Contribution ID: **478** Type: **Paper**

Threat Analysis of Steganographic and Covert Communication in Nuclear I&C Systems

Steganographic and covert communication is increasingly used for hiding attacks. The analysis of such criminal use of information hiding is also subject of the CUIng initiative [1] which cooperates with the Europol European Cybercrime Centre. Often information hiding is used by attackers in advanced persistent threats in order to operate without being noticed. Attackers might use it to hide data exfiltration or control channels for persistent malware.

Within the scope of industrial automation systems in general and nuclear instrumentation and control systems (I&C) in particular, information hiding is a new application field. This paper's objective is the analysis of existing attacks utilizing information hiding in the information technology (IT) domain, such as the Turla Backdoor [2] which could exfiltrate files, execute commands or download and execute files via an Exchange mail server, and their projection to the operational technology (OT, I&C) domain. In conjunction with that, attacker models are created, which might be used to extend the cyber design basis threat (cyber DBT). As a foundation the paper will summarize the general setup of I&C systems based on IEC 62443 [3] and zone concepts from IAEA Nuclear Security Series draft NST047 [4]. Based on this generalized architecture model, potential cover channels and the suitability of I&C specific communication for steganography are identified and analyzed. Such cover channels are formed by the usual communication within the I&C system including, but not limited to, Modbus/TCP, OPC UA, Syslog, etc. Using the generalized architecture model and the communication flows, the attack potential using information hiding is exemplary assessed. Subsequently, recommendations for a strategic and operational preparation for operators towards the prevention and detection of information hiding attacks are derived.

Information hiding can be used for different purposes. In the media it is widely used in invisible watermarking, e.g. for digital rights management. In communications, information hiding can be used to hide communication channels within normal network traffic. The objective of such hidden channels could be threefold: data exfiltration (unidirectional communication), data injection (unidirectional communication), command and control (bidirectional communication). The communication channel can be formed as a timing or a storage channel. In timing channels the existing communication is modified, e.g. by delaying network frames. In a storage channel the network frames are modified in order to embed the data. In the latter case it is crucial that the original purpose of the message is not influenced, otherwise the covert channel could be easily detected. A third option would be the introduction of additional network frames. However, such frames need to seem authentic and should not influence the processes at all.

For the threat analysis we use IEC 62443 [3] for I&C systems in combination with the zone concepts of NST047 [4]. With the required services such as Syslog for a secure operation of the equipment or the communication of process data via OPC UA, e.g. to a process and plant historian, several security zone border crossing network communication exist. Such communication is a suitable cover channel for information hiding. In particular, we consider scenarios for data exfiltration, also considering unidirectional communication, e.g. via data diodes, data injection, e.g. for triggering specific actions as well as a bidirectional command and control communication. For each scenario the communication across the different security zones is analyzed in order to estimate potential communication flows and the necessary effort for a successful attack. The analysis of the effort for the attack vectors considers potential infection vectors ranging from malware infection to directed attacks via the supply chain.

The general possibility of information hiding is demonstrated based on a small setup recreating the turbine governing system including the communication of this subsystem via OPC UA. Based on this setup the peculiarities of the I&C network communication are discussed and compared to standard IT systems. The paper will discuss the placement of network probes in order to prepare a detection of hidden communication channels. The main challenge, besides the mere detection of covert communication channels, is the concept of discovering such additional functionality during an assessment prior to the deployment of a component.

References:

[1] Criminal Use of Information Hiding (CUIng) Initative [Online] http://cuing.org, last accessed 05/27/19

[2] Matthieu Faou, "TURLA LIGHTNEURON One email away from remote code execution", ESET Research White papers 2019 [Online] https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf, last accessed 05/27/19

[3] International Electrotechnical Commission, "Industrial communication networks –Network and system security –Part 1-1: Terminology, concepts and models" IEC/TS 62443-1-1, 2009

[4] IAEA, “Computer Security Techniques for Nuclear Facilities”, NST047 Draft, [Online] https://www-ns.iaea.org/downloads/security/sec
series-drafts/tech-guidance/nst047.pdf, last accessed 05/27/19

State

Germany

Gender

Male

Primary authors: HILDEBRANDT, Mario (Otto-von-Guericke-University of Magdeburg); ALTSCHAFFEL, Robert (Otto-von-Guericke Universität Magdeburg); Mr LAMSHÖFT, Kevin (Otto-von-Guericke-University of Magdeburg); Mr LANGE, Mathias (Hochschule Magdeburg-Stendal); Mr SZEMKUS, Martin (Hochschule Magdeburg-Stendal); Mr NEUBERT, Tom (Technische Hochschule Brandenburg); Prof. VIELHAUER, Claus (Brandenburg University of Applied Sciences); Prof. YONGJIAN, Ding (Hochschule Magdeburg-Stendal); Prof. DITTMANN, Jana (Otto-von-Guericke-University of Magdeburg)

Presenters: HILDEBRANDT, Mario (Otto-von-Guericke-University of Magdeburg); ALTSCHAFFEL, Robert (Otto-von-Guericke Universität Magdeburg)

Track Classification: CC: Information and computer security considerations for nuclear security