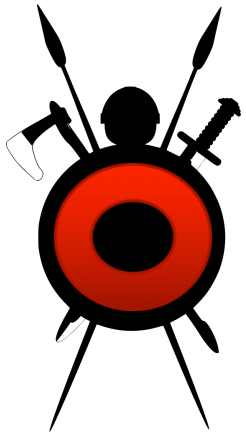


HANZO: Collaborative Network Defense for Connected Things

Aman Singh*, Shashank Murali*, Lalka Rieger[$], Ruoyu Li[$], Stefan Hommes[#], Radu State[#], Gaston Ormazabal[$], Henning Schulzrinne[$]

* Palindrome Technologies
[#] University of Luxembourg
[$] Columbia University

IPTComm 2018, October 16-17, Chicago, USA

Agenda

- Motivation - IoT Landscape
- Manufacturer Usage Description (MUD)
- Home Area Network Zero Operations (HANZO)*
  - System Model & Architecture
  - System Implementation & Evaluation
- Conclusions
- Future Work

*https://en.wikipedia.org/wiki/Hattori_Hanzo

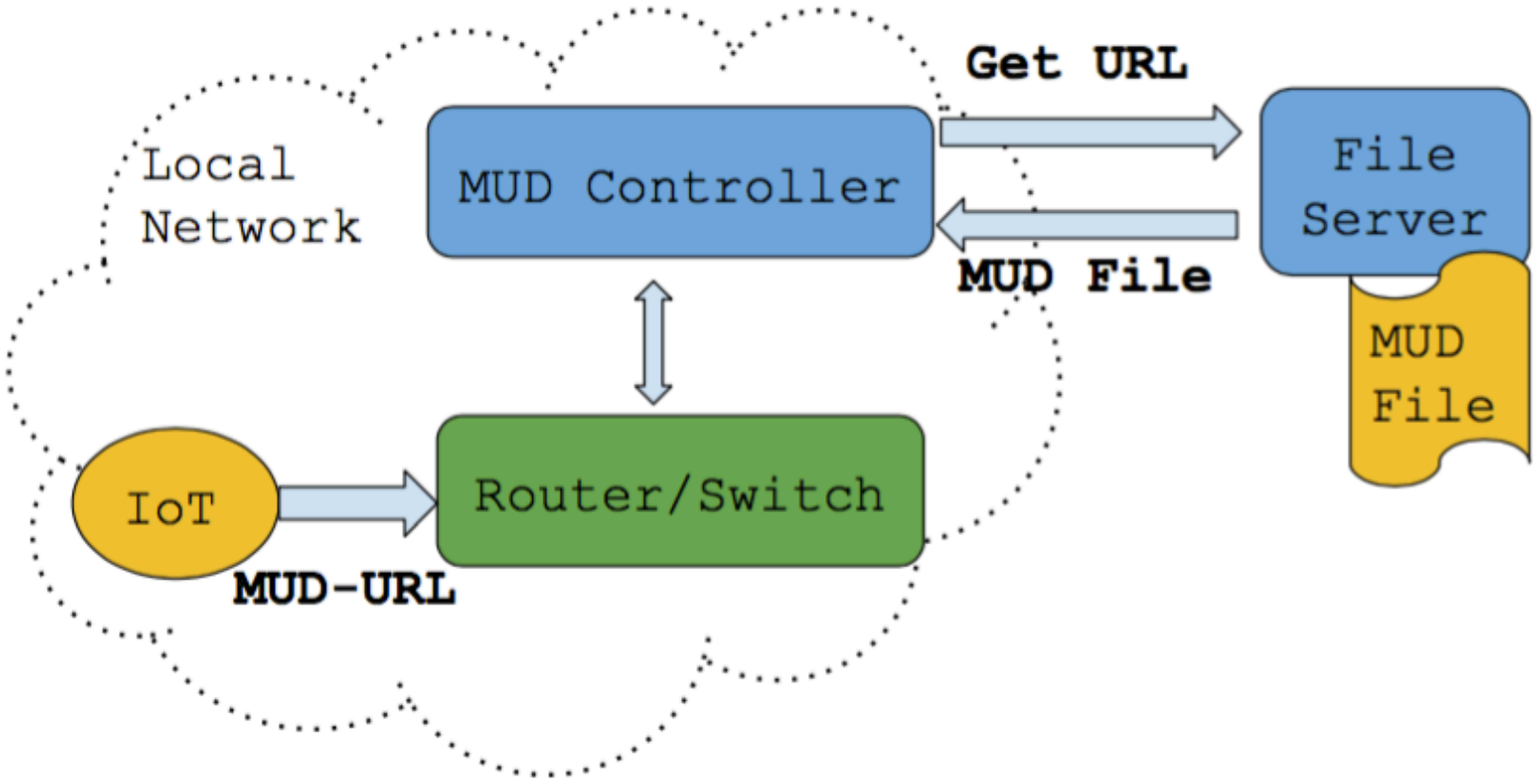
IoT Landscape

- Things everywhere
- Insecure default configurations
  - Passwords
  - Protocol configurations
- Attacks
  - Mirai vs. Hajime
  - Cryptocurrency Mining
  - Crime Proxies
  - Ransomware
  - Data Theft
- Home vs. Enterprise

Good Things

- Limited functionality
  - Sense – Communicate – Actuate
  - Communication endpoints
- Device manufacturers
  - Management
  - Notifications

Manufacturer Usage Description



*https://tools.ietf.org/html/draft-ietf-opsawg-mud-25

MUD Profile

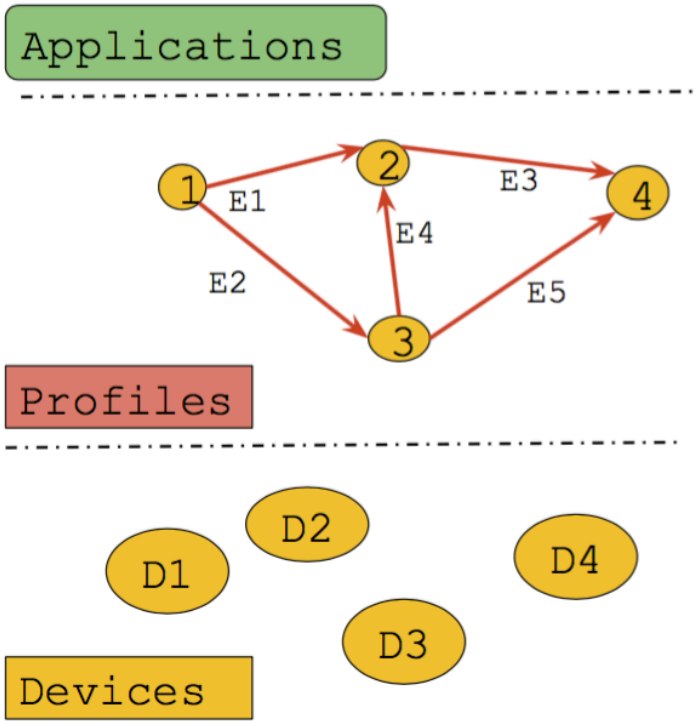
```
"ietf-mud:mud":
      "mud-version": 1
      "mud-url": "https://lighting.example.com/lightbulb2000"
      "last-update": "2018-03-02T11:20:51+01:00"
      "cache-validity": 48
      "is-supported": true
      "systeminfo": "The BMS Example Lightbulb"
      "from-device-policy":
        "access-lists":
          "access-list":
              "name": "mud-76100-v6fr"
       "to-device-policy":
        "access-lists":
          "access-list":
              "name": "mud-76100-v6to"
"ietf-access-control-list:acls":
      "acl":
        "name": "mud-76100-v6to"
        "type": "ipv6-acl-type"
        "aces":
          "ace":
            …….....
            "matches":
                "ipv6":
                  "ietf-acldns:src-dnsname": "test.example.com"
                "tcp":
                    "ietf-mud:direction-initiated": "from-device"
             "actions":
                  "forwarding": "accept"
        "name": "mud-76100-v6fr"
        "type": "ipv6-acl-type"
        "aces":
          "ace":
            …….....
              "matches":
                "ipv6":
                  "ietf-acldns:dst-dnsname": "test.example.com"
                "tcp":
                  "ietf-mud:direction-initiated": "from-device"
                "actions":
                  "forwarding": "accept"
```

HANZO* Controller

- Current IoT devices are not MUD enabled
- Create MUD Profile by traffic observation
- MUD Manager functionality
  - DHCP / MUD-URL String / Option Header 161
- Small networks
- Zero network operations

System Model

- Network-first Approach
- Devices
- Profiles – {Edges} → Communication constraints
- Applications



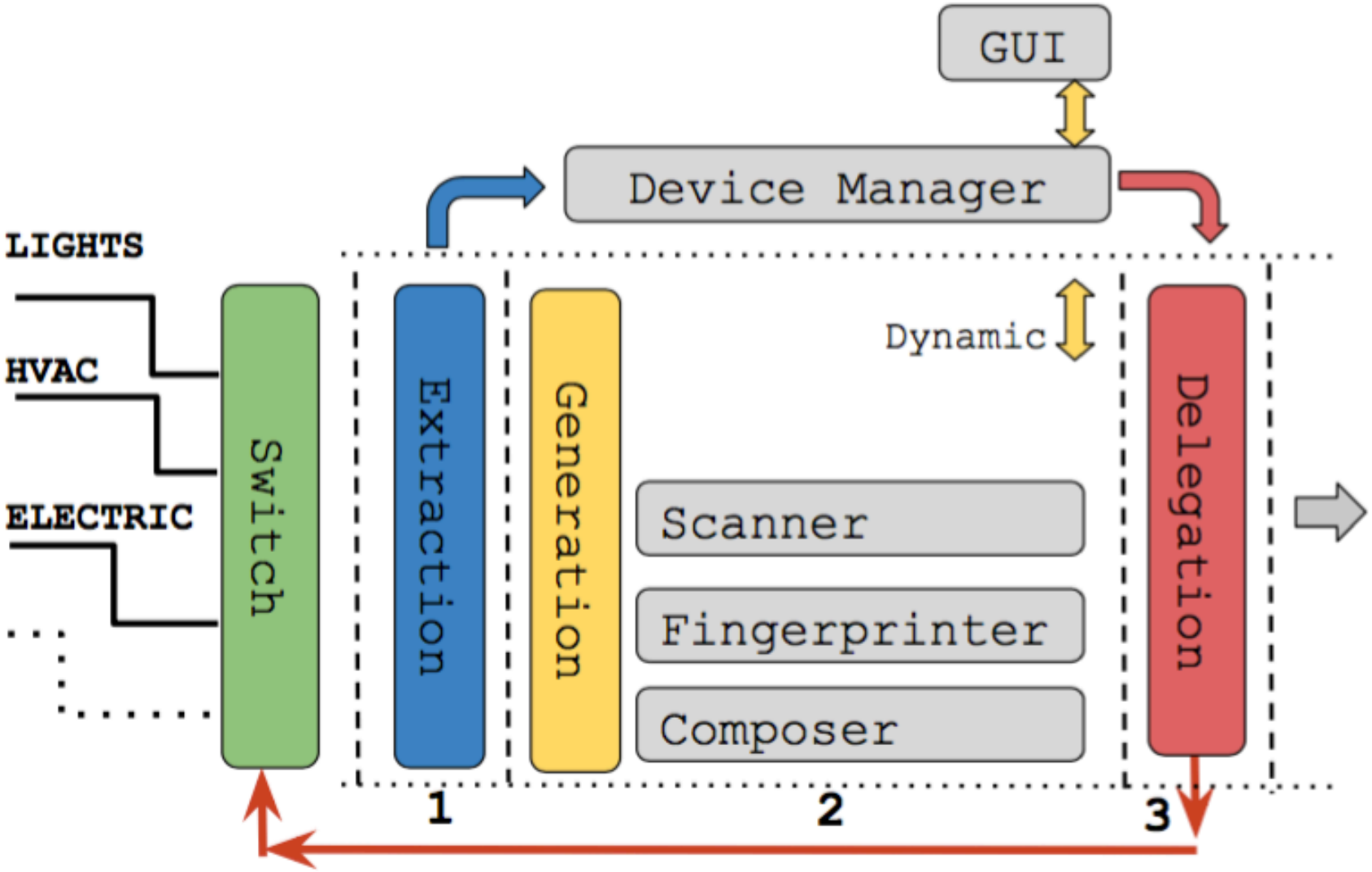
Device States

- Registration
- Configuration
- Operation
- Maintenance
- Quarantine

Home Network Testbed

Network	Device	Type	Quantity
Electric	LoneyShow	Plug	4
	VOCOLinc	Plug	2
	UPSTONE	Power Strip	1
Light	TP-Link	Light Bulb	2
	Sengled	Light Bulb	2
	UPSTONE	Light Bulb	1
Presence	EZVIZ	Camera	1
	Wansview	Camera	1
	iHome	Motion	1
HVAC	iHome	Temperature	1
	Honeywell	Fan	1
Data	ASUS	Access Point	1
	Apple	Phone	2
	Samsung	Phone	1
	Google	Streamer	1
	Amazon	Speaker	1
	Apple	Laptop	1
	Lenovo	Laptop	1
	Lexmark	Printer	1

System Architecture



System Phases

- Monitoring
  - Metadata
  - Endpoints
- Categorization
  - IoT vs General
- Enforcement

Device Metadata

- Link Layer – MAC
  - First 3 bytes are manufacturer identifier (OUI)
- DHCP Options Headers
  - Option 55 – Parameter Request List
  - Option 60 – Vendor Class Identifier
- DNS
  - Capture DNS request sequences
- WHOIS records
  - Manufacturers information

```
--------------------
DHCP Broadcast
--------------------
Session
('message-type', 1)
('client_id', '\x01\x00!\xb7\xfa\x92L')
('max_dhcp_size', 576)
('lease_time', 4294967295)
('requested_addr', '128.59.16.127')
('hostname', 'schedule\x00')
('param_req_list', '\x01\x03*\x04\x06\x07\x0c\x0f\x1a,36:;\xbe')
('vendor_class_id', 'Mfg=DELL;Typ=Printer;Mod=Dell 3330dn Laser Printer;Ser=7226FT5;')
{'manufacturer': u'LexmarkI', 'os': '', 'device_type': u'Lexmark Printer', 'mac_address': '00:21:b7:fa:92:4c'}
```

Metadata Observation

Vendor	OUI	WHOIS	OS
EZVIZ	AmpakTec	Nexperian	Linux
WANSView	Shenzen	Null	Linux
iHome	Azurewav	Evrythng	Java ME
LoneyShow	Espressi	Hangzhou	Null
Tp-Link	TP-LINK	TP-LINK	Null
Sengled	Espressi	Sengled	Null
Apple	Apple	Apple	iOS
Samsung	Samsung	Samsung	Android

Communication Endpoints

- Limited endpoints for IoT devices
- Converge quickly

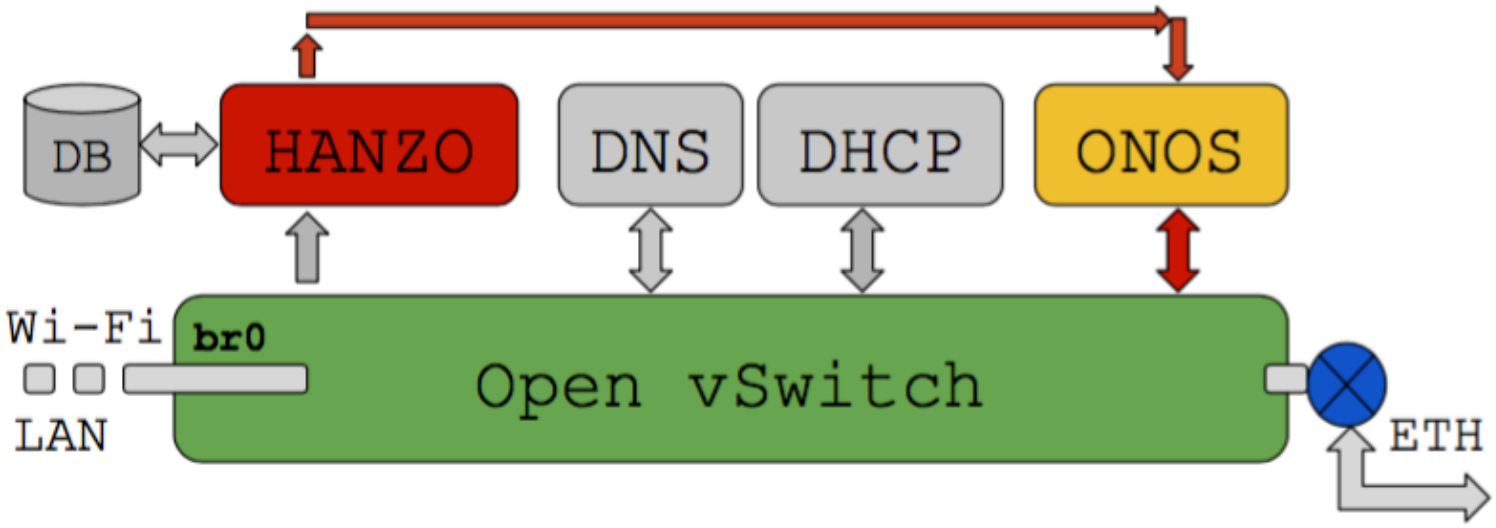
Device	1 min	5 min	10 min	20 min	30 min	60 min
EZVIZ/Camera	3	3	4	4	4	4
WANSView/Camera	3	4	10	10	10	10
iHome/Monitor	4	4	4	4	4	4
UPSTONE/Plug	4	4	4	4	4	4
TP-LINK/Light Bulb	2	2	2	2	2	2
Sengled/Light Bulb	2	2	2	2	2	2

Signature - IoT vs. General

- Supervised binary classfication
  - Support Vector Machines
- Network traffic context
  - Link – Frame headers
  - Network – IP headers
  - Transport – port, rate, size, sent/recv, count, inter-arrival
  - Application – DNS, HTTP, MQTT, DHCP

Implementation

1. Extraction – TCPDump with Python Scapy
2. Generation – Python modules with pub-sub event-bus
3. Delegation – ONOS Controller & Open vSwitch



Evaluation – Signature & Endpoints

Device	Type	IoT	Profile	#Endpoints
LoneyShow	Plug	Yes	Yes	2
VOCOLinc	Plug	Yes	Yes	2
UPSTONE	Power Strip	Yes	Yes	4
TP-Link	Light Bulb	Yes	Yes	2
Sengled	Light Bulb	Yes	Yes	2
UPSTONE	Light Bulb	Yes	Yes	6
EZVIZ	Camera	Yes	Yes	4
Wansview	Camera	Yes	Yes	10
iHome	Motion	Yes	Yes	4
iHome	Temperature	Yes	Yes	4
Honeywell	Fan	Yes	Yes	2
ASUS	Access Point	No	No	-
Apple	Phone	No	No	-
Samsung	Phone	No	No	-
Google	Streamer	No	No	-
Amazon	Speaker	Yes	Yes	18
Apple	Laptop	No	No	-
Lenovo	Laptop	No	No	-
Lexmark	Printer	Yes	Yes	4

Evaluation - Metadata

- MAC manufacturers are different from device
- No DHCP Option Headers on most IoT devices
- Device request sequences do not change
  - NTP servers – NIST, …
  - Cloud services – AWS, Azure, …
  - Manufacturer servers
  - Unencrypted MQTT brokers

Conclusions

- IoT communication endpoints are limited & converge quickly
- Easy to white-list valid network endpoints
- No single method for IoT device metadata
- Continuous security monitoring
  - Device compromise detection

Future Work

- Porting to OpenWRT
- netfilter enforcement support
- Crowd-sourcing device configuration

Questions?