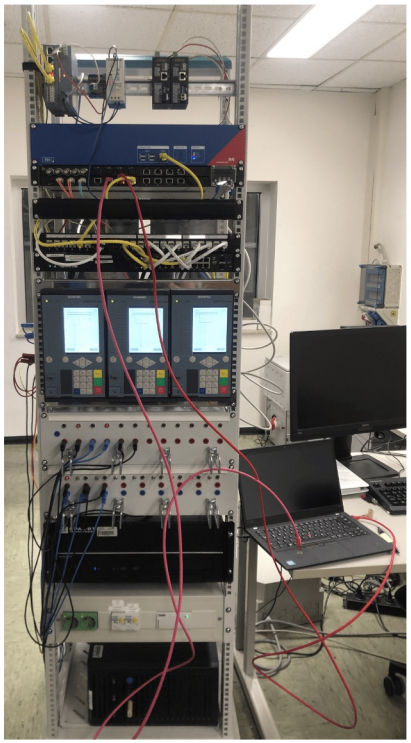
PowerDuck: A GOOSE Data Set of Cyberattacks in Substations

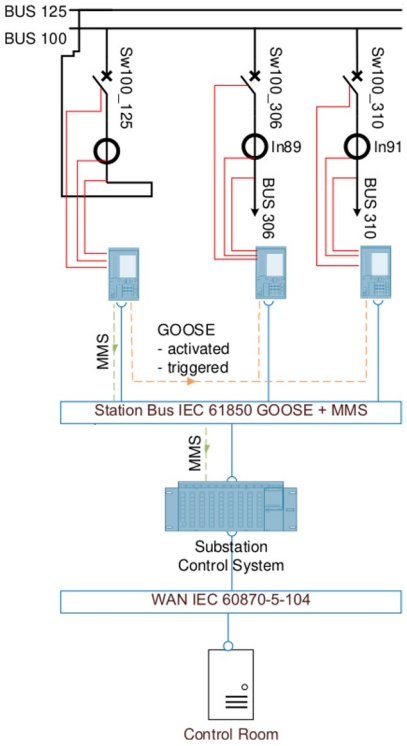
Sven Zemanek Fraunhofer FKIE	Immanuel Hacker RWTH Aachen University Fraunhofer FIT	Konrad Wolsing Fraunhofer FKIE RWTH Aachen University
Eric Wagner Fraunhofer FKIE RWTH Aachen University	Martin Henze RWTH Aachen University Fraunhofer FKIE	Martin Serror Fraunhofer FKIE

Fraunhofer FKIE Fraunhofer FIT RWTH AACHEN UNIVERSITY

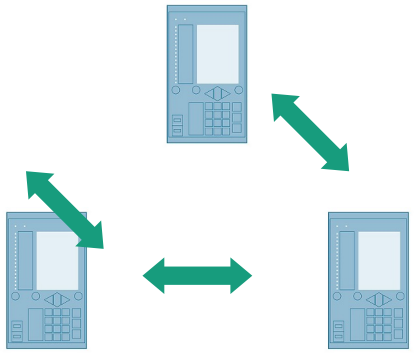
Cyber Security Research in Critical Infrastructures

Substation Testbed





- voltage measurement
- switch open/closed



Our Contribution:

The PowerDuck Data Set

4x Regular Traffic

3x Replay Attacks

6x Insertion Attacks

5x Suppression Attacks

2x Flooding Attacks

No.	ID
1	normal-1
2	normal-2
3	normal-3
4	normal-4
1	replay-opening-switch-isc
2	replay-opening-switch-w-
3	replay-old-measurements
4	insert-fake-open-w-intern
5	insert-fake-open-only-enc
6	insert-distort-meas-up-gr
7	insert-distort-meas-down-
8	insert-distort-meas-up-sh
9	insert-distort-meas-down-
10	sup-1-1-tbv0
11	sup-1-1-tbv1
12	sup-1-1-tbv2
13	sup-2
14	sup-1
15	flood-repeat
16	flood-bloat-repeat

Table 1: Description of the retrieval of the correspon

- PCAP files of GOOSE traffic!
- Attack packet IDs!
- IPAL transcriptions!

IPAL: Breaking up Silos of Protocol-dependent and Domain-specific Industrial Intrusion Detection Systems

Konrad Wolsing
Fraunhofer FKIE
RWTH Aachen University
konrad.wolsing@fkie.fraunhofer.de

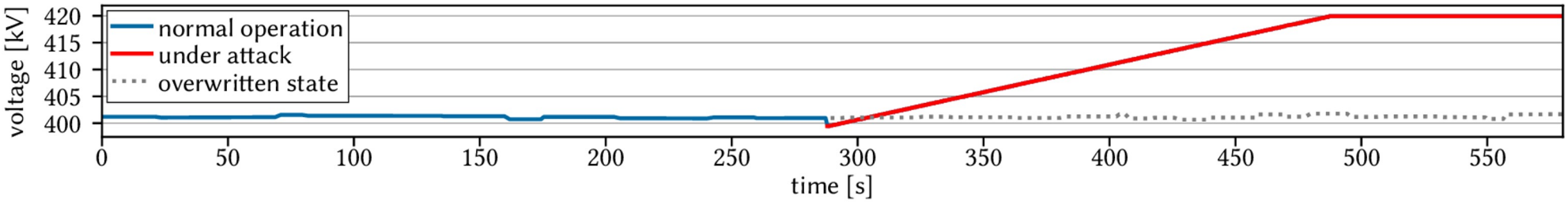
Eric Wagner
Fraunhofer FKIE
RWTH Aachen University
eric.wagner@fkie.fraunhofer.de

Antoine Saillard
RWTH Aachen University
Fraunhofer FKIE
antoine.saillard@rwth-aachen.de

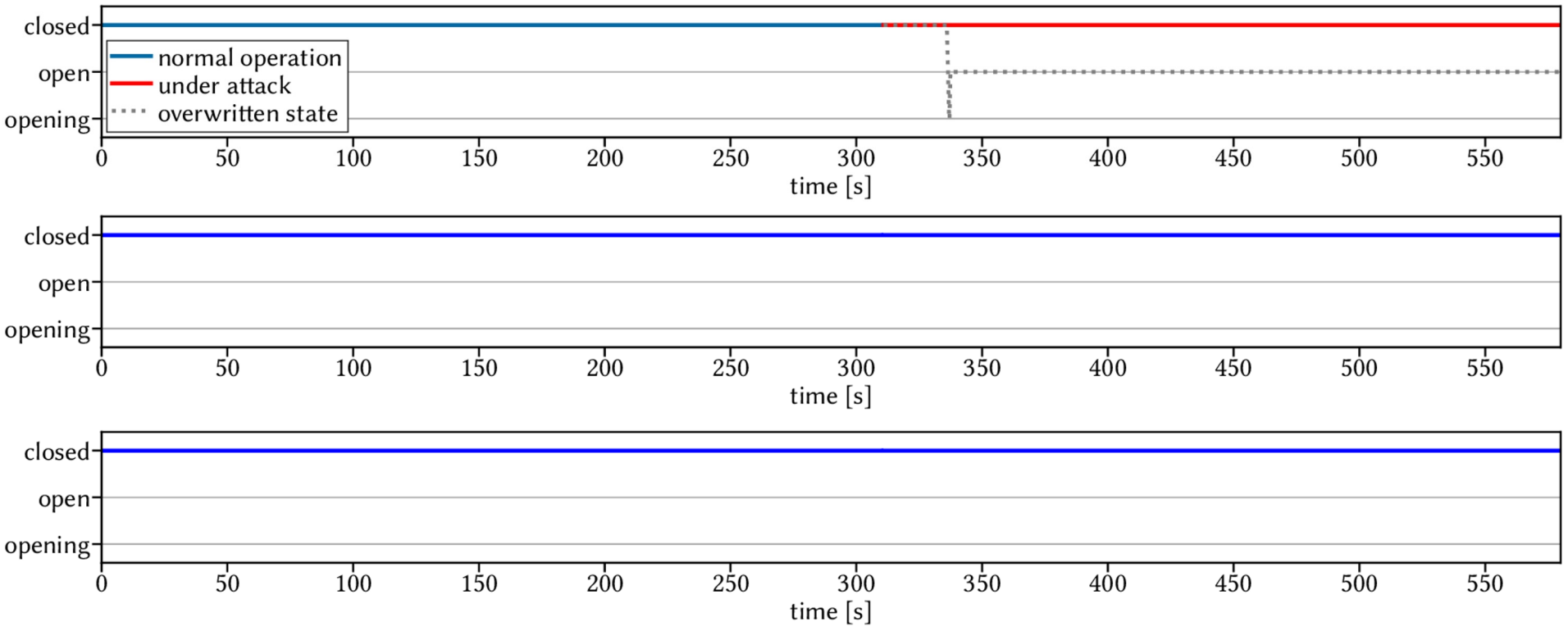
Martin Henze
RWTH Aachen University
Fraunhofer FKIE
henze@cs.rwth-aachen.de

Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2022

6-insert-distort-meas-up-grad



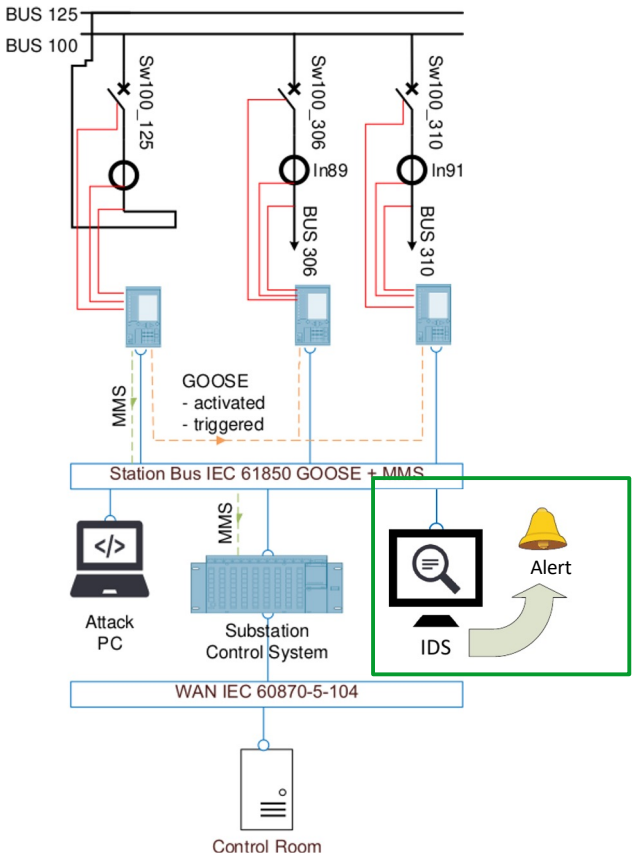
10-sup-1-1-tbv0



Outlook

- It’s GOOSE traffic from real devices
- with and without attacks

get the
Data Set



https://doi.org/10.5281/zenodo.6724225