



# 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







# 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

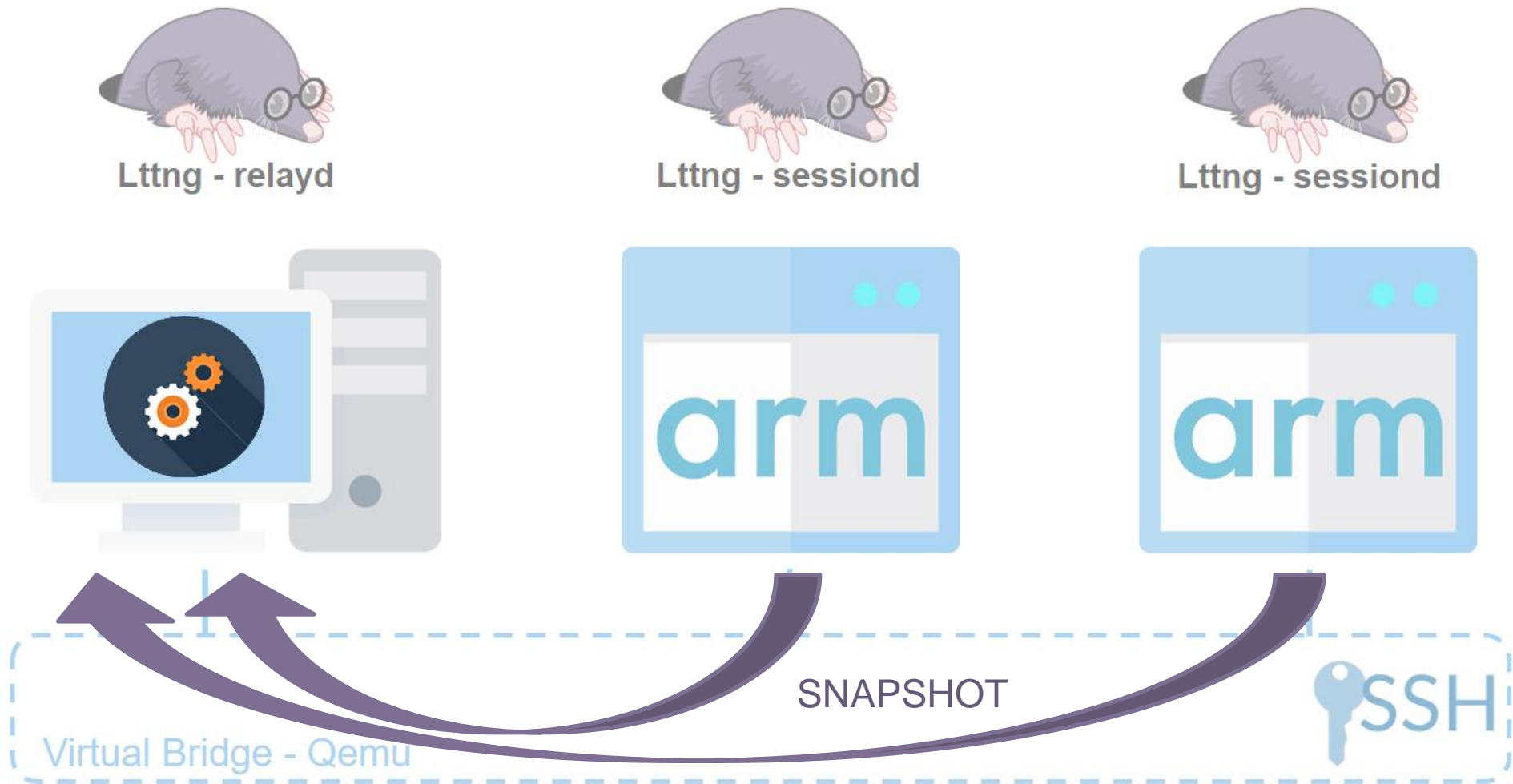


Virtual Bridge - Qemu



# Approach

## Tracing multiple systems



# Approach

---

## Analyzing multiple traces



- What to monitor?
- How to monitor anomalies?





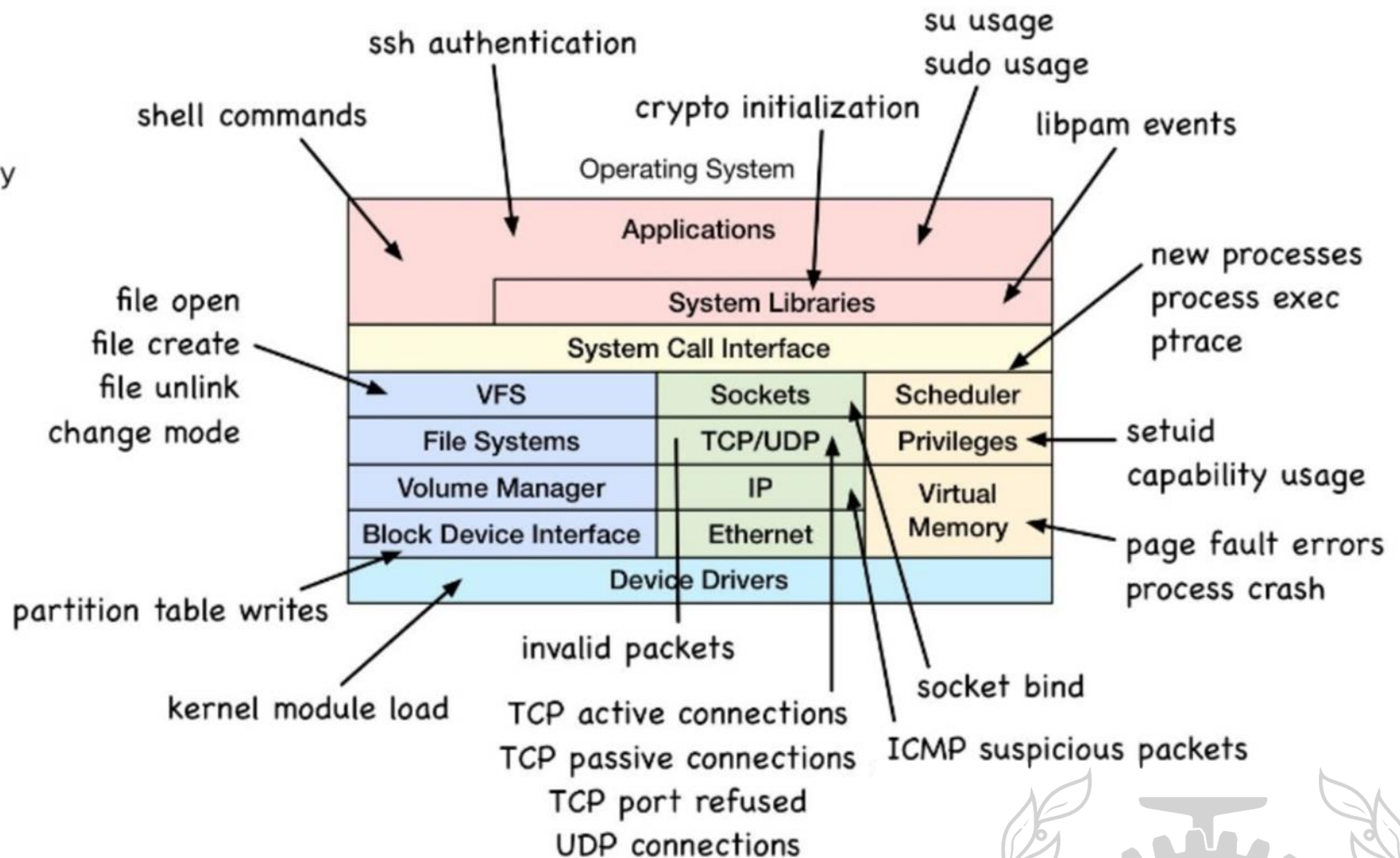
# Approach

## 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

---

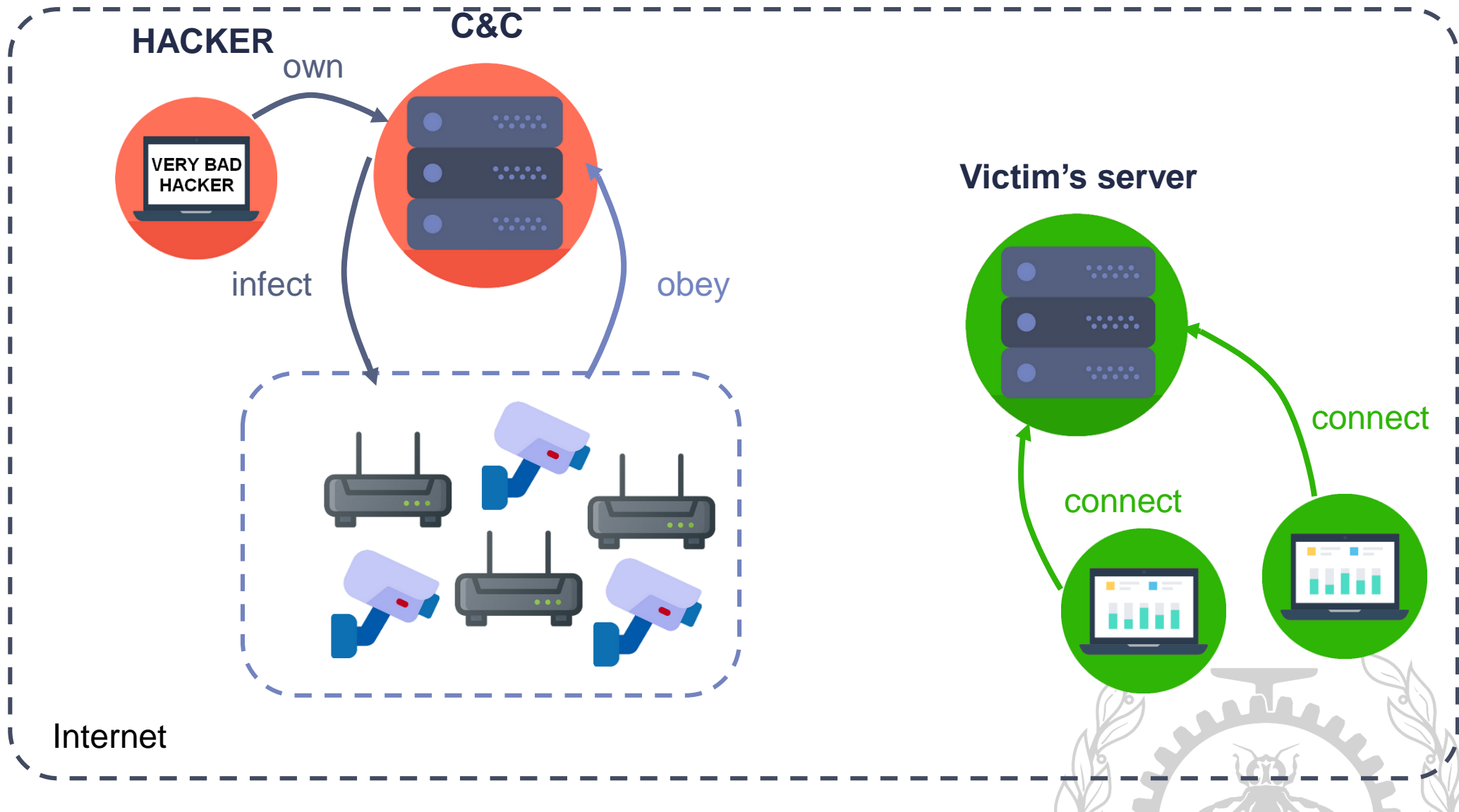
## What's Mirai?

- 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



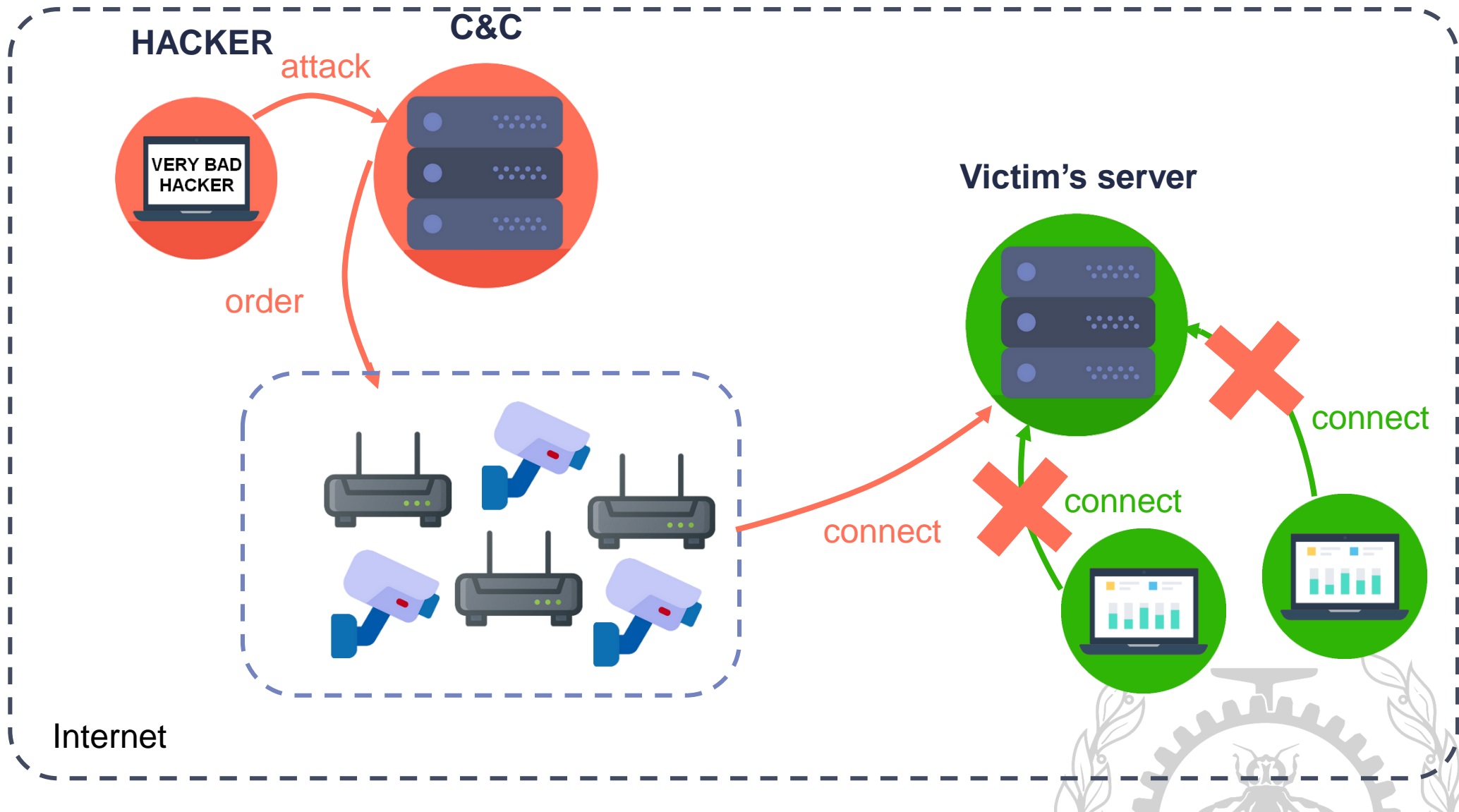
## Use-case

## What's Mirai?



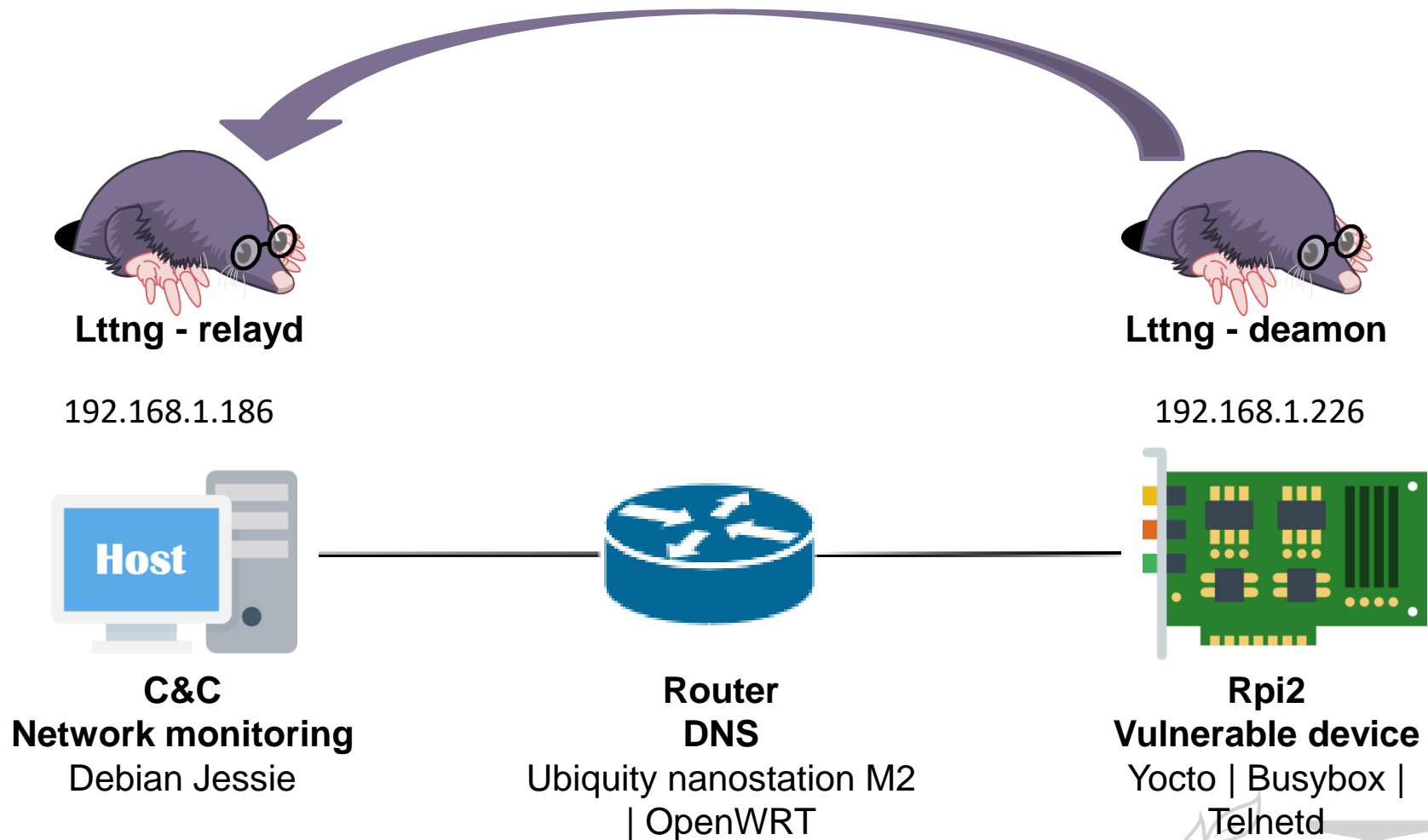
## Use-case

## 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

```

[22:09:12.708369353] (+0.000001979) raspberrypi2 syscall_entry_stat64: { cpu_id = 2 }, { filename = "dvrHelper", statbuf = 0x7ED8DB70 }
[22:09:12.708385915] (+0.000002396) raspberrypi2 syscall_exit_stat64: { cpu_id = 2 }, { ret = 0, filename = "dvrHelper", statbuf = 0x7ED8DB70 }
[22:09:12.708407009] (+0.000001198) raspberrypi2 syscall_entry_chmod: { cpu_id = 2 }, { filename = "dvrHelper", mode = 511 }
[22:09:12.933532165] (+0.000003958) raspberrypi2 syscall_entry_open: { cpu_id = 1 }, { filename = "dvrHelper", flags = 131649, mode = 438 }
[22:09:12.993886332] (+0.000002761) raspberrypi2 syscall_entry_lstat64: { cpu_id = 1 }, { filename = "dvrHelper", statbuf = 0x7EF43B70 }
[22:09:12.993930551] (+0.000001407) raspberrypi2 syscall_exit_lstat64: { cpu_id = 1 }, { ret = 0, filename = "dvrHelper", statbuf = 0x7EF43B70 }
[22:09:12.993943884] (+0.000000990) raspberrypi2 syscall_entry_stat64: { cpu_id = 1 }, { filename = "dvrHelper", statbuf = 0x7EF43B70 }
[22:09:12.993960499] (+0.000003386) raspberrypi2 syscall_exit_stat64: { cpu_id = 1 }, { ret = 0, filename = "dvrHelper", statbuf = 0x7EF43B70 }
[22:09:12.993983051] (+0.000000209) raspberrypi2 syscall_entry_chmod: { cpu_id = 1 }, { filename = "dvrHelper", mode = 511 }
[22:09:13.032415394] (+0.000013802) raspberrypi2 syscall_entry_execve: { cpu_id = 0 }, { filename = "./dvrHelper", argv = 0x147FDA0, envp = 0x147E5D0 }
[22:09:13.041602321] (+0.000002916) raspberrypi2 syscall_entry_open: { cpu_id = 1 }, { filename = "./dvrHelper", flags = 131072, mode = 0 }
[22:09:13.135535394] (+0.000022812) raspberrypi2 syscall_entry_open: { cpu_id = 3 }, { filename = "dvrHelper", flags = 131649, mode = 438 }
[22:09:13.183144040] (+0.000003281) raspberrypi2 syscall_entry_lstat64: { cpu_id = 0 }, { filename = "dvrHelper", statbuf = 0x7EE8CB70 }
[22:09:13.183186019] (+0.000000885) raspberrypi2 syscall_exit_lstat64: { cpu_id = 0 }, { ret = 0, filename = "dvrHelper", statbuf = 0x7EE8CB70 }
[22:09:13.183198780] (+0.000001823) raspberrypi2 syscall_entry_stat64: { cpu_id = 0 }, { filename = "dvrHelper", statbuf = 0x7EE8CB70 }
[22:09:13.183215238] (+0.000000729) raspberrypi2 syscall_exit_stat64: { cpu_id = 0 }, { ret = 0, filename = "dvrHelper", statbuf = 0x7EE8CB70 }
[22:09:13.183236384] (+0.000000365) raspberrypi2 syscall_entry_chmod: { cpu_id = 0 }, { filename = "dvrHelper", mode = 511 }
[22:09:13.211615707] (+0.000003594) raspberrypi2 syscall_entry_execve: { cpu_id = 2 }, { filename = "./dvrHelper", argv = 0x147FC38, envp = 0x147E5D0 }
[22:09:13.213655967] (+0.000000156) raspberrypi2 sched_process_exec: { cpu_id = 1 }, { filename = "./dvrHelper", tid = 478, old_tid = 478 }
[22:09:13.213750186] (+0.000015104) raspberrypi2 syscall_entry_unlink: { cpu_id = 1 }, { pathname = "./dvrHelper" }
[22:09:13.214387582] (+0.000000417) raspberrypi2 sched_stat_runtime: { cpu_id = 1 }, { comm = "dvrHelper", tid = 478, runtime = 1458333, vruntime = 454638527 }
[22:09:13.214395811] (+0.000003854) raspberrypi2 sched_switch: { cpu_id = 1 }, { prev_comm = "dvrHelper", prev_tid = 478, prev_prio = 20, prev_state = 1024, next_comm = "telnetd", next_tid = 306, next_prio = 20 }
[22:09:13.214719821] (+0.000000937) raspberrypi2 sched_switch: { cpu_id = 1 }, { prev_comm = "telnetd", prev_tid = 306, prev_prio = 20, prev_state = 1, next_comm = "dvrHelper", next_tid = 478, next_prio = 20 }
[22:09:13.214942426] (+0.000013646) raspberrypi2 signal_generate: { cpu_id = 1 }, { sig = 5, errno = 0, code = 0, comm = "dvrHelper", pid = 478, group = 1, result = 0 }
[22:09:13.215253103] (+0.000000417) raspberrypi2 sched_stat_runtime: { cpu_id = 1 }, { comm = "dvrHelper", tid = 478, runtime = 551719, vruntime = 455190246 }
[22:09:13.266604561] (+0.000000469) raspberrypi2 syscall_entry_open: { cpu_id = 1 }, { filename = "dvrHelper", flags = 131649, mode = 438 }
[22:09:13.661988311] (+0.000005000) raspberrypi2 syscall_entry_stat64: { cpu_id = 3 }, { filename = "dvrHelper", statbuf = 0x7E8B2B98 }
[22:09:13.662005498] (+0.000006614) raspberrypi2 syscall_exit_stat64: { cpu_id = 3 }, { ret = 0, filename = "dvrHelper", statbuf = 0x7E8B2B98 }
[22:09:13.662046696] (+0.000012344) raspberrypi2 syscall_entry_lstat64: { cpu_id = 3 }, { filename = "dvrHelper", statbuf = 0x7E8B2AA0 }
[22:09:13.662061748] (+0.000006250) raspberrypi2 syscall_exit_lstat64: { cpu_id = 3 }, { ret = 0, filename = "dvrHelper", statbuf = 0x7E8B2AA0 }
[22:09:13.662124977] (+0.000004843) raspberrypi2 syscall_entry_open: { cpu_id = 3 }, { filename = "dvrHelper", flags = 131265, mode = 33261 }
[22:09:13.662167790] (+0.000011927) raspberrypi2 syscall_entry_unlink: { cpu_id = 3 }, { pathname = "dvrHelper" }
[22:09:13.662477738] (+0.000007188) raspberrypi2 syscall_entry_open: { cpu_id = 3 }, { filename = "dvrHelper", flags = 131265, mode = 33261 }
[22:09:13.664871748] (+0.000118385) raspberrypi2 syscall_entry_open: { cpu_id = 1 }, { filename = "dvrHelper", flags = 131649, mode = 438 }
[22:09:13.674092165] (+0.000330208) raspberrypi2 syscall_entry_lstat64: { cpu_id = 3 }, { filename = "dvrHelper", statbuf = 0x7ED77B70 }
[22:09:13.674130602] (+0.000013020) raspberrypi2 syscall_exit_lstat64: { cpu_id = 3 }, { ret = 0, filename = "dvrHelper", statbuf = 0x7ED77B70 }
[22:09:13.674143571] (+0.000012969) raspberrypi2 syscall_entry_stat64: { cpu_id = 3 }, { filename = "dvrHelper", statbuf = 0x7ED77B70 }
[22:09:13.674159769] (+0.000006354) raspberrypi2 syscall_exit_stat64: { cpu_id = 3 }, { ret = 0, filename = "dvrHelper", statbuf = 0x7ED77B70 }
[22:09:13.674180498] (+0.000020729) raspberrypi2 syscall_entry_chmod: { cpu_id = 3 }, { filename = "dvrHelper", mode = 511 }
[22:09:13.819389873] (+0.000487344) raspberrypi2 syscall_entry_open: { cpu_id = 2 }, { filename = "dvrHelper", flags = 131649, mode = 438 }
[22:09:13.841362738] (+0.000333177) raspberrypi2 syscall_entry_lstat64: { cpu_id = 3 }, { filename = "dvrHelper", statbuf = 0x7EB4BB70 }
[22:09:13.841398884] (+0.000012500) raspberrypi2 syscall_exit_lstat64: { cpu_id = 3 }, { ret = 0, filename = "dvrHelper", statbuf = 0x7EB4BB70 }
[22:09:13.841411279] (+0.000012395) raspberrypi2 syscall_entry_stat64: { cpu_id = 3 }, { filename = "dvrHelper", statbuf = 0x7EB4BB70 }
[22:09:13.841427634] (+0.000006459) raspberrypi2 syscall_exit_stat64: { cpu_id = 3 }, { ret = 0, filename = "dvrHelper", statbuf = 0x7EB4BB70 }
[22:09:13.841448675] (+0.000021041) raspberrypi2 syscall_entry_chmod: { cpu_id = 3 }, { filename = "dvrHelper", mode = 511 }
[22:09:13.861758884] (+0.000035521) raspberrypi2 syscall_entry_execve: { cpu_id = 2 }, { filename = "./dvrHelper", argv = 0x1452DA0, envp = 0x14515D0 }
[22:09:13.870563727] (+0.000000416) raspberrypi2 syscall_entry_open: { cpu_id = 3 }, { filename = "./dvrHelper", flags = 131072, mode = 0 }
[22:09:13.993642998] (+0.000000312) raspberrypi2 syscall_entry_open: { cpu_id = 2 }, { filename = "dvrHelper", flags = 131649, mode = 438 }
[22:09:14.054013167] (+0.000013167) raspberrypi2 syscall_entry_lstat64: { cpu_id = 3 }, { filename = "dvrHelper", statbuf = 0x7E8B2B98 }

```





# Future work

---



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



Thank you!

Questions? Suggestions? Solutions?

*robin.gassais@polymtl.ca*

