

# Poster: ARGUS – Context-Based Detection of Stealthy IoT Infiltration Attacks

Phillip Rieger

Marco Chilese

Reham Mohamed

Markus Miettinen

Hossein Fereidooni

Ahmad-Reza Sadeghi

Technical University of Darmstadt

## Abstract

IoT application domains, device diversity and connectivity are rapidly growing. IoT devices control various functions in smart homes and buildings, smart cities, and smart factories, making these devices an attractive target for attackers.

On the other hand, the large variability of different application scenarios and inherent heterogeneity of devices make it very challenging to reliably detect abnormal IoT device behaviors and distinguish these from benign behaviors. Existing approaches for detecting attacks are mostly limited to attacks directly compromising individual IoT devices, or, require predefined detection policies. They cannot detect attacks that utilize the control plane of the IoT system to trigger actions in an unintended/malicious context, e.g., opening a smart lock while the smart home residents are absent.

In this paper, we tackle this problem and propose ARGUS, the first self-learning intrusion detection system for detecting *contextual attacks* on IoT environments, in which the attacker maliciously invokes IoT device actions to reach its goals.

ARGUS monitors the contextual setting based on the state and actions of IoT devices in the environment. An unsupervised Deep Neural Network (DNN) is used for modeling the typical contextual device behavior and detecting actions taking place in abnormal contextual settings. This unsupervised approach ensures that ARGUS is not restricted to detecting previously known attacks but is also able to detect new attacks. We evaluated ARGUS on heterogeneous real-world smart-home settings and achieve at least an F1-Score of 99.64% for each setup, with a false positive rate (FPR) of at most 0.03%.

## REFERENCES

- [1] RIEGER, P., CHILESE, M., MOHAMED, R., MIETTINEN, M., FEREDOONI, H., AND SADEGHI, A.-R. ARGUS: Context-Based Detection of Stealthy IoT Infiltration Attacks. In *32nd USENIX Security Symposium (USENIX Security 23)* (2023), USENIX Association.

