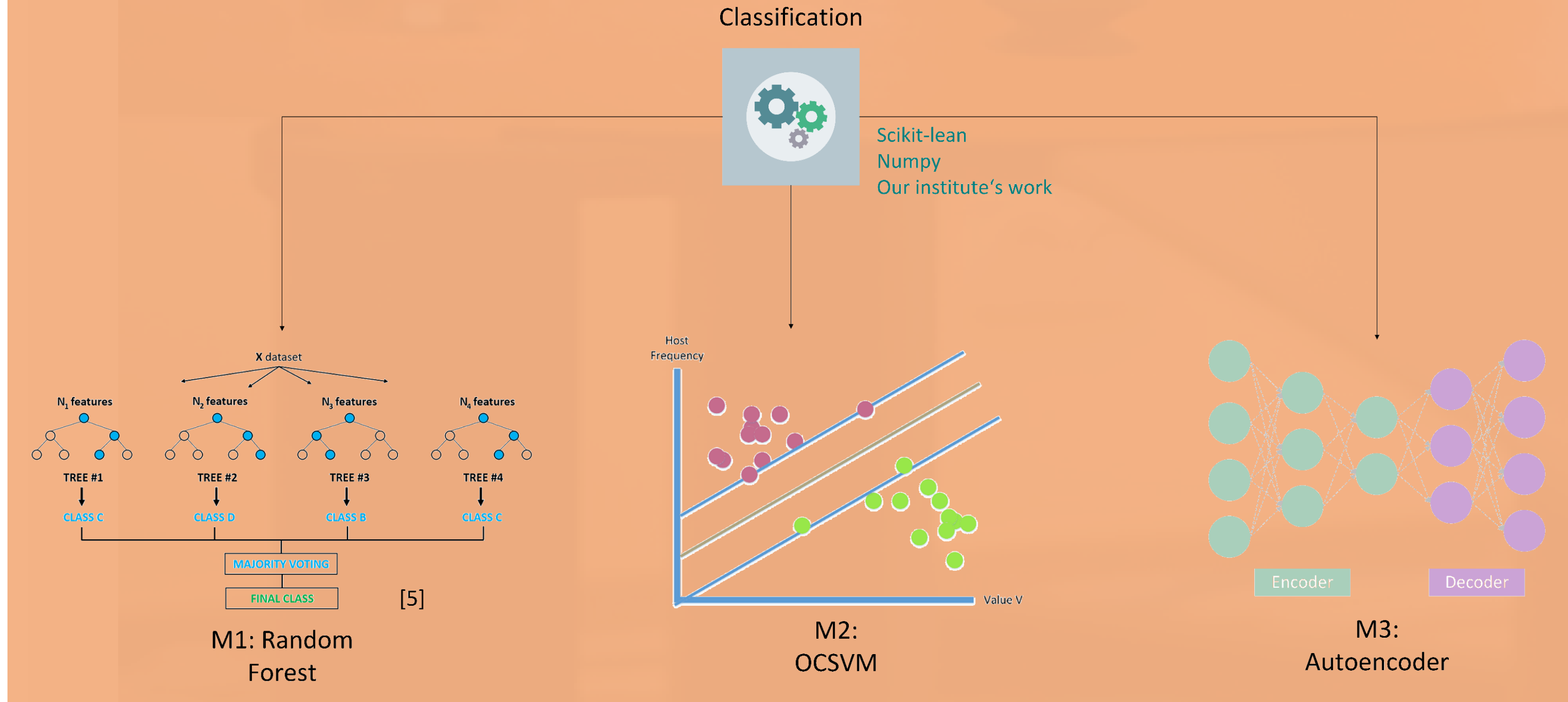

Fig. 4: Three different classification approaches are used in the S²IEM Prototype.

After extensive literature review and counseling, we decided for three approaches: Random forests, One-Class support vector machines (OCSVM) and Autoencoders, the latter two being unsupervised approaches.

[5] Medium, "Random Forest Classification", URL: https://medium.com/@ar.ingenious/applying-random-forest-classification-machine-learning-algorithm-from-scratch-with-real-24ff198a1c57 (Last access: 2021-03-22)

State of the Art

The current state of the art research provides evidence for the potential of anomaly-based intrusion detection in industrial networks. ICSs typically consist of a set-up that is well definable, with infrequent changes [1, 2], while the typically low data rates of ICS networks enable more complex data processing despite real-time constraints [3, 4].

Upcoming Steps:

Prototype

We currently test and optimize the performance of our prototype for our use cases and decide for (hyper)parameters. We then use these ML-based approaches in combination with existing technologies (signature-based intrusion detection).

Publications

Review paper about network anomaly detection in OT networks

Supervisor: Tanja Zseby (TU Wien)

Contact person: Thomas Doms (TÜV)

Project Cooperations: P1, P2, P4, P5, P7

[1] M. Mantere, I. Uusitalo, M. Sailio, and S. Noponen. Challenges of machine learning based monitoring for industrial control system networks. In 2012 26th International Conference on Advanced Information Networking and Applications Workshops, pages 968-972. IEEE, 2012.

[2] R. Sommer and V. Paxson. Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE symposium on security and privacy, pages 305-316. IEEE, 2010.

[3] R. R. Barbosa, R. Sadre, and A. Pras. Diculties in modeling scada trac: a comparative analysis. In International Conference on Passive and Active Network Measurement, pages 126-135. Springer, 2012.

[4] F. Schuster, A. Paul, and H. König. Towards learning normality for anomaly detection in industrial control networks. In IFIP International Conference on Autonomous Infrastructure, Management and Security, pages 61-72. Springer, 2013.