Securing homenets in the IoT

Cristian Hesselman

BotLeg Workshop | Amsterdam | June 1, 2018
Internet of Things

• Trillions of (tiny) special-purpose devices

• Continually sense and act upon users’ physical environment

• Encode people’s offline activities and send over the Internet

• Novel (data analysis) applications to ease our lives
  • Domains: human, home, retail, offices, factories, work sites, vehicles, cities, outside (ISOC)
  • Apps: health control, disease management, safety systems, energy control, traffic control
IoT devices widely heterogeneous

- Often tailored to a specific task (e.g., lighting, traffic sensing)
- Varying capabilities (hard/software, OS, configurations, UI)
- Autonomous operation (unattended, extended periods of time)
- Invisibly integrated into physical structures
- Intermittent connectivity (to the Internet and between devices)
- Cross-device interactions (networked or physical)
- Often no security protocols (e.g., SSL/TLS) or weak crypto
- Many manufacturers from various industries
- Many operators with widely varying networking skills
Example: device capabilities

Most attractive to attackers, because limited user interaction
IoT-powered DDoS attacks (Mirai)

https://www.arbornetworks.com/blog/asert/netscout-arbor-confirms-1-7-tbps-ddos-attack-terabit-attack-era-upon-us/
SPIN = Security and Privacy for In-home Networks

Protect the Internet/DNS (sources of DDoS attacks) and end-users
Research and prototyping
SPIN = open platform
SPIN position and targeted use

**Research**
- IoT anomalies (TUD, UT, OU)
- Pilots with end-users
- Course Security Services for the IoT (4TU M.Sc. CyberSec)
- M.Sc. projects
- Publications

**Example:** researchers using SPIN as a platform to develop and evaluate new botnet detection algorithms

**SPIN prototype**
- Platform (building block)
- Applications
- IoT security expertise
- Open source software

**Example:** an ISP interested in adding SPIN to their router software to further increase security of their customers

**New services**
- Applications built on top of SPIN platform
- By SIDN or other orgs
- Open or closed source
- Challenge: adoption

**Standaardization**
- IETF (e.g., Manufacturer Usage Descriptions)
- IoT working groups at SSAC and RIPE
SPIN implementation (May 2018)
Prototype

- Currently bundled with Valibox: http://valibox.sidnlabs.nl

- Source at https://github.com/SIDN/spin
SPIN privacy manager (a.k.a “visualizer”)

[Diagram of SPIN Traffic monitor prototype]
Ongoing work

SPIN agent + traffic network measurement facility

SPIN project

- Visualizer
- Profiles concept
- Profiles implementation (MUD)
- Anomaly Detection
- Incident Report System
Anomaly detection

- Status: “anomaly detector” fires if a device scans more than X addresses-port combinations in Y seconds and then blocks the device

- Goal: provide framework that enables researchers and 3rd parties to plug in anomaly detectors + include one or two examples

- Model and analyze traffic, and create and test anomaly detection approaches

- Status: early implementation in Go, live stream of data available over MQTT, historic data in (local) database
MUD profiles

- Manufacturer Usage Description (MUD), IETF Internet Draft
- JSON description of internet traffic that is or is not allowed from and to the device
- Translates almost directly to firewall rules
- Our work: automatic generation and extensions (e.g., add a bandwidth limitation or enable user-enriched profiles)

```
"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",
}
...
"name": "mud-76100-v6fr",
"type": "ipv6-acl-type",
"aces": {
  "ace": [
    {
      "name": "cl0-frdev",
      "matches": {
        "ipv6": {
          "ietf-acldns:dst-dnsname": "test.example.com",
          "protocol": 6
        },
        "tcp": {
          "ietf-mud:direction-initiated": "from-device",
          "destination-port": {
            "operator": "eq",
            "port": 443
          }
        }
      },
      "actions": {
        "forwarding": "accept"
      }
    }
  ]
}
```
Incident reporting system

AbuseHub

Abuse 192.0.2.123

ISP1
ISP2
ISP3
ISP4

home network 1
home network 2 (192.0.2.123)
home network 3

device1
device2
device3
device4

Abuse to 192.0.2.1 at <time>
Running prototype (v0.1)

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Destination address</th>
<th>Destination port</th>
<th>Source address</th>
<th>Source port</th>
<th>Severity</th>
<th>Type</th>
<th>Name</th>
<th>Notify</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1524581768</td>
<td>178.18.82.80</td>
<td>443</td>
<td>213.124.176.76</td>
<td>123</td>
<td>3</td>
<td>auto-generated for demo</td>
<td>demomalware</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1524582719</td>
<td>178.18.82.80</td>
<td>443</td>
<td>213.124.176.76</td>
<td>123</td>
<td>3</td>
<td>auto-generated for demo</td>
<td>demomalware</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1524582757</td>
<td>178.18.82.80</td>
<td>443</td>
<td>213.124.176.76</td>
<td>123</td>
<td>3</td>
<td>auto-generated for demo</td>
<td>demomalware</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1524582818</td>
<td>178.18.82.80</td>
<td>443</td>
<td>213.124.176.76</td>
<td>123</td>
<td>3</td>
<td>auto-generated for demo</td>
<td>demomalware</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Summary

• Open platform for IoT security in homenets for researchers and developers

• Aims to protect the Internet and end-users

• Key challenge: maximize deployment

• Work ahead: pilot, extend prototype, IETF, talk to ISPs/manufacturers
Potential legal-tech talking points

- Implications of temporarily limiting traffic to and from IoT devices
- Implications of fine-grained filtering vs. quarantining homenets as a whole
- Sharing security info (e.g., DDoS fingerprints) with SPIN devices
- Gathering (partial) DDoS fingerprints at SPIN devices
- Perhaps enough substance for a follow-up project?
Questions and discussion