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., Fereidooni, 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.

Paper Available at https://doi.org/10.48550/arXiv.2302.07589

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

Published in USENIX Security, 2023

Phillip Rieger, Marco Chilese, Reham Mohamed, Markus Miettinen, Hossein Fereidooni, Ahmad-Reza Sadeghi

Problem

- Stealthy IoT infiltration attacks, e.g., via insecure webservices
- Possible harm or damages

Contribution

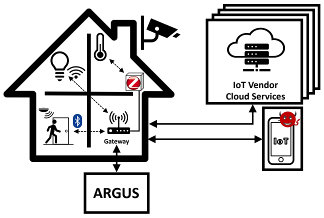
- Context-based self-learning intrusion detection system

Threat Model

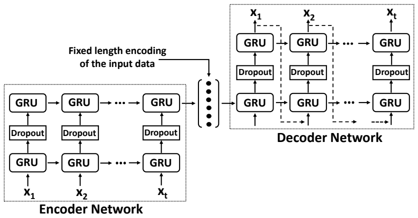
- $\mathcal{A}$ (Adversary) compromises part of IoT control plane to trigger normal looking actions IoT devices
- $\mathcal{A}$ has not access to IoT devices
- Context allows to distinguish benign actions and attacks

ARGUS System Design

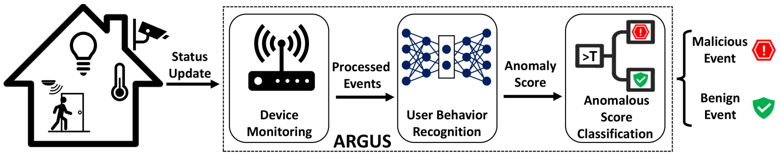
- No additional app: monitoring through Home Assistant
- Unsupervised Deep Recurrent Autoencoder (RAE)
- Time-adapting threshold for detection



ARGUS System Model

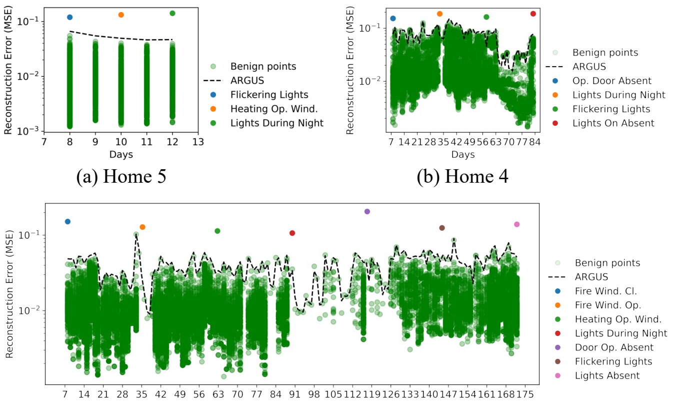


ARGUS Auto-Encoder (AE) Architecture



High-Level Overview of ARGUS's Components

Evaluation and Results

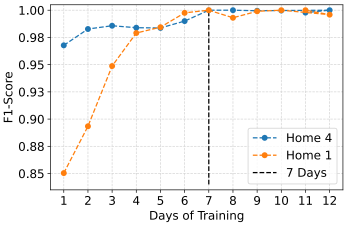


(a) Home 5

(b) Home 4

(c) Home 1

Anomaly Scores for different real-world homes for benign behavior and attacks



Evaluation depending on the duration of training data

Dataset	FPR	Pr	Re	F1-Score
Home 1	0.03	99.22	100.00	99.64
Home 2	0.00	100.00	100.00	100.00
Home 3	0.00	100.00	100.00	100.00
Home 4	0.00	100.00	100.00	100.00
Home 5	0.00	100.00	100.00	100.00

Performance on Real-World Setups

- 5 Real-world dataset
- 8 Real-world attacks
- Time-adapting threshold
- Perfect attack detection
- FPR ≤ 0.03%

Bibliographic Reference

Phillip Rieger, Marco Chilese, Reham Mohamed, Markus Miettenen, Hossein Fereidooni, and Ahmad-Reza Sadeghi. ARGUS: Context-Based Detection of Stealthy IoT Infiltration Attacks. In USENIX Security, 2023, DOI: https://doi.org/10.48550/arXiv.2302.07589

TECHNISCHE
UNIVERSITÄT
DARMSTADT

System
Security
Lab

Scan it for
more details