up customers. Taxis are directed to the pickup location with an automated number plate-based system. We focused on the pickup location to count the taxis leaving with customers (versus taxis leaving without customers).

We successfully identified car types (taxi or other), charging taxis, taxis waiting to charge and

taxis driving away. This enabled us to count taxis using the fast charging stations, with duration (time) slots for all activities. The taxi stand was much busier than the fast charging station, with many pedestrians and cars not related to the taxi pick up process moving through the video. We could identify and count the number of taxis picking up customers (per time slot). Owing to the many passers-by in the vicinity of the taxis, the algorithm could not be trained to identify the number of customers entering a taxi. The object tracking task was especially challenging due to unexpected walking patterns at this location; people passing the waiting taxis and leaving the images were often recorded as entering the taxi. In addition, owing both to the camera position and the fact that taxi drivers often leave the car multiple times, drivers are difficult to distinguish from customers.

The simpler tasks can be done in real time, taking an average of 13 minutes to analyze a 15-minute video. This includes tasks such as identifying and counting taxis and determining time slots. More complex tasks, such as counting the number of people entering a car, require more computational power and more location-specific training to achieve acceptable results.

The Municipality of Amsterdam is considering applying the new algorithms to new taxi stands and to other use-cases. This research is part of the research on energy transition of the Intelligence and Autonomous Systems group of the CWI and the IDOLAAD project [L1] at the Amsterdam University of Applied Science. Future research will focus on exploring ways to further automate the more complex tasks.

Link:
[L1]: https://www.idolaad.com/research/research.html

References:

[1] J. Redmon, A. Farhadi: "Yolov3: An incremental improvement", arXiv preprint arXiv:1804.02767, 2018.

[2] L. Leal-Taixé, et al.: "Tracking the trackers: an analysis of the state of the art in multiple object tracking", arXiv preprint arXiv:1704.02781, 2017

[3] S. R. E. Datondji, et al.: "A survey of vision-based traffic monitoring of road intersections", IEEE transactions on intelligent transportation systems, 17(10), 2681-2698, 2016

Please contact:

Maarten Groen, Amsterdam University of Applied Science, Netherlands, m.n.groen@hva.nl

Nanda Piersma, Amsterdam University of Applied Science, CWI, Netherlands, nanda.piersma@cwi.nl

Securing Home Automation Systems against Sensor Manipulation

by Albert Treytl, Edith Huber, Thilo Sauter (Danube University Krems) and Peter Kieseberg (St. Pölten University of Applied Sciences)

Home automation systems (HAS) can be important attack vectors, yet research on securing sensors is sparse, especially with respect to the analogous side of these components, i.e., detecting manipulations of the sensors themselves. Metadata together with the combination of several sensor nodes can be used to thwart such manipulation attacks.

The Internet of Things is a wide and diverse ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context, automate tasks and provide better situation awareness to react to customer needs. Home automation systems (HAS), which are commonly based on IoT, are a growing field for many applications, such as comfort, surveillance and access and energy saving. Since HAS generate a lot of private data, they are very appealing to attackers, who can use them to spy on or stalk inhabitants, or use them to facilitate more traditional criminal activities like burglaries [1]. The comprehensive interconnection of systems to an Internet of Things offers enormous potential to HAS, but also generates new cyber-risks. This has been discussed in-depth by many other researchers, often in the context of industrial or workplace environments, such as building automation and industrial IoT, pointing out that the quality and/or veracity of the source information, typically provided through sensors, forms the basis for securing IoT systems. Thus, both the acquisition and the communication of this information requires special attention in an IoT-environment.

Most of the basic HAS standards currently in use were developed the from the late eighties to early nineties, and IT-security, such as KNX, was added later on. There remain many open questions and challenges, especially in relation to security measures that rely directly on the sensor data and related meta-information. While there are several approaches to use meta-information to discover malicious software (e.g., [2]), the analogue side of the sensors (hardware) is typically neglected, even though manipulation on this side makes typical countermeasures obsolete. This also applies to the extraction of meta-information in the analogue sensor circuit, which could help detect such manipulations and thus help close the security gap in sensor systems [3]. Thus, two different attacker approaches must be considered for home automation systems:

- An attacker could manipulate the data in the digital realm, i.e., the sensor sends correct information, but it is modified in the network. This typical approach is often referred to in the academic literature. Even in this context new tech-

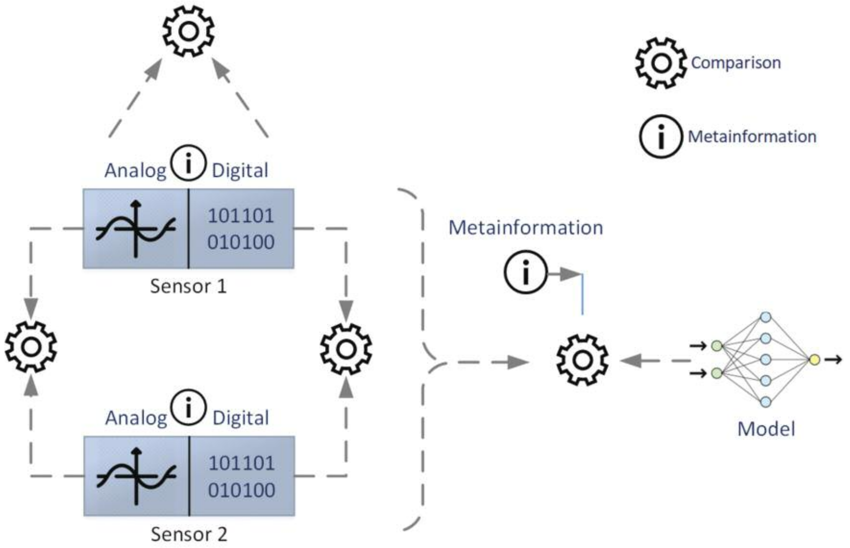

Figure 1: Comparing analogue and digital information and meta-information.

niques are required owing to the low performance of cheap sensors that cannot support standard techniques like signatures or other cryptographic schemes.
- Alternatively, the attacker could manipulate the sensor itself to make it publish incorrect information to the network. Particularly at the analogue level, substantial research is required on both sides: from the perspective of the attacker, to better understand the possibilities in real-world examples; and from the perspective of defence, to better understand these attacks and their impacts on meta-information in order to provide new means of defence.

While the effects of these attacks look similar, the mitigation strategies required to overcome them are very different and require different sets of skills, and the analogue side or circuit has been largely neglected in the security community. When considering meta-information, attacks could potentially be made much harder when extending the view of the defender from the single sensor to related meta-information and further to a multi sensor scenario, where information and especially meta-information, needs to fit together, i.e., the attacker needs to coordinate different attacks to remain undiscovered in a more complex physical model.

In our project “ARES”, we will therefore analyse the extended attack surface directly on the analogue side of common sensors, considering payload information as well as meta-information. A combination of sensor data and highly attack resistant meta-information will be used to increase the overall attack resistance. Through the combination of information from multiple sensors, as well as matching with (physical) models, the attacker would need to stay consistent between manipulated sensor signal and meta-information within a single device but also over several devices, making the attack much more difficult to carry out and thus raising the bar (see Figure 1).

Additionally, the success of technical measures always depends on user acceptance. International organisations, such as EUROPOL and ENISA, regard a multidisciplinary approach as indispensable, since HAS suffer from a security hostile environment including low cybersecurity awareness of users, as well as fast and extremely low cost implementation and unplanned installation compared to other fields such as industrial automation [1]. The continuous expansion of digitalisation into daily domestic life raises questions that are best addressed from a social science perspective, incorporating sociology, legal studies and economics. ARES will investigate these issues, providing an evidence-based analysis of cyber-risks and user requirements, and will use these findings to improve the design of the security measures.

References:

[1] E. Casey: “Digital evidence and computer crime: Forensic science, computers, and the internet”, Academic press, 2011
[2] A. Sadighian, et al.: “A context-aware malware detection based on low-level hardware indicators as a last line of defense”, 2017.
[3] P. Palensky, T. Sauter: “Security considerations for FAN-Internet connections” in 2000 IEEE Int. Workshop on Factory Communication Systems, Proceedings, Cat. No. 00TH8531, pp. 27-35, IEEE 2000.

Please contact:

Peter Kieseberg
University of Applied Sciences, St. Pölten, Austria
peter.kieseberg@fhstp.ac.at