# Beyond Telnet: Prevalence of IoT Protocols in Telescope and Honeypot Measurements

**Lionel Metongnon**[12] Ramin Sadre[1]

SIGCOMM-WTMC, 20th August 2018

[1]Institute of Information and Communication Technologies, Electronics and Applied Mathematics
Université catholique de Louvain, Belgium

[2]Institut de Formation et de Recherche en Informatique, Benin
Université d'Abomey-Calavi

# Internet of Things

**Definition**
IoT is a whole heterogeneous world with many services, devices and communication types as : Machine-to-Human communication (M2H), Radio Frequency Identification (RFID), Lab-on-a-Chip (LOC) sensors, Machine-to-Machine (M2M), etc.

- The IoT concept is an **evolution** of classic internet technologies;
- Many threats are **growing** with IoT (privacy invasion, DDoS attacks, ...);

# General challenges

- Many devices are present with a forecast of **50 billions** until 2020[2];
- Many Operating systems involved (Android, Contiki, RiOT, Windows, IOS, ...) and constrained OS **lack of security** requirements[2, 5];..;
- **Management difficulties** of devices (system upgrade and protection) ;
- Many different **data protocols** are used such as HNAP, HTTP, UPnP, CoAP, MQTT, AMQP, many proprietaries protocols, ...;
- New types of securities issues with nodes **online 24/7**.

# Motivation

## Motivation

We have seen a rise of powerful attacks originating from IoT devices in the last years (Mirai , Hajime, BrickerBot)[1, 4]. However, they are all using telnet protocol as vector.

Are any IoT specific protocols used to perform attacks nowadays ?

The question is important for designers of intrusion detection systems.

# Setup i

- The experiment run from 2017-09-01 to 2018-02-28 with some interruption due to technical difficulties, maintenance and security updates (Meltdown/Spectre);
- We used a setup with /15 network telescope to gain a global view of internet traffic;
- We used a setup with three honeypots (Cowrie, Dionaea, Honeypy) paired with 15 IPv4 addresses;

# Setup ii

- Cowrie is a middle-level honeypot with **ssh** and **telnet** protocols exclusively;
- Dionaea is a low-level honeypot used for **UPnP**, **HTTP**, **HNAP** and **MQTT** traffic;
- No CoAP honeypot exists until now so we used a prototype to interact properly with this protocol;

# Results i


**Figure 1:** Number of packets per day reaching the telescope. Note the scaling factor of 10 7 for the y-axis

# Results ii

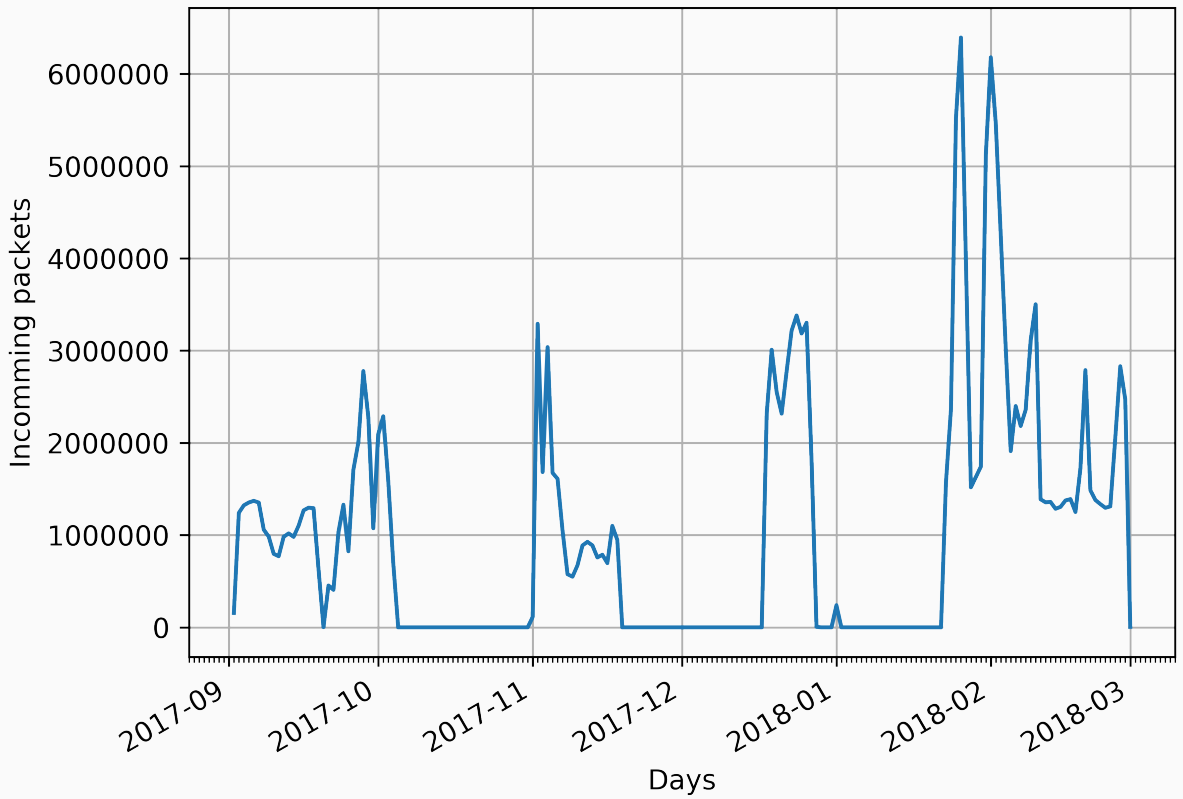


**Figure 2:** Number of packets per day reaching the honeypots

# Results iii

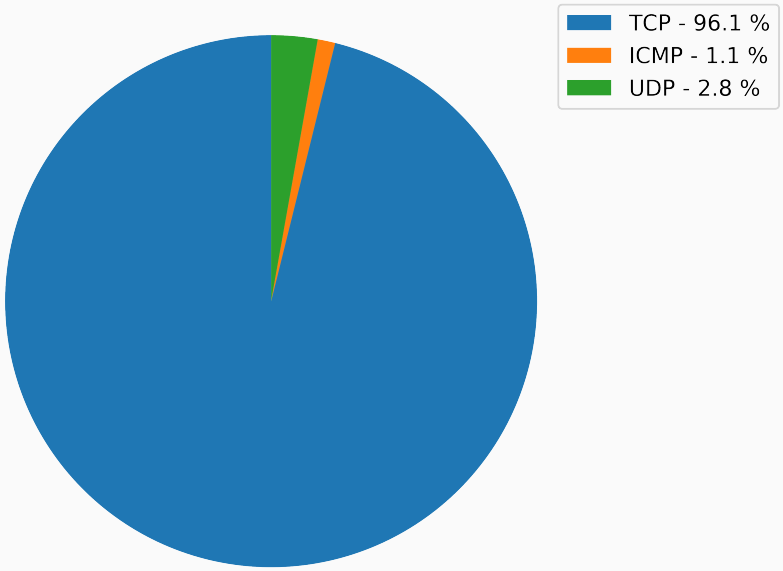


**Figure 3:** Protocols distribution of the telescope

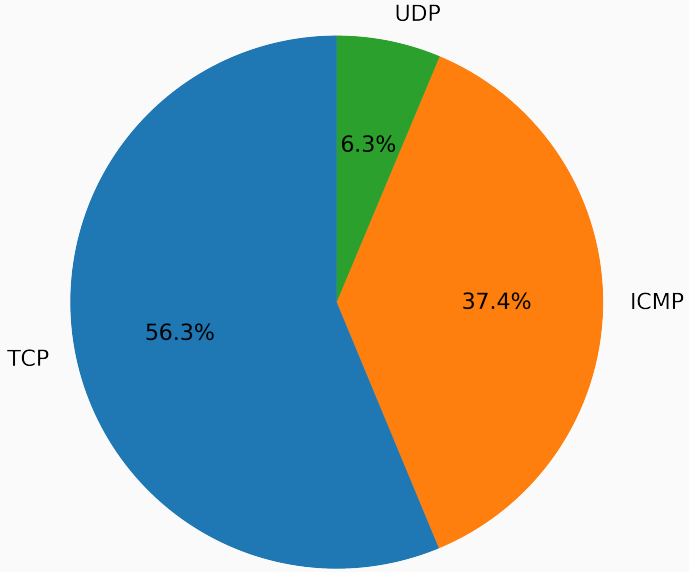


**Figure 4:** Protocols distribution of the honeypots

# Results iii

- A total of **68,031,379** probes were sent from only **2,355** different source addresses;
- Only **46.88%** of these addresses also sent TCP traffic and only **14.18%** sent UDP traffic ;
- **35 sources IP** send more than a million probes.

# Results iv

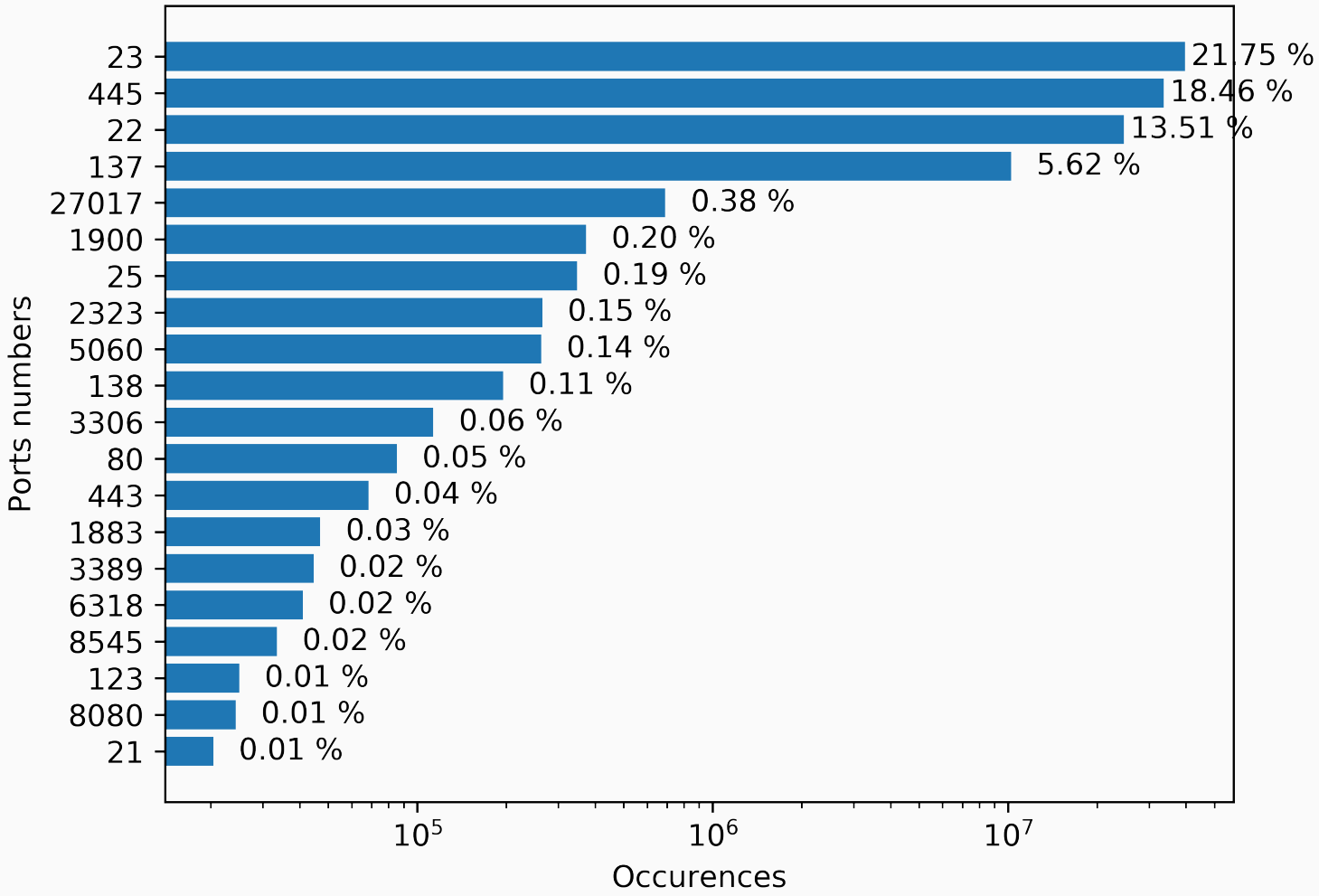


**Figure 5:** Ports access frequency of the honeypots

# Results v

- Many attempts on telnet with distinct procedure for mirai-malware infection are present, coupled with crypto-currency mining system;
- HTTP traffic is used to compromised home routers through CGI, we have Cisco, Linksys, and D-Link routers as targets;
- Cisco's HNAP protocol for the management of home networks is also targeted;
- Many attempts using UPnP's service discovery protocol (SSDP) to get network topology;

# Results vi

- MQTT is only a little bit targeted because the current honeypot is not interactive enough, a work is started with master student to improve it;
- Only one CoAP' command is used so the protocol is not yet fully exploited. This command is the standard resource **/.well-known/core** which allows to obtain the list of available resources from a server.

# Take away

- IoT brings many new challenges to the security world;
- Many protocols are currently exploited in IoT, not only telnet;
- However, telnet is still the most popular because it is so easy to attack;
- Hacked machines used for crypto-currency mining;
- Monitoring and improving honeypots supports will enhance our understanding of future threats;
- However, it is not a long term solution to understand all IoT threats.

Thank you for your attention !!!

Questions, Remarks

# Bibliography i



E. Bertino and N. Islam.
**Botnets and internet of things security.**
*Computer*, 50(2):76–79, 2017.


J. Frahim, C. Pignataro, J. Apcar, and M. Morrow.
**Securing the internet of things: A proposed framework.**
`https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html`.
Accessed: 2017-03-31.


L. Metongnon, C, and R. Sadre.
**Beyond telnet: Prevalence of iot protocols in telescope and honeypot measurements.**
ACM/SIGCOMM, 2018.

# Bibliography ii


Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow.
**Iotpot: analysing the rise of iot compromises.**
*EMU*, 9:1, 2015.

T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu.
**Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things.**
In *HotNets 2015*, 2015.