Cyber-physical systems: Classifying exposed devices

Michael Dodson, Alastair R Beresford and Daniel R Thomas

Cyber-physical systems (CPS) tightly integrate digital controls with physical sensors and actuators, often consist of a network of devices, and increasingly connect to the broader Internet for remote control and data collection. CPS is a broad designation which can be used to describe diverse areas such as industrial control systems (ICS), autonomous vehicles, smart grids, and the Internet of Things (IoT). The distinction between ICS and other mobile and ubiquitous CPS, such as autonomous vehicles and IoT, is blurring as ICS move toward greater reliance on remote, platform-independent access to data and control functions and the automotive and IoT industries move toward greater digital automation. This presentation will focus on the security of Internet-connected ICS, but will draw broader conclusions about risks to exposed CPS.

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

Shodan.io and Censys.io, among others, provide Internet-wide views of Internet-connected devices, including those responding on ICS protocol ports. These organisations scan the IPv4 address space and make response data publicly available. For example, the Shodan.io query `port:44818 country:GB' returns IP addresses, vendor names, model numbers, firmware versions, and serial numbers for at least 60 unique, Internet-connected devices that have port 44818 open. Port 44818 corresponds to the Common Industrial Protocol over Ethernet, known as Ethernet/IP, used in time-critical process automation applications. Protocols that provide similar levels of detail in the query response include Siemens S7 (port 102), typically used to control manufacturing processes, and BACnet (port 47808), designed for large-scale building automation.

Several previous studies used Shodan.io and Censys.io to demonstrate the growth of Internet-connected ICS devices. Our investigation uses this data to study the behaviour of ICS device owners and highlight the difficulty of securing these devices.

For several ICS protocols, publicly available scanning data is sufficient to passively fingerprint and classify an ICS device. Our passive method demonstrates the ability of an adversary to identify and track a target device without alerting the target to their interest and avoids potential side-effects of interacting with a device through our own active scans (though, of course, we are using third-party scanning data, which may have produced side-effects during their scanning).

Fingerprinting is a flexible tool and we have used it to characterise the behaviour of device owners and identify several issues related to securing ICS devices. For example, we have been able to identify whether a device has a dynamic or static IP address, which can be a useful proxy for where devices are installed: devices with dynamic IPs are likely connected via ADSL or cable modem, may be behind a Network Address Translation device, and are more likely

to be located at a small business or residential establishment (e.g., a building automation controller in a block of flats). Similarly, we have used fingerprints to track firmware versions and demonstrate that a significant percentage of device owners do not update firmware. Finally, we have shown that fingerprints can be used to identify ICS devices which are either infected by botnet software, such as Mirai, or sharing infrastructure with infected hosts. task of transferring over datasets.