The Homeland of Things (HoT) Framework

A Framework for Improving our Homeland's Security in Cyberspace

admin@homelandofthings.org

Table of Contents

Acknowledgements

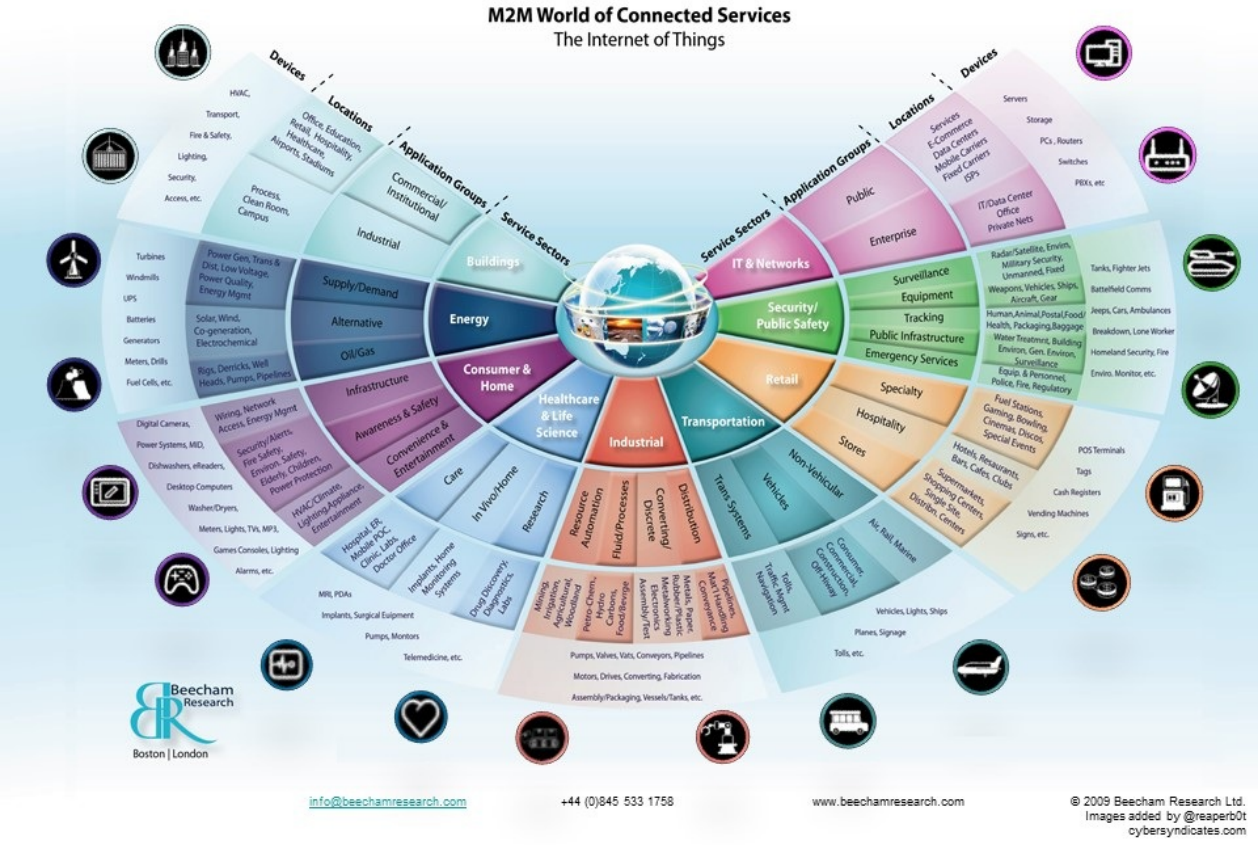
We would like to thank all of our family and friends who supported us throughout the duration of the tedious R&D and writing of this paper. This paper was developed in its entirety with open source information and does not reflect the views of the United States Government. We look forward to building partnerships with Federal and SLTT governments, NGOs, and the private sector (academia and industry) in developing this framework for the betterment of our Nation's security. In the near future, this framework and modular technical details will be available at https://homelandofthings.org, though we do hope that this framework or a derivative will take on the form of federal government doctrine.

Preface

Vulnerabilities, threats, and subsequent risks are inherit with Internet of Things (IoT) devices, which typically reside at the meeting place of critical infrastructure and cyberspace. We present the HoT Framework to promote best practices for all Federal and State, Local, Tribal, and Territorial (SLTT) governments, non-government organizations (NGOs), and the private sector to use as a foundation for the reconnaissance, interrogation, and hardening of IoT nodes that are characterized as existing within both critical and non-critical infrastructure throughout the physical network layer, logical network layer, and cyber-persona layer of cyberspace terrain. In addition, we propose solutions for, public awareness of, and information sharing regarding the vulnerabilities, threats, risks, mitigations, and countermeasures associated with the IoT. The HoT Framework serves to assist Federal and SLTT governments, NGOs, and the private sector in thwarting attacks against their IoT devices and preventing their IoT devices from being used as an attack platform. For the framework to be effective, we need direct support from the DHS, DoD, DOJ, and other Federal agencies. We will also need to establish partnerships with SLTT, NGO, and the private sector (academia and industry) to further enrich and develop the framework using real-world data.

The Internet of Things

In 1982, a Coke machine at Carnegie Mellon was modified to connect to the internet and provide information about its supply of soda and whether they were cold or not [1]. Since then the number of devices connected to the internet has exploded, with Cisco estimating that the number of connected devices to be approximately 22.9 billion devices with growth to 50.1 billion devices by 2020 [2]. The term “Internet of Things”, which is often abbreviated as IoT, was coined in 1999 by Kevin Ashton to describe non-traditional devices that are network connected [1]. Definitions of IoT devices vary but typically they are considered to be something that processes data; is “connected” via an internet connection, radio frequency identification (RFID), near field communications (NFC), cellular connections, or Bluetooth; and monitors or interacts with its environment.



A.Smart Things

Smart devices are devices intended for everyday use that extend the functionality of existing technologies. They have become increasingly popular in the mid to late 2000's. Smartphones are the most prolific and one of the earliest examples, although personal digital assistants (PDAs) were a precursor. Smartphones also provided an impetus for the propagation of other smart devices, as many smart devices use phone applications for remote control.

A common category of smart devices is home efficiency and improvement devices. Examples that fall into this category include smart thermostats, that learn the homeowners schedule and adjust the heat so that it is lower when nobody is home and warms back up just prior to the when it expects the house to be occupied. It will also allow the user to change the temperature via an application on their phone or a web application, which is useful if the owner has an unexpected change to their schedule. Smart lawn care systems will check online weather reports and adjust the watering schedule to make use of rainfall to optimize the amount of water used. Smart locks allow the user to check whether their doors are locked or unlocked and can be controlled through a phone application.

Another category of smart devices is wearable technology such as monitoring devices. Fitness trackers will monitor levels of activity, which can then be uploaded to the user's computer for long term tracking or sharing on social media. Also popular within this category are a range of tracking devices, that can be attached to keys, luggage, cars, etc. These devices will use GPS data and show the tracked objects location or emit a sound at the push of a button. Internet enabled video cameras allow users to set up home surveillance systems that can be monitored anywhere that an internet connection is available. Advanced systems will send alerts when movement is detecting when the user is not home. As technology advances, implantable medical devices, such as pacemakers and insulin pumps, have been made networkable. This allows medical professionals to adjust settings on the implant without surgically removing the device.

B.Industrial Things

Many industrial control systems (ICSs) have integrated network control features to make managing an increasingly larger and more dispersed infrastructure easier. These features are often implemented in the supervisory control and data acquisitions (SCADA) subsystems. SCADA systems are responsible for controlling a wide variety of functions in industrial equipment. In a power generation plant, the SCADA system would control fuel and oil pumps, pressure valves, HVAC systems to vent exhaust and control the temperature of the systems, etc. It would also have sensors responsible for monitoring the fuel and oil levels, ensuring that pressure within each component is within a safe range, and reporting power output levels. If an error is detected in one of the generators at the plant the SCADA

could shut off that generator until it could be repaired. In days past, each generator in a facility would have a SCADA system that would be controlled at the generator. Now, the SCADA systems for each generator would be networked and connected to a control/monitoring facility. The facility might be further networked to send automatic messages to plant supervisors and maintenance personnel when an error is detected.

C. All of the Things

The final, catch-all category of the IoT is embedded devices. These are small computer systems that are designed for a specific purpose and are part of a larger system. Some of the literature describe standalone embedded systems, and give examples of phones, home heating systems, and other items that this paper classifies as smart devices. Due to the difference in attacks against traditional and standalone embedded devices, these categories have been kept separate in this paper. Furthermore, tasks that embedded systems are designed to perform are determined by the manufacturer, not by the user, which differentiates them from the typical computer system and some customizable smart devices.

An example of an embedded system would be the computer control system in a vehicle. This system controls the vehicle’s fuel injection system, anti-lock brakes, transmission, cruise control, GPS, etc. The magazine “Military Embedded Systems” contains numerous examples of military applications of embedded systems to include tactical military vehicles.

The IoT in Cyberspace and Cyber-Electromagnetic Activities

For both critical infrastructure and non-critical infrastructure owners, it is important that they understand that regardless of whether or not their IoT devices are connected to a closed TCP/IP network or to the Internet, they are a target on a battlefield within the fifth domain of warfare, which is cyberspace. According to Joint Publication (JP) 3-12 (R) Cyberspace Operations, there are three layers of cyberspace: the physical network layer, the logical network layer, and the cyber-persona layer. The definitions are lengthy and can be summarized as follows:

A. Physical Network Layer

JP 3-12 defines the physical network as the geographic component (land, air, sea, or space) where the network resides and physical network components comprised of the hardware, systems software, and infrastructure that supports the network [3]. This layers used logical constructs as the primary method of security [3]. We would like to add that a network does not always imply a TCP/IP network. A network can be a simple CAN bus network in a vehicle or Modbus network between a master and slave PLC. In addition, we also present the fact that a node within cyberspace can be disparate. Specifically, there are IoT devices that are not connected to any network or they are only connected to a network on certain occasions, but they can still have both offensive and defensive cyber effects applied, especially through interfaces which can be accessed through the electromagnetic spectrum (e.g. 802.11x enabled devices). Due to this fact, the term physical network layer is misleading and should be changed to just the physical cyberspace layer.

B. Logical Network Layer

The next higher layer described by JP 3-12, the logical network layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node [3]. An example is given using a website that is hosted on servers in multiple locations where all content can be accessed through a single uniform resource locator (URL) [3]. We would also like to extend this layer to include items such as cloud computing services and VPNs, that allow an otherwise physically disparate node to logically replicate a physical connection.

C. Cyber-Persona Layer

According to JP 3-12, the cyber-persona layer consists of the people actually on the network [3]. A cyber-persona is the projection of a persona into cyberspace. Additionally, JP 3-12 states that cyber-personas may relate fairly directly to an actual person or entity, incorporating some biographical or corporate data, e-mail and IP address(es), Web pages, phone number, etc [3]. It is possible for a person to have a one-to-one persona to cyber-persona or a one-to-many persona to cyber-personas. It is also possible for a group of people to have many-to-one persona to cyber-persona, which makes attribution to a specific individual difficult [3]. However, some or all of the details in a cyber-persona can be inaccurate, outdated, or outright false.

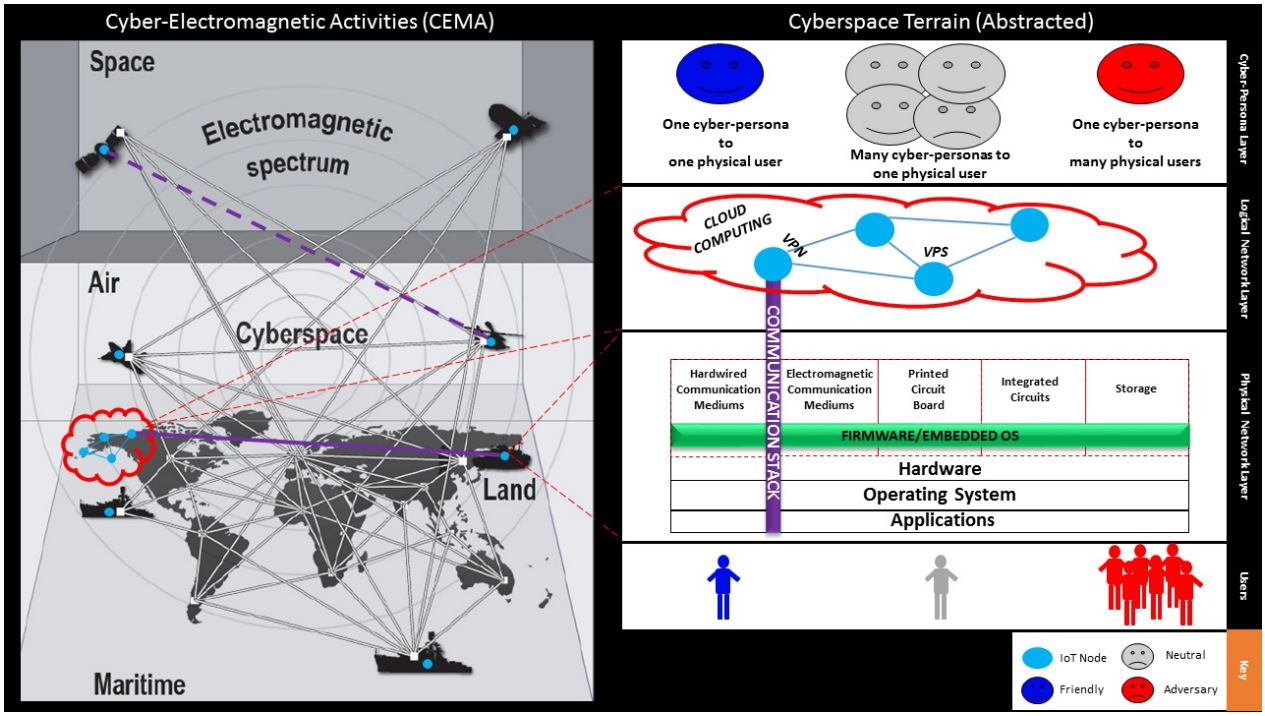
D. Cyber-Electromagnetic Activities (CEMA)

Army Field Manual (FM) 3-38 Cyber Electromagnetic Activities, defines CEMA as the consummation of cyberspace operations (CO), electronic warfare (EW), and spectrum management operations (SMO) [4]. FM 3-38 further designates that CEMA is leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system [4].

EW, can be used to affect IoT devices, specifically through electronic attack (EA) and electronic warfare support (ES). FM 3-38 defines EA as the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires [4]. EA tasks include countermeasures, electromagnetic deception, electromagnetic intrusion, electromagnetic jamming, electromagnetic pulse, and electronic probing [4]. FM 3-38 defines ES as actions to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations [4]. ES tasks include electronic reconnaissance, electronic intelligence, and electronics security [4].

Both EA and ES apply directly to IoT devices, regardless of whether or not the IoT device has an interface capable of communicating through the electromagnetic spectrum. This is evident with the publishing of information regarding TEMPEST activities, which refers to the spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations [5]. Furthermore, attacks against 802.11x using

attacks directed at the 2.4GHz and 5GHz frequency (e.g. jammers) as well as the protocol itself (e.g. deauthentication attacks) provide insight into what both EA and ES would look like from the perspective of IoT devices.



Vulnerabilities in the IoT

A. Physical Network Layer (Software, Hardware, Infrastructure)

There is no shortage of vulnerabilities associated with IoT nodes within the physical network layer. During the DEFCON IoT Village in August 2016, 47 new vulnerabilities affecting 23 devices from 21 manufactures were disclosed at the IoT security talks, workshops, and onsite hacking contests [6]. Vulnerabilities ranged from poor design decisions like the use of plaintext and hard-coded passwords to coding flaws like buffer overflows and command injection [6]. This is the second year that the IoT Village was held at DEFCON and to date the event has led to the discovery of 113 critical vulnerabilities across consumer and business IoT products [6]. These results are indicative of the failure of manufactures to develop secure IoT products. The following list captures the top ten vulnerability categories affecting IoT nodes, according to OWASP [7]:

1. Insecure Web Interface
2. Insufficient Authentication/Authorization
3. Insecure Network Services
4. Lack of Transport Encryption/Integrity Verification
5. Privacy Concerns
6. Insecure Cloud Interface
7. Insecure Mobile Interface
8. Insufficient Security Configurability
9. Insecure Software/Firmware
10. Poor Physical Security

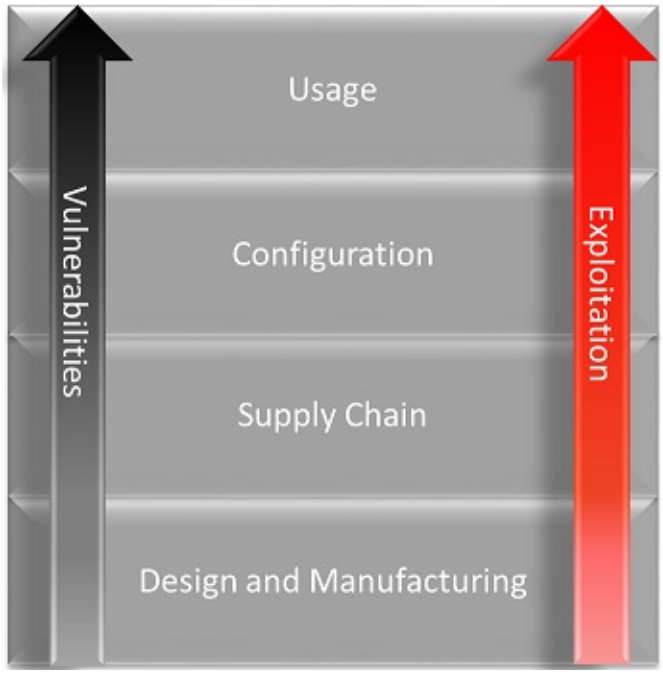
The first nine of the top ten are associated with software vulnerabilities, albeit the vulnerabilities associated with the physical security of hardware are likely the most difficult to mitigate. Concerns with physical security range from supply chain cybersecurity and onsite physical security manipulation to the use of electronic warfare (EW) concepts described within the broader context of CEMA. Examples include:

- Implanting, embedding, or piggybacking inorganic embedded systems (e.g. microprocessors, microcontrollers, or other integrated circuits (IC)), within an IoT device to include devices that provide an out-of-band backdoor communication medium (e.g. RF technologies such as GSM within an implanted inorganic embedded system).
- Removal and reprogramming of microprocessors using desoldering and reprogramming

techniques. Manipulating the embedded operating system (e.g. firmware) and/or physical hardware through inter-board communication and configuration interfaces and protocols such as JTAG, SPI, I2C, UART, USB, RS-232, and Firewire.

- Manipulating the embedded operating system and/or hardware using hardwired (e.g. Ethernet) or electromagnetic spectrum enabled I/O interfaces (e.g. RF communications such as 802.11x).
- Manipulating ICs during the manufacturing process, through a method known as “stealthy dopant level hardware Trojans” [8].

At the physical network layer, it is clear that vulnerabilities are introduced and exploitation can occur at all phases of a product’s life including design, manufacturing, the supply chain, configuration, and usage. This is depicted in Figure 3.



B. Logical Network Layer

Vulnerabilities at this layer are focused around data in transit, data at rest, and many of the general privacy and security concerns associated with a cloud computing environment. Most of these vulnerabilities will be mitigated at the physical network layer from the perspective of the IoT device and the devices within the cloud infrastructure.

C. Cyber-Persona Layer (People/Artificial Intelligence)

When discussing the particulars of the cyber-persona layer as it relates to the IoT, the first question that came to mind was “Can a device have a cyber-persona?” The second was, “Can a device have a mind of its own?” To the best of our knowledge this is an area that has not yet been explored. The relevant explorations in this area will probably lie in IoT devices that have artificial intelligence. While there is not any technology that meets this criterion at this time, the issue can only be postponed for a few years. Several commercial businesses are developing artificial intelligences that will be used in a variety of industries, and the Department of Defense has looked at robotics and artificial intelligence in several projects, such as the DARPA Grand Challenge. General Paul Selva, the Vice Chairman of the Joint Chiefs of Staff, has alluded to the “Terminator Conundrum”, where an autonomous system with no human operator has lethal capabilities [29]. It is possible for these machines to maintain cyber-personas.

For our purposes, our focus is on the people, associated with IoT devices within the physical network layer of our terrain, that are projecting the cyber-personas into cyberspace. This would include taking the appropriate steps to analyze all known cyber-personas for those people in their work and personal lives, to include social media, if possible. From an information security perspective, it is well known that people have always been the weakest link. From the perspective of cybersecurity, the implications of an uninformed user in cyberspace can be even greater. From a homeland security perspective, every individual plays a key role in protecting our homeland in cyberspace. Being that cyberspace is a domain of warfare, every individual can be targeted and can quickly become engulfed within a battlespace that resides within a virtual abstract of our physical homeland.

Some Americans have expressed openly that they would take up arms and resist an invasion of our homeland by traditional adversarial kinetic forces. Our homeland is currently being invaded by a plethora of cyber threats, so why aren’t more individuals taking up arms and resisting in cyberspace? Even if one was not concerned with adversaries invading their home network and pillaging their private information, every individual should be concerned with their home router, home entertainment system, smart refrigerator, or smart toilet being used as part of an IoT botnet like Mirai. This holds especially true when the botnet is being leveraged to attack critical infrastructure that is vital to our homeland’s security and prosperity.

Failure to exercise due diligence by mitigating risks associated with IoT devices, such as conducting software and firmware updates on these devices, aids the enemy by providing a safe haven from which they can launch attacks against the United States. According to 18 U.S. Code § 2381:

> Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason and shall suffer death, or shall be imprisoned not less than five years and fined under this title but not less than $10,000 [9].

Luckily, for the time being the United States Government is not prosecuting citizens for treason under this title as a result of their IoT devices being used to conduct attacks against the United States. However, it should still serve to remind citizens of the United States of their obligation to resist our enemies, even within cyberspace.

Threats to the IoT

There are two categories of human threats in cyberspace, 1) nation-state cyberthreats (state sponsored hackers) and 2) non-state cyberthreats (i.e. cyber-terrorists, cyber-criminals, hacktivists, and script-kiddies). The intent and capability of each category and sub-category of cyber threats varies and will not be described in detail. However, we would like to point out that the Edward Snowden NSA leaks have allowed security researchers (and likely nation-state actors) to reverse engineer technologies pertaining to the exploitation and attack of IoT devices. This presents a unique threat to our homeland's security in cyberspace.

Risks to Homeland Security

The National Infrastructure Protection Plan (NIPP) states that:

> Critical infrastructure that has long been subject to risks associated with physical threats and natural disasters is now increasingly exposed to cyber risks, which stems from growing integration of information and communications technologies with critical infrastructure operations and an adversary focus on exploiting potential cyber vulnerabilities [10].

Cybersecurity and Homeland Security Doctrine Review

Risks and shortfalls associated with the IoT are addressed indirectly by the components within the two cybersecurity related mission priorities of the DHS Fiscal Years (FY) 2014-2018 Strategic Plan and specific statements, requirement, and mandates within the Homeland Security Act of 2002, PPD-21, Executive Order 13636, the NIPP, the National Cybersecurity Protection Act of 2014, the Cybersecurity Enhancement Act of 2014, the Cybersecurity Information Sharing Act of 2014, the Cybersecurity and Infrastructure Protection Agency Act of 2016, the State and Local Cyber Protection Act of 2015, the Cyber Preparedness Act of 2016, and the Small Business Cyber Security Improvement Act of 2016.

Within “Mission 4: Safeguard and Secure Cyberspace” of the Department of Homeland Security’s FY 2014-2018 Strategic Plan are two Mission Priorities:

> Reduce national cyber risk through the Cybersecurity Framework, threat awareness, public awareness campaigns, and best practices, all of which increase the baseline capabilities of critical infrastructure [11].
>
> Enhance critical infrastructure security and resilience, with respect to physical and cyber risks, by reducing vulnerabilities, sharing information on threat, consequences and mitigations, detecting malicious activity, promoting resilient critical infrastructure design, and partnering with critical infrastructure owners and operators [11].

The National Cybersecurity Protection Act of 2014 mandates that:

> The Under Secretary appointed under section 103(a)(1)(H) shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in section 212(5)), owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks (as defined in section 226) to critical infrastructure [12].

This requires a thorough assessment of the software and hardware components of critical infrastructure which is typically implemented as an IoT node, whether in the form of an ICS/SCADA solution or another category of IoT node. Title II – Cybersecurity Research and Development section (201)(a)(1) of the Cybersecurity Enhancement Act of 2014 states that

applicable agencies and departments will work with the National Science and Technology Council and the Network and Information Technology Research and Development Program to develop a strategic plan to meet the following objectives:

> How to test and verify that software and hardware, whether developed locally or obtained from a third party, is free of significant known security flaws; [13]
>
> How to test and verify that software and hardware obtained from a third party correctly implements stated functionality, and only that functionality; [13]

The Cybersecurity Information Sharing Act of 2014 section 103 states that:

> This title requires the Director of National Intelligence (DNI) and the Departments of Homeland Security (DHS), Defense (DOD), and Justice (DOJ) to develop and promulgate procedures to promote the sharing of: (1) classified and declassified cyber threat indicators in possession of the federal government with private entities, nonfederal government agencies, or state, tribal, or local governments; (2) unclassified indicators with the public; (3) information with entities under cybersecurity threats to prevent or mitigate adverse effects; and (4) cybersecurity best practices with attention to the challenges faced by small businesses [14].

The Cybersecurity and Infrastructure Protection Agency Act of 2016 states that the Cybersecurity and Infrastructure Protection Agency (CIPA) must:

> Administer a National Infrastructure Coordination Center to be co-located with the National Cybersecurity and Communications Integration Center (NCCIC) to collect, share, and provide recommendations about critical infrastructure information [15]
>
> Perform critical infrastructure assessments to determine the risks posed by particular types of terrorist attacks within the United States [15]
>
> Recommend measures necessary to protect critical infrastructure in coordination with other federal entities and in cooperation with nonfederal entities [15]

The State and Local Cyber Protection Act of 2015 amends the Homeland Security Act of 2002 to require the DHS’s NCCIC to assist state and local governments with cybersecurity by:

> Upon request, identifying system vulnerabilities and information security protections to address unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by, or information systems used or operated by, state or local governments or other organizations or contractors on their behalf; [16]
>
> Providing via a web portal updated resources and guidelines related to information security; [16]
>
> Coordinating through national associations to implement information security tools and policies to ensure the resiliency of state and local information systems; [16]
>
> Providing training on cybersecurity, privacy, and civil liberties; [16]
>
> Providing requested technical assistance to deploy technology that continuously diagnoses and mitigates cyber threats and to conduct threat and vulnerability assessments; [16]
>
> Coordinating vulnerability standard developed by the National Institute of Standards and Technology; [16]
>
> Ensure that state and local governments are aware of DHS resources and other federal tools to ensure the security and resiliency of federal civilian information systems. [16]

The Cyber Preparedness Act of 2016 amends the Homeland Security Act of 2002 to require the Department of Homeland Security's (DHS's) State, Local, and Regional Fusion Center Initiative to coordinate with the national cybersecurity and communications integration center (NCCIC) to provide state, local, and regional fusion centers with expertise on DHS cybersecurity resources [17]. (A fusion center serves as a focal point within the state and local environment for the receipt, analysis, gathering, and sharing of threat related information between the federal government and state, local, tribal, territorial, and private sector partners) [17]. The Act states that DHS must:

> Provide timely access to technical assistance, risk management support, and incident response capabilities for cybersecurity threat indicators, defensive measures, risks, and incidents, including cybersecurity risks to equipment and technology related to the electoral process; [17]
>
> Review cybersecurity risk information gathered by fusion centers to incorporate into DHS's cybersecurity risk information; [17]
>
> Disseminate cybersecurity risk information to fusion centers. [17]

The Small Business Cyber Security Improvement Act of 2016 directs the Small Business Administration (SBA) and DHS to include in their small business development centers (SBDC) cyber strategy:

> Counsel[ing] and assistance to improve small businesses' cyber security infrastructure, threat awareness, and training programs for employees, including agreements with Information Sharing and Analysis Centers to gain awareness of actionable threat information that may be beneficial to small businesses; and an analysis of how SBDCs can leverage federal agency programs and develop partnerships to improve cyber support services to small businesses [18].

Homeland Cybersecurity Risk Assessment

After thorough review of applicable laws and policies, the importance of collaboration, critical infrastructure protection and cybersecurity is evident from Federal and SLTT governments to small businesses. Moreover, it seems that mitigating risks where critical infrastructure and cyberspace meet are of upmost priority. IoT devices are typically at the center of this meeting point. The extremely high risks presented to homeland security by the IoT is attributed to the growing sophistication of human threats, the abundance of vulnerabilities, and the exponential growth of the IoT within critical and non-critical infrastructure. Failure to mitigate the risks associated with the IoT within critical infrastructure will likely result in a catastrophic event that will have both tangible and intangible effects including the compromise of our Nation's security, prosperity, and values. Additionally, this catastrophic event will likely have a global impact affecting the global economy and international order. It is of the utmost priority to the United States Government (USG) that we follow the NIST's Framework for Improving Critical Infrastructure Cybersecurity Framework Core to identify, protect, detect, respond, and recover to risks as they pertain to critical infrastructure cybersecurity, specifically as it applies to IoT devices [19].

Certainly, there are already vulnerability, threat, and risk assessments tailored to handle the Industrial Things, but to what depth, breadth, and standard? To our knowledge other than the NIST's Framework for Improving Critical Infrastructure Cybersecurity, there appears to be no other standardized framework available to assist Federal and SLTT governments, non-government organizations (NGOs), and the private sector in dealing with the cybersecurity risks associated with critical infrastructure. In the executive summary, the Framework authors admit that it is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure [19]. The authors states that organizations will continue to have unique risk – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary [19]. Furthermore, there appears to be no solution that provides a semi-technical framework to assist in identifying and mitigating specific risks that IoT devices possess within critical and non-critical infrastructure, through all layers of cyberspace terrain. There also does not appear to be information sharing involving methods to discover or mitigate advanced threat tactics such as manipulation of supply chain.

Homeland of Things Framework

The Homeland of Things (HoT) Framework seeks to meet two all-encompassing objectives, 1) provide a framework and promote best practices for all Federal and SLTT governments, NGOs, and the private sector to use as a foundation for the reconnaissance, interrogation, and hardening of IoT nodes that are characterized as existing within both critical and non-critical infrastructure throughout the physical network layer, logical network layer, and cyber persona layer of cyberspace terrain, 2) provide solutions for, public awareness of, and information sharing regarding the vulnerabilities, threats, risks, mitigations, and countermeasures associated with the IoT. The HoT Framework serves to help Federal and SLTT governments, NGOs, and the private sector in stopping their devices from being attacked and from being used as an attack platform.

In addition to outlining tactics, techniques, and procedures (TTPs), success in the HoT Framework will be largely driven by new and reinvigorated partnerships between government, academia, industry, and the individual in implementing and providing feedback for the improvement and further development of the HoT Framework. It is important to note that the steps in this framework do not have to be executed in the order that they are presented. The reconnaissance and interrogation portions of this framework can be used for periodic security assessments, periodic penetration tests, and incident response purposes.

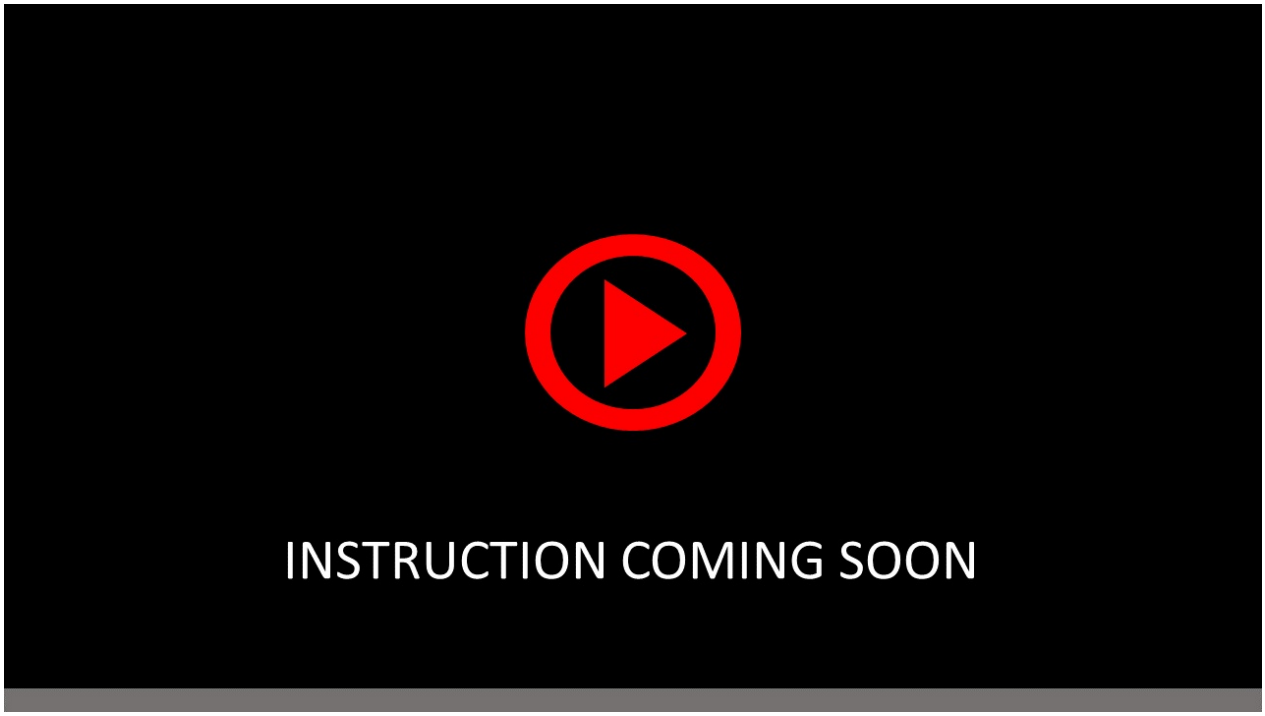
Reconnaissance and Interrogation to Detect Vulnerabilities and Adversary Presence within the Physical Network Layer

When conducting reconnaissance and interrogation at the physical network layer there are several steps that must be accomplished:

- Gather and prepare hardware and software tools
- Recon and identify IoT device hardware
- Interrogate hardware to detect vulnerabilities
- Interrogate hardware to detect adversary presence
- Interrogate firmware to detect vulnerabilities in the operating system and applications
- Interrogate firmware to detect adversary presence in the operating system and applications
- Recon and identify IoT device electromagnetic spectrum capabilities
- Interrogate electromagnetic spectrum capabilities to detect vulnerabilities
- Interrogate electromagnetic spectrum capabilities to detect adversary presence
- Recon and identify IoT device software, ports, protocols, and services that are accessible from the network
- Interrogate software, ports, protocols, and services that are accessible from the network to detect vulnerabilities
- Interrogate software, ports, protocols, and services that are accessible from the network to detect adversary presence
- Recon and identify logs from intrusion detection systems, network appliances, and log aggregation services that are monitoring the IoT device
- Interrogate/analyze logs for adversary presence
- Recon and identify systems that can control the IoT device within the local network (e.g. HMIs)
- Interrogate control systems for vulnerabilities and adversary presence

Whether supply chain risk management (SCRM) has failed, does not exist, or if on-site physical manipulation is suspected, cyber defenders should have hardware verification methods that allow them to verify the device's internal hardware and firmware against a trusted manufacturer known-good. A National database that is maintained by the NCICC or other component of the DHS and would be made accessible to Federal and SLTT governments, NGOs, and the private sector. This database would include, at a minimum, 1)

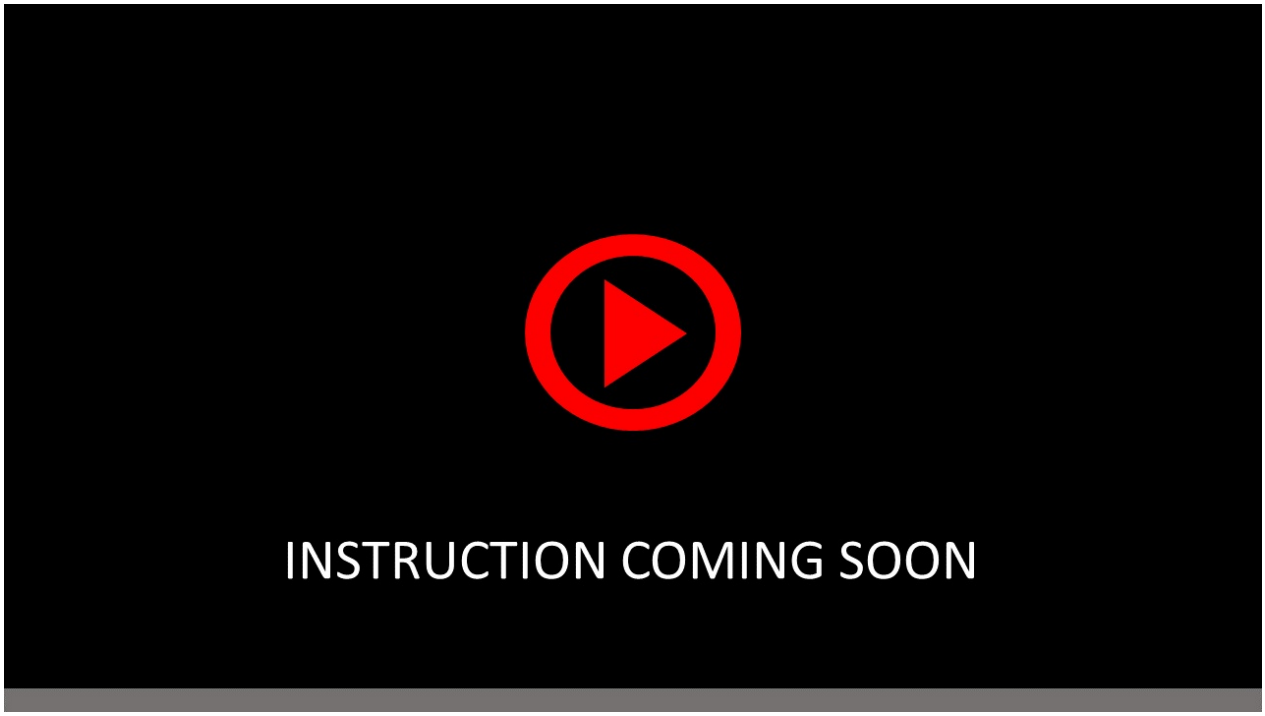
vulnerabilities and indicators of compromise associated with the IoT device, 2) manufacture generated imagery (optical/acoustic/x-ray microscopy) and/or schematics of the printed circuit board (PCB) and all other associated internal hardware components of the IoT device, 3) the IoT device's embedded operating system or firmware (compiled and/or source code) that has been verified by the vendor through cryptographic hashes, 4) manufacturer device manuals and device specifications, 5) electromagnetic spectrum capabilities, frequencies, and protocols of the IoT device.



The cyber defender will need to gather various "hardware hacking tools" to analyze the IoT device, 1) oscilloscopes, logic analyzers, and protocol analyzers for signal monitoring and analysis, 2) USB-to-Serial adapters (e.g. Hardsploit, Bus Pirate, GoodFET, ChipWhisperer, JTAGulator, RIFF Box, and Facedancer) that and capable of connecting to serial debug interfaces such as UART, JTAG, SPI, and I2C for signal monitoring, signal analysis, and firmware analysis, 3) soldering irons, rework stations, and device programmers for destructive and non-destructive analysis and manipulation of ICs, 4) optical microscopy, acoustic microscopy, and X-ray microscopy equipment for imaging PCBs and ICs [20]. Once the tools are gathered the cyber defender will recon and identify the IoT device's physical hardware. Once located, the devices will need to be opened to provide maximum exposure of the PCB so the cyber defender can interrogate the hardware to detect vulnerabilities and adversary presence. The device may need to be powered down and fully disassembled to conduct proper hardware analysis. It is important to note that if adversary presence is suspected, powering down the device will destroy forensic evidence of the adversary in volatile storage, such as memory. If this is an issue, it may be necessary to passively monitor the network for adversary presence first or the situation may require conducting

reconnaissance and interrogation of the hardware, firmware, and electromagnetic spectrum capabilities after conducting reconnaissance and interrogation of the IoT device's software, ports, protocols, and services that are accessible from the network.

Disassembly and interrogation of hardware may void vendor warranties or contracts. Before conducting hardware analysis, it may be necessary to conduct a holistic risk assessments that takes into consideration the threats, vulnerabilities, probability, and impact associated with each IoT device if the voidance of warranties or contracts is of concern. It also may be necessary for the consumer to request an inclusion of a clause within the warranty or contract to allow the conduct of the steps required in this framework.Interrogation of the hardware needs to first be conducted using either the naked-eye or, if possible, optical, acoustic, or x-ray microscopy. This is interrogation should be conducted and compared to imagery in the National database. In the future, research and development of field expedient and affordable methods for the automated analysis of hardware using accurate imagery technology techniques should be conducted.

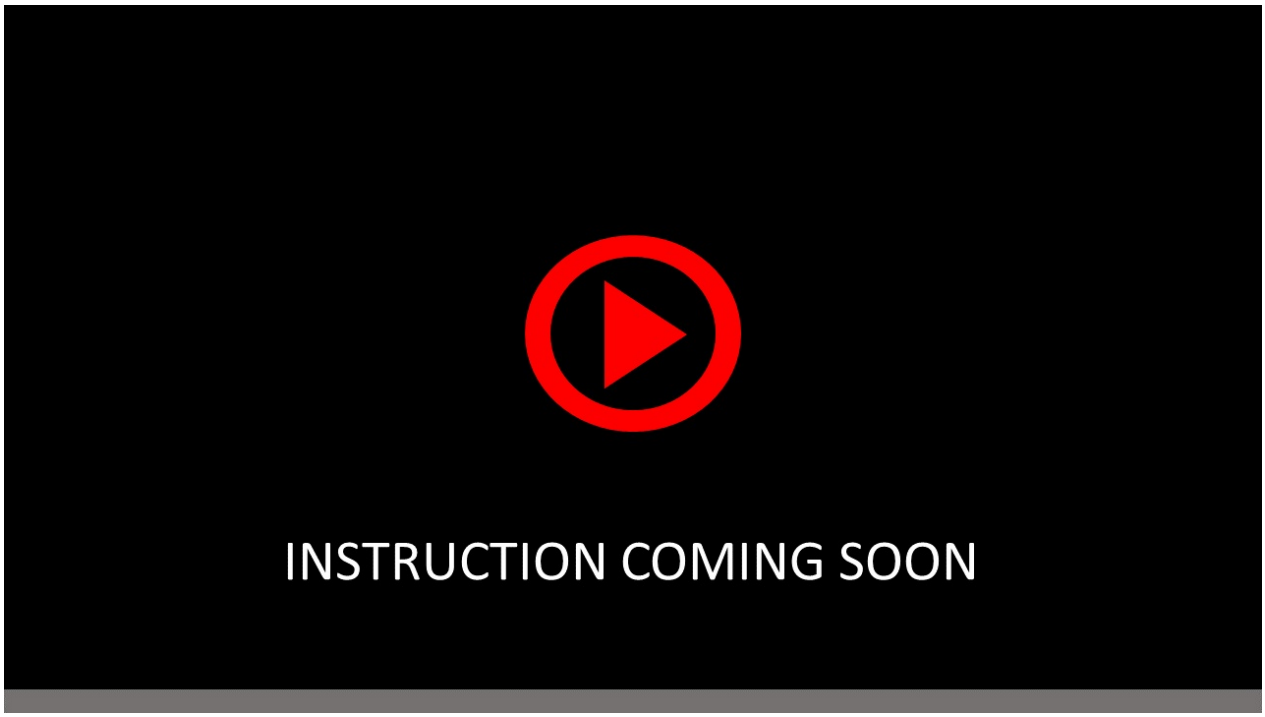


Next, the cyber defender will utilize hardware tools in combination with software tools, such as those found in Mercenary-Linux and Kali Linux, to interrogate the hardware and firmware. There are two paths for "hardware hacking" that we have discovered through our research, that can be applied to interrogate the firmware to detect vulnerabilities and adversary presence within the operating system and applications: non-destructive analysis and destructive analysis.

NON-DESTRUCTIVE ANALYSIS

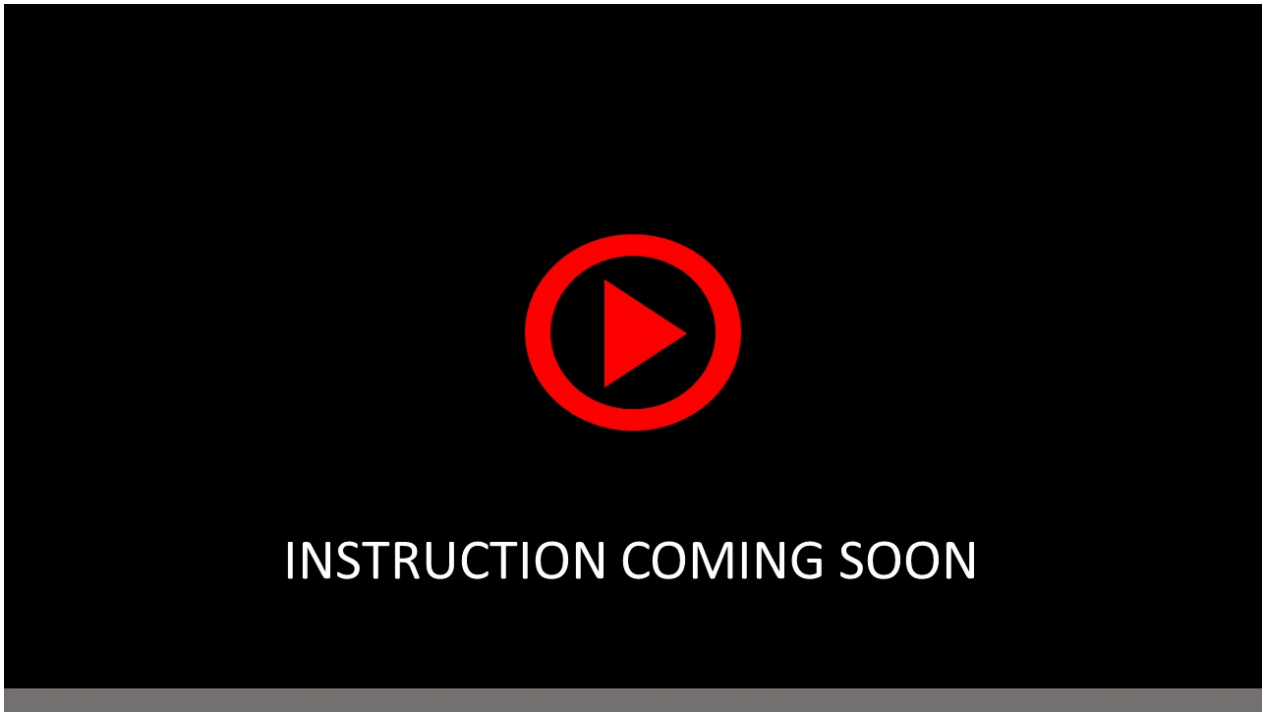
1. Locate and access the serial debug interface using an applicable hardware tool and an emulator

2. Escalate privileges to root (if necessary and not given root privileges upon connection)
3. Extract the firmware (if possible)
    i. Calculate and compare the cryptographic file hash of the firmware to those in the National database
    ii. If the firmware is compiled and/or obfuscated, deobfuscate and reverse engineer the firmware
    iii. Analyze the firmware using binwalk and other applicable software tools
    iv. Identify vulnerabilities and adversary presence in the operating system and applications
4. If firmware extraction is not possible, utilize scripts to audit the IoT device from the serial debug interface



DESTRUCTIVE ANALYSIS

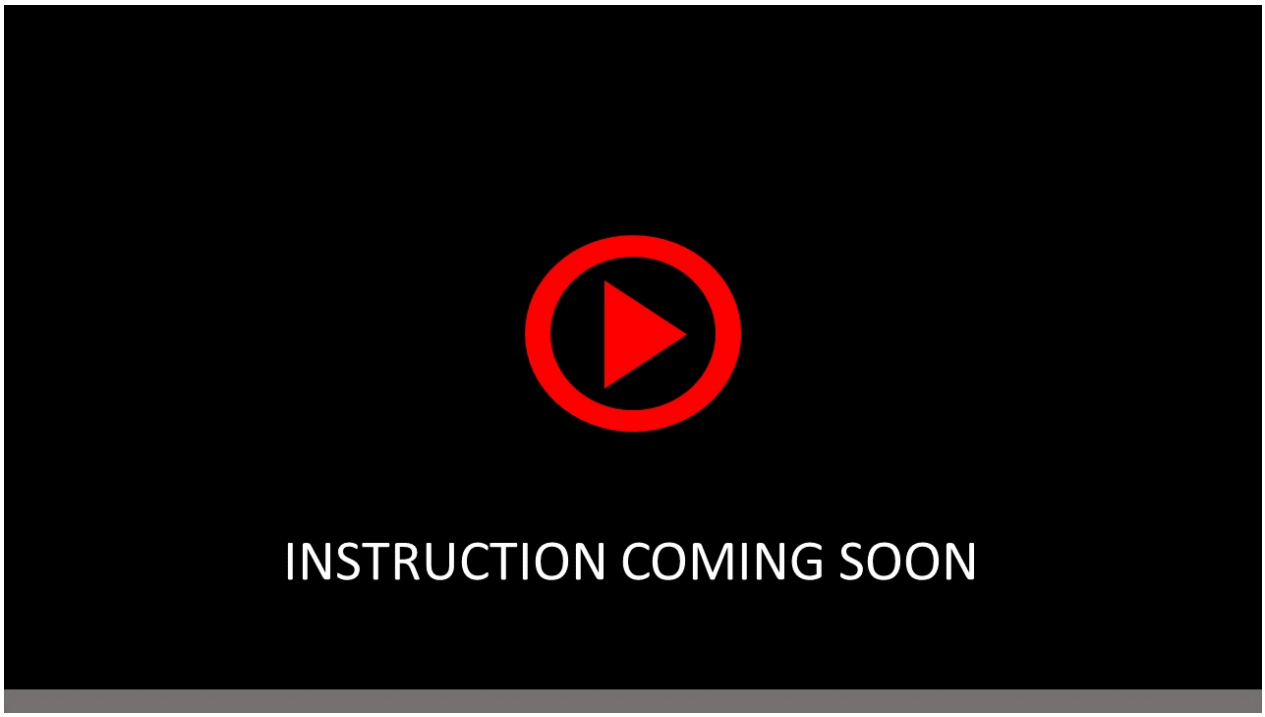
1. Utilizing desoldering techniques, remove the IC
2. Connect to an applicable device programmer
3. Extract the firmware (if possible)
    i. Calculate and compare the cryptographic file hash of the firmware to those in the National database
    ii. If the firmware is compiled and/or obfuscated, deobfuscate and reverse engineer the firmware
    iii. Analyze the firmware using binwalk and other applicable software tools
    iv. Identify vulnerabilities and adversary presence in the operating system and applications



Other related projects include Stealthy Dopant-Level Hardware Trojans and Low-Observable Physical Host Instrumentation for Malware Analysis (LO-PHI). Dopant-Level Hardware Trojans apply techniques to change the dopant polarity of specific parts of a gate during the manufacturing process [8]. Sugaware et al, rebuttal with research that proves that stealthy dopant-level circuits can be detected with scanning electron microscopy (SEM) or focused ion beam (FIB) imaging using a technique called passive voltage contrast [21]. LO-PHI is capable of physical-machine introspection of both non-volatile and volatile memory, i.e., hard disk and system memory [22].

Reconnaissance and identification of a device's electromagnetic spectrum capabilities can be trivial, unless manufacturer specifications are available. Hardware tools such as spectrum analyzers and software defined radio (SDR) peripherals to include the HackRF One, bladeRF, Ubertooth One, USRP B200/210, RFIDIer and others listed on rtl-sdr.com can be utilized to recon, identify, and analyze the frequencies and protocols that are utilized by an IoT device's electromagnetic spectrum capabilities [20]. There are also specialized communication tools built specifically to work with certain frequencies and protocols, e.g. 802.11x (2.4Ghz/5Ghz). There are a variety of protocols and associated vulnerabilities that can be found within electromagnetic spectrum capabilities. Examples include reverse engineering vintage wireless keypads, decoding public utility meters, hacking the Z-wave protocol, decoding NRF24L01+ and Bluetooth Low Energy (BLTE) transceivers, hacking wireless doorbells, decoding the Long Range(LoRa) IoT protocol, and the infamous Jeep hack [23][24][25][26][27][28]. We recommend referencing the book "Wireless Communications Security Solutions for the Internet of Things" by Jyrki T.J. Penttinen to learn about the different wireless technologies that are employed by IoT devices. Interrogating electromagnetic spectrum capabilities will follow a similar methodology to a classic 802.11x

wireless security assessment or penetration test, 1) remove all wireless communication devices from the area (smartphones, tablets, etc.), 2) with the assistance of manufacturer device manuals, recon and identify electromagnetic spectrum capable hardware (e.g. protruding antennas or modules on the PCB), 3) utilize a spectrum analyzer or SDR with spectrum analysis capabilities to pinpoint the frequency of electromagnetic energy radiating from the device, 4) utilize an SDR and software protocol analyzer to capture and parse the protocols transmitted over the identified frequencies, 5) interrogate captured traffic to detect vulnerabilities and adversary presence.

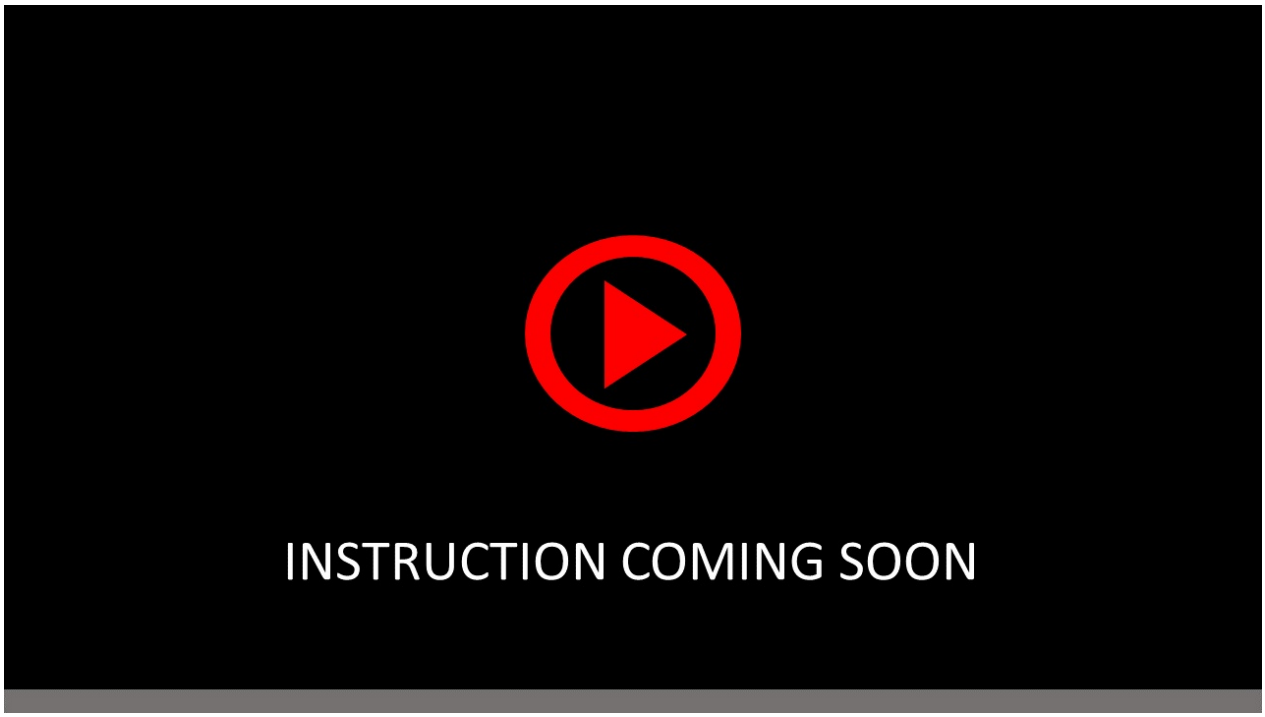


It is important to remember that even if an IoT device does not have organic electromagnetic spectrum capabilities, there could potentially be an inorganic embedded system implanted within the IoT device that provides an out-of-band (OOB) backdoor communication medium (e.g. RF technologies such as GSM within an implanted inorganic embedded system). This would mean that traffic leaving over this OOB backdoor communication medium would not be traversing your network and would be otherwise undetectable! This implant should have been detected if you have already conducted the aforementioned hardware recon and interrogation, but if it hasn't it should be found by analyzing the electromagnetic spectrum with a spectrum analyzer. If a device is emitting electromagnetic spectrum capabilities when the manufacturer's specifications do not include these capabilities, you could be dealing with an implant.

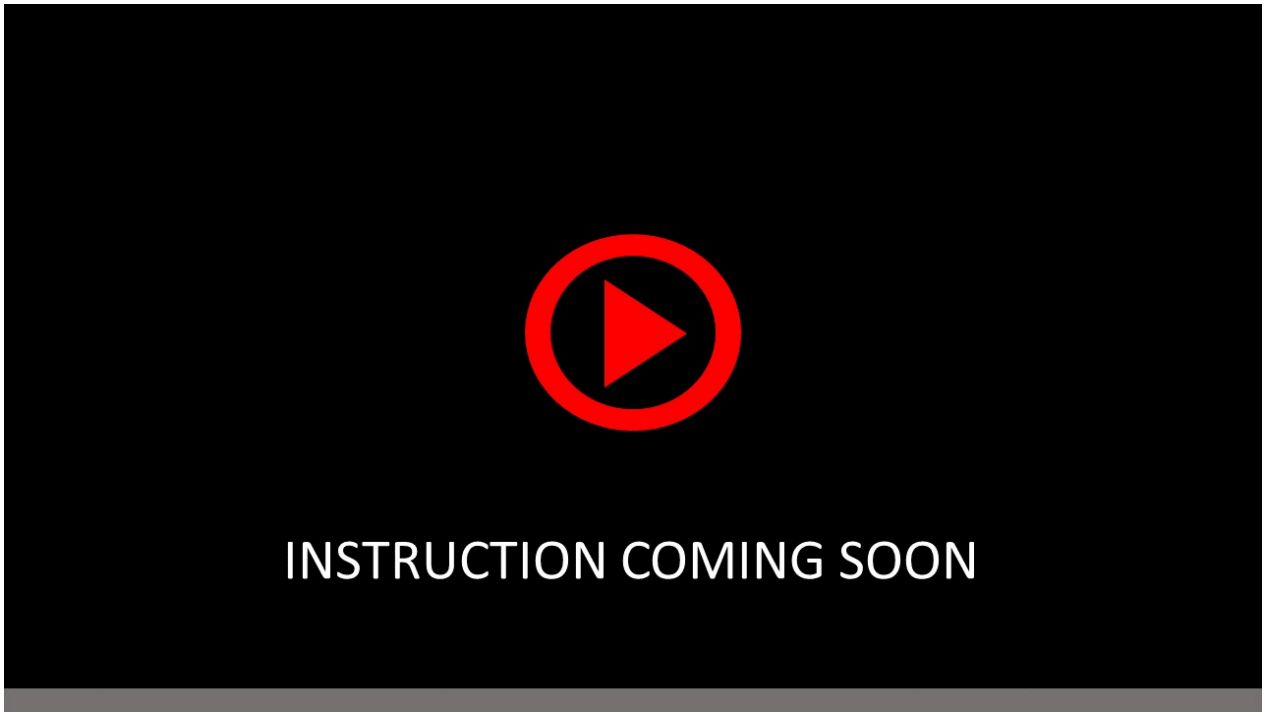
It is likely that most IoT devices will be susceptible to some form of aforementioned EA and ES tasks, to include electromagnetic jamming, electromagnetic pulse, and TEMPEST collection. Replicating these effects can be trivial, destructive, and potentially a violation of Federal or State laws. Thus, conducting a proper assessment may not be possible, however there are mitigations that can be put in place to protect against EW.

At this point our hardware, firmware, and electromagnetic spectrum capabilities reconnaissance and interrogation should be complete and the cyber defender should be ready to conduct reconnaissance and interrogation similar to a more familiar traditional security audit, vulnerability assessment, and penetration test. Some IoT devices may have limited terminal access from the network for configuration over SSH, rlogin, or telnet. Some IoT devices may not have direct access to the operating system, except through serial debug interfaces that require physical access. Configuration of other IoT devices may only be possible via a web service. What is interesting is that if a remote code execution (RCE) vulnerability exists within a network facing application or service, an adversary may be able to exploit that vulnerability to gain shell access that even the administrator might not have! Thus, when conducting the steps below, the cyber defender must be thorough:

- Passively analyze network traffic to identify vulnerabilities (e.g. lack of transport encryption) and adversary presence (e.g. beacons) in communication protocols

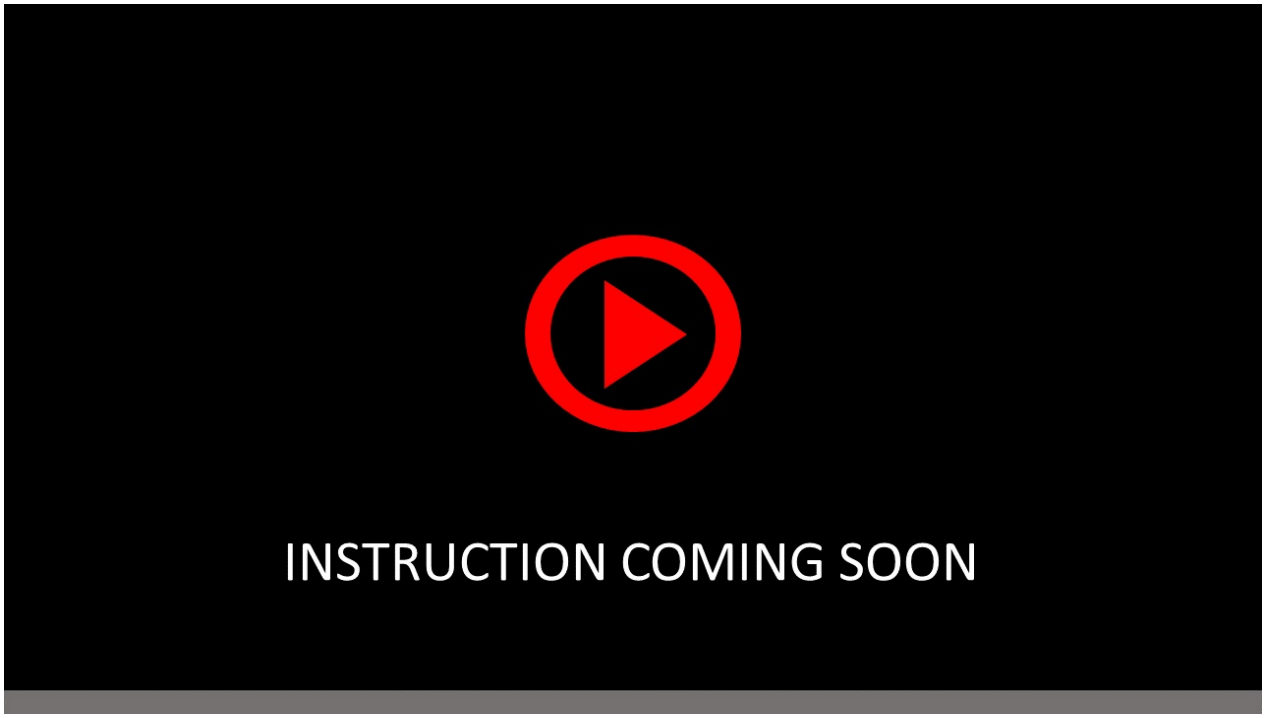


- Scan devices to identify open ports and services
- Conduct vulnerability assessments and penetration tests on services, paying special attention to web applications/interfaces, remote login services (e.g. telnet), and network services (e.g. SNMP, NTP, and others that allow control of the IoT device).
- Vulnerability scanners may not be able to conduct vulnerability assessments of uncommon IoT services, so manual interaction or fuzzing may be necessary. In addition, the cyber defender may be able to interrogate the service with custom scripts (e.g. Python scripts using Scapy libraries)



- If the cyber defender can access a remote login service (preferably as root), custom scripts and programs can be run to audit the operating system and applications to identify vulnerabilities, poor configurations, and adversary presence

The last portion of the physical network layer assessment is to recon and identify logs from intrusion detection systems, network appliances, and log aggregation services that are monitoring the IoT device and then analyzing those logs for adversary presence. It is also imperative that the cyber defender recon and identify systems that can control the IoT device within the local network (e.g. HMIs). These systems will also need to be interrogated for vulnerabilities and adversary presence using applicable methods within this framework



When executing these steps the depth and breadth to which a cyber defender can interrogate the IoT device may be limited by time, capability, and experience. It is very important that the cyber defender consider these variables and the criticality and function of the IoT device before an active engagement. Older embedded systems are notorious for having easily crashed services, so it would prove beneficial to conduct these steps on a non-production IoT device in a laboratory environment first.

Reconnaissance and Interrogation to Detect Vulnerabilities and Adversary Presence within the Logical Network Layer

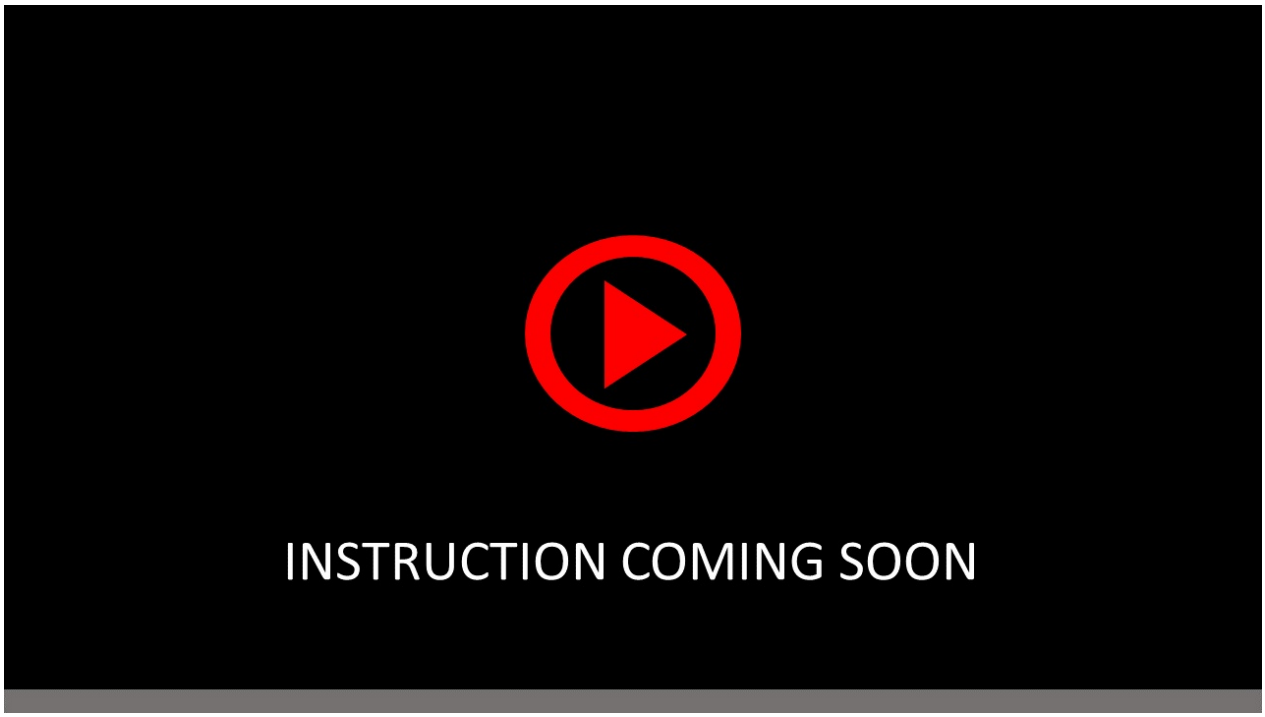
Extending an IoT device's capabilities into the cloud can provide many useful features including data aggregation and centralized management and administration. This additional functionality inherits additional complexities and risks. This includes complexities arising from the use of cloud services (e.g. Amazon EC2, Microsoft Azure, Twitter, etc.) that are hosted or managed by third party cloud providers. In addition, cloud services can change physical locations, to include locations outside of the homeland. It may not be possible to conduct reconnaissance and interrogation at the physical network layer on the cloud infrastructure. This should not limit the ability of the cyber defender in the conduct of reconnaissance and interrogation of the cloud service, though it should be understood that a compromise of the underlying cloud infrastructure at the physical network layer would also compromise the cloud service.

The primary concerns are data-in-transit to and from the cloud, data-at-rest in the cloud, and cloud interfaces which provide administrative access to and control of the IoT device in question. Holistically the steps would include:

- Recon and identify cloud services that are utilized by the IoT devices
- Interrogate data-in-transit to detect vulnerabilities and adversary presence
- Interrogate the cloud services to detect vulnerabilities and adverary presence
- Interrogate the cloud service's access to and control over the IoT device
- Interrogate the cloud service's protection mechanisms for data-at-rest

During the reconnaissance and interrogation of the physical network layer, the cyber defender passively analyzed network traffic to determine vulnerabilities in the IoT device's communication protocols, such as a lack of transport encryption. Repeating this step should not be necessary. The cyber defender would then need to access and interrogate each cloud service to detect vulnerabilities and adversary presence. This may include conducting actions covered in the reconnaissance and interrogation of the physical network layer against the cloud service and related physical hardware. It may be necessary to check contracts with the service provider before moving forward. The cyber defender can still analyze application vulnerabilities, password strength and other items even if it is only possible to access the cloud service itself. Furthermore, the cyber defender should interrogate the cloud service's access to and control over the IoT devices. This would include determining what users have access, what control can be manipulated (e.g. firmware

updates), what authentication mechanisms exist for the server and client side for control and data-in-transit. Lastly, the cyber defender should interrogate the cloud service's protection for data-at-rest. This includes determining whether drive and database encryption exists.

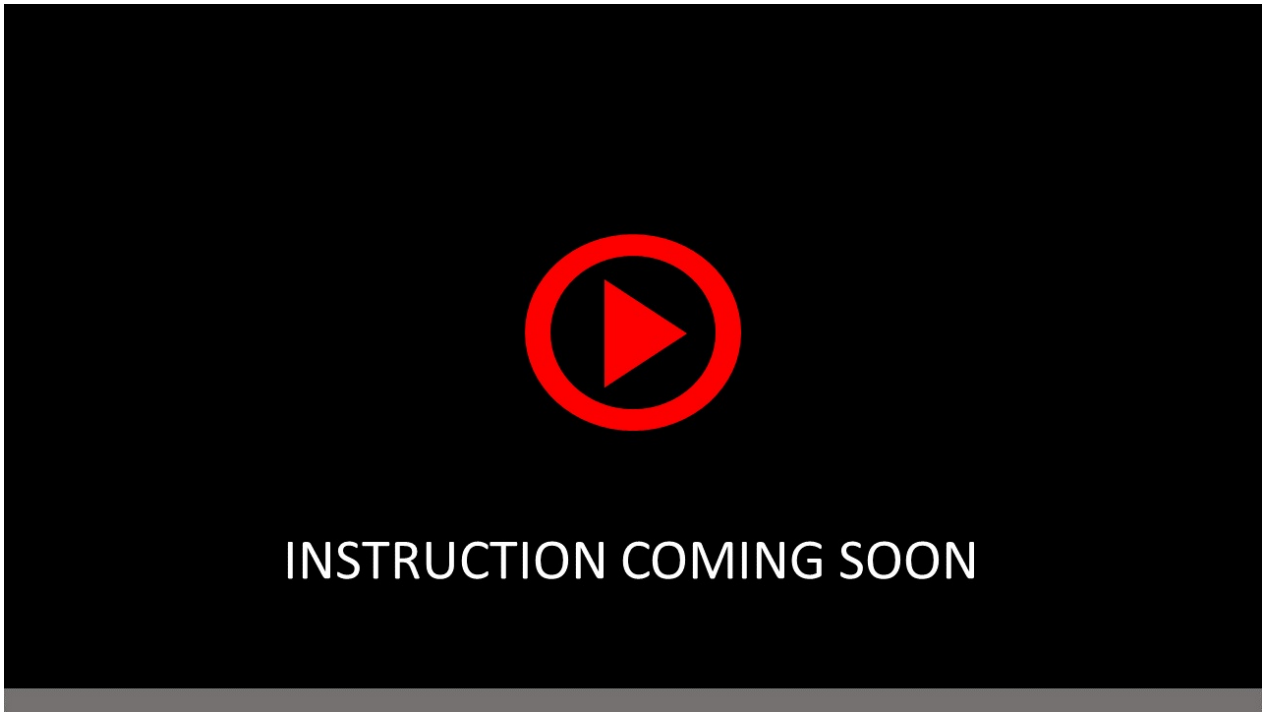


Reconnaissance and Interrogation to Detect Vulnerabilities and Adversary Presence within the Cyber-Persona Layer

Within the cyber-persona layer our primary objective is to identify the people associated with the IoT and the vulnerabilities that these people expose through the projection of their cyber-personas. This portion of the framework is less technical than previous sections, though technical methods (e.g. search engines) can be deployed to improve the efficiency of the steps required to conduct reconnaissance and interrogation and this layer. A good starting place for researching cyber-personas is “Untangling the Web: A Guide to Internet Research” which is a book written by the NSA. It is important to note that there may be legal concerns with conducting this portion of the framework if data that is not publicly available is required. The following steps should be employed to identify the cyber-personas associated with IoT devices:

- Recon and identify the people associated with the IoT device (e.g. system administrators)
- Recon and identify individual work user accounts, individual work e-mail addresses, etc. associated with the person
- Recon and identify group accounts, organizational mailboxes, and distribution lists associated with the person
- Recon and identify publicly available information about the person via search engines
- Recon and identify legitimate and illegitimate social media accounts (e.g. Facebook, PlayStation Plus, Twitter, etc.) associated with the person
- Compile a profile of collected information and analyze to determine vulnerabilities and adversary presence (e.g. insider threats) within each cyber-persona

It is critical to understand the cyber-persona(s) and associated information that people are projecting into cyberspace, as it can be leveraged by an adversary to obtain access to the IoT device. Further development of the section of the framework will require assistance from law enforcement, intelligence analysts, and others who have a firm understanding of human intelligence targeting and the human’s relation to the IoT device. Additionally, the framework should include steps to recon and identify adversary cyber-personas.

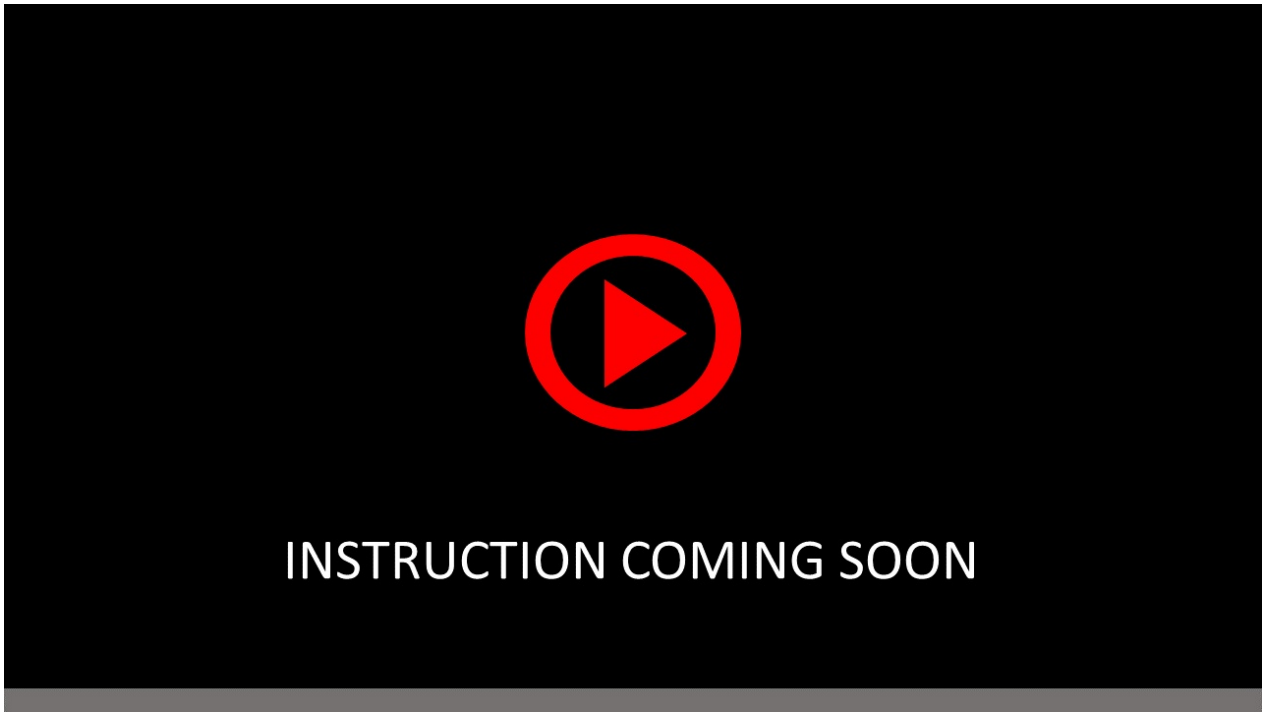

INSTRUCTION COMING SOON

Mitigating Vulnerabilities and Protecting Against Adversary Attacks within the Physical Network Layer

Within the physical network layer there are steps that can be taken to mitigate the vulnerabilities and protect against adversary attacks identified during the reconnaissance and interrogation steps:

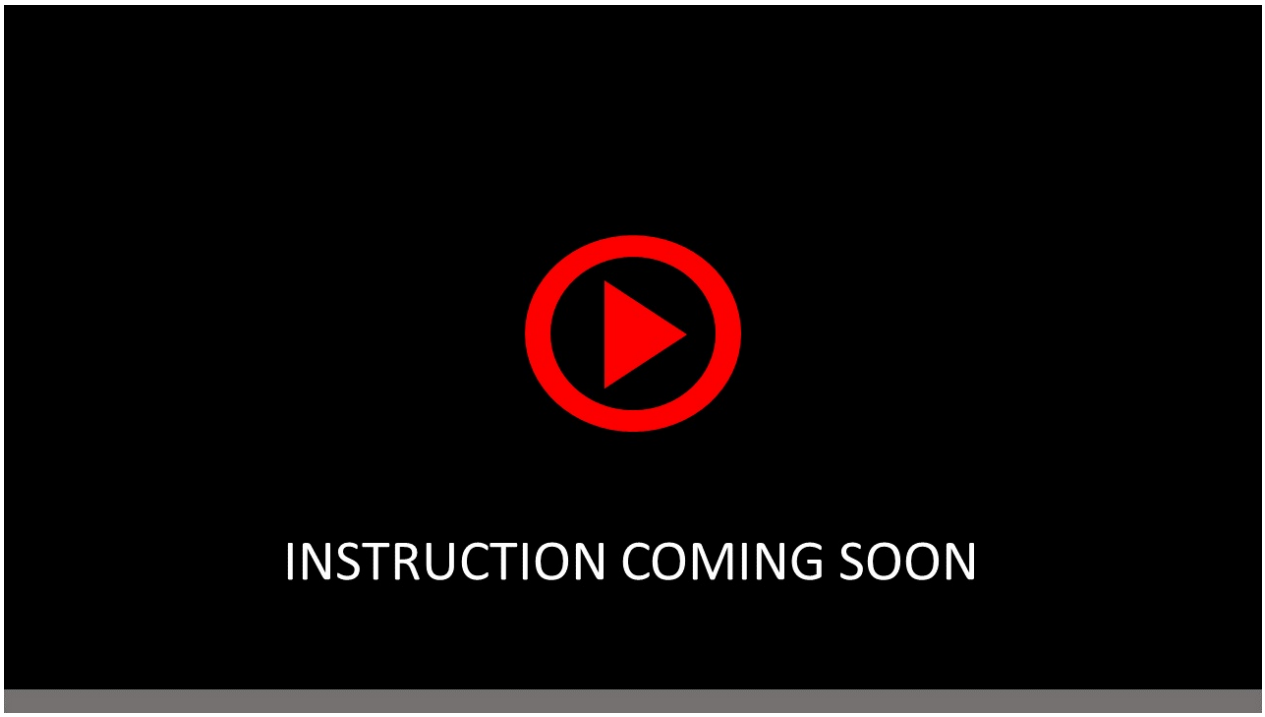
- Ensuring that the manufacturer sources electronic components from trusted sources
- Ensuring that the manufacturer tests electronic components, such as ICs, for adversary presence
- Integrating tamper evident security devices and enclosures for IoT devices during the supply chain process
- Integrating tamper evident security devices and enclosures for IoT devices while deployed
- Building and tuning intrusion detection systems (IDS) and intrusion prevention systems (IPS) to applicable vulnerabilities on both TCP/IP and non-TCP/IP networks that are operating over physical or electromagnetic spectrum communication mediums
- Patching vulnerabilities within the embedded OS and applications
- Securely configuring the embedded OS and applications, to include the use of secure network communication protocols
- Protecting devices from EW effects

To the cyber defender, many of the mitigation and protection techniques are self-explanatory. However, it is important to remember that services like Telnet may be hardcoded to be enabled and cannot be shutoff unless the firmware is modified (especially in older devices). This may require that the cyber defender contact the vendor when he discovers new vulnerabilities, so they can be patched. It may also be possible for the cyber defender to patch the firmware/embedded operating systems and applications in house, however the cyber defender should report the findings for integration into the National database.
To protect devices from EW effects (when electromagnetic capabilities are not needed) the cyber defender will need to implement enclosures, cabinets, or building materials that produce an “radio frequency (RF) shielding”, “electromagnetic shielding”, or “high-altitude electromagnetic pulse protection (HEMP) shielding” that follows applicable guidance such as IEEE Std. 299.1-2013, MIL-STD-188-125-1, NSA 94-106, NSA 73-2A, ASTM D4935, and MIL-HDBK-1195. Essentially, the cyber defender will create a faraday cage to protect each individual IoT device, an enclosure of IoT devices, or an entire facility. This may only be useful if the device does not have electromagnetic spectrum capabilities.


INSTRUCTION COMING SOON

Mitigating Vulnerabilities and Protecting Against Adversary Attacks within the Logical Network Layer

At the logical network layer the cyber defender’s focal point will be mitigating vulnerabilities associated with data-in-transit to the cloud, data-at-rest in the cloud, and the cloud service’s access to and control over the IoT. Most of the mitigations will involve fixing poor security configurations and protecting data-in-transit and data-at-rest.



Mitigating Vulnerabilities and Protecting Against Adversary Attacks within the Cyber-Persona Layer

Did the previous statement about categorizing negligence that leads to your IoT devices harboring cyber actors as treason catch your attention? If not, maybe you can develop a better narrative to raise awareness about this issue? That's exactly what will help mitigate the security violations that arise from people being associated with the IoT devices. Through almost a year of interaction with other cyber defenders, I have found that most are not familiar with the IoT or embedded systems. However, many of those cyber defenders do know what SCADA/ICS is, but they did not realize that the PLC and DCS have many relatives in the IoT that surround us every day. Though the focus at the USG level is on critical infrastructure, there are so many things that control our safety, security, and livelihood every single day. It is up to each individual to decide the criticality of each, if not all, IoT devices that they own or interact with. There are also narratives that are meant to scare people, such as their cars being run off the road by hackers. For the betterment of humanity, it is best that people feel comfortable embracing the IoT with understanding, rather than discarding it out of fear.

It is also important that we help each person understand their responsibility in reducing their exposure in cyberspace via their cyber-personas, especially if they interact with IoT devices within critical infrastructure. Even if it older information, it really is not necessary to put the PLC manufacturer, model number, and precise area within the manufacturing facility that the PLC resides and operates on LinkedIN (Figure 4). It makes the person a target for phishing attacks and other social engineering attacks and aids adversaries in their quest for swiss cheese in the maze that is cyberspace.


Search for people, jobs, companies, and more...
GM Spring Hill Assembly Plant, TN.
Support ICS SCADA Cimplicity D/V Routing and Tracking within the CIM Routing in . Knowledge of Cimplicity NT (devices, points, alarms, events, CimBasic, CimEdit, CimView, Data logging, etc). Knowledge of GE-Fanuc and Allen Bradley PLCs (Series 6, 90/30, & 90/70, etc).
INSTRUCTION COMING SOON

REFERENCES

[1] M. U.Farooq, M. Waseem, S. Mazhar, A. Khairi and T. Kamal, "A Review on Internet of Things (IoT)", International Journal of Computer Applications, vol. 113, no. 1, pp. 1-7, 2015.

[2] C. Benson, "The Internet of Things, IoT Systems, and Higher Education", EDUCAUSE Review, no., pp. 34-43, 2016.

[3] Chairman Joint Chiefs of Staff, "Joint Publication 3-12 Cyberspace Operations", Chairman Joint Chiefs of Staff, 2013.

[4] United States Army, "FM 3-38: Cyber Electromagnetic Activities", United States Army, 2014.

[5] "Tempest (codename)", En.wikipedia.org, 2016. [Online]. Available: https://en.wikipedia.org/wiki/Tempest_\(codename\). [Accessed: 08- Dec- 2016].

[6] L. Constantin, "Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON", CSO Online, 2016. [Online]. Available: http://www.csoonline.com/article/3119765/security/hackers-found-47-new-vulnerabilities-in-23-iot-devices-at-def-con.html. [Accessed: 08- Dec- 2016].

[7] D. Miessler, "Securing the Internet of Things: Mapping Attack Surface Areas Using the OWASP IoT Top 10", in RSA Conference 2015, San Francisco, 2015.

[8] G. Becker, F. Regazzoni, C. Paar and W. Burleson, "Stealthy dopant-level hardware Trojans: extended version", Journal of Cryptographic Engineering, vol. 4, no. 1, pp. 19-31, 2014.

[9] "18 U.S. Code § 2381 - Treason", Legal Information Institute, 2016. [Online]. Available: https://www.law.cornell.edu/uscode/text/18/2381. [Accessed: 08- Dec- 2016].

[10] Department of Homeland Security, "National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience", Department of Homeland Security, 2013.

[11] Department of Homeland Security, "Fiscal Years 2014-2018 Strategic Plan", Department of Homeland Security, 2014.

[12] United States Congress, "National Cybersecurity Protection Act of 2014", United States Congress, 2014.

[13] United States Congress, "Cybersecurity Enhancement Act of 2014", United States Congress, 2014.

[14] United States Congress, "Cybersecurity Information Sharing Act of 2014", United States Congress, 2014.

[15] United States Congress, "Cybersecurity and Infrastructure Protection Agency Act of 2016", United States Congress, 2016.

[16] United States Congress, "State and Local Cyber Protection Act of 2015", United States Congress, 2015.

[17] United States Congress, "Cyber Preparedness Act of 2016", United States Congress, 2016.

[18] United States Congress, "Small Business Cyber Security Improvement Act of 2016", United States Congress, 2016.

[19] National Institute for Science and Technology, "Framework for Improving Critical Infrastructure Cybersecurity", National Institute for Science and Technology, 2013.

[20] J. Grand, "Tools of the Hardware Hacking Trade", Black Hat Webcast, 2014.

[21] T. Sugawara, D. Suzuki, R. Fujii, S. Tawa, R. Hori, M. Shiozaki and T. Fujino, "Reversing stealthy dopant-level circuits", Journal of Cryptographic Engineering, vol. 5, no. 2, pp. 85-94, 2015.

[22] C. Spensky, H. Hu and K. Leach, "LO-PHI: Low-Observable Physical Host Instrumentation for Malware Analysis", Graduate, Massachusetts Institute of Technology-Lincoln Laboratory, 2016.

[23] "Reverse Engineering a Vintage Wireless Keypad with an RTL-SDR", rtl-sdr.com, 2015. [Online]. Available: http://www.rtl-sdr.com/reverse-engineering-a-vintage-wireless-keypad-with-an-rtl-sdr/. [Accessed: 08- Dec- 2016].

[24] "Decoding Public Utility Meters with an RTL-SDR", rtl-sdr.com, 2015. [Online]. Available: http://www.rtl-sdr.com/decoding-public-utility-meters-with-an-rtl-sdr/. [Accessed: 08- Dec- 2016].

[25] "Sniffing and Decoding NRF24L01+ and Bluetooth LE Packets with the RTL-SDR - rtl-sdr.com", rtl-sdr.com, 2014. [Online]. Available: http://www.rtl-sdr.com/sniffing-decoding-nrf24l01-bluetooth-le-packets-rtl-sdr/. [Accessed: 08- Dec- 2016].

[26] "Hak5: Hacking Wireless Doorbells and Software Defined Radio tips", rtl-sdr.com, 2016. [Online]. Available: http://www.rtl-sdr.com/hak5-hacking-wireless-doorbells-and-software-defined-radio-tips/. [Accessed: 08- Dec- 2016].

[27] "Decoding the LoRa IoT Protocol with an RTL-SDR", rtl-sdr.com, 2016. [Online]. Available: http://www.rtl-sdr.com/decoding-the-iot-lora-protocol-with-an-rtl-sdr/. [Accessed: 08- Dec- 2016].

[28] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It", WIRED, 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Accessed: 08- Dec- 2016].

[29] J. Garamone, "Vice Chairman: Military, Nation Need Dialogue About New Technologies," 21 January 2016. [Online].Available: http://www.defense.gov/News/Article/Article/643978/vice-chairman-military-nation-need-dialogue-about-new-technologies.