TECHNISCHE UNIVERSITÄT DARMSTADT

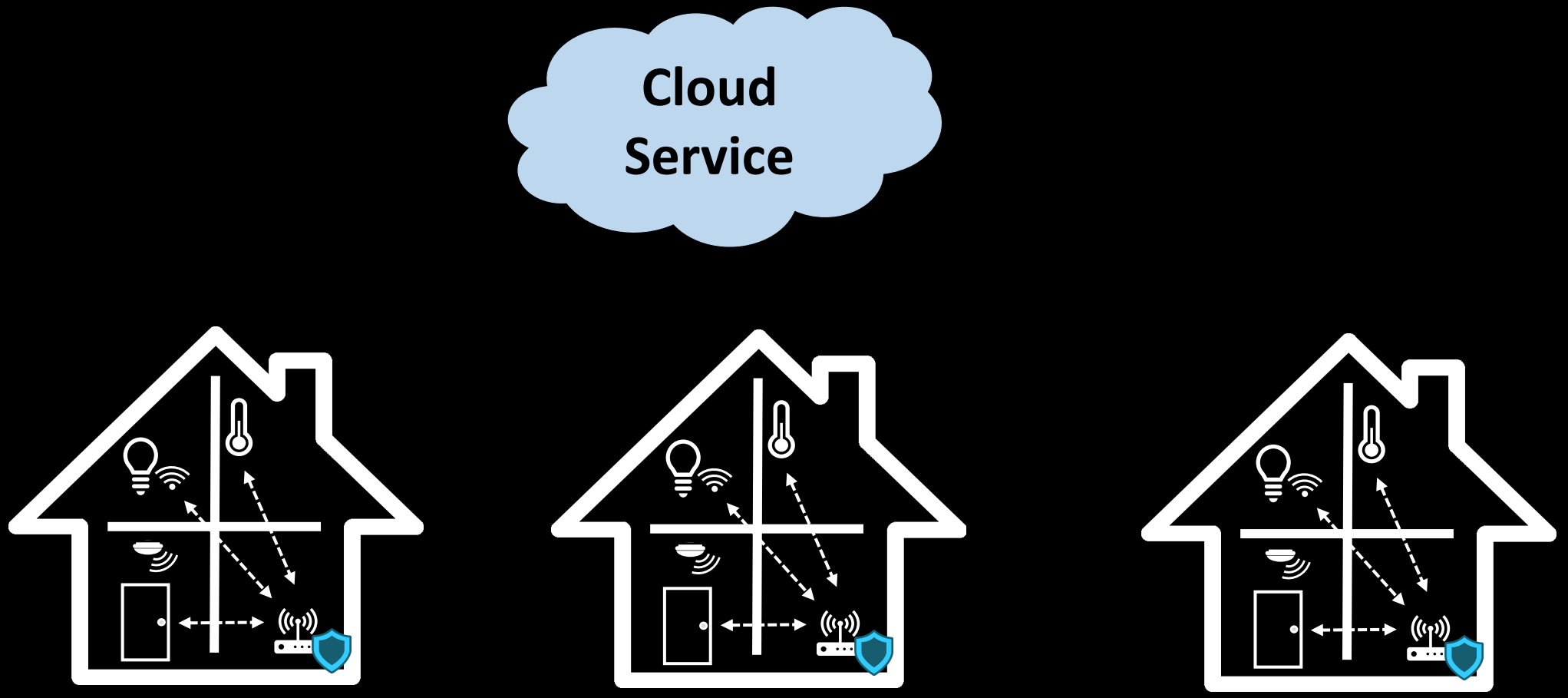
ARGUS: Context-Based Detection of Stealthy IoT Infiltration Attacks

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

The 32nd USENIX Security Symposium 2023

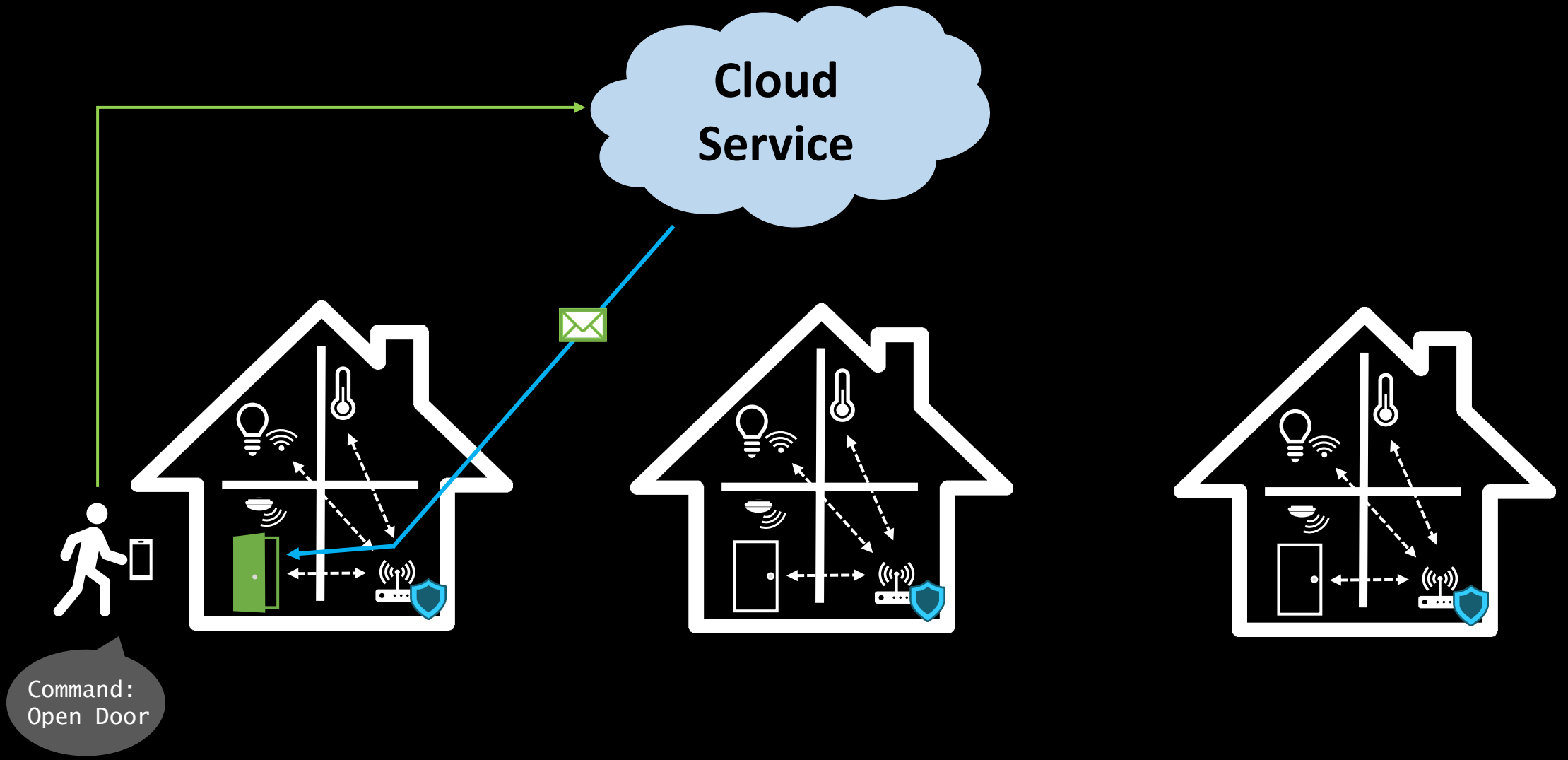
System Security Lab

Contextual Attacks



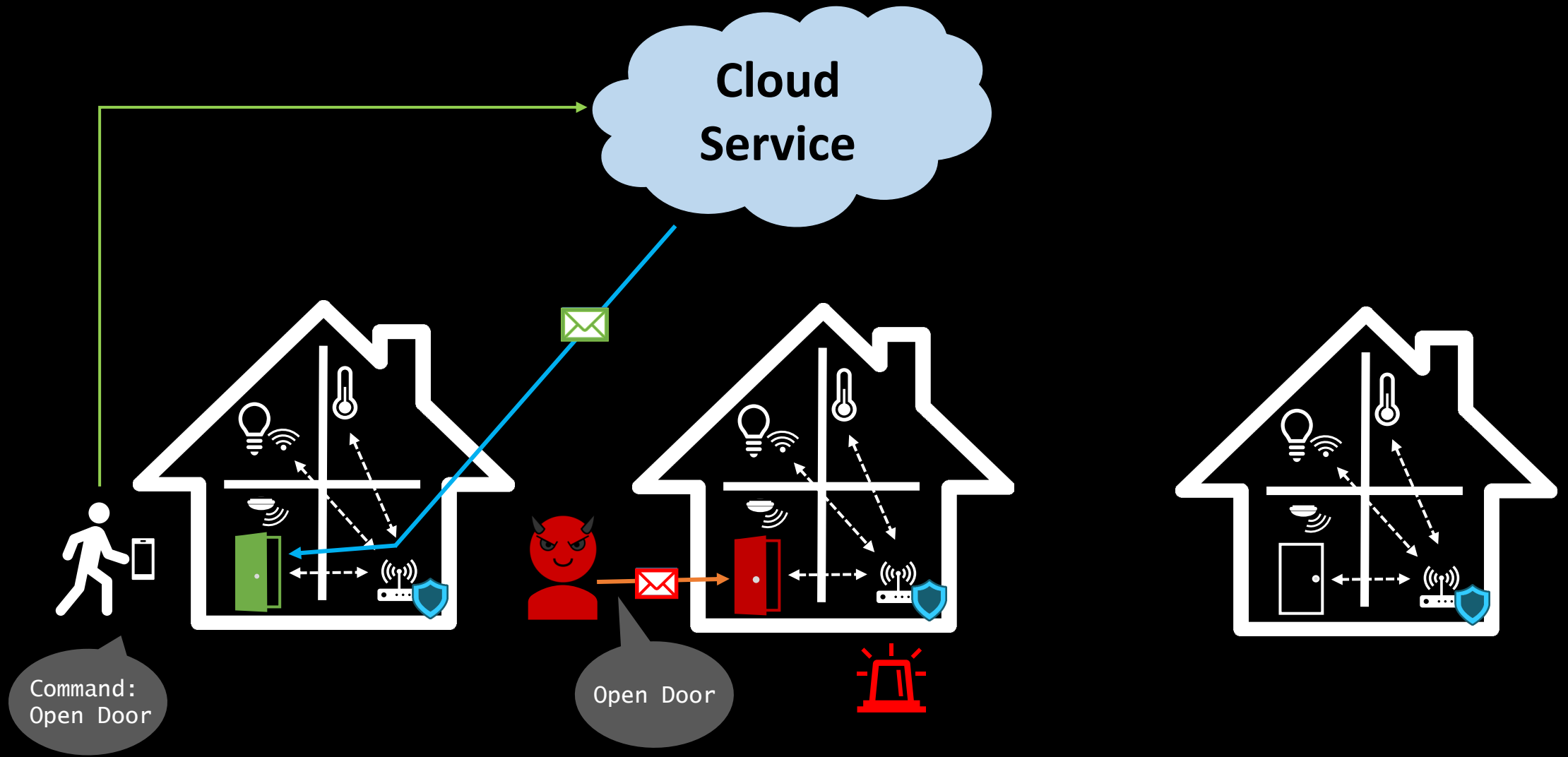
Benign Scenario

Contextual Attacks



Benign Scenario

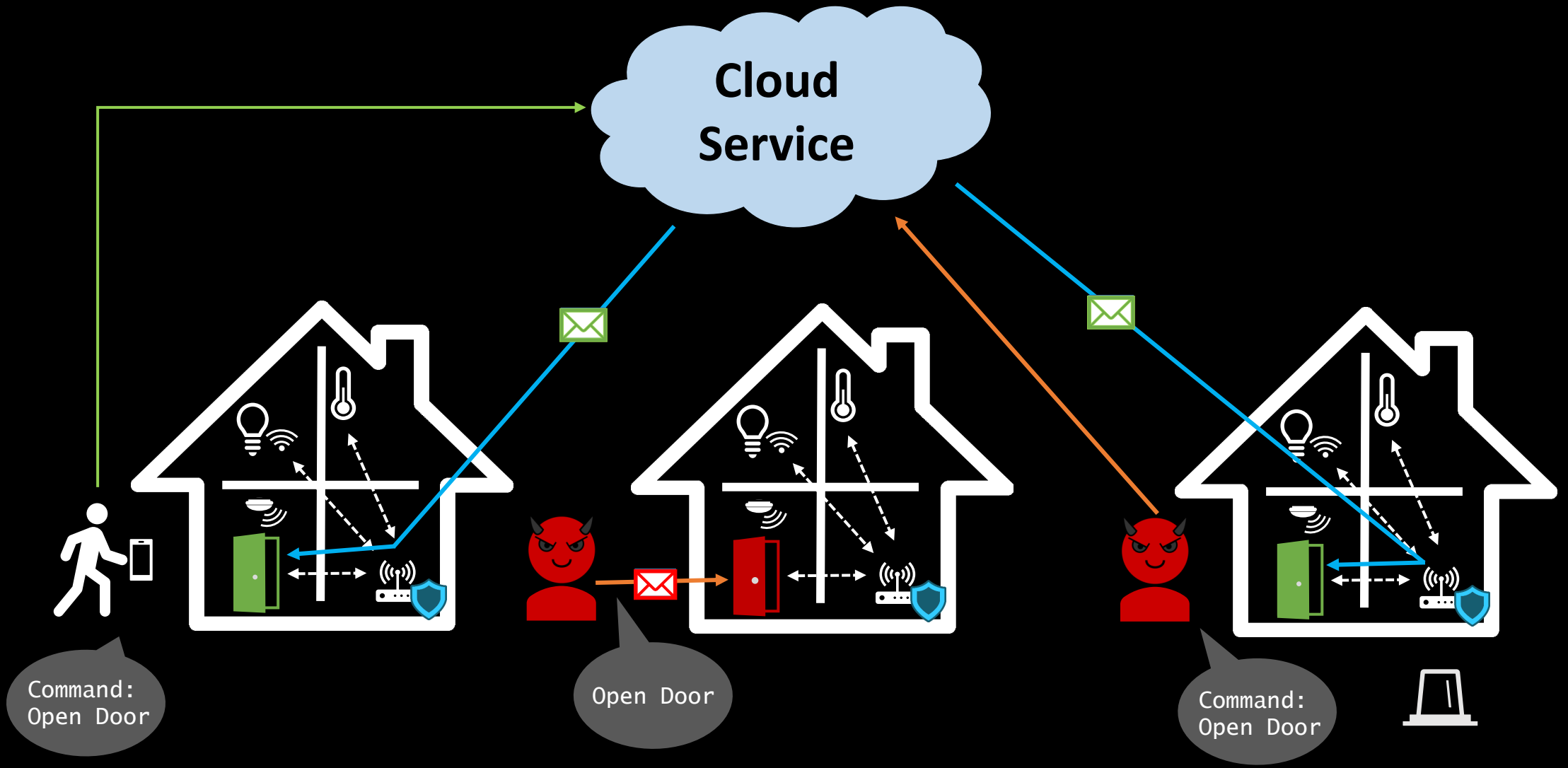
Contextual Attacks



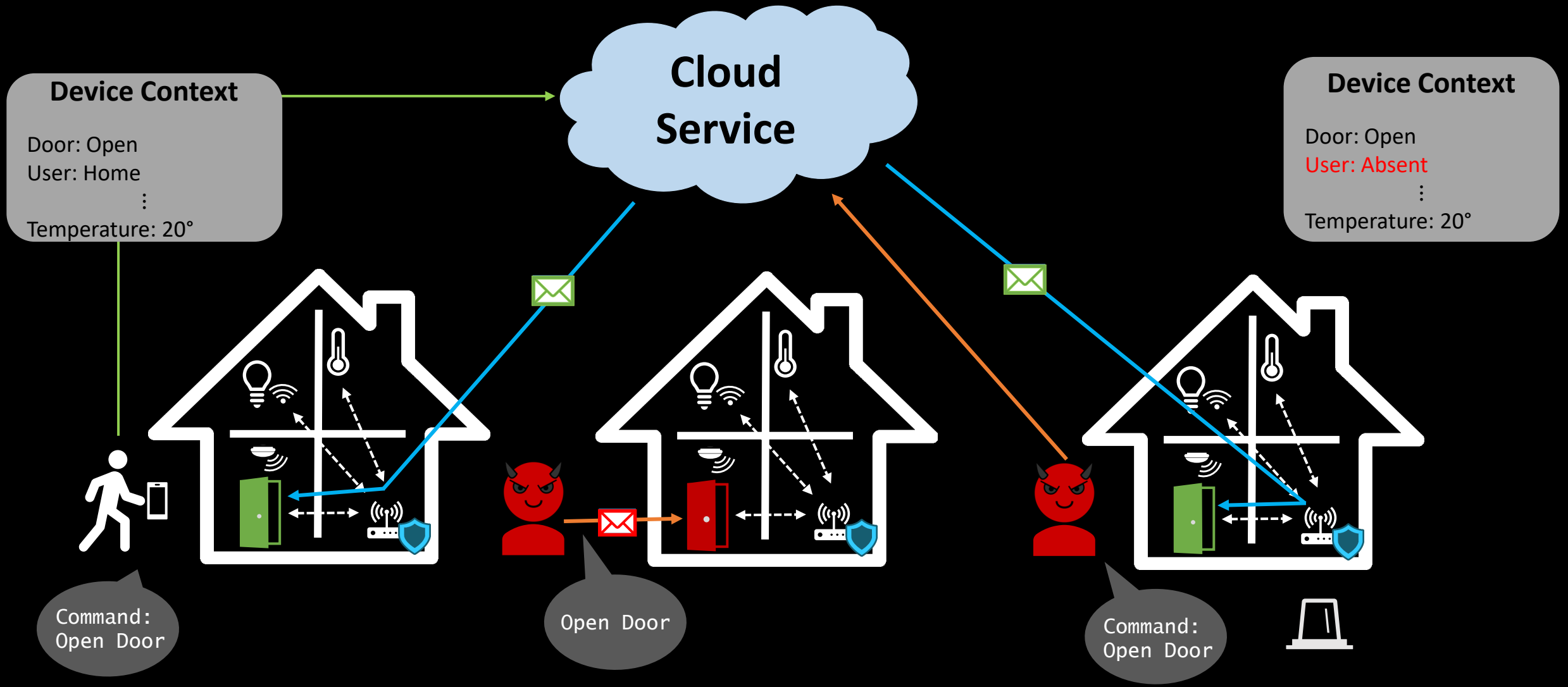
Benign Scenario

Compromised IoT Device

Contextual Attacks



Contextual Attacks



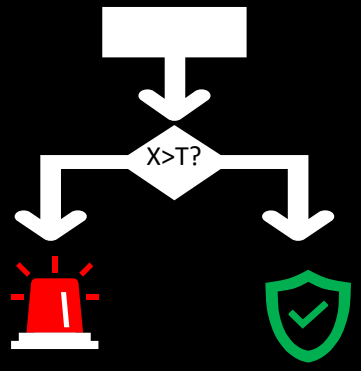
Existing Solutions

Network-Intrusion Detection

Cannot detect attacks exploiting control-infrastructure

[Nguyen et al., ICDCS 2019]
[Fan et al., BigDataSE 2020]
[Oconnor et al., WISEC 2019]

Policy-Based Detection

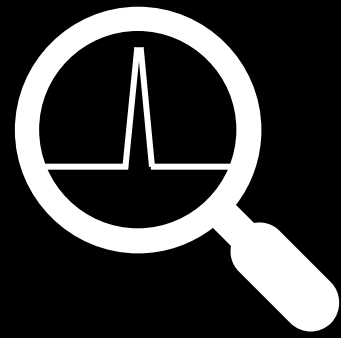


Requires tedious setup by users

Attacker might find gap in policies

[Yahyazadeh et al., SACMAT 2019]
[Celik et al., USENIX ATC 2018]

Contextual Anomaly Detection

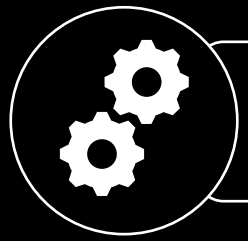


1. Require additional information about devices
2. Restricted to known attacks
3. Consider only commands

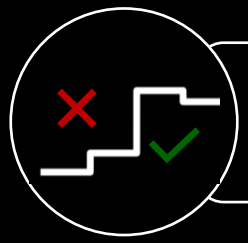
1. [Fu et al., USENIX Security 2021]
2. [Dai et al., IWCC 2022]
3. [Amraoui et al., CRISIS 2020]

Contributions

- Detects contextual attacks being invisible for network inspection-based systems



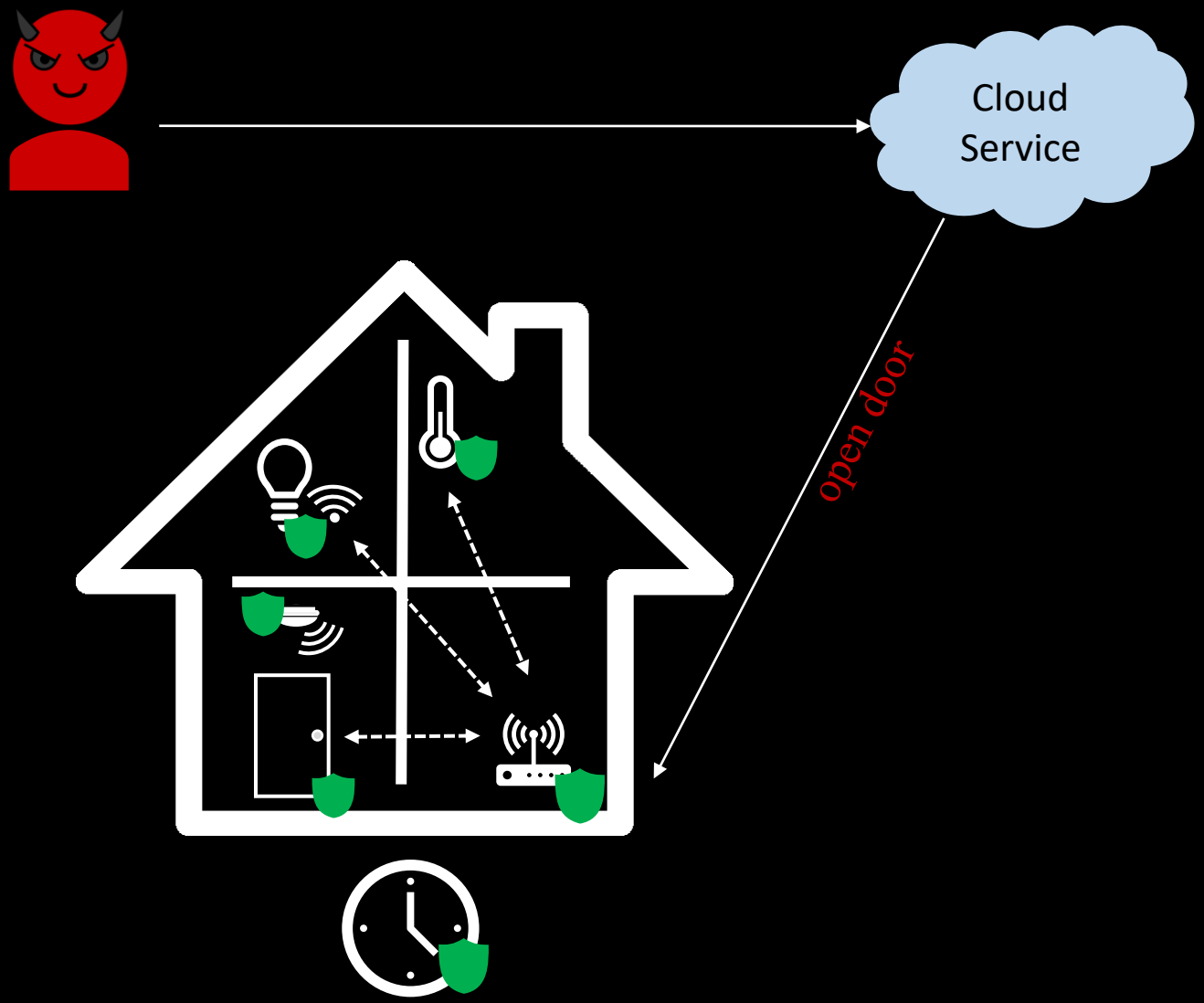
- Operates without manual configuration or knowledge of the devices



- Automatic tuning of detection boundary for classifying anomaly scores

- Evaluated on 5 real-world diverse smart-home setups
- Dataset published as benchmark for future work

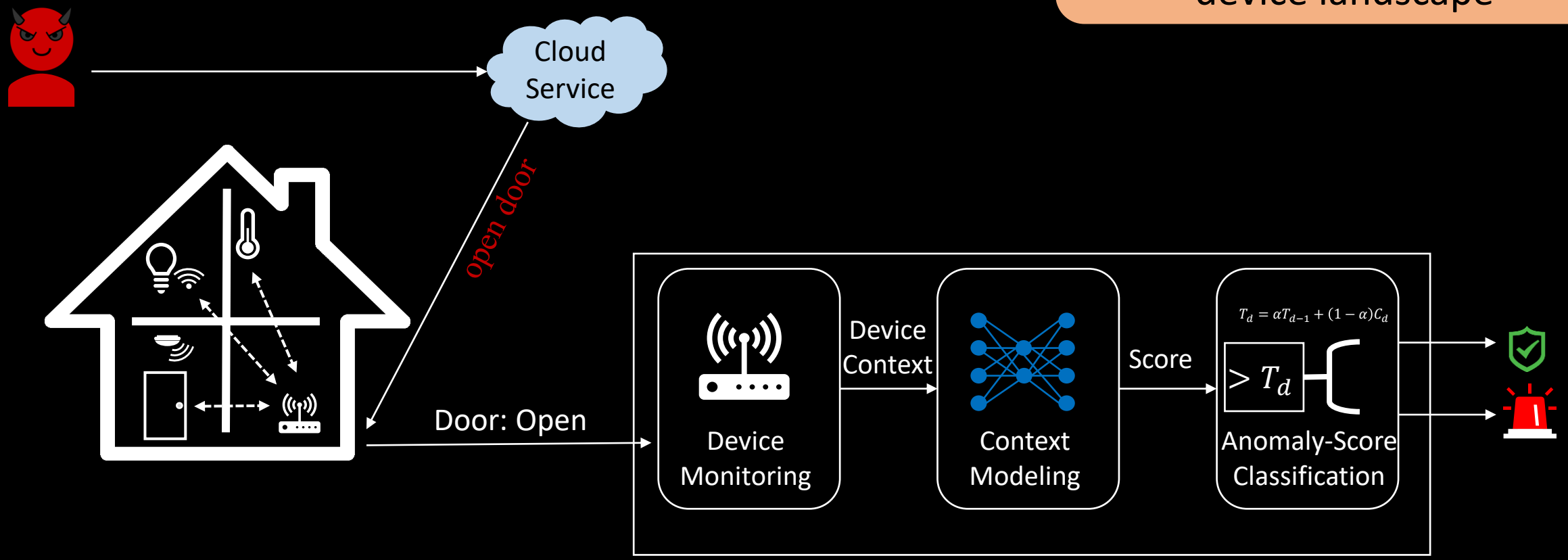
Argus – Assumptions



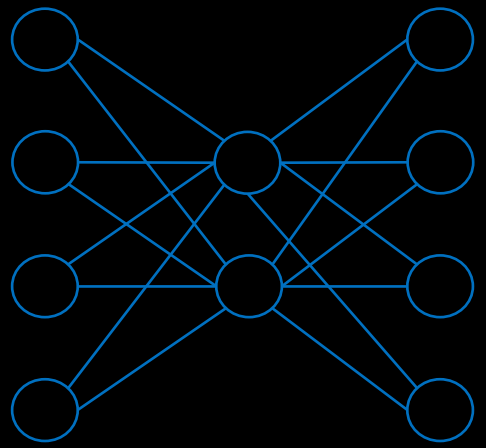
- Security device not compromised
- Benign Setup Phase
- IoT devices itself not compromised

Argus – High Level Overview

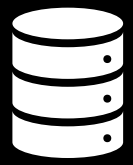
Technical Challenge: Obtain context for heterogenous device landscape



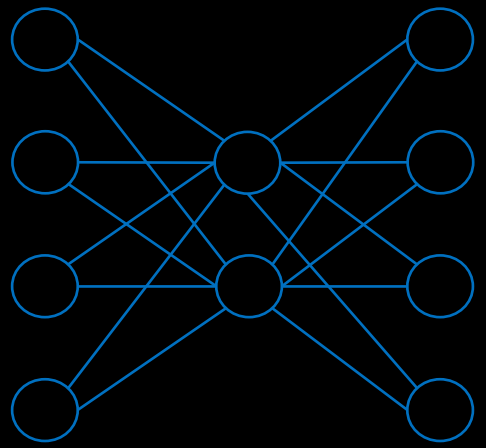
Argus – Context Modelling



Argus – Context Modelling

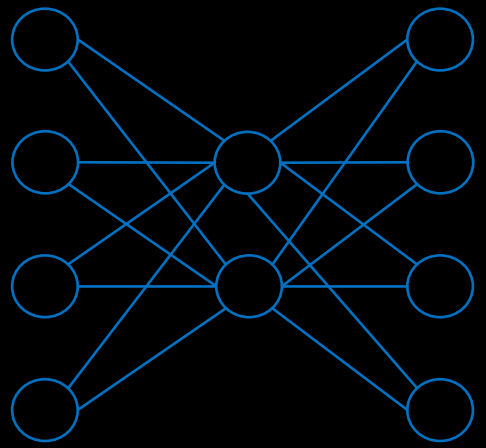


Captured
Normal Behavior

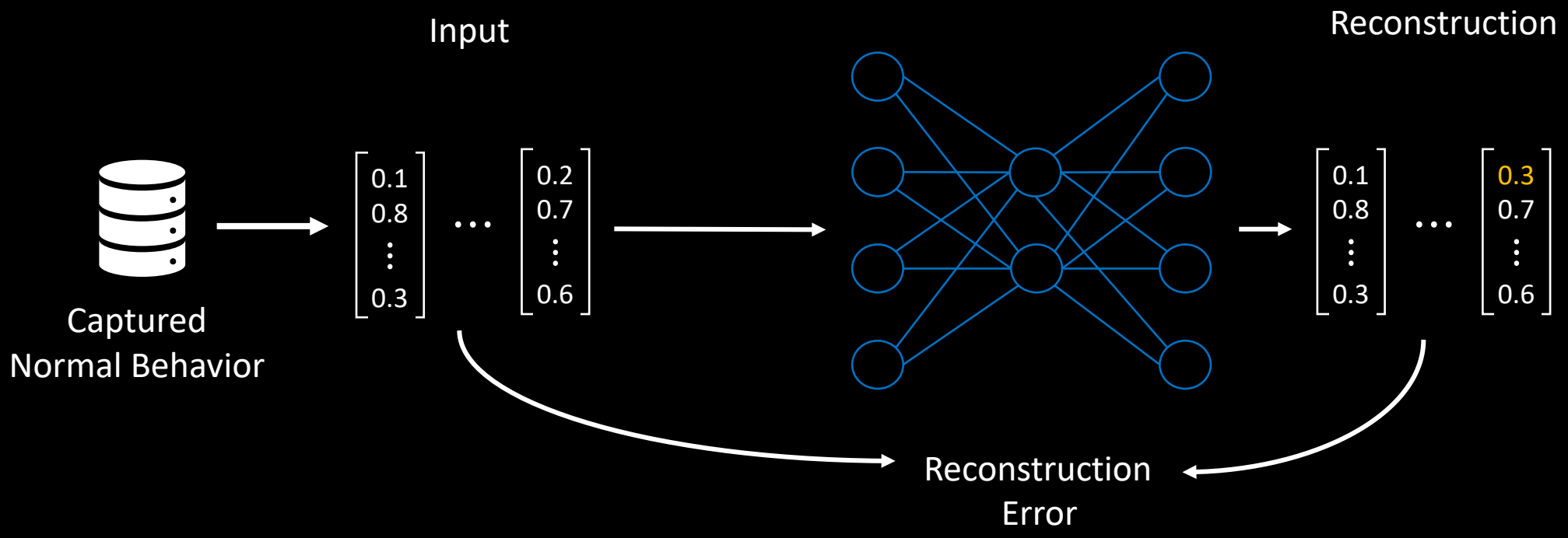


Argus – Context Modelling

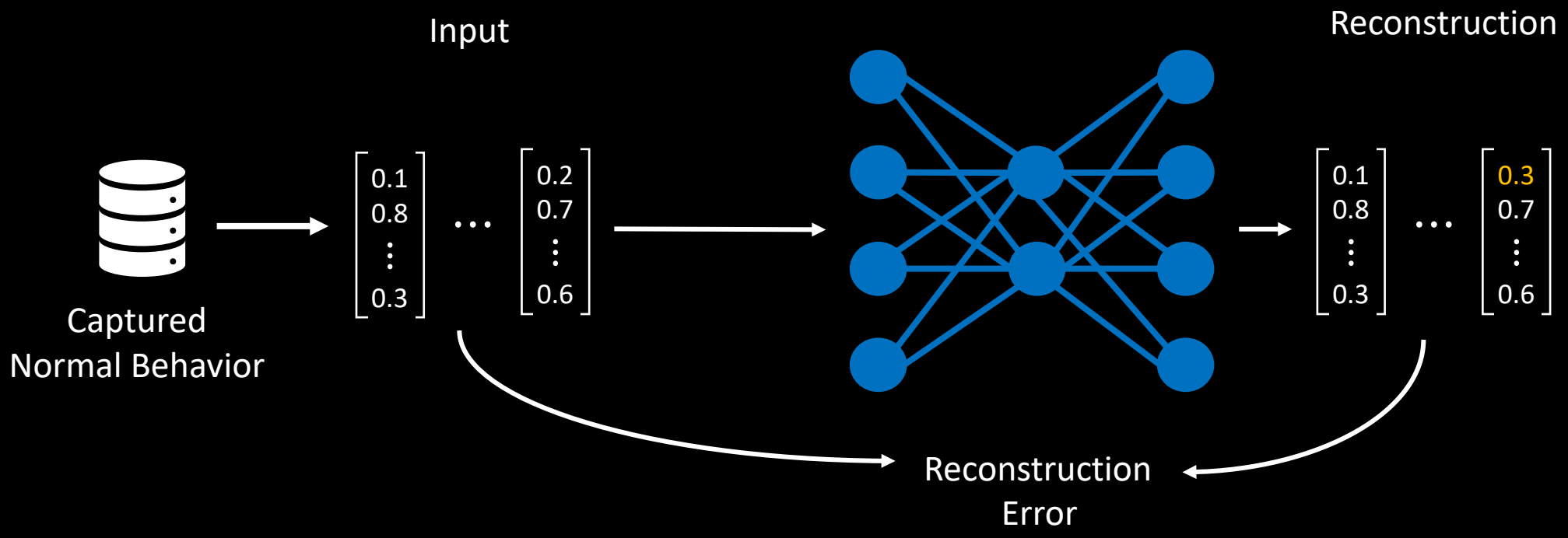
Technical Challenge: Train system without attack samples



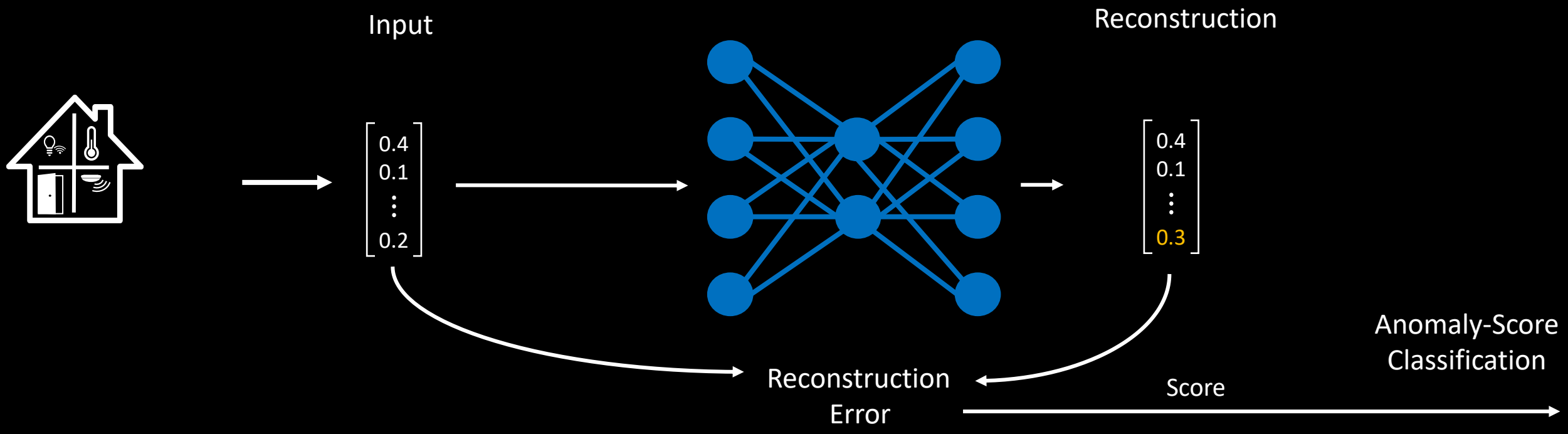
Argus – Context Modelling



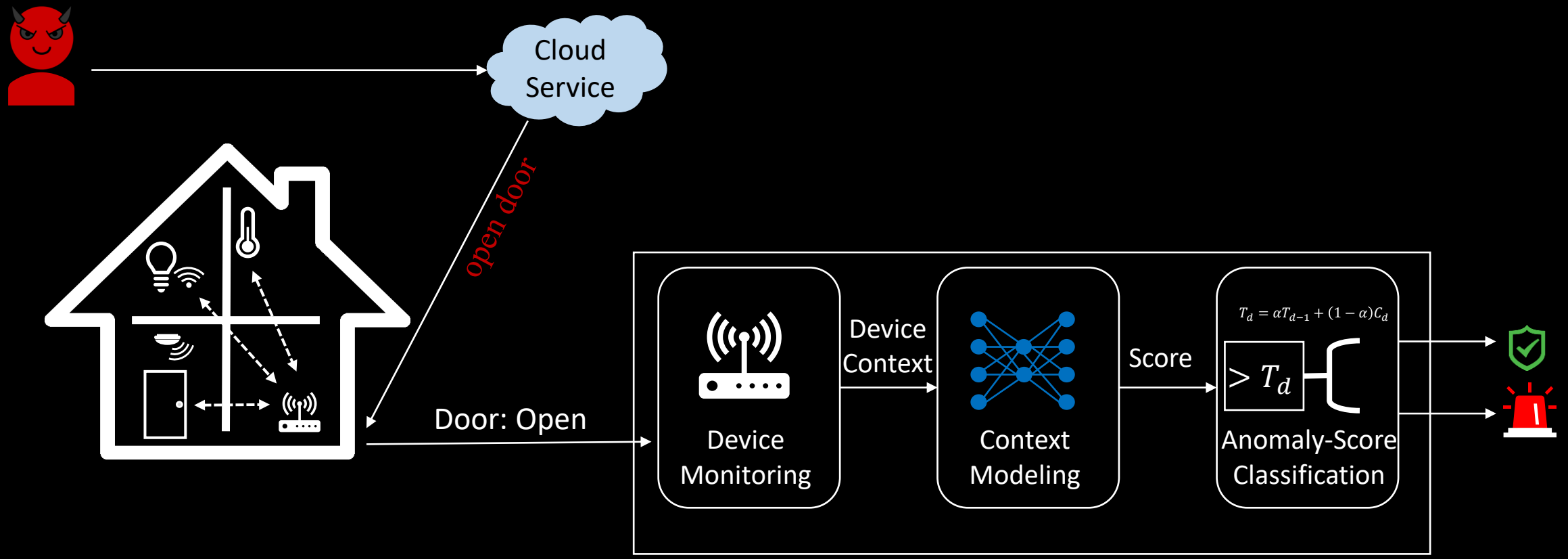
Argus – Context Modelling



Argus – Context Modelling



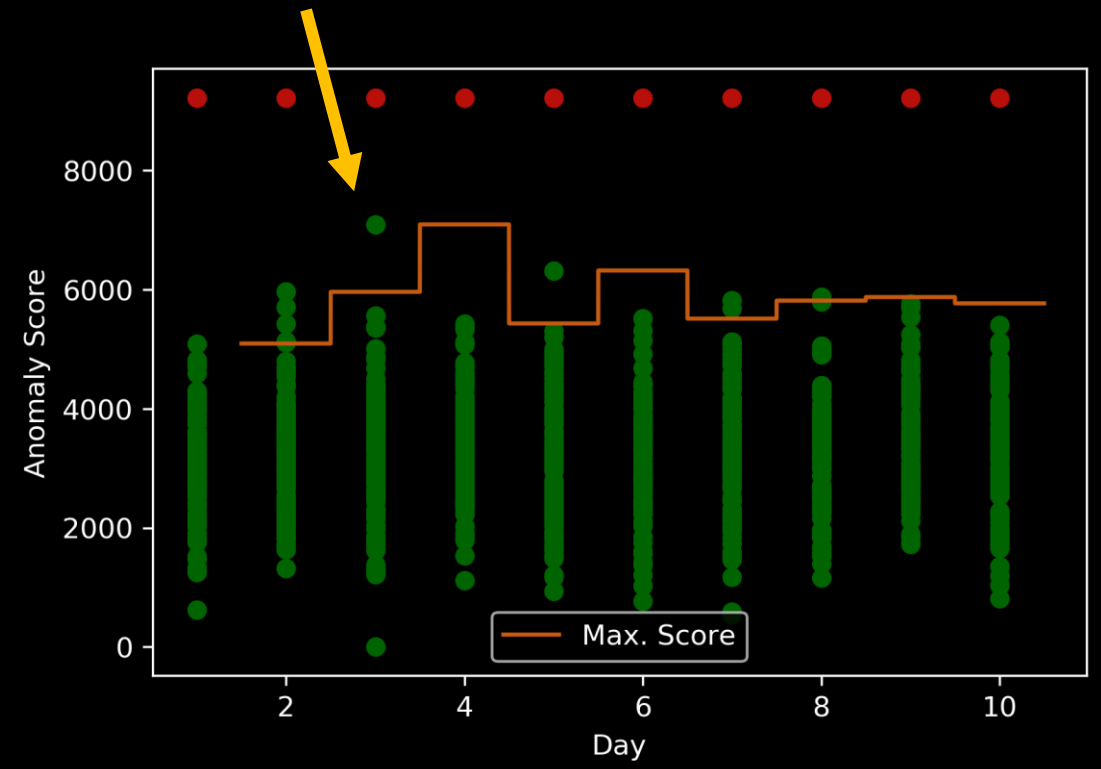
Argus – High Level Overview



Argus – Anomaly-Score Classification

1. Calculate max. score of previous day

$$Max_{d-1} = \max(Scores_{d-1})$$



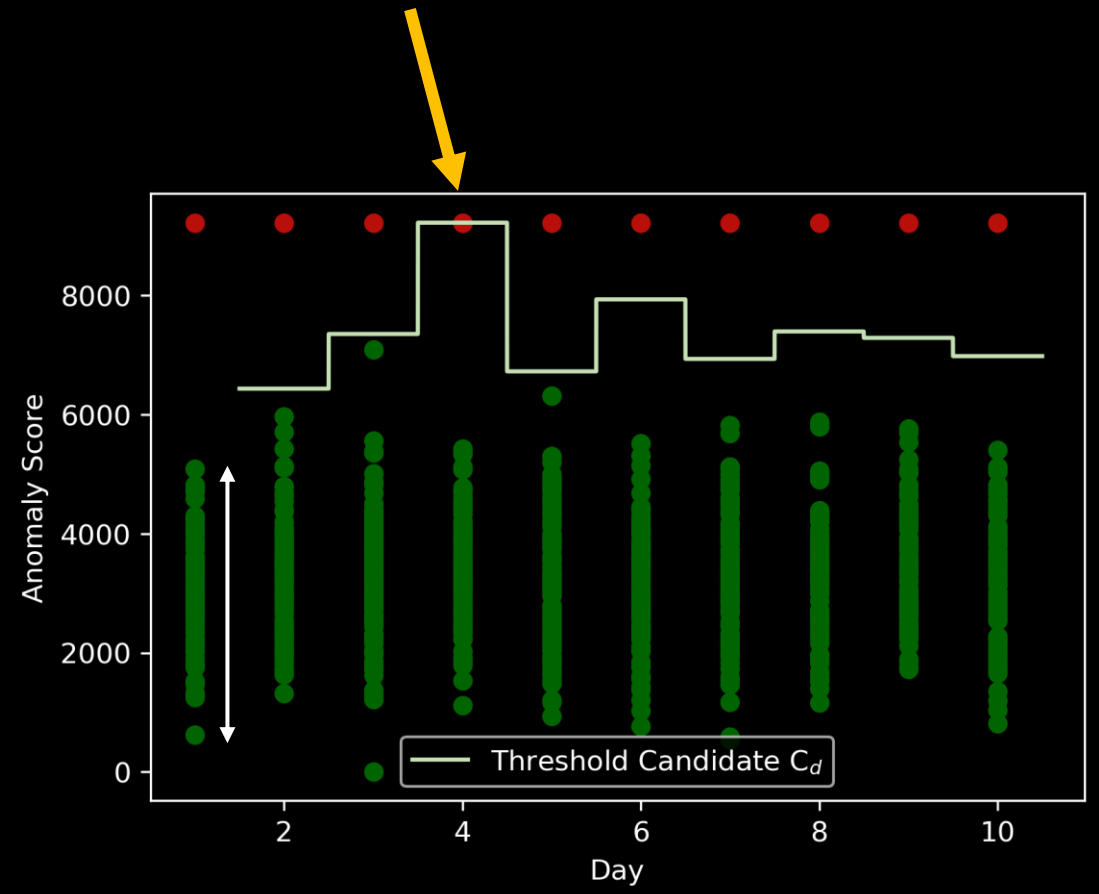
Argus – Anomaly-Score Classification

1. Calculate max. score of previous day

$$Max_{d-1} = \max(Scores_{d-1})$$

2. Add interval of values from previous day
   - Multiply interval with security level β
   - Threshold Candidate C_d:

$$C_d = Max_{d-1} + \beta \cdot (Max_{d-1} - Min_{d-1})$$



Argus – Anomaly-Score Classification

1. Calculate max. score of previous day

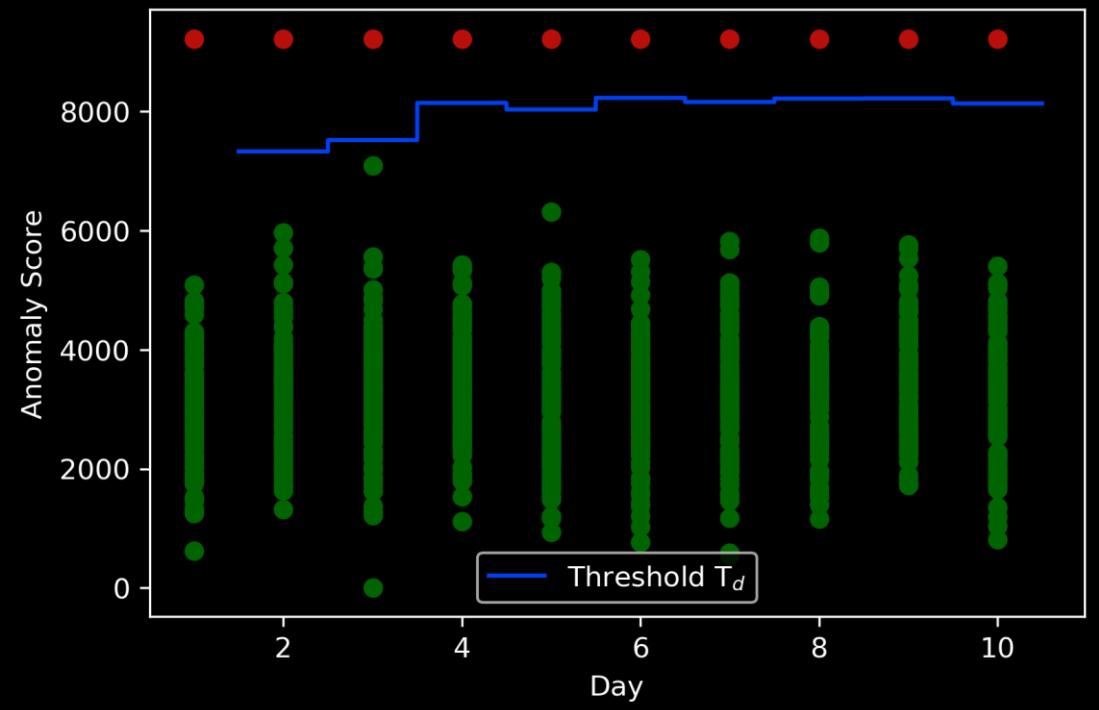
$$Max_{d-1} = \max(Scores_{d-1})$$

2. Add interval of values from previous day
   - Multiply interval with security level β
   - Threshold Candidate C_d:

$$C_d = Max_{d-1} + \beta \cdot (Max_{d-1} - Min_{d-1})$$

3. Consider history to avoid extreme changes
   - Multiply with aging factor α
   - Threshold T_d:

$$T_d = \alpha \cdot T_{d-1} + (1 - \alpha) \cdot C_d$$

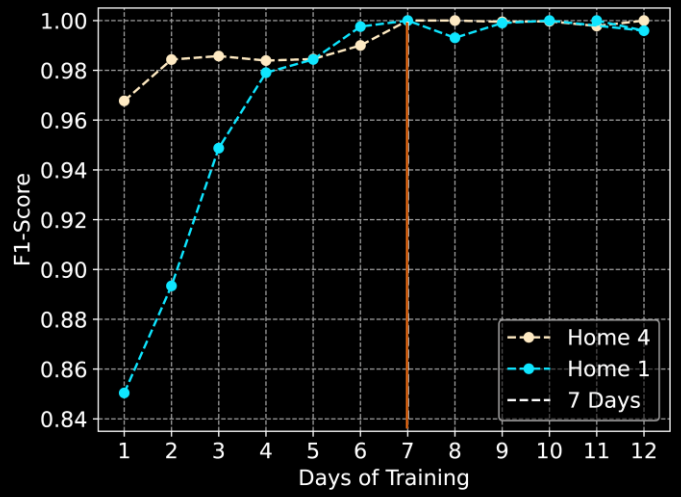


Evaluation Results

FPR: False Positive Rate
PRC: Precision
REC: Recall

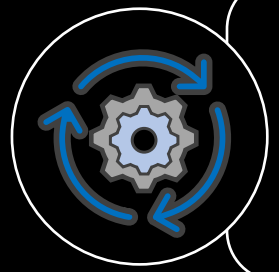
- Evaluation Setup
  - 5 Real World Homes
  - Child and Adult Inhabitants
  - Apartments, Single-Room Apartment, Room in shared Flat
- Evaluated Attacks Include:
  - Door Open during Absence
  - Lights-On during Absence
  - Movement during Absence
  - Lights-On During Night
- 7 Days of Training Data Sufficient

Dataset	FPR	PRC	REC	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%



Conclusion

- IoT Devices are vulnerable to attacks via insecure control devices
- Network-Based Detection mechanisms fail detecting such attacks as network traffic is indistinguishable
- Existing contextual defenses requires manual setup or information about devices



- ARGUS monitors IoT device context to detect attacks exploiting insecure control plane
- Models normal behavior using Deep Auto-Encoder to calculate anomaly score
- Calculates dynamic threshold to classify anomaly-score

- No knowledge on devices or attacks necessary
- Works without manual setup
- 7 days of training data achieved F1-Score $\geq$ 99.64% on 5 real-world homes