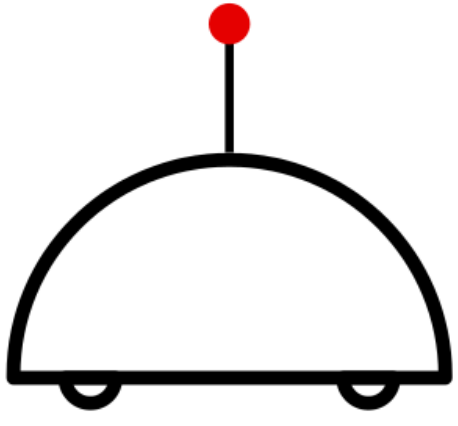
Honeypots in Robotics

Learning From Robot Hackers

Francisco Javier Rodríguez-Lera, Ángel Manuel Guerrero-Higueras, Camino Fernández-Llamas, and Vicente Matellán-Olivera

Grupo de Robótica. Universidad de León

León, March 3, 2020



Overview

Overview

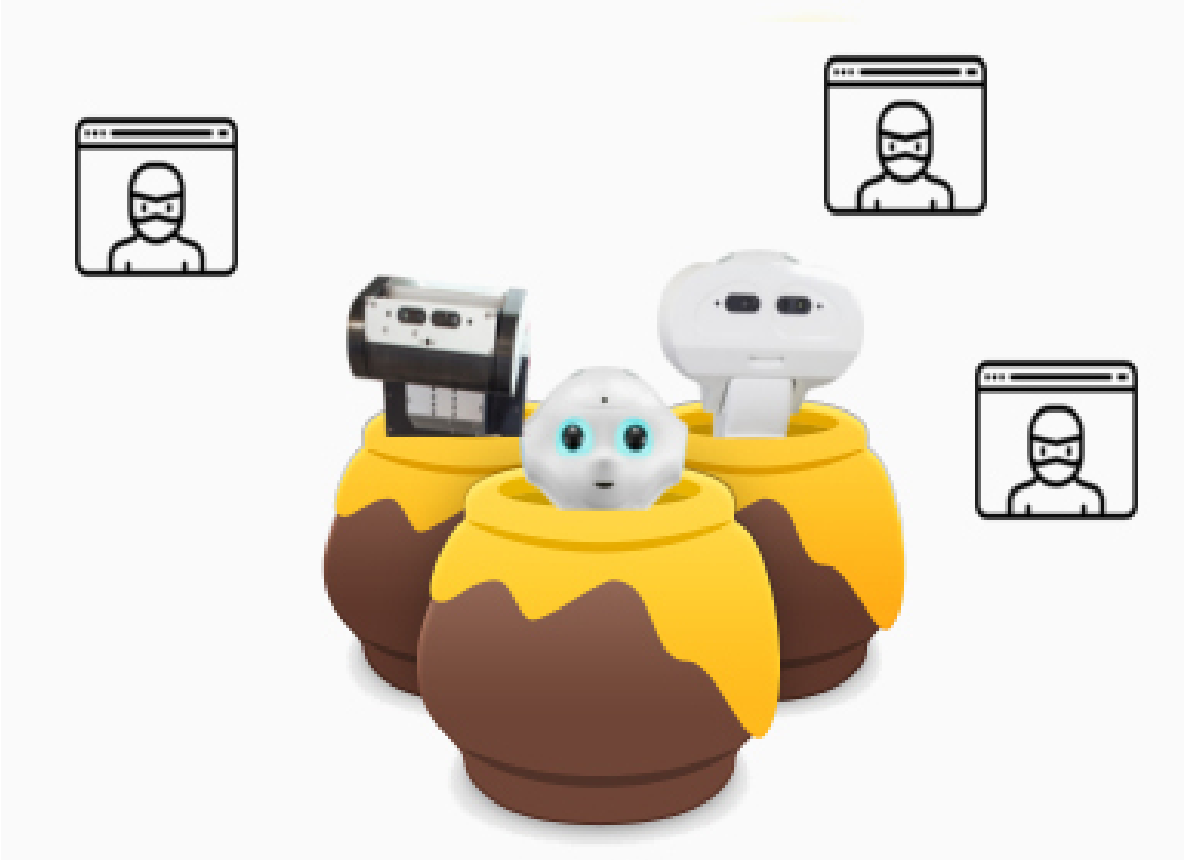
Robot Industry Trends

Robots are being deployed everywhere.

Problem: Security Policy

- Identify: Evaluate and perform a depth analysis of cybersecurity issues for understanding cybersecurity risk and threats to robot systems, their assets, the data, and their capabilities.
- Protect: the ability to limit and restrain the impact of a potential cybersecurity event and threats.
- Detect: The process of performing an appropriate set of activities to identify the occurrence of a cybersecurity events and threats.
- Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event and threats..
- Recover: Define the set of activities for restoring the system under cybersecurity event and maintain the resilience.

Solution: Honeypot



References:
- Irvene, C., Formby, D., Litchfield, S., and Beyah, R. (2017). HoneyBot: A honeypot for robotic systems. Proceedings of the IEEE, 106(1), 61-70.
- Daubert, J., Boopalan, D., Mühlhäuser, M., and Vasilomanolakis, E. (2018, April). HoneyDrone: A medium-interaction unmanned aerial vehicle honeypot. In NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium (pp. 1-6). IEEE.

Proposal

Deploying baitrobot to understand which is the state of art on cybersecurity events and treaths on robotics scenarios.

Research Questions

- What are the implications of leaving robots as a honeytraps?
- The malicious users are there, how we can recognized them?
- How do we deploy a baitrobot?
- Defining monitoring tools. Where is the data in a robotic platform?
- Analyzing the gathered data. What are the next steps?

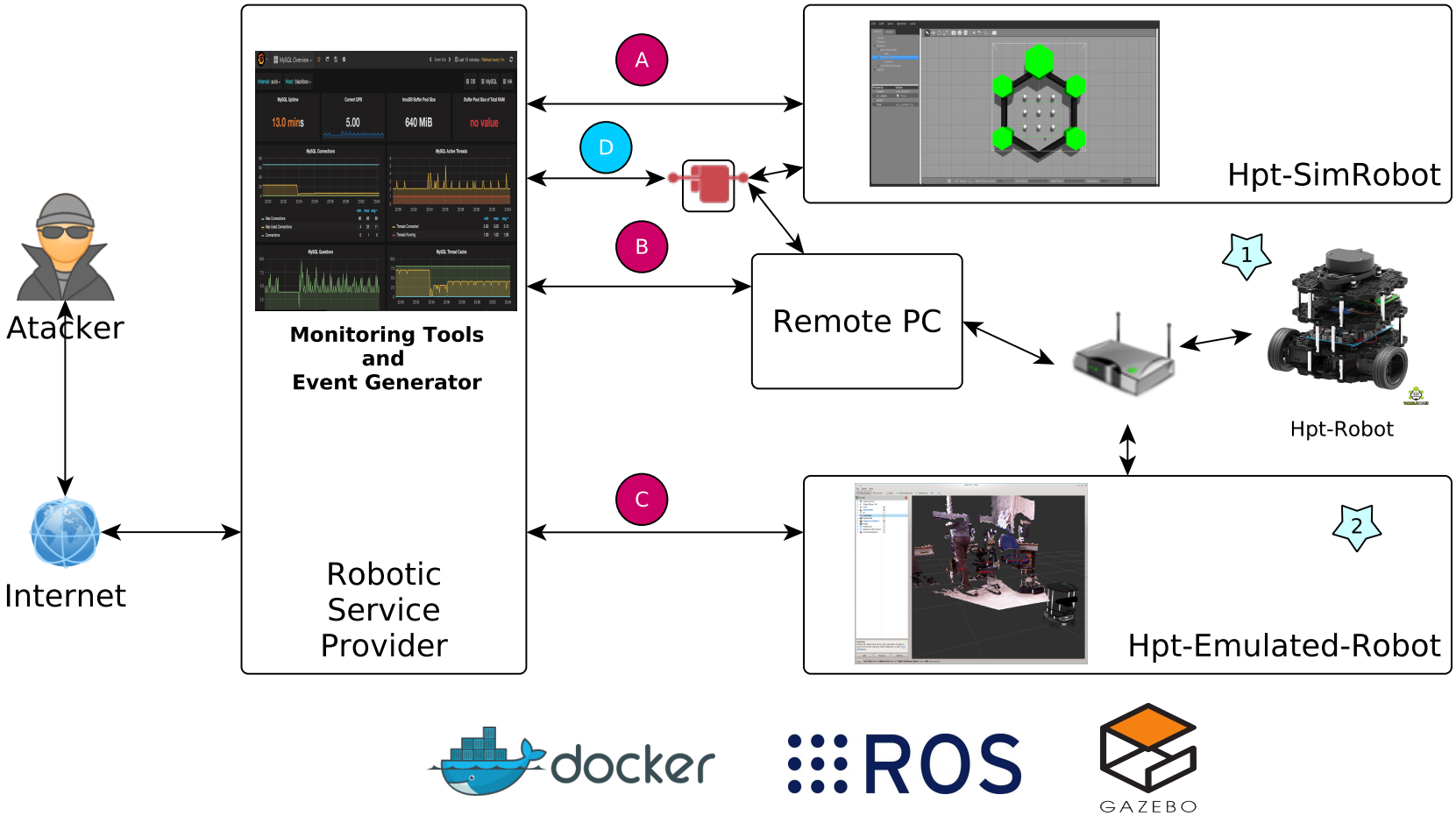
Overview

Honeypot Models[1]

- Field of operation:
  - Production Honeypots
  - Research Honeypots
- Type by direction of the interaction :
  - Server: Passive Honeypots
  - Client: Active Honeypots
- Type by Interaction Level:
  - High-Interaction Honeypot (HIHP)
  - Med-Interaction Level (MIHP)
  - Low-Interaction Level (LIHP)
- Type by physicality:
  - Physical Honeypots
  - Virtual Honeypots

[1] Nawrocki, M., Wahlisch, M., Schmidt, T. C., Keil, C., and Schonfelder, J. (2016). A survey on Honeypot software and data analysis. arXiv preprint arXiv:1608.06249.

Proposed Architecture



Proposed Honeypot Approaches

- High-Interaction Honeypot
  - A → HIHP in Virtual Environment + Virtual (Simulated) Robot
  - B → HIHP in a Physical Network Environment + Physical or Virtual (Emulated) Robot
  - C → HIHP in Virtual Environment + Virtual (Emulated) Robot
- Low-Interaction Honeypot
  - D → LIHP + Virtual (Simulated) Robot or Physical Robot

Overview

Monitoring System

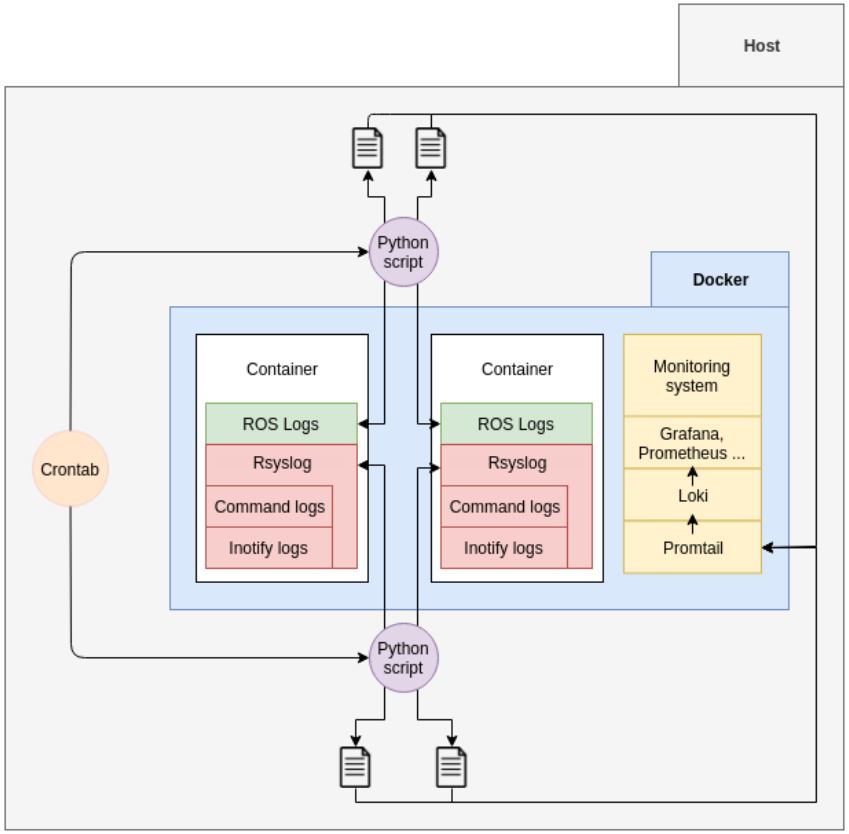
Monitoring

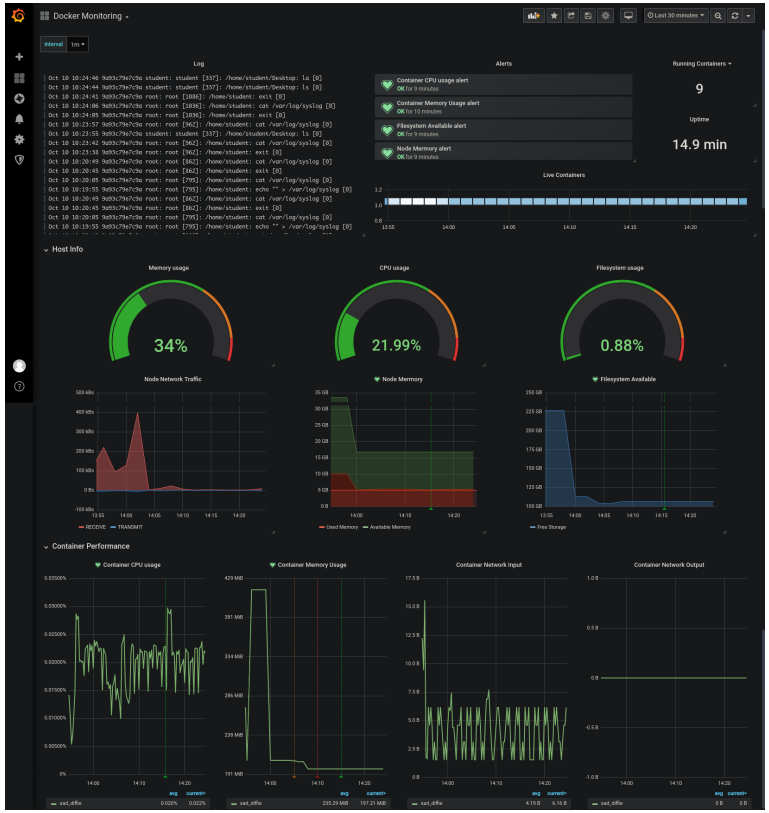
- Communications
  - Physical networks
  - Virtual networks
- Data Capture
  - Attacks
  - Events
  - Intrusions

Containment

- None
- Slowdown
- **Defuse**
- **Block**

Monitoring Architecture





Overview

File system

```
Jan 29 10:20:26 faf07e232dde rsyslogd: [origin software="rsyslogd" swVersion="8.16.0" x-pid="66" x-info="http://www.rsyslog.com
Jan 29 10:20:26 faf07e232dde rsyslogd-2039: Could not open output pipe '/dev/xconsole':: Permission denied [v8.16.0 try http://
Jan 29 10:20:26 faf07e232dde inotifywait[76]: Setting up watches.
Jan 29 10:20:26 faf07e232dde rsyslogd-2007: action 'action 9' suspended, next retry is Wed Jan 29 10:20:56 2020 [v8.16.0 try ht
Jan 29 10:20:26 faf07e232dde inotifywait[76]: Watches established.
Jan 29 10:20:26 faf07e232dde inotifywait[79]: Setting up watches.
Jan 29 10:20:26 faf07e232dde inotifywait[79]: Watches established.
Jan 29 10:20:26 faf07e232dde inotifywait[112]: Couldn't watch /home/student/.bash_profile: No such file or directory
Jan 29 10:20:26 faf07e232dde inotifywait[115]: Setting up watches.
Jan 29 10:20:26 faf07e232dde inotifywait[115]: Couldn't watch /home/student/.config/autostart-scripts: No such file or director
Jan 29 10:20:26 faf07e232dde inotifywait[119]: Setting up watches.
Jan 29 10:20:26 faf07e232dde inotifywait[119]: Couldn't watch /home/student/.config/autostart/: No such file or directory
Jan 29 10:20:26 faf07e232dde rsyslogd-2222: command 'KLogPermitNonKernelFacility' is currently not permitted - did you already
Jan 29 10:20:26 faf07e232dde rsyslogd: imklog: cannot open kernel log (/proc/kmsg): Operation not permitted.
Jan 29 10:20:26 faf07e232dde rsyslogd-2145: activation of module imklog failed [v8.16.0 try http://www.rsyslog.com/e/2145 ]
Jan 29 10:20:26 faf07e232dde rsyslogd: rsyslogd's groupid changed to 117
Jan 29 10:20:26 faf07e232dde rsyslogd: rsyslogd's userid changed to 111
Jan 29 10:20:29 faf07e232dde pulseaudio[237]: [autospawn] core-util.c: Failed to create secure directory (/home/student/.config
Jan 29 10:20:29 faf07e232dde pulseaudio[237]: [autospawn] lock-autospawn.c: Cannot access autospawn lock.
Jan 29 10:20:29 faf07e232dde pulseaudio[237]: [pulseaudio] main.c: Failed to acquire autospawn lock
```

Command Line Tracker (CLT)

```
Jan 29 10:21:24 faf07e232dde root:  root [295]: /home/student:  [0]
Jan 29 10:21:43 faf07e232dde root:  root [295]: /home/student: apt update && apt install iputils-ping [0]
Jan 29 10:21:52 faf07e232dde root:  root [295]: /home/student: ping 10.0.20.1 [1]
Jan 29 10:40:17 faf07e232dde root:  root [295]: /home/student: ping 10.0.20.1 [1]
Jan 29 10:40:18 faf07e232dde root:  root [295]: /home/student: ifconfig [0]
Jan 29 10:44:12 faf07e232dde root:  root [1125]: /home/student: ifconfig [0]
Jan 29 10:44:19 faf07e232dde root:  root [1125]: /home/student: ping 10.0.20.1 [0]
Jan 29 11:00:10 faf07e232dde root:  root [1351]: /home/student: ping 10.0.20.1 [0]
Jan 29 11:00:11 faf07e232dde root:  root [1351]: /home/student: ifconfig [0]
Jan 29 11:01:08 faf07e232dde root:  root [1438]: /home/student: ifconfig [0]
Jan 29 11:01:09 faf07e232dde root:  root [1438]: /home/student: ifconfig [0]
Jan 29 11:01:20 faf07e232dde root:  root [1438]: /home/student: ping 10.0.20.1 [0]
Jan 29 11:01:24 faf07e232dde root:  root [1438]: /home/student: ping 10.0.20.1 -I eth1 [2]
Jan 29 11:01:28 faf07e232dde root:  root [1438]: /home/student: ping 10.0.20.1 -I eth2 [0]
Jan 29 11:01:36 faf07e232dde root:  root [1438]: /home/student: ping 10.0.20.176 [0]
Jan 29 11:04:21 faf07e232dde root:  root [1438]: /home/student: clear [0]
Jan 29 11:04:23 faf07e232dde root:  root [1438]: /home/student: ls [0]
Jan 29 11:04:55 faf07e232dde inotify: root MOVE_SELF: /home/student/.bashrc
Jan 29 11:04:55 faf07e232dde inotify: root DELETE_SELF: /home/student/.bashrc
Jan 29 11:04:56 faf07e232dde root:  root [1438]: /home/student: vim .bashrc  [0]
Jan 29 11:04:57 faf07e232dde root:  root [1438]: /home/student: ifconfig [0]
Jan 29 11:05:14 faf07e232dde root:  root [1438]: /home/student: vim .bashrc  [0]
Jan 29 11:05:17 faf07e232dde root:  root [1438]: /home/student: source .bashrc  [0]
Jan 29 11:05:22 faf07e232dde root:  root [1438]: /home/student: rostopic list  [1]
Jan 29 11:05:34 faf07e232dde root:  root [1438]: /home/student: ping 10.0.20.150 [1]
Jan 29 11:05:35 faf07e232dde root:  root [1438]: /home/student: ifconfig [0]
Jan 29 11:05:45 faf07e232dde root:  root [1438]: /home/student: ping 10.0.20.176 [0]
Jan 29 11:05:59 faf07e232dde root:  root [1438]: /home/student: vim .bashrc  [0]
Jan 29 11:06:03 faf07e232dde root:  root [1438]: /home/student: source .bahsr [1]
Jan 29 11:06:07 faf07e232dde root:  root [1438]: /home/student: source .bashrc [0]
Jan 29 11:06:10 faf07e232dde root:  root [1438]: /home/student: rostopic list  [0]
Jan 29 11:08:42 faf07e232dde root:  root [1438]: /home/student: rostopic list  [0]
Jan 29 11:08:49 faf07e232dde root:  root [1438]: /home/student: rostopic echo /scan [0]
```

Who is knocking? Origin by IP[2]

- Europe/London
- Europe/Madrid
- Europe/Paris
- Europe/Prague
- Europe/Warsaw
- Asia/Ho Chi Minh
- Asia/Kathmandu
- Asia/Seoul
- Asia/Shanghai
- Asia/Tokyo

- America/Argentina/Buenos Aires
- America/Bogota
- America/Chicago
- America/Denver
- America/Detroit
- America/Los Angeles
- America/New York
- America/Santiago
- America/Toronto

[2] Data extracted using ipwhois python package: `https://pypi.org/project/ipwhois/`

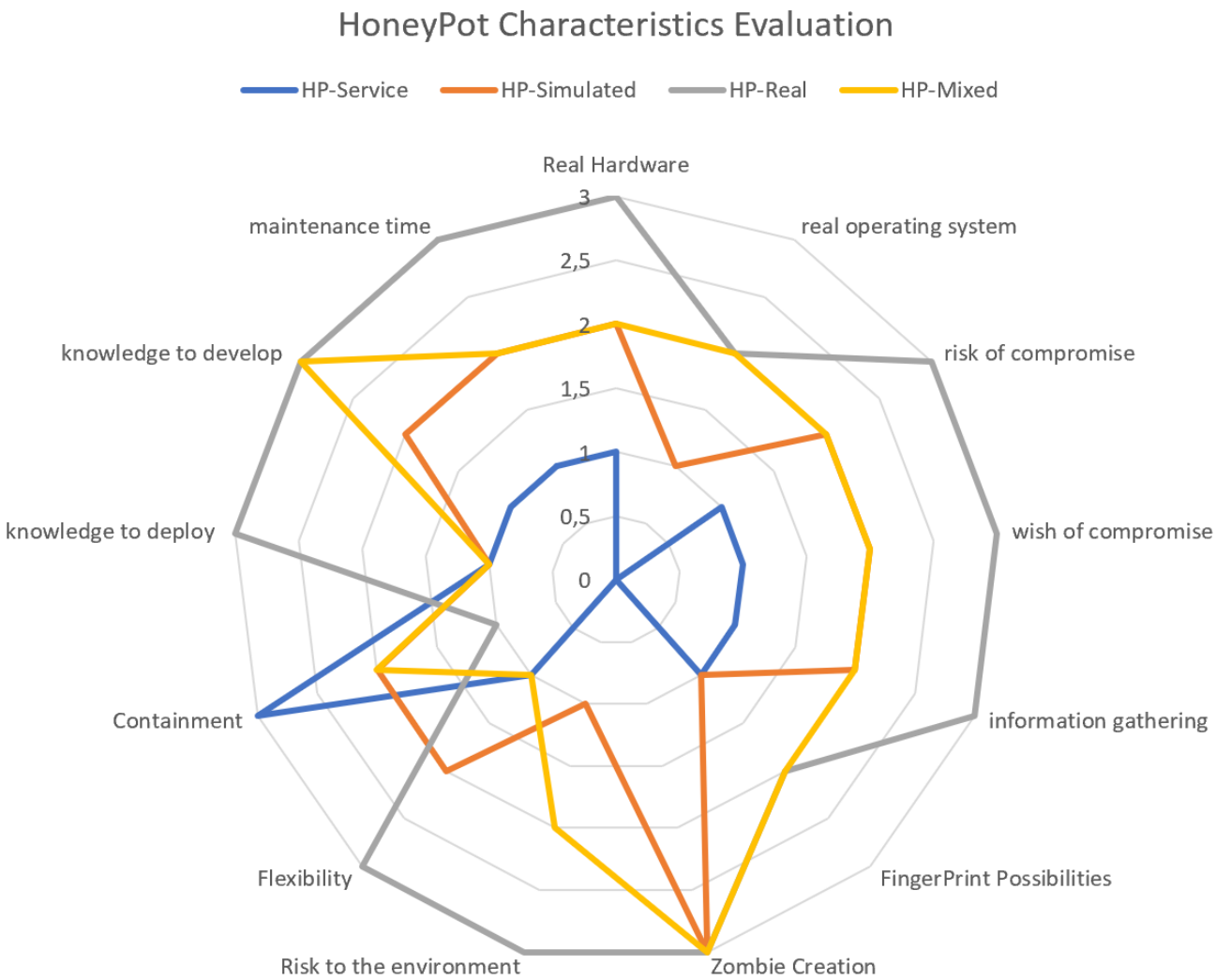
Who is knocking? Network Names by IP [3]

```
1  u'36056', 'asn'
1  u'AMAZON-ICN', 'asn'
1  u'AMAZO-ZPDX9', 'asn'
1  u'AT-88-Z', 'asn'
1  u'Baidu', 'asn'
2  u'CHINANET-JS', 'asn'
1  u'DEDIPA-45-85-188-0', 'asn'
1  u'DIGITALOCEAN-7', 'asn'
1  u'DO-13', 'asn'
1  u'ES-FCSC-20161125', 'asn'
1  u'ES-XFERA-201112', 'asn'
1  u'GOOGLE', 'asn'
1  u'GOOGLE-CLOUD', 'asn'
1  u'hitiit', 'asn'
1  u'HO-2', 'asn'
1  u'INAP-LAX-NUCLEARFALLOUT-64-94-100-0', 'asn'
1  u'INAP-NYM-NUCLEARFALLOUT-0920', 'asn'
1  u'INSTYTUT-TELE-I-RADIOTECHNICZNY', 'asn'
1  u'KEYSTONE', 'asn'
1  u'KR_PLZENSKY', 'asn'
1  u'NFOSERVERS-ACS-3', 'asn'
1  u'NFOSERVERS-CHI-3', 'asn'
1  u'NFOSERVERS-CHI-9', 'asn'
1  u'OctoVPN', 'asn'
1  u'ODS-VNNIC-VN', 'asn'
```

```
1  u'OVH_154563725', 'asn'
1  u'OVH_261104801', 'asn'
1  u'OVH-ARIN-7', 'asn'
2  u'OVH', 'asn'
1  u'OVH-CUST-14428113', 'asn'
1  u'OVH-CUST-293348', 'asn'
1  u'OVH-CUST-298023', 'asn'
1  u'OVH-CUST-298076', 'asn'
4  u'OVH-DEDICATED-FO', 'asn'
1  u'PNAP-SEF-NUCFLT-RM-03', 'asn'
1  u'PONYNET-04', 'asn'
1  u'PONYNET-07', 'asn'
1  u'RIMA', 'asn'
1  u'Scaleway', 'asn'
1  u'SKYCA-3', 'asn'
1  u'SOHO-PPPoE-2', 'asn'
1  u'StreamlineServers', 'asn'
1  u'SYM-20180216-CA-MT2', 'asn'
1  u'TencentCloud', 'asn'
1  u'TENCENT-CN', 'asn'
1  u'UNICOM-JS', 'asn'
1  u'UNILEON', 'asn'
1  u'VIS-BLOCK', 'asn'
1  u'VPS-GRA6', 'asn'
1  u'VPS-OVH', 'asn'
1  u'VPS-SBG6', 'asn'
1  u'ZunYi-Power-Supply-Burea', 'asn'
```

[3] Data extracted using ipwhois python package: `https://pypi.org/project/ipwhois/`

Overall Evaluation



*On development given initial feedback and experience

Overview

Conclusions

Pros

- Containment
- Resources control + Flexibility
- Zero-Day-Exploit Detection
- Framework Platform-Independent*
- Physical networks on the loop
- Real robots on the loop

Cons

- Being Fingerprinted
- Limited Field of View
- Risk to the Environment
- Zombie creation

Further work I

1. Here we have presented the technical infrastructure, **where is the cognitive side of a robotic platform?**

Extra Points:Legal Issues

- Entrapment Challenges
- Privacy

Acknowledgements

Honeypots in Robotics

Learning from Robot Hackers

1. Junta de Castilla y León (FEDER) - LE028P17
2. Scayle (HPC)
3. INCIBE
4. Proyectos Ministerio de Ciencia, Innovación y Universidades - RTI2018-100683-B-I00