Tracing IoT devices for anomaly detection purposes

Robin Gassais

December 7, 2017

École Polytechnique de Montréal

DORSAL lab

Agenda

Context

- IoT – Smart Home

Approach

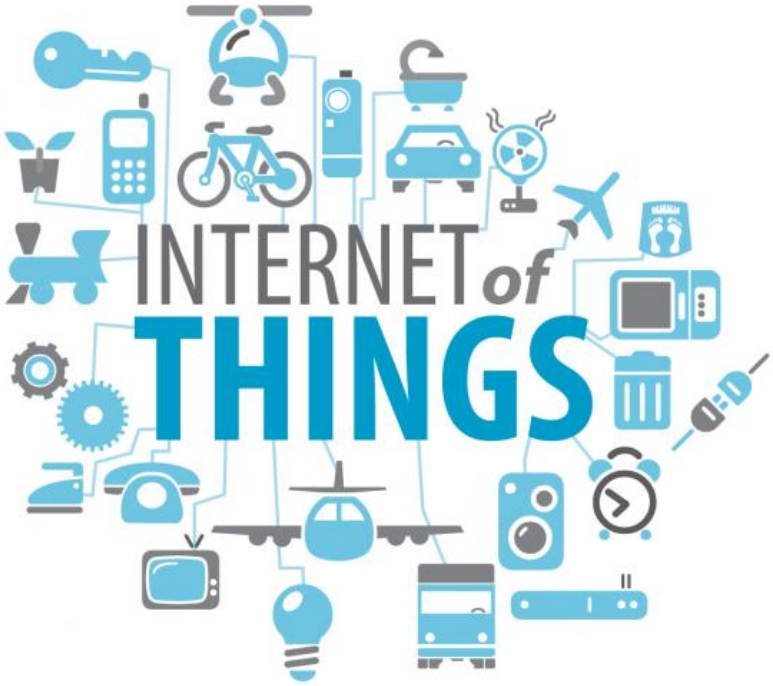
- Tracing multiple systems
- Analyzing multiple traces

Use-case

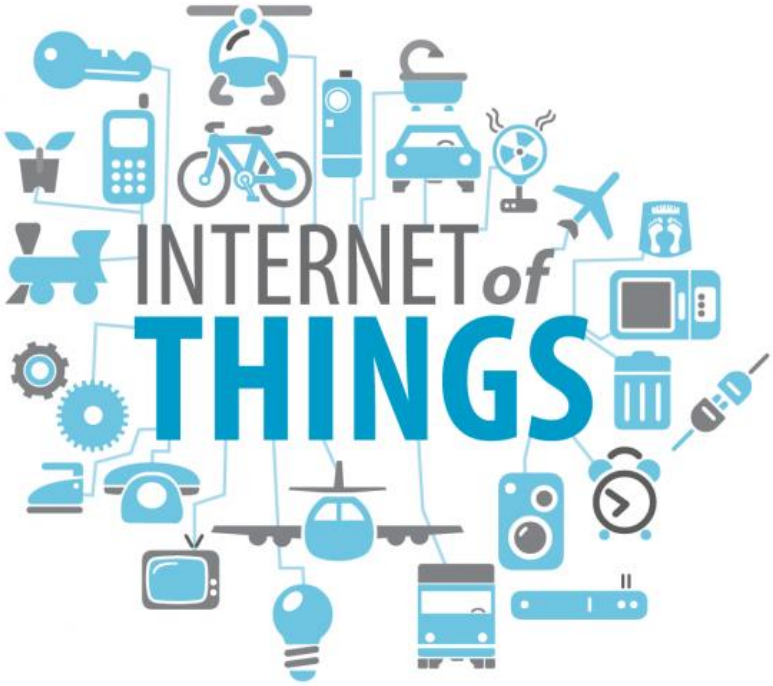
- Mirai botnet

Future Work

Context



Context



- Embedded Linux based systems
- Limited resources
- 20 billions of smart devices in 2020
- Heterogeneous market

Approach

Tracing multiple systems

- ARM virtual machine
- Central device to collect and analyse the traces
- Safe communication : SSH

Approach

Tracing multiple systems

Lttng - relayd

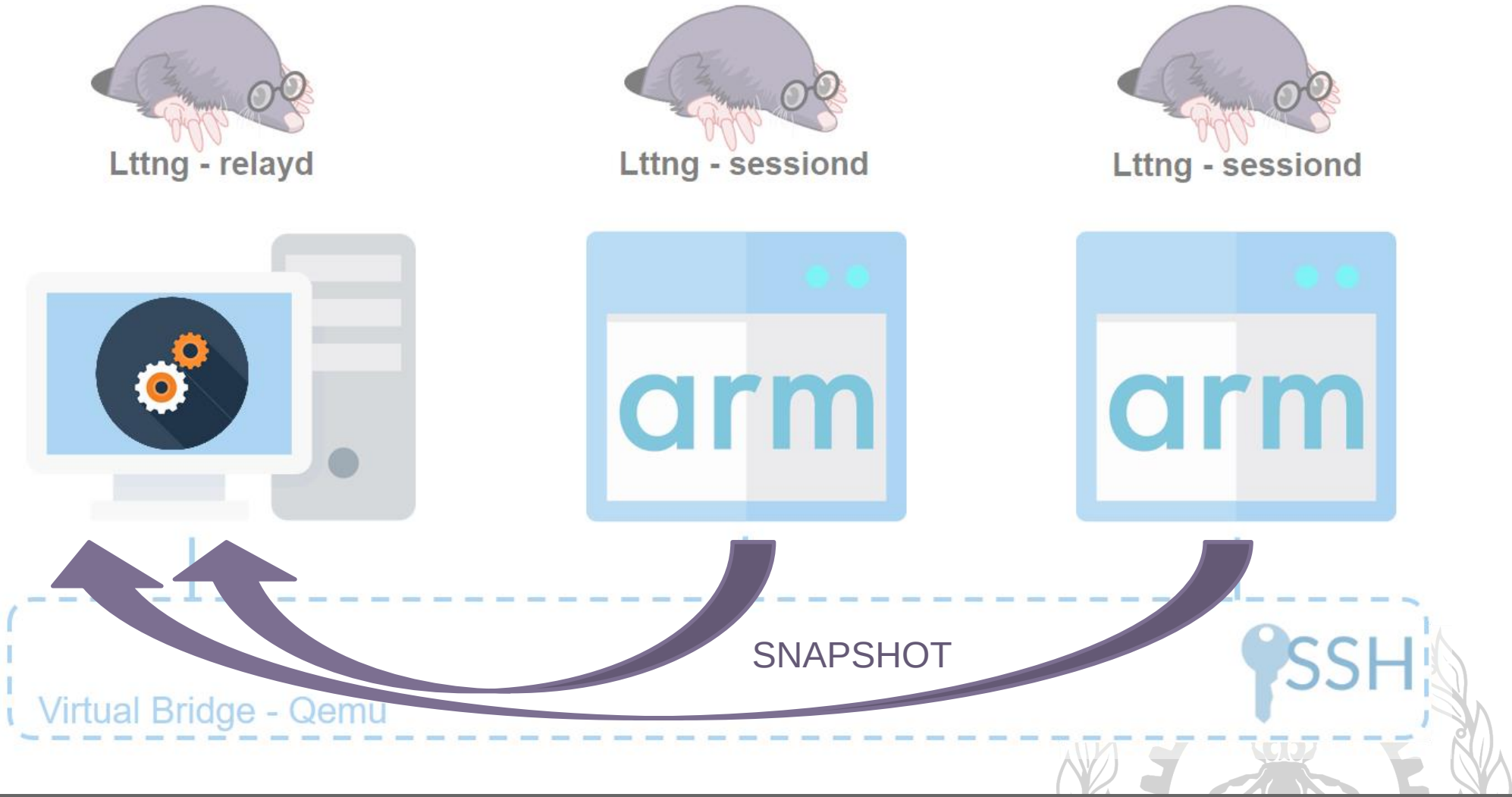
Lttng - sessiond

Lttng - sessiond

Virtual Bridge - Qemu

Approach

Tracing multiple systems



Approach

Analyzing multiple traces

?

- What to monitor?
- How to monitor anomalies?

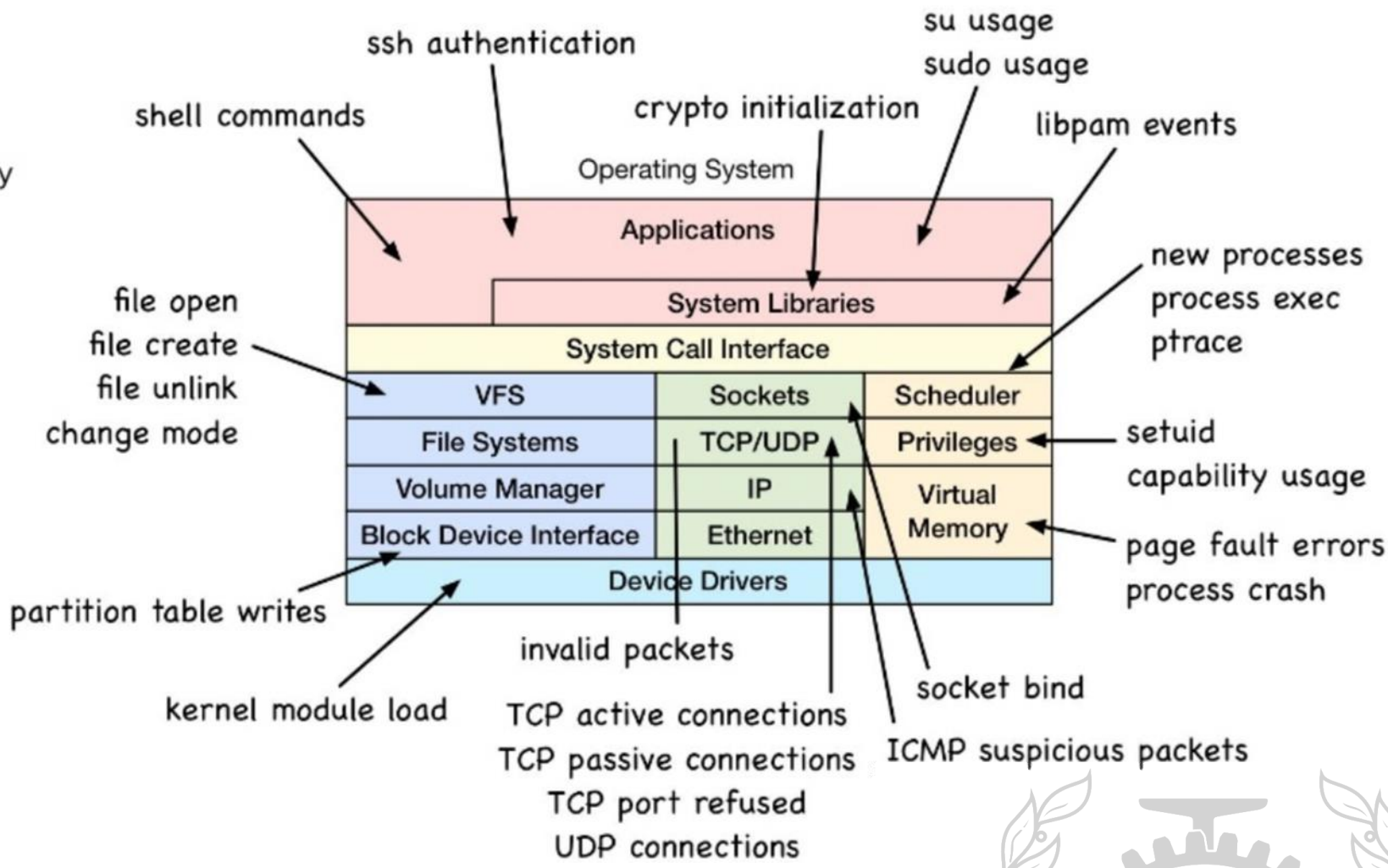
Approach

Analyzing multiple traces

WHAT TO MONITOR

Trace low-frequency events wherever possible to lower overhead

Eg, TCP connection init; not TCP send/receive



Source : Slideshare - **Security Monitoring with eBPF** - Alex Maestretti, Brandan Gregg

Approach

Analyzing multiple traces

Babeltrace

- What to monitor?
- How to monitor anomalies?

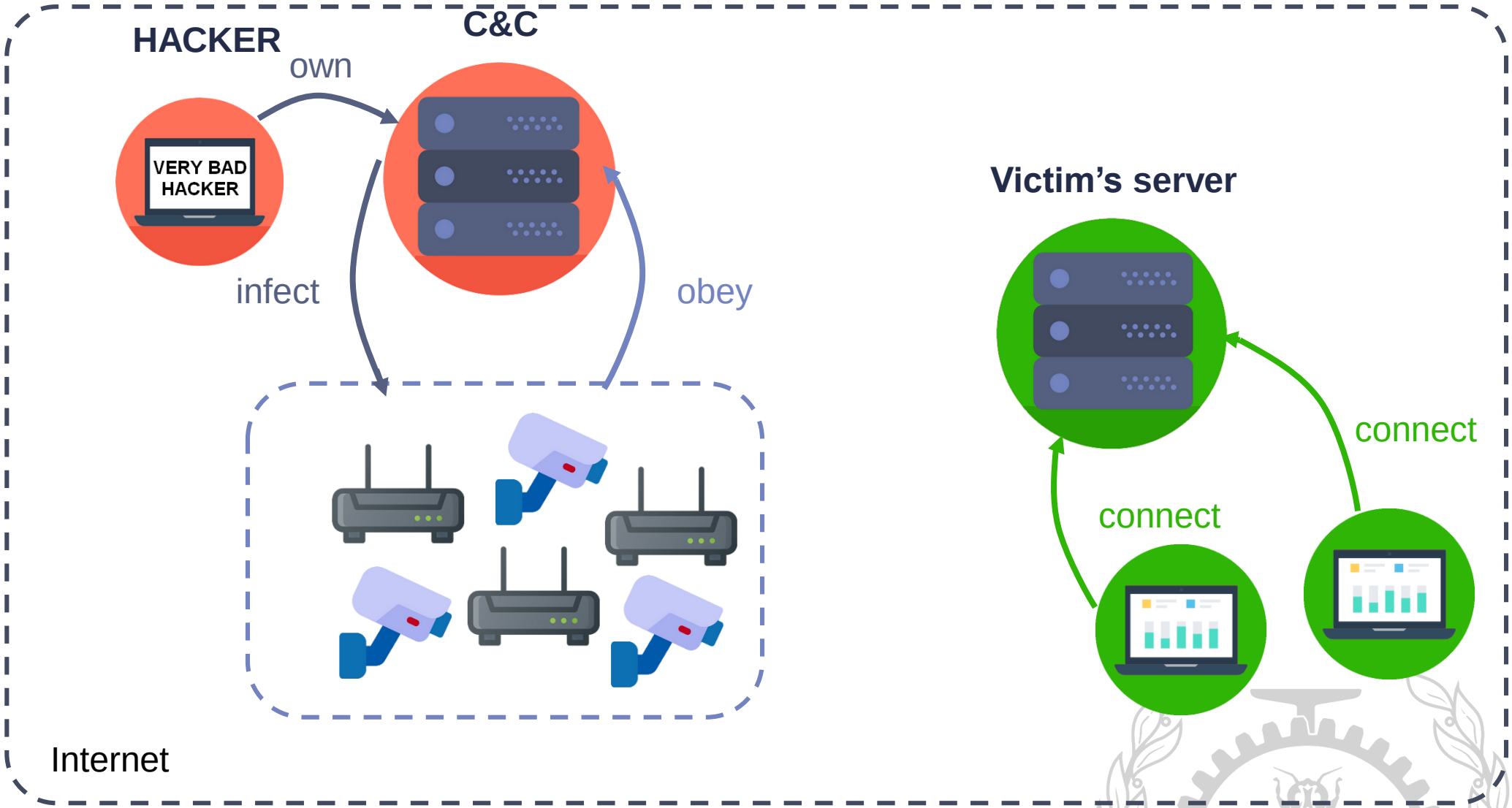
Use-case

What's Mirai?

- Biggest DDoS attack ever seen : 3 Tbps, 500 000 devices
- IP surveillance camera, video recorder, router
- Twitter, Ebay, Netflix, Github, Paypal down via Dyn DNS

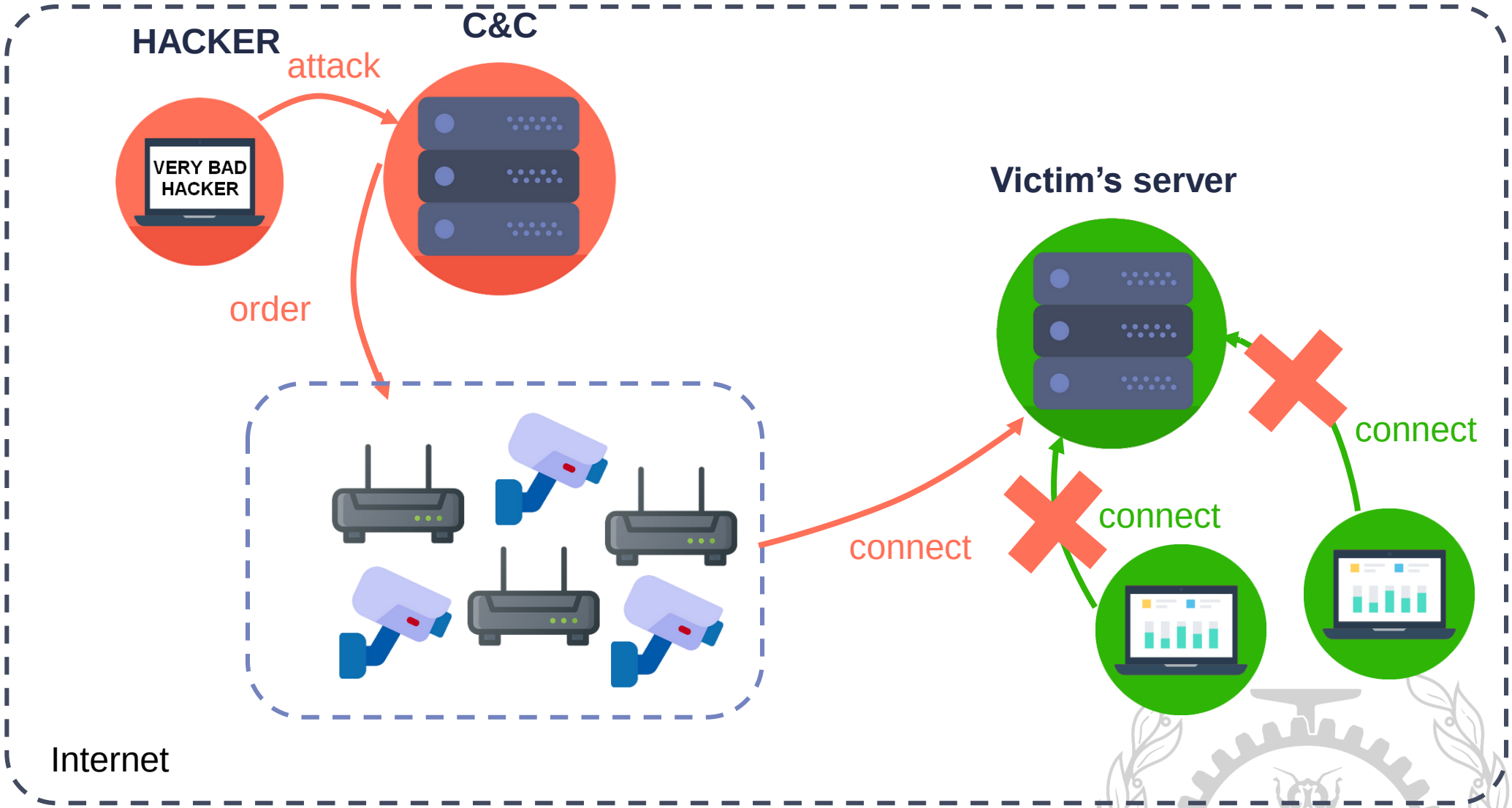
Use-case

What's Mirai?



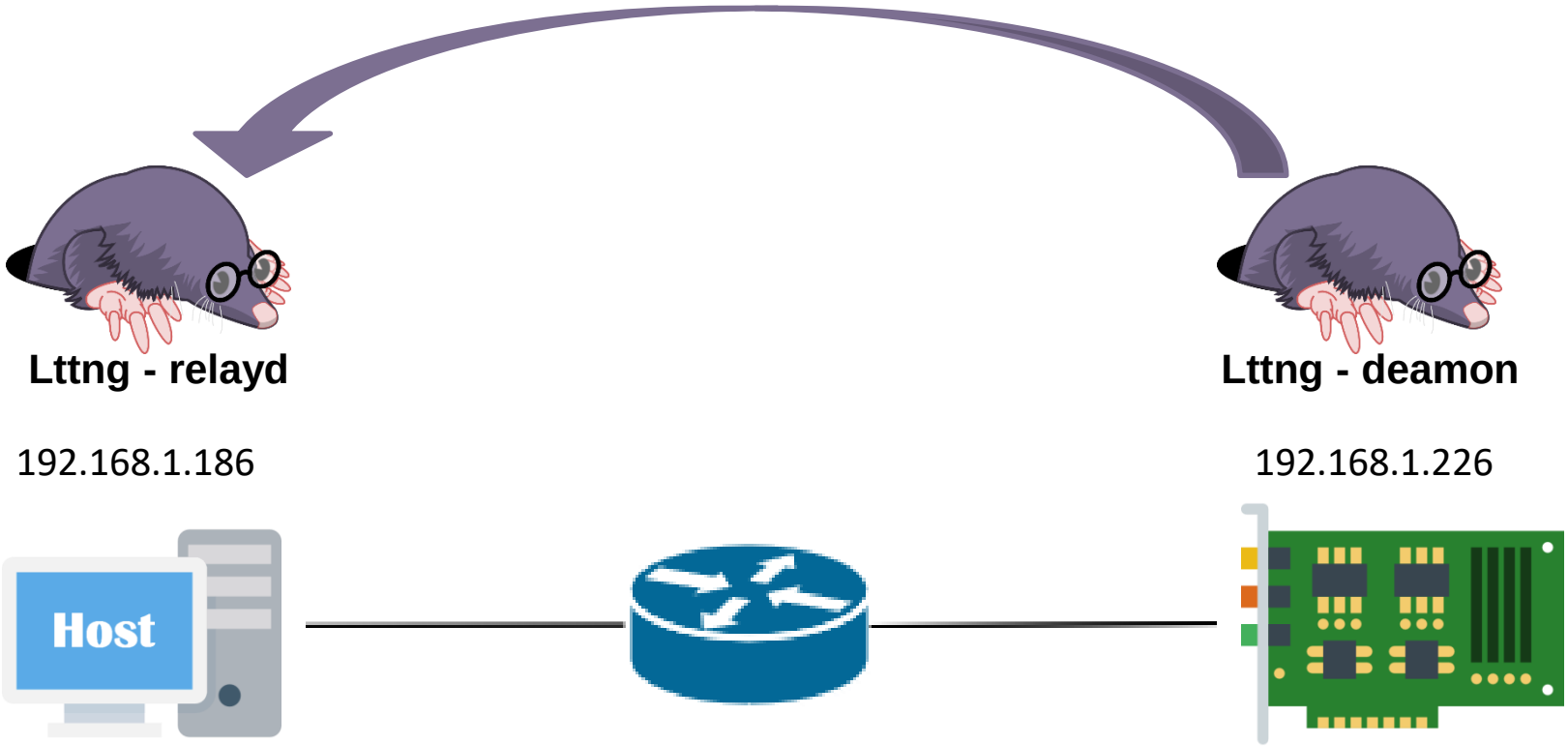
Use-case

What's Mirai?



Use-case

Experiment



Use-case

Results

Mirai

- Telnet -> upload file -> chmod on it : **14,9 s**

  Using all the kernel tracepoints – live mode

Now

- Chmod on a new created directory: **1,33 s**

  execve, faccessat, chmod – snapshot mode (send 1s)

- Chmod on a new created directory: **0,98 s**

  faccessat, chmod – snapshot mode (send 0,7s)

No Network, not physical devices

Use-case

Results

Future work

- Detection rules? Machine learning?
- Physical objects
- Tradeoff between snapshot frequency, nomber of tracepoints to monitor and performance of the device

Thank you!

Questions? Suggestions? Solutions?

robin.gassais@polymtl.ca