Secure Systems Group, Aalto University

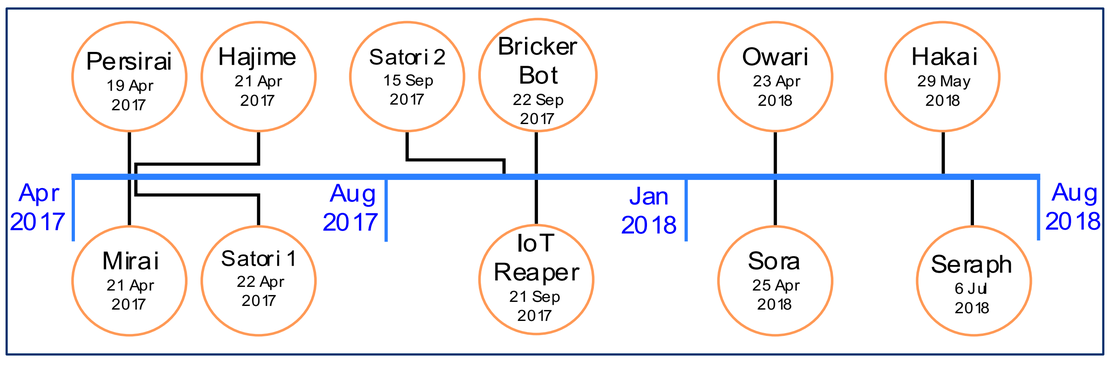
Amit Tambe [§], Samuel Marchal [§], Nils Ole Tippenhauer [†] and N. Asokan [§]

[§] Aalto University, [†] CISPA Saarland

Amplifying IoT honeypots with dynamic traffic replay

Motivation:

- Intensified attacks on IoT devices
  - BrickerBot, IoTReaper
- Plenty of vulnerable IoT devices deployed



[1]

- Honeypots can detect such large-scale attacks

Limitations of honeypots:

- Contain a few devices
  - limited vulnerability discovery
- Attack traffic targeted to single device
  - Device may not be vulnerable

Our goals:

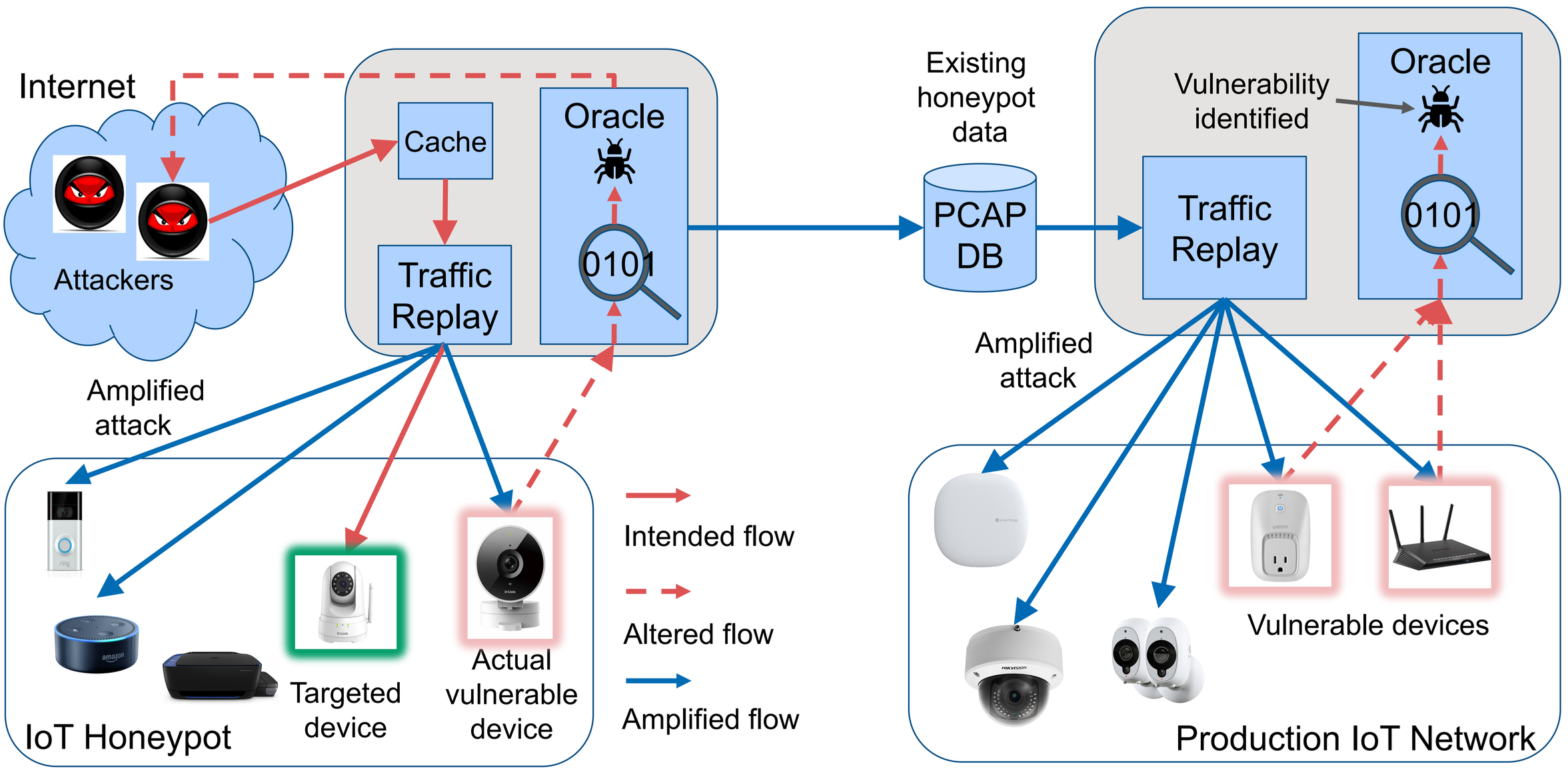
- Greater attacker engagement even with untargeted IoT devices - Traffic amplification
- Discover vulnerabilities in large number of IoT devices - Traffic replay

Traffic amplification in honeypot:

- Proxy to handle real-time traffic
- Classify malicious incoming traffic
- Cache – impede repetitive attacks
- Oracle – Identify vulnerabilities

Vulnerable devices discovery:

- Replay honeypot traffic in IoT network
- Identify vulnerable devices from responses
- Discover new vulnerable IoT devices (not in honeypot)



[1] Amit Tambe, Yan Lin Aung, Ragav Sridharan, Martin Ochoa, Nils Ole Tippenhauer, Asaf Shabtai, and Yuval Elovici. 2019. Detection of Threats to IoT Devices using Scalable VPN-forwarded Honeypots. (2019).

Aalto University

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY