Detecting Anomalies in IoT Device Communication Based on MUD Profiles with Zeek and Python

Rohan Nunugonda¹, Vyas Sekar², Matthew McCormack², Timothy Corica¹

The Peddie School¹, Carnegie Mellon University²

**Background: IoT and MUD**

**Problem: IoT Attacks On the Rise!**

- Hackers can "Faxploit" Connected Fax Machines
- RCE Vulnerability in Hikvision devices could lead to network compromise

**Goal: Log suspicious connections using MUD**

MUD: Manufacturer Usage Description

**Our Work: Synthesize IDS policies from MUD profiles**

**Workflow Diagrams**

- MUD Profile ➔ Python Parser ➔ Zeek Template ➔ Returns Log file
- Returns the List of Destination IPs
- Create Empty List destinationIP List
- Need to populate with allowed values
- Open MUD Policy JSON
- If line in MUD policy contains "destination-iplist-network".
- Strip Line & Add IP Network to destinationIP

**Full Project Workflow**

**Python Script Workflow**

```python
module amazonio;
export
  rebuf eminent LogID => { amazonio:LOG };
const allowed = set("4.3.2.1-2.2.2.1", "10.0.1.1-1.1.1.1", "2001:0:0:0:0:0:0:0:0/0", "2001::0:0:0:0:0:0/0", "0.0.0.0/0", "0.0.0.0/0");

type Info: record {
  tsi time blog;
  origin: addr Alog;
  stringsP: addr Alog;
  stringsPort: addr blog;
  dict;
};

function check_log[Log, ($$var$|Info);]
  event zeek listener[Log, ($$var$|Info)]:
  if ($$var$ in allowed)
    log.write[Log, Info][tsi:time blog,
    'origin: addr Alog;
    stringsP: addr Alog;
    stringsPort: addr blog;
    dict;]
}
```

**MUD ➔ Zeek**


**Future Work**

- Run Zeek Scripts with PCAP test data
- Automate scripts for real-time checks
- Use connection ports and protocol

**Acknowledgements**

- Dr. Vyas Sekar & Matthew – CMU mentors for research
- Dr. Peretz and Ms. Cozine – Peddie EXP mentors
- Mr. Corica and Ms. Wolfe – Peddie project mentors