CAPSTONE PROJECT

TEAM “THE HOMIES”

HACK-A-HOME Research Project

FULLSTACK ACADEMY

2311-FTB-ET-CYB-FT-B

Bryan Ramirez, Matthew Cepiel, Sarah Garrett, Jonah Bohumir

February 2024

HACK-A-HOME

"The Internet of Things (IoT) has transformed various domains in our lives by enabling seamless communication and data exchange between interconnected devices, necessitating robust networking infrastructure… Code injection attacks exploit security weaknesses in applications or software and can have severe consequences, such as data breaches, financial losses, and denial of service… IoT applications are exposed to such attacks… victims' devices become exposed to a full range of cyber-attacks following a successful severe code injection attack… By understanding the vulnerabilities and potential consequences of code injection attacks on IoT networks and devices, researchers and practitioners can develop more secure IoT systems and better protect against these emerging threats." (Noman & Abu-Sharkh, 2023)

"Billions of Internet of Things (IoT) devices and sensors are expected to be supported by fifth generation (5G) wireless cellular networks. This highly connected structure is predicted to attract different and unseen types of attacks on devices, sensors, and networks that require advanced mitigation strategies and the active monitoring of the system components. Therefore, a paradigm shift is needed, from traditional prevention and detection approaches toward resilience." (Uslu et al., 2022)

Threats Identified

A DDoS attack is an attempt to make a device or network unavailable to its legitimate users by flooding it with traffic or requests for information. Hijacked IoT devices can be used to overwhelm servers and cause downtime, which hackers can exploit to ransom businesses.

In a man-in-the-middle attack, a hacker intercepts communication between two devices or networks and impersonates one of the parties to gain access to confidential information. Man-in-the-middle attacks can lead to loss or theft of personal data and compromise a business's

reputation. Due to the large number of endpoints of IoT systems, man-in-the-middle attacks are unfortunately common.

A password attack is an attempt to gain access to a device or network by guessing or brute-forcing the password. It is vital to make sure you have chosen a secure and unique password, as passwords can be leaked, and data sold on the dark web. Making sure you use strong, unique passwords for all devices and applications can help reduce vulnerabilities.

Malware is software that is designed to damage or disable a device or network. IoT devices are particularly vulnerable to malware because they often have less security than traditional devices or computers. Making sure your devices are updated with the latest patches, as well as securing them with other measures helps to prevent malicious malware attacks.

Physical attacks on IoT devices are becoming more common as hackers realize that many of these devices are not well-secured against tampering. Physically attacking an IoT device can allow a hacker to bypass security measures on one device or multiple devices and gain access to sensitive data or control of the device itself.

These updates replace legitimate firmware with malicious code that can be used to take over the device or steal data stored on it. Due to the need to update IoT devices often, they can be exploited easily by malicious firmware update vulnerability.

Wireless connections that are not properly secured can be exploited by attackers in order to gain access to the network or devices connected to it. Due to low security measures on IoT devices, and their need to be connected to the internet, hackers can exploit poorly secured devices.

These attacks exploit human weakness rather than attack surface weaknesses in the IoT. In a social engineering attack, an individual or group will be targeted by a hacker posing as a

legitimate entity. They will then attempt to exploit this by gaining access to details that will help them compromise the whole IoT system.

Phishing is a type of online fraud that involves tricking someone into giving away their personal information, such as their login credentials or credit card number. Hackers can use phishing emails or fake websites to try to steal your information. To protect yourself from phishing attacks, be suspicious of any email or website that asks for personal information, especially if it looks like it could be fake.

Finally, “eavesdropping” attacks are also becoming more common as IoT devices become more prevalent. These occur when an attacker listens in on communications between devices to gather sensitive information such as passwords or credit card numbers. (José, 2023)

Vulnerable Devices

With a simple $14 laser pointer, hackers can hijack your home and disable smart locks and other sensitive electronics from as far as 360 feet! These are some common smart devices in your home Internet of Things (IoT) devices that hackers can hijack.

Wireless Laptops. This first item may seem obvious, but laptops can be accessed remotely, through the Internet, with phishing emails (where you click links or update credentials under false pretenses) or compromised USB, to name a few. In a short time, a hacker can access your bank’s login and password, social security number, credit card information and much more.

Online Gaming Systems. The player in online gaming is the biggest security weakness in this scenario, not the gaming console. Don’t share private information with other players in a multi-player game that will allow malicious efforts to gain control of your account and other personal information, which may provide access to other systems.

Webcams. Home surveillance systems, smartphone cameras and traditional webcams can all spy on you. Webcam spy software can be spread with spam emails and infected attachments,

links to fake websites and other malware attacks. Many webcam lights, which typically notify you when they're on, can be turned off while the webcam is recording. Want a quick fix? Cover your webcam or disable it. The camera can still hear you, but at least you can't be watched. Also, make sure your software is up to date to ensure your firewall is enabled and only use your cameras over a secure connection. In other words, avoid public WIFI! And as always, think before you click and update software when prompted.

Home Wireless Network. A wireless router allows multiple devices to connect to your Internet provider, or home network, quickly. With so many wireless devices connecting to this out-of-sight, out-of-mind device, it's important to remember it's also one of the most critical gateways into your home! In addition to a strong password, you can enhance its security by Changing the name of your Wi-Fi network.

Relocate its location to the most central part of your home, essentially increasing its signal reach to the entire house and decreasing the signal strength from the road (where the signal can be intercepted by cybercriminals).

Change the default IP address (and then make sure to type in the new IP address in the Web browser bar). Disable remote access. Keep software up to date. Unfortunately, this is often a manual process since routers don't tend to update automatically.

Smart Light Bulbs. According to a recent study by the University of Texas at San Antonio, many of these smart light bulbs are infrared enabled, meaning hackers can send commands via the infrared invisible light emanating from the bulbs to either steal data or spoof other connected IoT devices on the home network. In other words, anything saved to your computer, such as photos, or your phone's text messages, can be stolen. Learn more about this new security gap here.

Smart TVs. Internet-enabled TVs are soft targets for hackers. Known for having security vulnerabilities, cybercriminals are often able to exploit these flaws in some TVs, from simply messing with your TV settings (such as changing your channels or volume) to using its built-in digital assistants to access your home's digital thermostats, security cameras, online shopping accounts, and other on-demand services.

Coffee Makers. Does scheduling your morning brew from a smartphone app sound appealing? Hackers think so! Smartphones can connect to almost anything these days, including smart coffee makers. To work, however, the coffee maker must be connected to your home WIFI network. If a hacker can access your coffee maker, then they can infiltrate everything else in your home.

Smart Phones. Considering how smartphones are now used to store sensitive data, photos, email, and more. They can also be used for purchasing goods, banking, and paying at cash registers, mobile phones are a valuable target for cyber attackers. Additionally, smartphones share many of the same vulnerabilities as your computer. Read this US-Cert report on threats to mobile phones and how to protect them.

Smart Refrigerators. Does your smart fridge have a Web browsing capability or WIFI signal linked to your smartphone to update you on grocery content? Then it too is vulnerable to hackers. A smart fridge may not have any obvious personal risks, but they are still connected to various Web services, banking systems, and other institutions, including the manufacturer. Many smart refrigerators can also have generic admin email accounts associated with them, which allows repairmen to access their software for updates or other repairs quickly. If a cybercriminal is aware of these weaknesses, they can access your data and other pertinent information.

Portable Radios. Is it connected to Internet radio, and therefore your home's WIFI network? Then it's susceptible to cyber vulnerabilities.

Remember, “smart” doesn’t always mean “secure”. It’s up to each of us to take responsibility for our cybersecurity and ensure the privacy of our own smart homes. Hackers are not likely going to use their skill set to open the locks to your front door, but they may use these IoT devices to exploit your data or the systems they’re connected to, such as banks or security companies.) ("Hackers can hijack your home with these 10 smart devices," 2024)

Remediation

Here are some tips on how to defend connected devices against IoT hacks: First and foremost, make sure your devices are running the latest software updates. Hackers are constantly finding new ways to exploit vulnerabilities, so manufacturers are always working to patch them. By keeping your devices updated, you’ll be able to stay one step ahead of hackers. Next, enable two-factor authentication wherever possible. This will add an extra layer of security to your accounts and make it much harder for hackers to gain access. Finally, be careful about what information you share online. Hackers can use IoT devices to collect data about you, so it’s important only to share what you’re comfortable with making public. Think carefully before sharing things like your address, birthday, or credit card number online. There are several steps that you can take to prevent yourself from being vulnerable to an IoT hack. By following best practices such as using strong passwords, keeping your mobile devices always updated with the latest software, and monitoring your network for suspicious activity or malware you can protect yourself from any attack. (José, 2023)

There’s no way to guarantee your home will be 100 percent secure. However, you can take some simple steps to create a more secure environment.

To begin, research smart devices before you buy. Ask yourself, are there any known vulnerabilities that can expose your home network? If yes, can you secure the device? It’s also important to take inventory of the devices in your home and identify how they are connected to

your WIFI system. Take note of each device's ISP and password, if appropriate, and make sure each password is unique.

Upon purchasing your smart device, take time to read the fine print and consider its default privacy and data-sharing settings. Unless the device needs to provide a constant stream of data to the manufacturer or a third party, turn off this setting. Of course, if your devices are connected to your home's WIFI router, make sure that the router is also secure.

Increased incidents of phishing scams, malware intrusions, and other cybersecurity breaches will only increase as our homes become more dependent on IoT devices. There's no need to stay off the grid. However, if we all take precautions now to stay aware of cybersecurity concerns, we can stop hackers from hijacking our homes and create a safe space for everyone. ("Hackers can hijack your home with these 10 smart devices," 2024)

Intro

Smart TVs have become an integral part of our homes, offering both entertainment and connectivity. However, as these devices become more sophisticated and interconnected, there's a growing concern about their vulnerability to hacking. In this exploration, we'll delve into the potential risks associated with smart TVs, examining how their advanced features and connectivity options can pose threats to user privacy and data security. Understanding these potential vulnerabilities is crucial for users to navigate the landscape of smart TV technology securely.

Potential Vulnerabilities in a Smart TV

- Insecure Network Connections
- Weak or default Wi-Fi passwords can be exploited by attackers to gain unauthorized access to the smart TV and potentially other connected devices on the network.

- “Hackers can mine your TV apps (Netflix, Hulu, etc.) for payment information and can use your TV as a gateway to get into other connected devices in your home.” (Mckinley, 2022)
- Outdated Firmware and Software
- Smart TVs may run outdated firmware or software, lacking the latest security patches. Attackers can exploit known vulnerabilities present in outdated versions.
- Insecure Communication Protocols
- Weak or improperly implemented encryption protocols in communication channels between the smart TV and other devices may expose data to interception or tampering.
- Unauthorized Access to USB Ports
- USB ports on smart TVs could be exploited for unauthorized access or the injection of malicious files if not properly secured.
- “Another way hackers can gain access to your smart TV is by using an infected USB drive. This works by inserting the USB drive into the device, which then executes any malicious code stored on it. The inserted USB drive can install additional malicious software on the smart TV and compromise its security.” (Bhardwaj, 2023)
- Insecure Application Stores
- Some smart TVs allow users to download and install third-party applications. If the application store lacks proper security measures, users may inadvertently download malicious apps.
- “Man-in-the-middle (MitM) attacks occur when a hacker intercepts communication between two parties, acting as an intermediary. Hackers can use this technique to gain access to a smart TV's data by intercepting the packets of information passing between the device and its intended destination.” (Bhardwaj, 2023)
- Weak Authentication Mechanisms

- Smart TVs may use weak authentication methods, making them susceptible to unauthorized access or brute-force attacks on login credentials.
- Privacy Concerns with Microphones and Cameras
- Smart TVs with built-in microphones and cameras raise privacy concerns. If not properly secured, attackers could potentially compromise user privacy by accessing these features.
- “A few years ago, according to the FBI, app developers Vizio, LG, and Samsung were caught snooping on viewers. The FTC had to step in and stop them. Also, the CIA and MI5 were able to access information on smart TVs and listen in on private conversations using the camera and microphones on these devices.” (Whitney, 2023)
- DDoS Attacks
- Smart TVs connected to the internet may be vulnerable to Distributed Denial of Service (DDoS) attacks, where attackers overload the device or network, causing disruptions.
- Unsecured API Endpoints
- Smart TVs often use APIs (Application Programming Interfaces) for communication. If these endpoints are not properly secured, attackers might exploit them to manipulate the device or extract information.
- Lack of User Awareness
- Users may inadvertently contribute to vulnerabilities by not being aware of security best practices, such as using weak passwords or failing to update firmware regularly.
- Manufacturer-Specific Issues
- Security vulnerabilities can arise from manufacturer-specific software or hardware issues. Some manufacturers may prioritize usability over security, potentially exposing devices to risks.

Raise Awareness on Potential Security Risks on Hacking Smart TVs

Educational Campaigns:

Develop educational materials, or online content explaining common security risks associated with smart TVs. Highlight the importance of staying informed and implementing security measures

Social Media Outreach:

Utilize social media platforms to share concise and visually appealing infographics, videos, or posts about smart TV security. Create awareness campaigns using popular hashtags to reach a wider audience.

Collaborate with Tech Communities:

Engage with technology communities, both online and offline, to share insights on smart TV security. Collaborate with cybersecurity experts to provide credible information and guidance.

Create an Awareness Website or Blog:

Establish a dedicated website or blog focused on smart TV security. Provide regularly updated content, tips, and news to keep users informed about the latest threats and preventive measures.

Ring doorbells revolutionize home security and convenience by integrating cutting-edge technology into a familiar household fixture: the doorbell. With a Ring doorbell, homeowners gain the ability to see, hear, and speak to visitors at their door, whether they're at home or away. These smart doorbells feature motion detection, HD video recording, and two-way audio

communication, allowing users to monitor their doorstep and communicate with guests or intruders remotely via a smartphone app. Ring doorbells provide peace of mind, enabling users to enhance the security of their homes and streamline package deliveries, all with the convenience of modern technology.

Vulnerabilities

- **Privacy Concerns**: Ring doorbells have faced criticism regarding user privacy, particularly regarding the handling of user data and video footage. There have been instances of unauthorized access to Ring cameras, leading to concerns about the security of personal information.
- **Weak Passwords**: Like many IoT devices, Ring doorbells can be vulnerable to attacks if users set weak passwords or fail to change the default password. Hackers may exploit this vulnerability to gain access to the device and its associated accounts.
- **Unencrypted Communication**: In the past, there have been concerns about unencrypted communication between Ring devices and the Ring servers, potentially exposing sensitive information to interception by malicious actors.
- **Firmware Vulnerabilities**: Vulnerabilities in the firmware of Ring doorbells could be exploited by attackers to gain unauthorized access to the device, intercept video streams, or execute other malicious activities.
- **Physical Tampering**: Ring doorbells installed in public areas could be subject to physical tampering or vandalism, leading to potential security breaches or disruption of service.

- **Denial of Service (DoS) Attacks**: Ring doorbells could be targeted by DoS attacks, which overwhelm the device or the associated network with a flood of traffic, rendering them unavailable for legitimate use.
- **Third-Party Integration Risks**: Integrating Ring doorbells with third-party services or devices may introduce additional vulnerabilities, especially if those services or devices have their own security flaws.

Lawsuit

Ring doorbell as stated by the FTC (Federal Trade Commission) says that rings' poor privacy and lax security let employees spy on customers through their cameras, including those in their bedrooms or bathrooms, and made customers' videos, including videos of kids, vulnerable to online attackers. Hackers exploited those vulnerabilities and harassed, insulted, and propositioned children and teens through their Ring cameras. Some hackers even live streamed customers' videos. In a settlement, Ring agreed to establish a privacy and security program and delete the videos it shouldn't have — in addition to paying $5.8 million to affected customers

Findings and exploitation

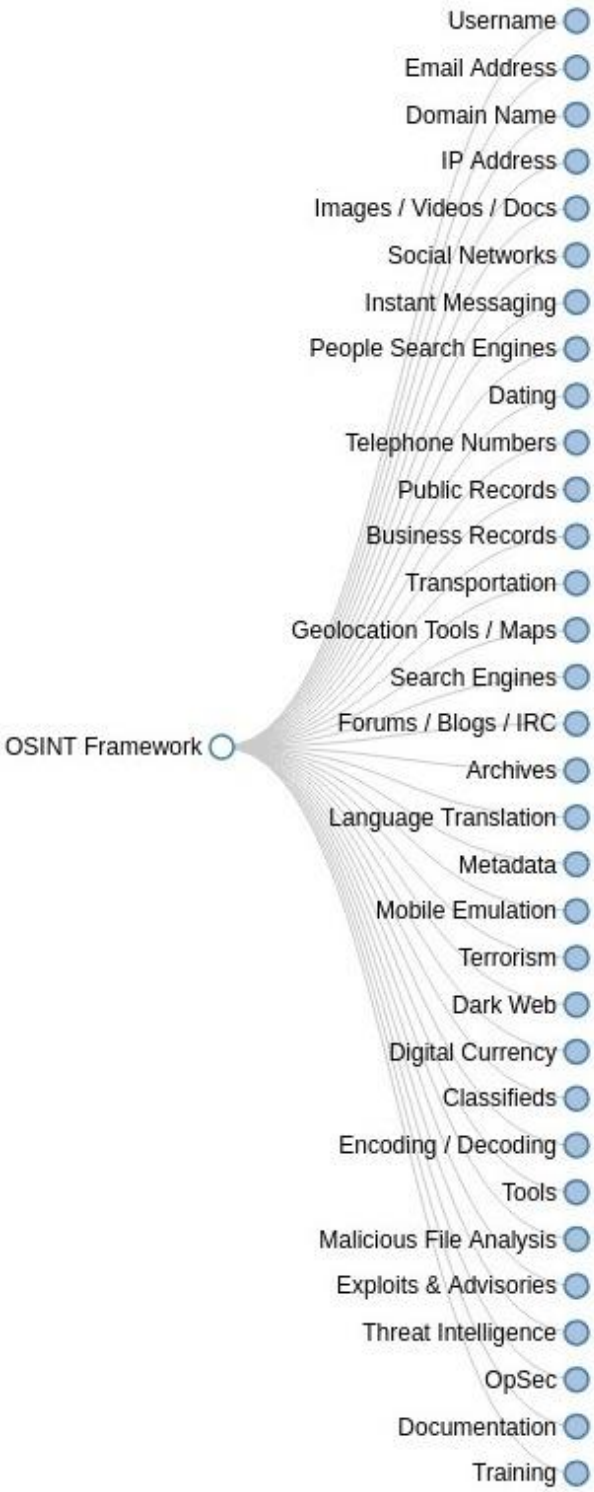
- I used an IP address from the home network to find any open hosts or ports I could use to start my attack. When I tried that a message came back saying that a firewall is protecting it from pinging to Nmap. So, then I used the command with -Pn which is to try to skip host discovery, but I still came back with nothing.

- Overall, my findings were that having a well secured network with a strong password will help deter if not keep hackers from being able to get into your network.

The original purpose of our hack-a-home project was, as you might ascertain, to hack our home. However, after a lot of trial and error trying to find just the right exploits to "PWN" my family member's devices, I started to think more about how and why such personal devices might be targeted. This led to a more broad research oriented investigation with regards to the types of devices we're becoming increasingly reliant on writ large, and a sort of call to arms to raise awareness in defense of our collective privacy and security. This project would serve equally well and informative for private individuals as well as organizations, for tech industry professionals as well as laypeople.

Aspiring cybersecurity professionals like us will know all about OSINT, passive reconnaissance, Google Dorking, and many more tricks of the trade useful for gathering information and intelligence. In saying that, the layperson is likely not to be familiar with these things and may not understand the possible impact a little research can have in our increasingly interconnected world.

Let’s begin with OSINT, or open source intelligence, which is the collection and analysis of data gathered from open sources, usually online, and they may be covert sources or PAI, publicly available information. OSINT may consist of data from six different categories: media, such as print newspapers, magazines, radio, and television, the internet, such as online publications, blogs, discussion groups, YouTube, and other social media websites, public government data such as public government reports, budgets, and hearings, professional and academic publications, commercial data, and finally, grey literature, such as technical reports, preprints, patents, working papers, business documents, unpublished works, and newsletters. OSINT collection methodologies may include social media intelligence, search engine data mining or scraping, public records checking, and information matching and verification.


OSINT Framework
Username
Email Address
Domain Name
IP Address
Images / Videos / Docs
Social Networks
Instant Messaging
People Search Engines
Dating
Telephone Numbers
Public Records
Business Records
Transportation
Geolocation Tools / Maps
Search Engines
Forums / Blogs / IRC
Archives
Language Translation
Metadata
Mobile Emulation
Terrorism
Dark Web
Digital Currency
Classifieds
Encoding / Decoding
Tools
Malicious File Analysis
Exploits & Advisories
Threat Intelligence
OpSec
Documentation
Training

The OSINT framework image displayed above shows what kinds of information may be out there and where it can be found. Included here is the link to the site with the interactive OSINT framework image: https://osintframework.com/ (note that I do not take credit for this image).

There is an intelligence cycle with regards to OSINT, which may recur based on the information one finds, where it comes from, and when it is discovered. This cycle consists of five stages: preparation, collection, processing, analysis and production, and dissemination. Remember here that information may be useful, or it may be useless and doesn't become intelligence until it is analyzed.

Closely related to OSINT is passive reconnaissance, which includes the collection of network information through indirect or direct methods, but without probing the target, and some of the same tools may be used for both. In spite of some potential overlap, as passive reconnaissance tends to include OSINT, passive reconnaissance is also distinct and can involve environmental assessments for details about an individual's or an organization's operating environment, infrastructure, or configuration. Passive recon can also involve network examination for details about an individual's or an organization's network or internet connections. This is sometimes done in conjunction with wardriving, the act of locating and possibly exploiting wireless connections. Wardriving itself borders on the final piece of common passive recon activities, which consists of physical searches. Digging through trash or data from discarded devices can provide a potential inroad.

Some common sites and tools that may be used to conduct OSINT and passive recon may include the following:

- Amass
- Babel Street
- Babel X
- BuiltWith
- DarkSearch.io
- EmailHippo
- Google
- Grep.app
- Intelligence X
- Lampyre
- Maltego
- Metagoofil
- Metasploit
- Mitaka
- Nessus
- Nikto
- Nmap
- OpenVAS
- Osmodeus
- PhoneInfoga
- Recon-ng
- Searchcode
- Seon

- Sherlock
- Shodan
- Social Analyzer
- SpiderFoot
- Spokeo
- Spyse
- theHarvester
- VirusTotal
- Wireshark

Finally, we arrive at Google Dorking, a technique used to discover vulnerable websites or sensitive information, including IoT devices. The importance of Google hacking lies in its ability to uncover information that is not typically visible through standard web searches, potentially leading to privacy violations.

For protection against Google hacking, robots.txt is a well known file used to disallow everything or specific endpoints, which prevents Google bots from crawling those sensitive endpoints.

Even so, a simple Google search such as intitle:"webcam XP 5" can reveal a feed to an unsecured device as shown above. Many kinds of devices, and especially IoT devices, are susceptible to open access to anyone with the motivation or the inclination to hijack them. Common reasons for this include the facts that many of these devices are not password protected, rely on default passwords, and are not, or can not be patched or updated, so exposed vulnerabilities may be difficult if not impossible to remediate. As more and more kinds of "smart" devices are being created and connected to the internet, susceptibilities such as these are becoming increasingly common.

The most common IoT devices that can be easily targeted include the following:

- Wireless cameras (CCTV)
- Wireless printers
- Wireless NAS and routers
- Baby monitors
- Smart home assistants
- Smart thermostats
- Smart door locks
- Doorbell cameras
- Smart light switches
- Smart smoke alarms
- Sensors
- Fitness devices
- Health devices

Of these types of IoT devices, each has known common vulnerabilities and exposures, or CVEs, associated with them.

Wireless CCTV cameras of all makes and models have 135 known CVEs associated with them, including two which specifically refer to “IoT” in their descriptions. CVE-2023-6248. The Syrus4 IoT gateway utilizes an unsecured MQTT server to download and execute arbitrary commands, allowing a remote unauthenticated attacker to execute code on any Syrus4 device connected to the cloud service. The MQTT server also leaks the location, video and diagnostic data from each connected device. An attacker who knows the IP address of the server is able to connect and perform the following operations: * Get location data of the vehicle the device is connected to * Send CAN bus messages via the ECU module (https://syrus.digitalcomtech.com/docs/ecu-1 https://syrus.digitalcomtech.com/docs/ecu-1) * Immobilize the vehicle via the safe-immobilizer module (https://syrus.digitalcomtech.com/docs/system-tools#safe-immobilization https://syrus.digitalcomtech.com/docs/system-tools#safe-immobilization) * Get live video through the connected video camera * Send audio messages to the driver (https://syrus.digitalcomtech.com/docs/system-tools#apx-tts https://syrus.digitalcomtech.com/docs/system-tools#apx-tts). CVE-2020-11624. An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. They do not require users to change the default password for the admin account. They only show a pop-up window suggesting a change but there's no enforcement. An administrator can click Cancel and proceed to use the device without changing the password. Additionally, they disclose the default username within the login.js script. Since many attacks for IoT devices, including malware and exploits, are based on the usage of default credentials, it makes these cameras an easy target for malicious actors.

Wireless printers of all makes and models have 315 known CVEs associated with them.

Wireless NAS and routers of all kinds have 2268 known CVEs associated with them, including one which specifically refers to “IoT” in its description. CVE-2022-29730. USR IOT 4G LTE Industrial Cellular VPN Router v1.0.36 was discovered to contain hard-coded credentials for its highest privileged account. The credentials cannot be altered through normal operation of the device.

Baby monitors of all makes and models have 5 known CVEs associated with them.

Smart home assistants of all kinds have 42 known CVEs associated with them, including one which specifically refers to “IoT” in its description. CVE-2022-24796. RaspberryMatic is a free and open-source operating system for running a cloud-free smart-home using the homematicIP / HomeMatic hardware line of IoT devices. A Remote Code Execution (RCE) vulnerability in the file upload facility of the WebUI interface of RaspberryMatic exists. Missing input validation/sanitization in the file upload mechanism allows remote, unauthenticated attackers with network access to the WebUI interface to achieve arbitrary operating system command execution via shell metacharacters in the HTTP query string. Injected commands are executed as root, thus leading to a full compromise of the underlying system and all its components. Versions after `2.31.25.20180428` and prior to `3.63.8.20220330` are affected. Users are advised to update to version `3.63.8.20220330` or newer. There are currently no known workarounds to mitigate the security impact and users are advised to update to the latest version available.

Smart thermostats of all makes and models have 1519 known CVEs associated with them, including three which refer specifically to “IoT” in their descriptions. CVE-2022-24796. RaspberryMatic is a free and open-source operating system for running a cloud-free smart-home using the homematicIP / HomeMatic hardware line of IoT devices. A Remote Code Execution

(RCE) vulnerability in the file upload facility of the WebUI interface of RaspberryMatic exists. Missing input validation/sanitization in the file upload mechanism allows remote, unauthenticated attackers with network access to the WebUI interface to achieve arbitrary operating system command execution via shell metacharacters in the HTTP query string. Injected commands are executed as root, thus leading to a full compromise of the underlying system and all its components. Versions after `2.31.25.20180428` and prior to `3.63.8.20220330` are affected. Users are advised to update to version `3.63.8.20220330` or newer. There are currently no known workarounds to mitigate the security impact and users are advised to update to the latest version available. CVE-2020-13702. The Rolling Proximity Identifier used in the Apple/Google Exposure Notification API beta through 2020-05-29 enables attackers to circumvent Bluetooth Smart Privacy because there is a secondary temporary UID. An attacker with access to Beacon or IoT networks can seamlessly track individual device movement via a Bluetooth LE discovery mechanism. CVE-2019-9013. An issue was discovered in 3S-Smart CODESYS V3 products. The application may utilize non-TLS based encryption, which results in user credentials being insufficiently protected during transport. All variants of the following CODESYS V3 products in all versions containing the CmpUserMgr component are affected regardless of the CPU type or operating system: CODESYS Control for BeagleBone, CODESYS Control for emPC-A/iMX6, CODESYS Control for IOT2000, CODESYS Control for Linux, CODESYS Control for PFC100, CODESYS Control for PFC200, CODESYS Control for Raspberry Pi, CODESYS Control RTE V3, CODESYS Control RTE V3 (for Beckhoff CX), CODESYS Control Win V3 (also part of the CODESYS Development System setup), CODESYS V3 Simulation Runtime (part of the CODESYS Development System), CODESYS Control V3 Runtime System Toolkit, CODESYS HMI V3.

Smart door locks of all makes and models have six known CVEs associated with them.

Doorbell cameras of all makes and models have 241 known CVEs associated with them, including one which refers specifically to “IoT” in its description. CVE-2020-11624. An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. They do not require users to change the default password for the admin account. They only show a pop-up window suggesting a change but there's no enforcement. An administrator can click Cancel and proceed to use the device without changing the password. Additionally, they disclose the default username within the login.js script. Since many attacks for IoT devices, including malware and exploits, are based on the usage of default credentials, it makes these cameras an easy target for malicious actors.

Smart light switches of all makes and models have 64 known CVEs associated with them.

Smart smoke alarms of all makes and models have 1537 known CVEs associated with them, including two which refer specifically to “IoT” in their descriptions. CVE-2022-24796. RaspberryMatic is a free and open-source operating system for running a cloud-free smart-home using the homematicIP / HomeMatic hardware line of IoT devices. A Remote Code Execution (RCE) vulnerability in the file upload facility of the WebUI interface of RaspberryMatic exists. Missing input validation/sanitization in the file upload mechanism allows remote, unauthenticated attackers with network access to the WebUI interface to achieve arbitrary operating system command execution via shell metacharacters in the HTTP query string. Injected commands are executed as root, thus leading to a full compromise of the underlying system and all its components. Versions after `2.31.25.20180428` and prior to `3.63.8.20220330` are affected. Users are advised to update to version `3.63.8.20220330` or newer. There are currently no known workarounds to mitigate the security impact and users are advised to update to the latest version available. CVE-2020-13702. The Rolling Proximity Identifier used in the

Apple/Google Exposure Notification API beta through 2020-05-29 enables attackers to circumvent Bluetooth Smart Privacy because there is a secondary temporary UID. An attacker with access to Beacon or IoT networks can seamlessly track individual device movement via a Bluetooth LE discovery mechanism.

Sensors of all kinds have 34 known CVEs associated with them, including two which refer specifically to “IoT” in their descriptions. CVE-2019-10583. Use after free issue occurs when camera access sensors data through direct report mode in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, MDM9607, MSM8909W, Nicobar, QCS605, SA6155P, SDA845, SDM429W, SDM670, SDM710, SDM845, SM6150, SM8150, SM8250, SXR1130, SXR2130. CVE-2019-10582. Use after free issue due to using of invalidated iterator to delete an object in sensors HAL in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8096AU, MSM8909W, Nicobar, QCS605, SA6155P, SDA845, SDM429W, SDM670, SDM710, SDM845, SM6150, SM8150, SM8250, SXR1130, SXR2130

Fitness devices of all kinds have 6053 known CVEs associated with them, including 74 which refer specifically to “IoT” in their descriptions, of which the first five will be listed. CVE-2023-34367. Windows 7 is vulnerable to a fully blind TCP/IP hijacking attack. The vulnerability exists in Windows 7 (any Windows until Windows 8) and in any implementation of TCP/IP, which is vulnerable to the Idle scan attack (including many IoT devices). NOTE: The vendor considers this a low severity issue. CVE-2023-33975. RIOT-OS, an operating system for Internet of Things (IoT) devices, contains a network stack with the ability to process 6LoWPAN frames. In version 2023.01 and prior, an attacker can send a crafted frame to the device resulting in an out of bounds write in the packet buffer. The overflow can be used to corrupt other packets and the

allocator metadata. Corrupting a pointer will easily lead to denial of service. While carefully manipulating the allocator metadata gives an attacker the possibility to write data to arbitrary locations and thus execute arbitrary code. This issue is fixed in pull request 19680. As a workaround, disable support for fragmented IP datagrams. CVE-2023-33974. RIOT-OS, an operating system for Internet of Things (IoT) devices, contains a network stack with the ability to process 6LoWPAN frames. In versions 2023.01 and prior, an attacker can send multiple crafted frames to the device to trigger a race condition. The race condition invalidates assumptions about the program state and leads to invalid memory access resulting in denial of service. This issue is patched in pull request 19679. There are no known workarounds. CVE-2023-33973. RIOT-OS, an operating system for Internet of Things (IoT) devices, contains a network stack with the ability to process 6LoWPAN frames. In versions 2023.01 and prior, an attacker can send a crafted frame which is forwarded by the device. During encoding of the packet, a NULL pointer dereference occurs. This crashes the device leading to denial of service. A patch is available at pull request 19678. There are no known workarounds. CVE-2023-28116. Contiki-NG is an open-source, cross-platform operating system for internet of things (IoT) devices. In versions 4.8 and prior, an out-of-bounds write can occur in the BLE L2CAP module of the Contiki-NG operating system. The network stack of Contiki-NG uses a global buffer (packetbuf) for processing packets, with the size of PACKETBUF_SIZE. In particular, when using the BLE L2CAP module with the default configuration, the PACKETBUF_SIZE value becomes larger than the actual size of the packetbuf. When large packets are processed by the L2CAP module, a buffer overflow can therefore occur when copying the packet data to the packetbuf. The vulnerability has been patched in the "develop" branch of Contiki-NG and will be included in release 4.9. The problem can be worked around by applying the patch manually.

Health devices of all kinds have 4 known CVEs associated with them.

Many of these threats have no known workarounds…

So far, we have discussed OSINT, passive reconnaissance, and Google hacking. One may be wondering now why this matters to us as individuals and to the organizations we are a part of. Privacy and security go hand in hand, and in our increasingly interconnected world, our privacy will ebb away in the tide of the internet and our internet connected devices, and so too will our security, even in the sanctity of our own homes, as we have demonstrated.

This is cause to raise awareness of our digital footprints. To know what all devices we have, even on our own personal home networks, to know what kinds of information may be out there about us, and to understand how it may be used against us.

I like to compare this openly available information to the government's policy with regards to document classification. Documents that are unclassified or under classified on their own may need to be made secret when compiled or upgraded from secret to top secret. The information they contain may be harmless on its own, but when put together may constitute something harmful. Small details such as our names or those of our Wi-Fi networks may be meaningless, but after conducting OSINT, passive reconnaissance, and Google hacking, those combined details may be enough to pose threats to our privacy and security, potentially resulting in threats and intimidation, doxxing, full blown identity theft, and much more.

As Mikey V. once said, the difference between a tech enthusiast and a tech industry professional is that a tech enthusiast has every IoT device under the sun, would love to install a chip in their brain, and is eagerly awaiting the singularity, while a tech industry professional has maybe a computer at most.

Being aware of our surroundings, including our digital surroundings, has never been more important, and will continue to become increasingly relevant for the foreseeable future.

References

12 ways hackers can attack and take control of your smart TV. (2023, January 12). MUO. https://www.makeuseof.com/ways-hackers-attack-smart-tv/

17 everyday things you didn't know could be hacked. (2022, December 9). Reader's Digest. https://www.rd.com/list/everyday-things-you-didnt-know-could-be-hacked/

Buil-Gil, D., Kemp, S., Kuenzel, S., Coventry, L., Zakhary, S., Tilley, D., & Nicholson, J. (2023, August). https://www.sciencedirect.com/science/article/pii/S0747563223001218

Gvozdenovic, S., Becker, J. K., Mikulskis, J., & Starobinski, D. (2022, April 6). arXiv.org e-Print archive. https://arxiv.org/pdf/2204.02538.pdf

Hackers can hijack your home with these 10 smart devices. (2024, February 6). The UTSA CIAS – Center for Infrastructure Assurance and Security. https://cias.utsa.edu/hackers-can-hijack-your-home-with-these-10-smart-devices/

Hwang, Y. W., Lee, I. Y., Kim, H., Lee, H., & Kim, D. (2022, February 18). Current status and security trend of OSINT. Publishing Open Access research journals & papers | Hindawi. https://www.hindawi.com/journals/wcmc/2022/1290129/

José, L. (2023, September 19). 10 common IoT hacks and how to defend against them. Device Authority Ltd. https://www.deviceauthority.com/blog/10-common-iot-hacks/

Noman, H. A., & Abu-Sharkh, O. M. (2023). Code injection attacks in wireless-based Internet of things (IoT): A comprehensive review and practical implementations. *Sensors*, *23*(13), 6067. https://doi.org/10.3390/s23136067

Pastor-Galindo, J., Nespoli, P., Marmol, F. G., & Perez, G. M. (2020, January 9). IEEE Xplore full-text PDF: IEEE Xplore. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8954668

Puig, Alvaro, et al. “Ring’s Privacy Failures Led to Spying and Harassment through Home Security Cameras.” *Consumer Advice*, 30 Oct. 2023, consumer.ftc.gov/consumer-alerts/2023/05/rings-privacy-failures-led-spying-and-harass-through-home-security-cameras.

Uslu, S., Kaur, D., Durresi, M., & Durresi, A. (2022). Trustability for resilient Internet of things services on 5G multiple access edge cloud computing. *Sensors*, *22*(24), 9905. https://doi.org/10.3390/s22249905

Vacas, I., Madeiros, I., & Neves, N. (n.d.). Detecting Network Threats using OSINT Knowledge-based IDS. https://www.di.fc.ul.pt/~nuno/PAPERS/EDCC18_ids_osint.pdf

Watch out: How to stop your smart TV from spying on you. (2023, April 5). PCMAG. https://www.pcmag.com/how-to/how-to-stop-smart-tvs-from-snooping-on-you

Further Reading

https://cve.mitre.org/

https://osint.industries/

https://osintframework.com/

https://www.exploit-db.com/google-hacking-database

https://www.forknerds.com/how-to-hack-cctv-cameras-and-iot-devices/

https://www.iottechnews.com/

https://www.sciencedirect.com/topics/computer-science/passive-reconnaissance