Industrial Control Systems: Quantifying Exposed Devices

Michael G. Dodson, Alastair R. Beresford & Daniel R. Thomas
University of Cambridge, https://www.cl.cam.ac.uk/
{md403, arb33, drt24}@cam.ac.uk

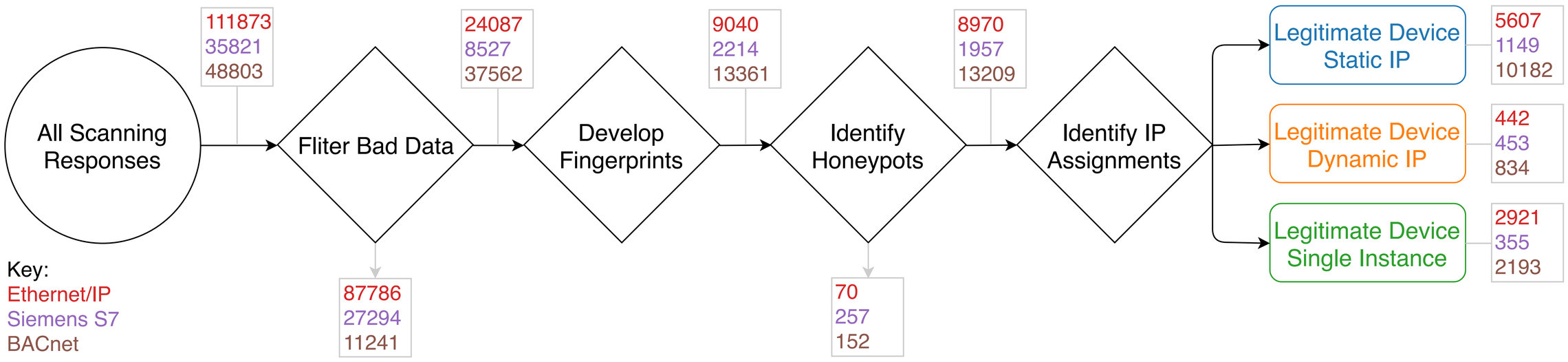

Figure 1: ICS classification decision tree using data from Shodan between 10 and 31 December 2018

Motivation and Summary

Thousands of Industrial Control System (ICS) devices are connected to the Internet using legacy point-to-point or broadcast protocols layered on top of Ethernet and TCP/IP. Most of these protocols have no authentication or encryption mechanisms, allowing an adversary to take control of a system simply by sending well-formed packets [1].

Previous studies surveyed the growing number of Internet-connected ICS devices [1, 2]. Our investigation focuses on the following:

- Fingerprinting individual ICS devices using public data
- Accurately counting and tracking unique ICS devices
- Flagging potential security mis-configurations
- Identifying ICS devices co-located with Mirai-like botnet hosts

ICS Classification and Tracking

Shodan [3] and Censys [4] provide Internet-wide views of devices responding on ICS protocol ports by scanning the IPv4 address space and making response data publicly available. Table 1 is a sample response for the query 'port:44818 country:GB', for which there are at least 60 unique, Internet-connected devices. Port 44818 corresponds to the Common Industrial Protocol over Ethernet, known as Ethernet/IP, used in time-critical process automation applications. Other protocols discussed here include Siemens S7 (port 102), typically used to control manufacturing processes, and BACnet (port 47808), designed for large-scale building automation [1].

For most ICS protocols, devices provide sufficient data to fingerprint and classify the device in response to a well-formed request. The fingerprint can be used to track a device across dynamic IPs, track firmware changes, or monitor for mis-configured security devices such as firewalls and VPNs.

Host IP	81.133.32.86
Vendor ID	Rockwell Automation/Allen-Bradley
Product / Firmware	1766-L32BXBA / B14.00
Serial Number	0x4062e267
Device IP	192.168.52.2

Table 1: Example Shodan Response

The decision tree used to classify each IP address responding on a given ICS protocol port is shown in Figure 1. The fingerprint allow us to accurately count and classify the number of Internet-connected, and therefore vulnerable, ICS devices. Passive device fingerprinting relies on ability to find device-specific, static characteristics or collections of characteristics (e.g., device serial number). Honeypot identification is largely based on known, default characteristics of common honeypot libraries and likely under-predicts. The IP assignment classification for the dataset in Figure 1 is shown in Figure 2. Unique devices classified as 'single instance' provided sufficient data to fingerprint, but were only observed during one scan. They may be:

- A honeypot with changing configuration information
- An ICS device behind a temporarily mis-configured security device

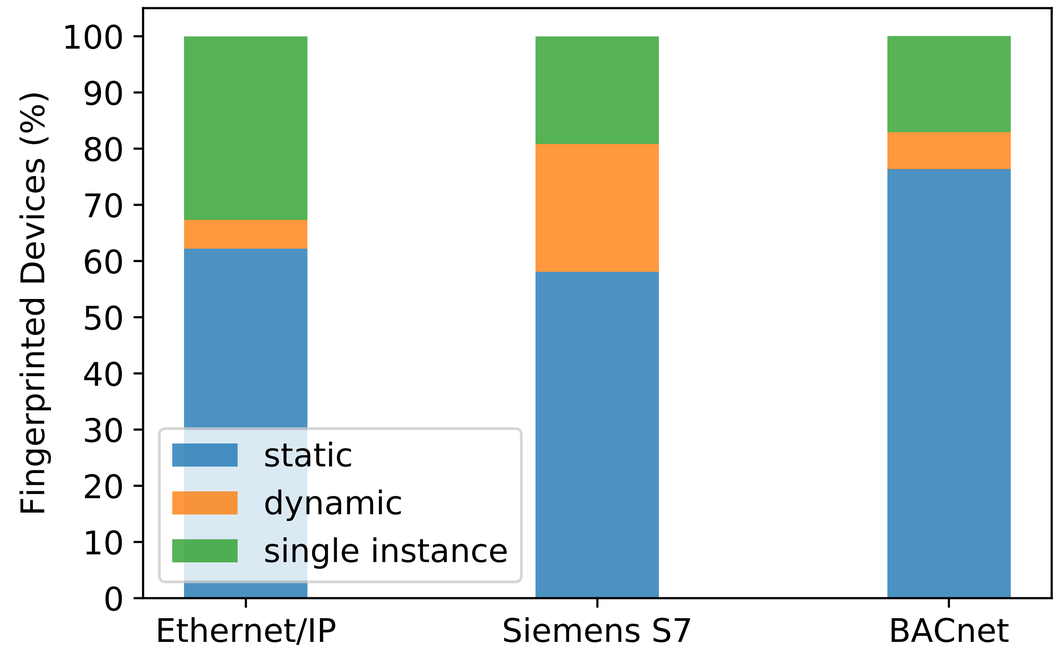

Figure 2: IP assignment classification for fingerprinted ICS devices

ICS Scanning

We also identified ICS devices and Mirai botnet-like Internet scanners with common IPs (i.e., IP addresses responding to requests on ICS ports and simultaneously scanning). Scanners may be actual Mirai hosts or other scanners mimicking Mirai. If the former, the result confirms that ICS networks can be trivially compromised at scale. We are currently working to disambiguate scanner host locations (e.g., the ICS device itself, router, another device behind a router) and identify if any Linux-based ICS devices are compromised or only sharing a gateway with a compromised device.

References

[1] Ariana Mirian et al. "An Internet-wide view of ICS devices". In: *14th Annual Conference on Privacy, Security and Trust* (2016).
[2] Eireann P Leverett. "Quantitatively assessing and visualising industrial system attack surfaces". In: *MPhil Thesis* (2011).
[3] John. C. Matherly. *Shodan search engine*. URL: https://www.shodan.io/.
[4] Zakir Durumeric et al. "A search engine backed by Internet-wide scanning". In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (2015).

Acknowledgements: This work is supported by the Gates Cambridge Trust and EPSRC [grant number EP/M020320/1]