THREAT ANALYSIS OF STEGANOGRAPHIC AND COVERT COMMUNICATION IN NUCLEAR I&C SYSTEMS

M. Hildebrandt[1], R. Altschaffel[1], K. Lamshöft[1], M. Lange[2], M.Szemkus[2], T. Neubert[3], C.Vielhauer[1,3], Y. Ding[2], J. Dittmann[1]

[1] Otto-von-Guericke University, Magdeburg, Germany

[2] Magdeburg-Stendal University of Applied Sciences, Magdeburg, Germany

[3] Brandenburg University of Applied Sciences, Brandenburg, Germany

The work in this paper has been funded by the German Federal Ministry for Economic Affairs and Energy (BMWi, Stealth-Szenarien, Grant No. 1501589A, 1501589B and 1501589C) within the scope of the German Reactor-Safety-Research-Program.

This document was produced in part with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

Outline

- Movitvation/Introduction
- State-of-the-Art
  - OT Infrastructure: NST047, IEC 62443
  - Steganography and Data Hiding
- Hidden Communication in Networks
  - Hidden communication in IT networks
  - Potential hidden communication in OT networks
- Exemplary supply chain attacks
- Strategic preparation and detection approaches
- Summary and future work

Motivation/Introduction

- Operational Technology (OT) / Instrumentation and Control Systems (I&C) consist of Sensors, Computing Units and Actors – including the communication between those components
- Increasing tendency of using hidden communication channels in Information Technology (IT) networks within advanced persistent threats (APT)
- Information Hiding can be used to exfiltrate information/commands, inject information/commands or to establish a command&control channel without being detected
- Typical protocols in OT networks, (Modbus/TCP, OPC UA, Syslog, …) can be potentially used as cover data for hidden communication

State-of-the-Art

Architecture

- NST047 [3]:
  - 5 Security Levels, SL1 systems vital to the facility (e.g. safety&emergency systems), SL2 operational control systems, SL3 supervision systems, SL4 technical data mangement systems, SL5 business systems
  - Traffic between security levels is restricted (e.g. no communication from SL2 to SL1, but communication from SL1 to SL2, Acknowledgements and control packates can be sent from SL3 to SL2, well-specified communication is allowed from SL4 to SL3)
- IEC62443 [2]:
  - Definition of foundational requirements, e.g. restricted data flow; System Requirements and Requirement Enhancements
  - 5 Security levels (SL0 no security, SL4, highest security requirements)

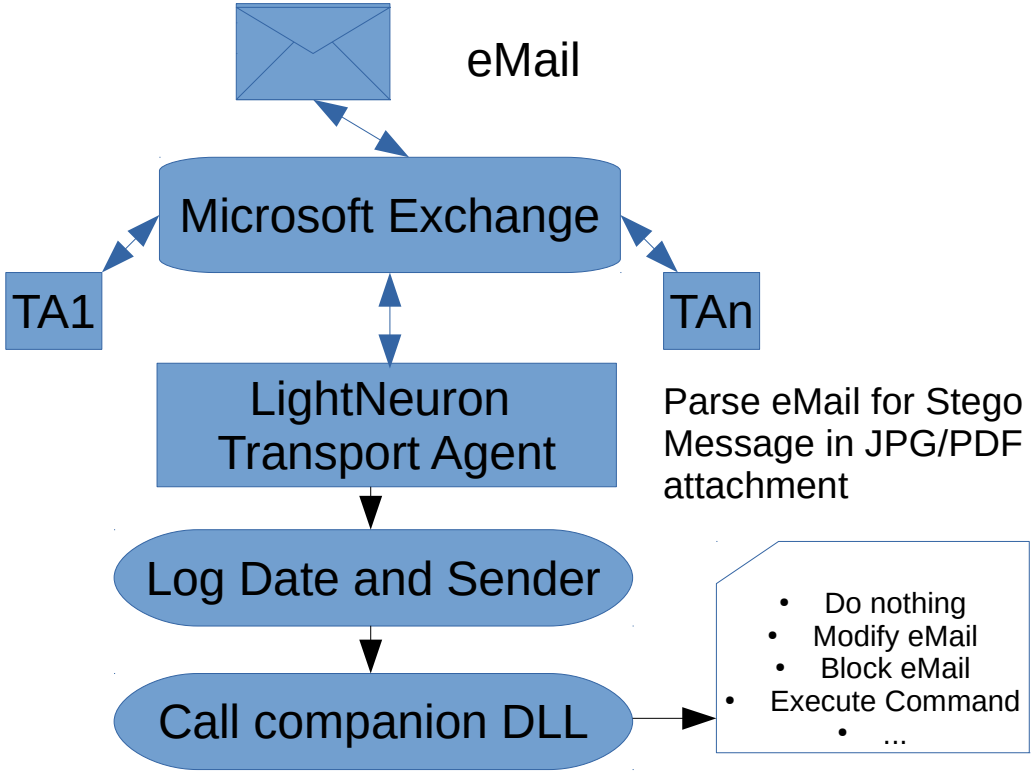
Information Hiding

- Derived from secret communication - Prisoners' Problem with the presence of a warden → communication should remain unnoticed and confidential
- IH is increasingly used in APT
- Cover channel/objects: data to hide stego data within
- Stego data: hidden communication
- Requirements: protocol compliance, warden compliance, ideally should follow Kerckhoffs' Principle [8]
- Active steganography: end-to-end; passive steganography: in some parts of the communication path only

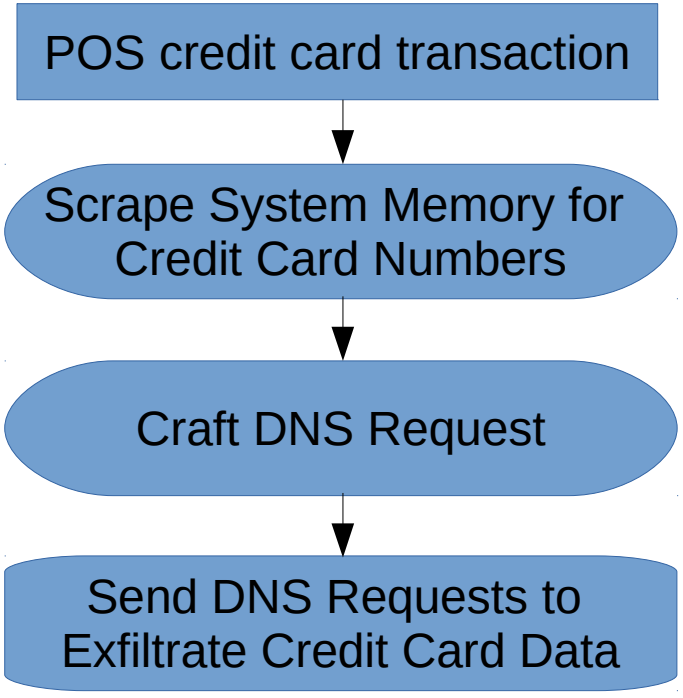
[2] CAN/CSA-IEC/TS 62443-1-1:2017-10-01, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models (Adopted IEC technical specification 62443-1-1:2009, first edition, 2009-07) (2017)
[3] IAEA- INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, Nuclear Security Series no 47, NST047 DRAFT (2017)
[8] Ker, A.: Information Hiding (complete), (2016) http://www.cs.ox.ac.uk/andrew.ker/docs/informationhiding-lecture-notes-ht2016.pdf

Hidden communication in desktop IT networks

- Turla Lightneuron Backdoor [1]



- UDPoS Malware [12]



[1] Faou, M., TURLA LIGHTNEURON One email away from remote code execution, ESET Research White papers, May 2019 (2019) https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf
[12]Cylance Threat Research Team, Threat Spotlight: Inside UDPoS Malware, (2018) https://threatvector.cylance.com/en_us/home/threat-spotlight-inside-udpos-malware.html

Potential hidden communication in OT networks

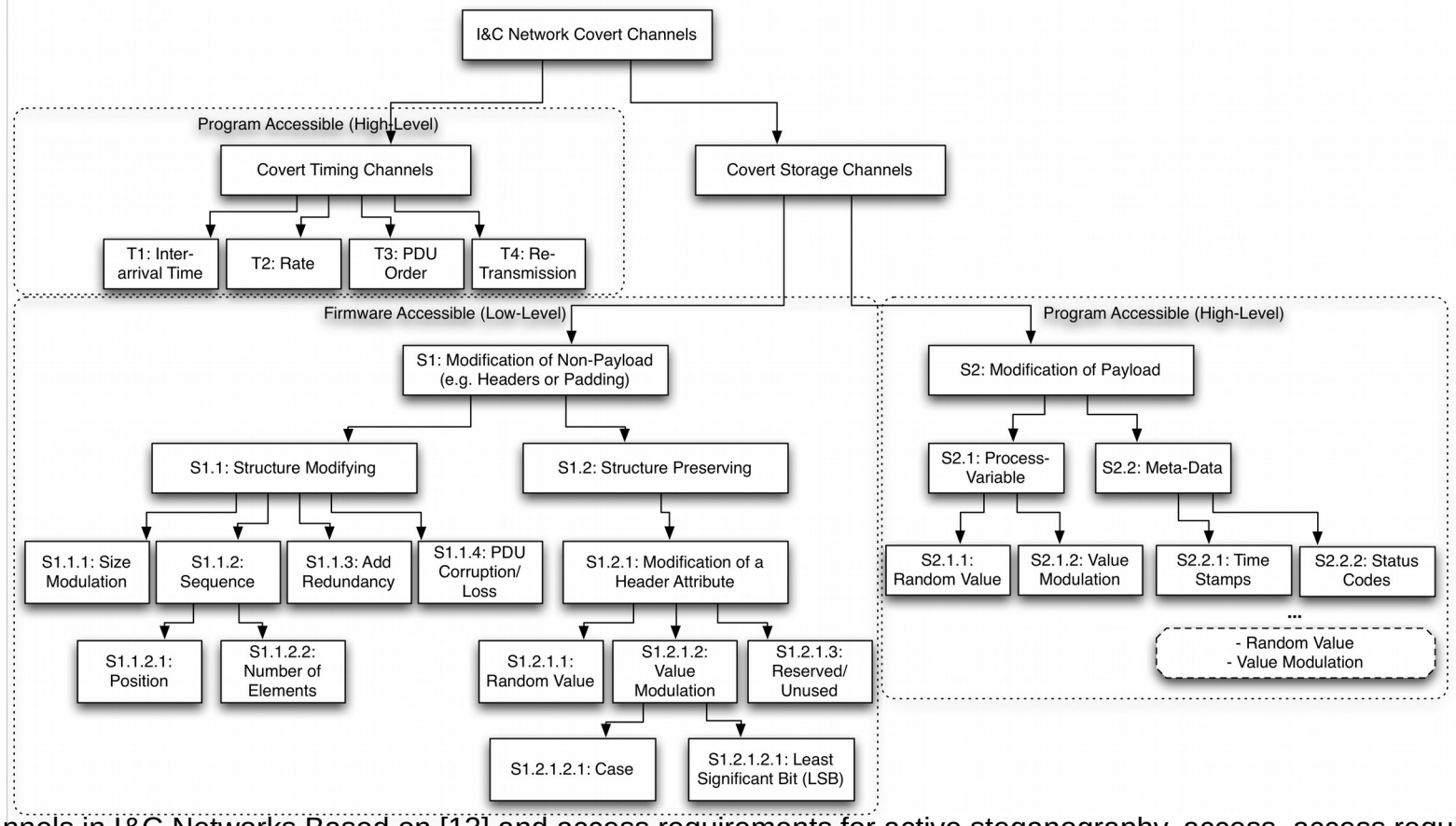


Fig. 1. Covert Channels in I&C Networks Based on [13] and access requirements for active steganography, access, access requirements

[13] Wendzel, S., Zander, S., Fechner, B., Herdin, C., Pattern-Based Survey and Categorization of Network Covert Channel Techniques, CSUR 47 3 (2015)

Exemplary supply chain attacks based on OPC UA

- Storage channel based on source timestamp CC_s

DTL Data Type for Timestamps:

Data field	Year	Month	Day	Week day	Hour	Minute	Second	Nanosecond
Data type	UInt	USInt	USInt	USInt	USInt	USInt	USInt	UDInt

Milliseconds			Microseconds			Nanoseconds		
1/10s	**4**	**2**	**M**	**N**	**O**	0	0	0

Synchronization

POKE_BOOL(Area, DBNumber, Byteoffset = 8 + M, Bitoffset = N, Value= O)

Result: arbitrary manipulation of digital outputs

- Hybrid channel based on source timestamp CC_h
  - Digit sum of the second field is kept odd or even for a longer period of time
  - PLC will trigger a hidden function if the time exceeds a certain threshold
  - Capacity is very limited in comparison to the storage channel

Strategic preparation and detection approaches

- Strategic preparation:
  - Communication data needs to be monitored and captured
  - Data capturing must be non-identifiable by the potential attacker, otherwise countermeasures (anti-forensics) might be utilized
  - Standard system behavior need to be known
- Detection:
  - CC_s - analysis of the source time stamps focusing on the distribution of microsecond digit O: normally uniformly distributed, with stego channel limited to a few values
  - CC_h – analysis of the delta times of the source timestamps between two OPC UA responses: delta times are not uniformly countiunuous if the stego channel is active

Summary and future work

- Steganographic communication channels are possible within OT networks
- A supply chain attack might introduce hidden functions that are not triggered during an isolated evaluation → source analysis is necessary
- Simple stego channels can be detected be performing an anomaly detection: normal traffic needs to be known
- In future work more advanced channels including the application of keys and a more dynamic behavior need to be evaluated towards potential detection approaches

Thank you for your kind attention!

Contact information:
Mario Hildebrandt
Department of Computer Science
Research Group Multimedia and Security
Institute of Technical and Business Information Systems
Otto-von-Guericke-University of Magdeburg

Universitaetsplatz 2
39106 Magdeburg, Germany
EMail: mario.hildebrandt@iti.cs.uni-magdeburg.de
Phone: +49 (391) 67 51603