Plume®

Security and privacy IoT vulnerabilities: The danger of too many entry points

A Plume® whitepaper

October, 2022

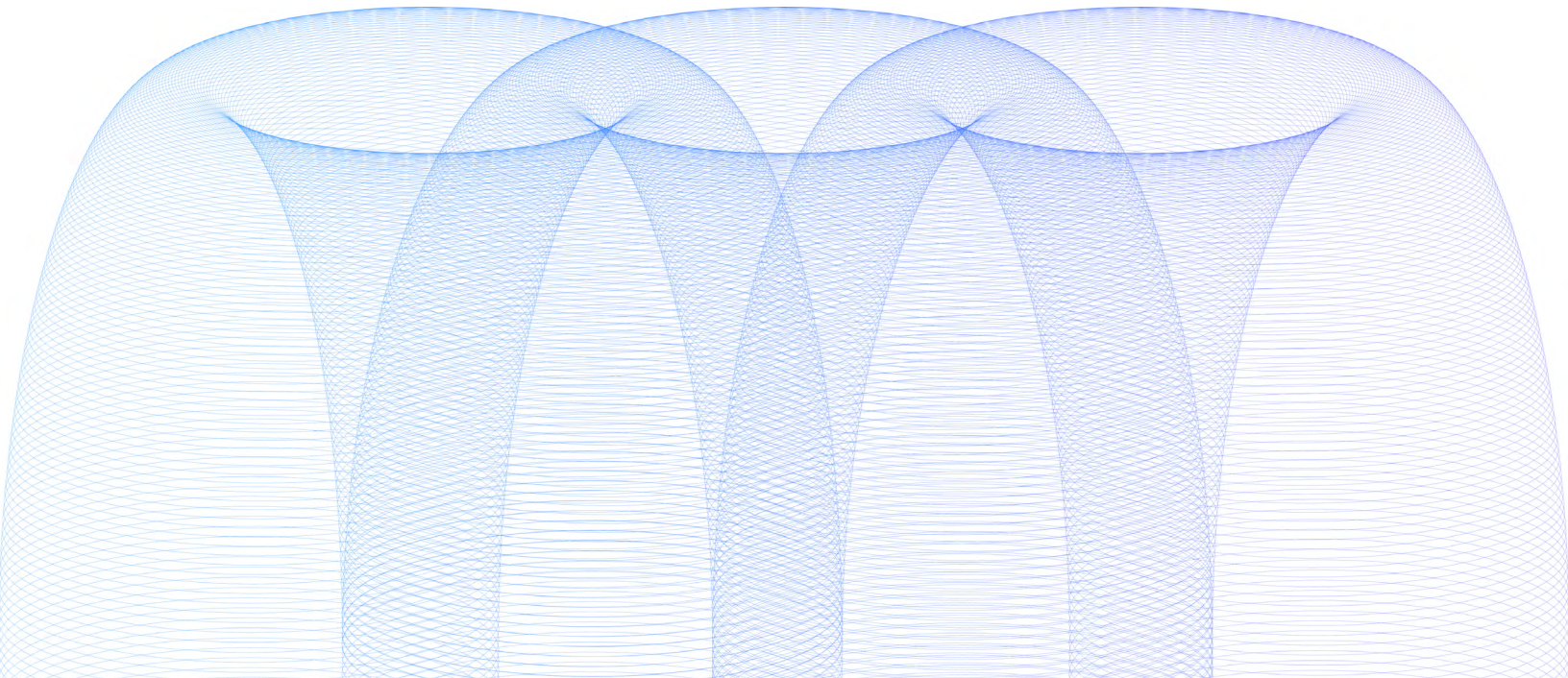

Table of contents

Introduction

While the Internet of Things (IoT) solves some important concerns for consumers, it also poses significant risks because IoT devices are attractive targets for attack. IoT devices have a history of being vulnerable, they can't be intrinsically protected like less constrained devices, and because they are configured by non-professional/layman users they are ripe for exploitation.

Many IoT devices, including everyday objects like kitchen appliances, thermostats, baby monitors, and light control systems, have minimal security built in as compared to full-featured smart devices and are mostly unprotected.

Because they are inexpensive and of limited purpose, IoT devices may have unpatched software flaws. They often have resource-constrained environments with limited processing, memory, and power that make them challenging to secure. Users are mostly non-technical and often lack the knowledge it takes to manage the IoT devices on their networks.

The decline in the overall security profile of homes and offices makes IoT devices a low-hanging fruit for cyberattacks. Attackers can easily get a foothold on the device, exploiting a vulnerability like a weak password or other software flaws. Once a cybercriminal gets access to one device, they can use lateral movement techniques to find other vulnerable devices in the home and conduct severe attacks like ransomware, crypto-mining, password-stuffing, and remote code execution.

There is a critical need for an effective solution that can address the consumer's security concerns and provide state-of-art, enterprise-grade security to homes and business owners. The solution should be able to proactively detect and protect against the security vulnerability which is the primary attack vector in IoT. Communications Service Providers (CSPs) are ideally positioned to play a critical role in mitigating cyberattacks on IoT devices by providing an end-to-end, integrated solution encompassing discovery, detection, monitoring, and resolution.

Consumers' security concerns

These attack trends have made users wary of the consequences of security breaches, reducing the adoption of IoT. For any transformation, it is essential to build consumers' trust and ensure security is in-built from the design stage. According to a recent survey, consumers have raised concerns (Figure 1) and have called out cyber protection as a requirement.

Figure 1—Consumers' security concerns

IoT clearly presents a security challenge for both homes and small businesses. Based on data gathered from the over 41 million homes and small businesses currently connected to Plume's network, around 67% of homes have high/critical vulnerabilities to attacks on IoT devices. According to analysts, small businesses (SMBs) are the primary targets of cyberattacks and face the most damage in terms of money and customer trust. Around 66% of SMBs in US have been impacted by at least one incident between 2018-2020.

Software vulnerabilities are the primary attack vector for IoT devices and provide an easy foothold for cybercriminals. A recent BotenaGo IoT attack was identified by AT&T Alien Labs in November 2021 as a new malware that exposed millions of IoT devices. The BotenaGo backdoor vulnerability exploits IoT through the open networking port or related modules. There have been countless such incidents in the past and the trend suggests an ongoing increase in these attacks.

Understanding IoT security challenges

The majority of IoT devices are not built with security-first design principles. As a result, these devices have inherent software vulnerabilities. Many IoT devices cannot be patched with security fixes and, as a result, almost all devices will be at risk. Hackers are now actively targeting IoT devices such as routers and webcams because their inherent lack of security makes them vulnerable and easy to compromise.

These IoT security challenges are partly due to the technical nature of the IoT ecosystem as well as unique security requirements. The technical ecosystem must deal with scalability, distribution, heterogeneity, low energy, and the omnipresent nature of IoT devices. Authentication, confidentiality, integrity, and end-to-end security, on the other hand, are inherent security requirements. Fulfilling all security requirements is difficult given the constraints and limitations in computational and power resources within the devices.

IoT ecosystem challenges

Identity and authentication

IoT devices need a unique identity on the network to provide mutual authentication, however, there is no consistent mechanism for this. An academic survey found that there are more than 80 different authentication mechanisms proposed or implemented. There is no authentication standard at this point and when many entities (i.e., devices, humans, software, etc.) are involved, authentication becomes difficult. Authentication can also become more complex due to the scale and size of the IoT fabric.

Compute power

Because IoT devices have limited computing and power capabilities, designing, and implementing encryption or authentication methods is difficult. For maximum IoT security, these cryptographic algorithms must be able to work on small devices and be compatible with the device's compute capabilities. Lightweight and pluggable solutions should be created and deployed to match the limited compute power of IoT devices.

IoT device heterogeneity

IoT devices are heterogeneous in their capabilities, communication protocols, technical interfaces, etc. This poses serious challenges when trying to provide an end-to-end security solution that requires devices to share information and collaborate.

User awareness

Consumers lack awareness about the connected devices installed in their homes and businesses. Often, the devices are unpatched, have weak or default credentials, have vulnerable open ports and services, or are exposed to the internet. Most users are non-technical and lack the expertise to understand the security implication, patch vulnerabilities, or fix the security issues (Figure 2).

Figure 2—Limited consumer security awareness

Work-from-home trends

The pandemic has transformed business functions forever and working from home (WFH) has been growing in popularity. However, WFH comes with a slew of security risks, according to the CISO magazine (Figure 3): The rise of the remote workforce has multiplied the attack surface by adding more endpoints that can be vulnerable to security breaches and device access over insecure network connections. This makes WFH users vulnerable and an easy target for attackers, making the task of security providers even more challenging.

However, rising to this challenge is critical as many users are now doing business-critical work—using sensitive customer data—on machines connected to networks with unknown security weaknesses and populated by many unvetted devices. A joint advisory issued by the US Cybersecurity and Infrastructure Security Agency and the UK's National Cyber Security Centre says the rise of WFH during the COVID-19 pandemic has seen an increase in bad actors targeting individuals and organizations.

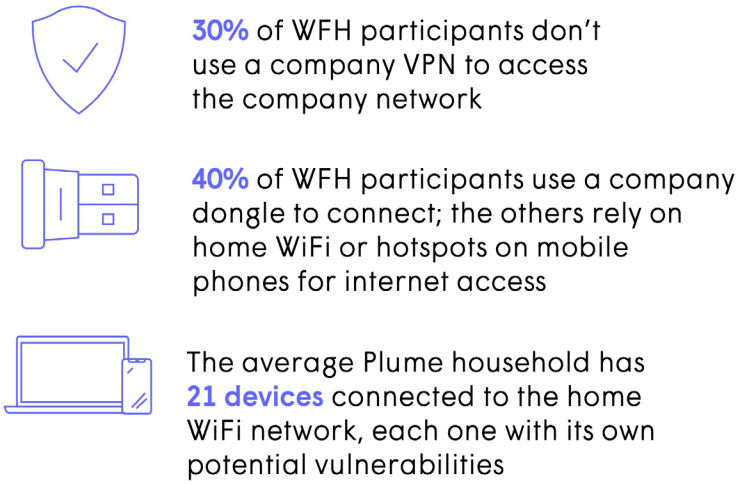

Figure 3—Work-from-home security concerns

Attacker motivations and challenges

Organizations fail to give enough importance to IoT security as attacker motivations and security risks are not well understood. Security is often completely ignored when, instead, efforts should be focused on critical areas. It is important to understand that the motivation for attacks depends on the attacker and the domain. Attacker types can range from novice, petty thieves, and hectivities to professional crime facilitators. A new class of malicious actors that are knowledgeable and well-funded is emerging.

The primary motives for attackers in the context of homes and small businesses include:

- Financial gain—Attacks geared towards stealing personal and financial information, followed by monetization.
- State-sponsored hacking

- Recognition and popularity
- Revenge

The challenge lies in intelligently narrowing down the attacker type and motivation for any given home or business. A careful audit and profiling of the assets is essential to identify what would be attractive to attackers. This profiling needs to include the inventory of confidential and sensitive data and the industry that the user belongs to.

Figure 4—Attack motivations

The evolving landscape

The IoT landscape—including IoT adaptation, threats, and solutions—is evolving at a rapid pace. While attacks are becoming more evasive and easier to conduct, the solutions should also evolve using AI-driven, data-centric, cloud-based solutions that allow protections to be adaptive. CSPs need to keep up with the demands of the ever-changing consumer threat landscape.

Threat landscape

Everyone with access to the internet must have cybersecurity protection. Cyber-attacks reached a peak in 2021 as data breaches grew by over 17% from 2020, according to the Identity Theft Resource Center. In fact, cybersecurity is now considered a growing human rights issue, with the UN Security Council holding its second-ever cybersecurity meeting in 2020.

Businesses and government organizations aren't the only ones who should be worried about cyber threats. Consumers are increasingly vulnerable to these attacks as they fill their homes

with connected devices. Our research has found that the number of devices per Plume-powered US household increased by 38% during the pandemic, with an average of 18 devices per household. And we're not just talking about laptops and smartphones. There was a 223% increase in virtual reality devices, a 132% increase in fitness bikes and trainers, and a 110% increase in smart light bulbs.

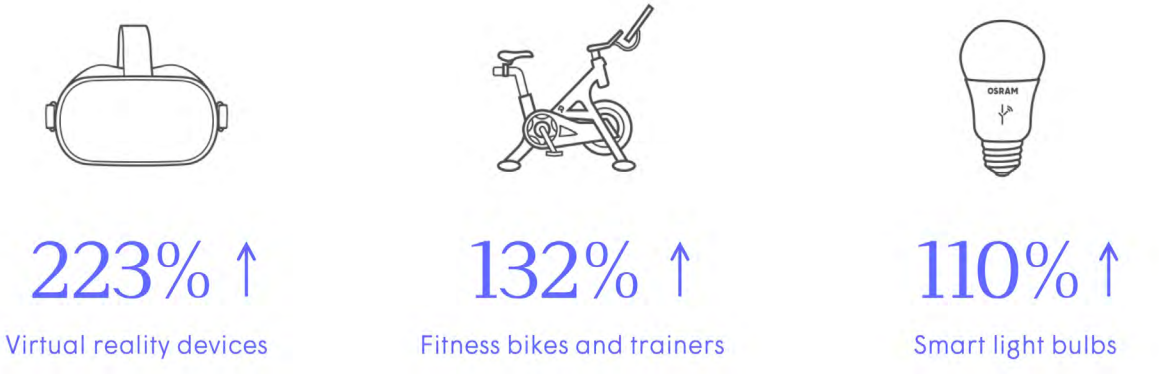

Figure 5—Growth in IoT devices at home (Source: Plume)

It was hypothesized that criminals would likely take advantage of the fear, confusion, and increased use of the internet during a pandemic. Sadly, it turns out this was true. Figure 6 below shows the increase in various types of threats before and after COVID-19, with several attack types doubling in frequency. In fact, across the period of this study, 87% of the homes connected to Plume's network experienced some type of cybersecurity attack.

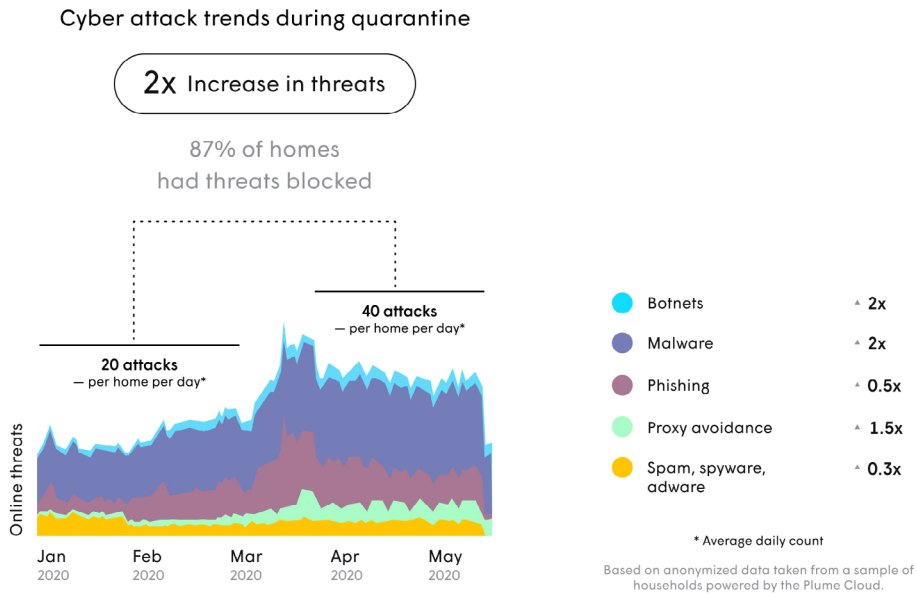

Figure 6—Cyber-attack trends

As cyber criminals create new ways to wreak havoc on smart homes, CSPs must stay one step ahead of them. A multi-layered approach to security, with services that act across every potential threat area—from anomaly detection and device quarantining to cyber-intrusion protection—is the answer. Analysis of data taken from the Plume Cloud showed that 87% of households were attacked. 85% of those attacks were DNS-based while preventing dangerous outbound and inbound IP events accounted for 37% and 8% respectively.

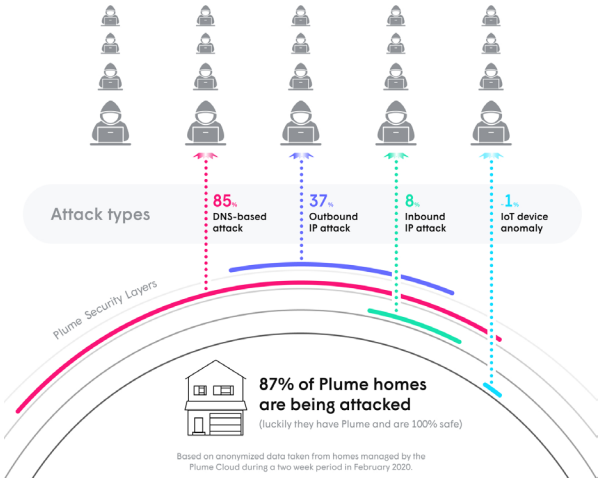

Figure 7—Cyber-attack types

CSP security services

Plume predicts that by 2024, connected devices in Plume homes will grow from the current 21 (or so) to exceed 38 devices across all categories—computers, mobile phones, tablets, set-top boxes, voice assistants, smart TVs, printers, surveillance cameras, game consoles, and more. Each of these devices opens a unique door to potential attacks. These attacks could be from websites and the servers they connect to. They could be the result of exploiting weak or reused passwords and unpatched software, and they could take the form of targeted phishing, spam, fraud attacks, and more.

CSPs are in the best position to deliver security to homes and small businesses. In addition, they can differentiate themselves by helping customers create a more secure environment—with more control over, and visibility into, their personal IT security. CSPs that adopt this role stand a good chance of achieving significant revenue gains; it's a win-win for CSPs and consumers.

CSPs can choose to build a complex and robust architecture that delivers a unified, multi-layer security service network, CPE, and endpoint that takes care of all the intricacies for the end users. This is time consuming and slows the delivery and adoption of services. Alternately the CSP can adopt a cloud-based, security-as-service model eliminating the dependencies and limitations of hardware-based solutions. The ongoing silicon shortage continues to affect consumers' ability to get new hardware—be it a dishwasher, laptop, or network server. CSPs who rely too heavily on their hardware may have their hands tied by this issue. But those who offer cloud-based solutions can continue to adapt and expand.

Now that consumers are welcoming cloud-based services into their homes, CSPs should leverage this shift and set up the delivery platform to offer new value-added services quickly, using the same hardware already deployed on customer premises.

Vulnerabilities lifecycle and risks

Vulnerabilities are the primary source of attacks. A vulnerability lifecycle is divided into the following phases: Discovery, Disclosure, Patch, and Patch installed. Each of these life cycle phases has a corresponding risk exposure phase with unique characteristics and criticality. Risk exposure phases are discussed below (Figure 8).

It is challenging for a non-technical user to track vulnerabilities across the entire life cycle; however, they are constantly at risk right from the discovery until the patch installation phase.

Risk exposure phases

High risk

High-risk phases live between the Discovery and Disclosure phases of the vulnerability lifecycle. In this phase, a subset of motivated attackers could be aware of this vulnerability and would already be engaged in developing an exploit. There is no public knowledge, resolution, or patch available in this phase. In this phase, behavior anomaly detection techniques are most relevant and effective to detect attacks and protect against compromises.

Elevated risk

This phase exists when a vulnerability is discovered and disclosed publicly. Vendors are still working on a fix/patch and release plans while users wait. Exploits could already be publicly available for ready use by a wider community of attackers. It is very likely that the attacks are already active, making it the riskiest zone. In addition to the protection techniques of the high-risk phase, proactive vulnerability scanning, detection, and protection are the keys to safeguarding against attacks in this phase. A virtual patch to remediate the vulnerability is effective in restricting the exploits before the official patch is available.

Medium risk

This is the period between patch availability and patch installation. Exposure during this period is under the direct control of users and vendors. The successful protection strategy includes publishing the vulnerability and patch availability, providing a patch installation mechanism, and ensuring that the patch is applied to the devices. Success in this phase relies on a collaborative approach between users and vendors.

A good security solution works on all the above phases and provides an end-to-end solution by breaking the cycle with complete vulnerability remediation.

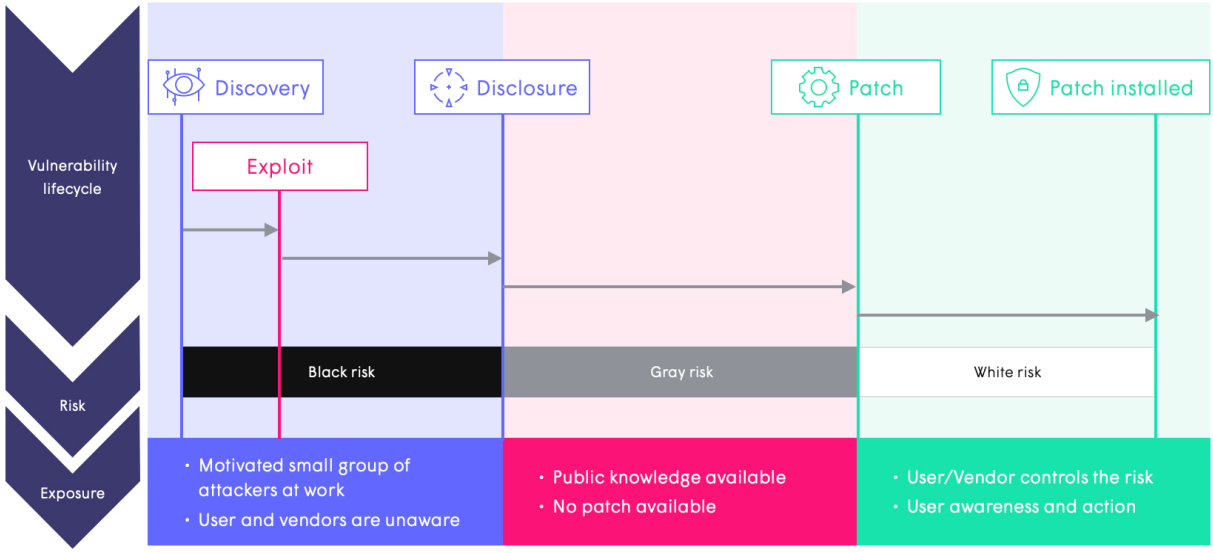

Figure 8—Attack lifecycle and exposure zones

Vulnerabilities and open doors

Open ports

According to the latest stats from Shodan there are too many IoT devices operating with open ports. These open ports are like ticking time bombs, ready to be scanned by automated botnet crawlers, uncovering the known vulnerabilities, and leading to compromises and attacks

Open and exposed ports are problematic as the services listening on the ports are often vulnerable to exploits. The open ports increase the attack surface for an attacker to exploit. As per a previous study by F5 in total, 2,171,934 IoT ports were found to be exposed. Focusing on the most important 119 IoT ports, the top 10 exposed ports and their services are shown in Table 1 below. The listed 10 ports account for 84.7% of exposed ports in the Irish IP address space.

Table 1—Top 10 open IoT ports

TCP port	Service	Ports open	% of Overall exposed
443	HTTPS	772,258	35.6%
80	HTTP	670,789	30.9%
22	SSH	184,848	8.5%
3389	RDP	40,893	1.9%
8443	HTTPS-Alt	391,000	1.8%
8080	HTTP_Alt	30,502	1.4%
21	FTP	30,059	1.4%
8081	HTTP_Alt	27,187	1.3%
25	SMTP	23,901	1.1%
8000	Applications	21,028	1.0%

UPnP port is another critical port that is dangerous and a popular attack vector. UPnP allows zero-configuration connection implying no authentication is required to establish connections. Ports are forwarded automatically to establish a connection for a UPnP request, making it easy for attackers to establish an internet connection with the devices behind the firewall and exploit vulnerabilities. While the intended purpose of UPnP is convenience, it poses a serious threat to device security. UPnP is yet another technology that trades convenience for security.

The enormity of the problem is apparent from the fact that there are 6M+ open UPnP ports worldwide. These are easily discoverable over Shodan (Figure 9). As per the July 2022 stats, most of these open ports are reported from devices in USA (12%) and China (11%).

Total results

6,201,899

Top countries

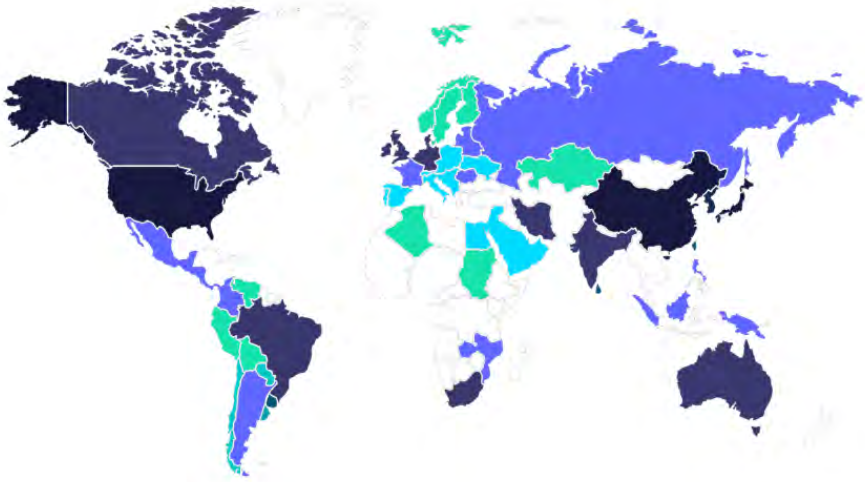

Figure 9—Open UPnP ports globally (Shodan)

From the analyst reports, the top IoT device types that are exposed are routers, media devices, game console, NAS, printers, and smart TVs. The brands include some of the top names.

A recent attack (in the long list of attacks) was discovered in February 2022. Eternal Silence (a UPnP based attack campaign) exposed 1.7 million devices to attacks via UPnProxy abuse. UPnProxy was reported back in 2018 by Akamai researchers. The attackers targeted the routers vulnerable to UPnProxy and exploited the unpatched vulnerabilities—EternalBlue (CVE-2017-0144) and EternalRed (CVE-2017-7494)—on unpatched Windows and Linux systems.

Vulnerability numbers on the rise

The number of vulnerabilities is increasing exponentially every year. In 2021, 20,169 new vulnerabilities were reported. Halfway through 2022, we already have 13,948 new vulnerabilities reported and counting.

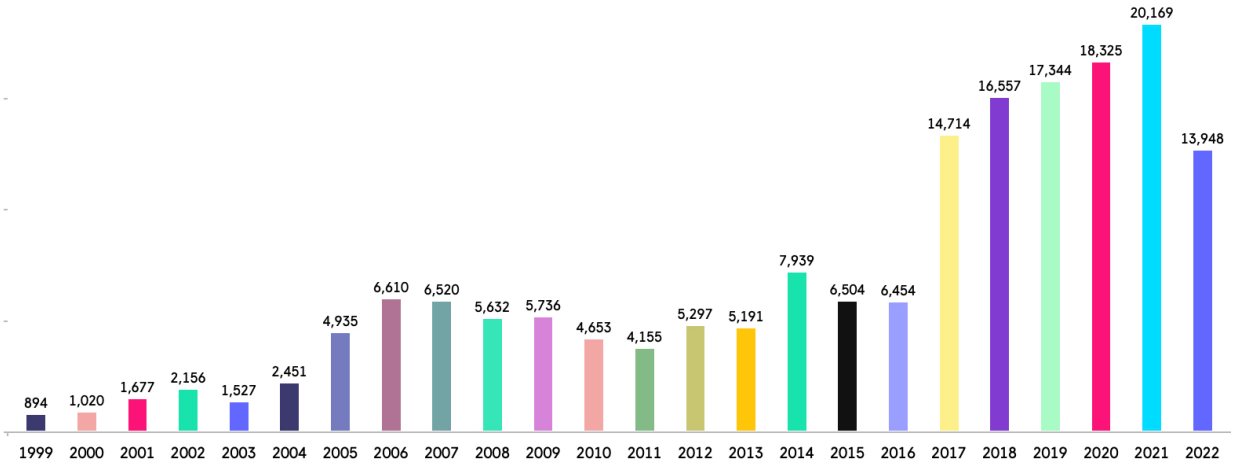

Figure 10—Vulnerabilities reported each year

Software vulnerabilities is one of the primary attack vectors in the cyber incidents. Software vulnerabilities, together with phishing attributes to 70% of the attacks. Software vulnerabilities contribute 31%. Attackers scan the network for known vulnerabilities before vendors can release and apply the patches. Time to patch these vulnerabilities is getting shorter and the vulnerability exploits are getting much faster, almost practically coinciding with the patch. For example, Palo Alto Networks released a Threat Prevention signature for the F5 BIG-IP Authentication Bypass Vulnerability (CVE-2022-1388), and within just 10 hours, the signature triggered 2,552 times due to vulnerability scanning and active exploitation attempts.

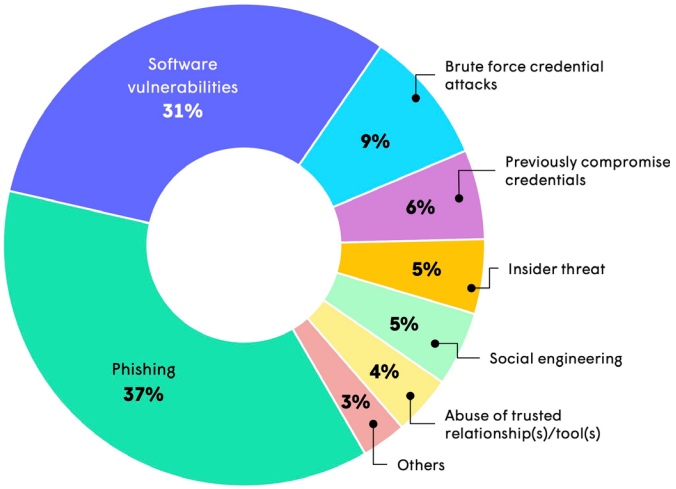

Figure 11—Common attack vectors

The CISA maintains a list of known exploited vulnerabilities. As per the list, 789 vulnerabilities have been recently exploited in the last year. New vulnerabilities are added to this list frequently based on the evidence of active exploitation.

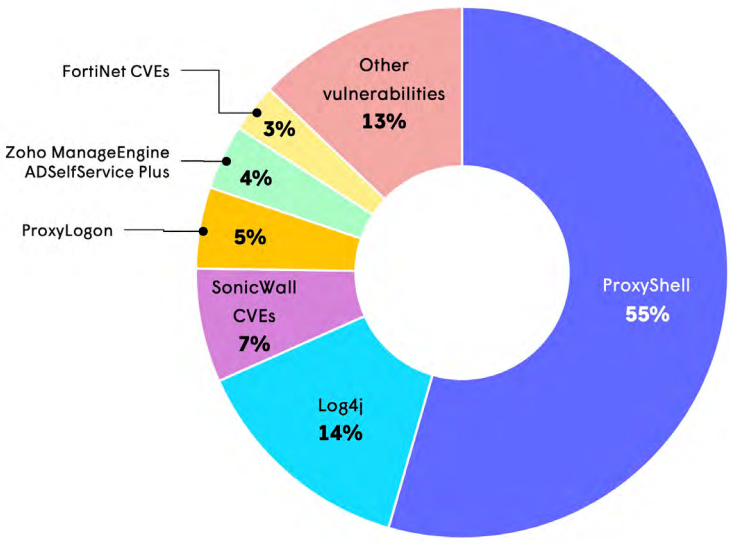

Figure 12—Most exploited vulnerabilities

Log4j remains the most highly exploited zero-day vulnerability in 2021-2022.

Vulnerability prioritization

The following table shows vulnerability severity scores and their percentage distribution over the past year. It is important to note that more than 30% of the vulnerabilities reported were high- or critical-severity issues (CVSS >7). This implies that 30% have high attack and damage potential. It does not take advanced technical skills to exploit these vulnerabilities.

Table 2—Distribution of all vulnerabilities by CVSS scores

CVSS score	Number of vulnerabilities	Percentage
0-1	1,007	0.60
1-2	1,196	0.70
2-3	8,327	4.60
3-4	9,460	5.20
4-5	4,2973	23.70
5-6	34,116	18.80
6-7	27,136	15.00
7-8	36,000	19.90
8-9	895	0.50
9-10	19,978	11.00
Total	**181,088**	

What is CVSS?

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. The NIST National Vulnerability Database (NVD) defines the CVSS score as a mechanism for organizations to properly assess and prioritize their vulnerability management processes.

CVSS comprises three metrics: base, temporal, and environmental. Base metrics provide a static score ranging from 0 to 10. Temporal scores define metrics that change over time due to events external to the vulnerability. Environmental scores define metrics customized to reflect the impact of the vulnerability on your organization. The base score can then be modified by scoring the temporal and environmental metrics. The NVD does not currently provide "temporal scores" or "environmental scores". NVD does provide a CVSS calculator to allow an organization to compute the temporal and environmental score data.

Consumer organization and security solutions should augment the CVSS system with a risk-based vulnerability prioritization system for isolating the immediate focus areas. Exploitability is the primary factor that decides the vulnerability priority and includes an analysis of essential factors such as threat landscape, attack taxonomy, industry vertical, and geolocation, etc. In addition, the security solutions also need to leverage the data feeds from the sources like CISA and prioritize remediating vulnerabilities that are actively exploited.

Vulnerability and attack taxonomy

IoT architecture

A generic IoT architecture is a hierarchical model with four layers: application, middle, network, and device.

Application

This layer implements different applications for different IoT scenarios and business verticals. As this is the front end for IoT solutions, the security issues mainly arise from authentication, illegal access, data theft, and permissions. Attackers can exploit software vulnerabilities to attack systems and disrupt functionality.

Middle layer

The middleware layer or the service support layer sits between the network layer and backend cloud systems. This layer obtains the data from the network layer and connects the system to the cloud and data repositories. This layer is also responsible for data processing and storage. Data repository security and cloud security are the main concerns in the middleware layer, as these can affect the quality of service in the application layer.

Network

This layer is responsible for the connectivity of the IoT infrastructure. It also collects data from the device layer and transmits it to the upper layer. The transmission medium can be wired or wireless, and the main technologies are ZigBee, WiFi, Bluetooth, 3G, and so on. Attacks on the network layer are diverse, typically affecting the coordination of work and information-sharing among devices.

Device

The main challenges for this layer are the attacks on sensors and identification technology, which interfere with the collection of data from devices. An attack can send incorrect device states and other crucial statistics interrupting the entire system.

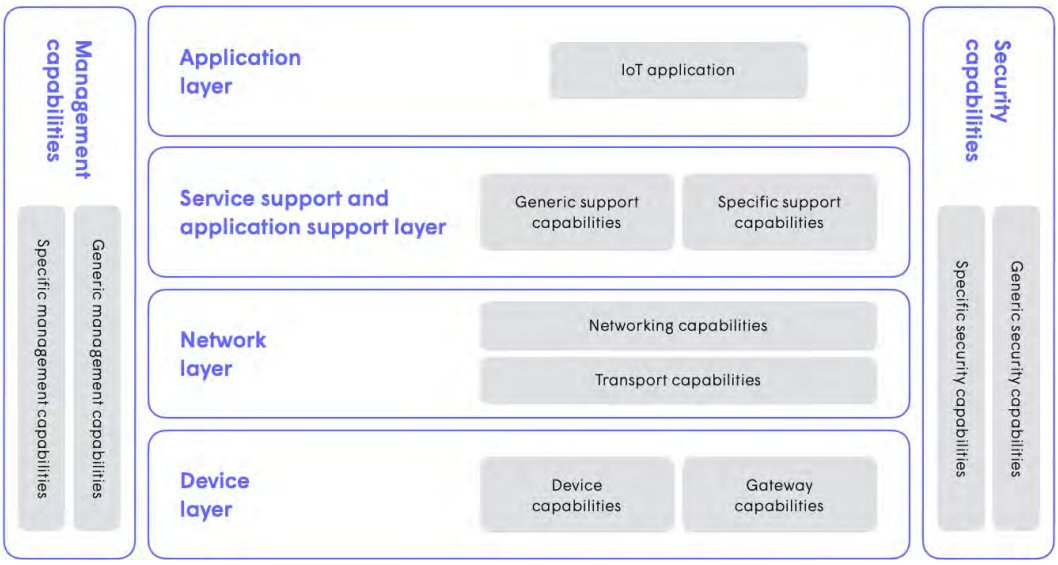

Figure 13—IoT reference model

The taxonomy of vulnerabilities in IoT

To understand the IoT vulnerabilities and their impact, this section discusses vulnerability taxonomy. This taxonomy provides a good reference for CSPs and network defenders.

Weak authentication mechanisms

The interfaces in the IoT ecosystem like mobile, cloud, firmware, and web should be secured with strong authentication mechanisms. Weak, guessable, and hardcoded passwords on these interfaces give attackers unauthorized access to the IoT ecosystem. These vulnerabilities can be exploited in numerous ways and are used as one of the entry points into the network. Some common attacks that leverage authentication vulnerabilities are DDos attacks, dictionary attacks, Sybil attacks, etc.

The Mirai attack, which almost brought down the internet, was carried out by compromising various IoT devices that were configured with default weak credentials (say: admin/admin).

Insecure network services

Unwanted and vulnerable network services exposed and listening on devices are easily compromised to gain access to the device itself, to inject malicious code, modify firmware, bypass security, move laterally to scan other devices, and infect more devices. A wide range of attacks can be launched via these open ports.

Such vulnerabilities are fatal, especially when exposed over the internet. The attackers can gain access to the devices and remote control the network.

An SSH port with an old and vulnerable service version is one of the main attack vectors used in Ransomware attacks.

Lacking privacy and data protection

Users' personally identifiable information (PII) and other personal data are stored everywhere in the ecosystem including devices, the middle layer, and the network layer. If the data is stored, accessed, or processed without proper access control policies and encryption, it can lead to data breaches/losses with a significant damaging impact on personal lives and businesses.

Data breach incidents have been rated topmost when it comes to revenue, brand value, and customer trust loss. In addition, stolen personal information is available and sold on the dark web for minimal cost.

Most IoT devices use wireless communication media, like Zigbee, LoRa, 802.11. a, SigFox, and 802.15.4. These protocols are less reliable and as a result, the devices are more susceptible to data leakage attacks.

Organizations must comply with regulatory guidelines such as CCPA and GDPR when handling personal and business sensitive data. Country-specific guidelines should be followed to safeguard the users when handling of their personal information. IoT devices require a central security policy to correctly handle personal data including detecting, operating, collecting, and storing data. PKI should be used, where possible, to provide a robust encryption methodology rather than relying on hard-coded secrets to authenticate. The data-in-motion should be securely transmitted over the network ensuring that confidentiality, integrity, and availability are guaranteed.

Weak device hardening

The device boot process is vulnerable to attacks if the secure boot is not implemented. Malicious actors can compromise the firmware, boot loader, and boot process sequence by replacing legit executables with a malicious component. With a secure boot process in place, the reboot process would identify the malicious executable file and prevent it from running.

Different types of rootkits load at different phases of the boot process: Device manufacturers should follow the best practices and implement secure boot on the devices. Various types of rootkits have been discovered and discussed previously.

The recent UFEI rootkit, CosmicStrand, discovered in July 2022 is a classic example that rootkits are not rare.

The discussion above explains how IoT vulnerabilities open up a plethora of attack vectors for adversaries and the possible attacks that originate from each vulnerability. Alternatively, the figure below (Figure: 14) provides a view of the layer-based examination of the potential attacks concerning each layer of the IoT architecture.

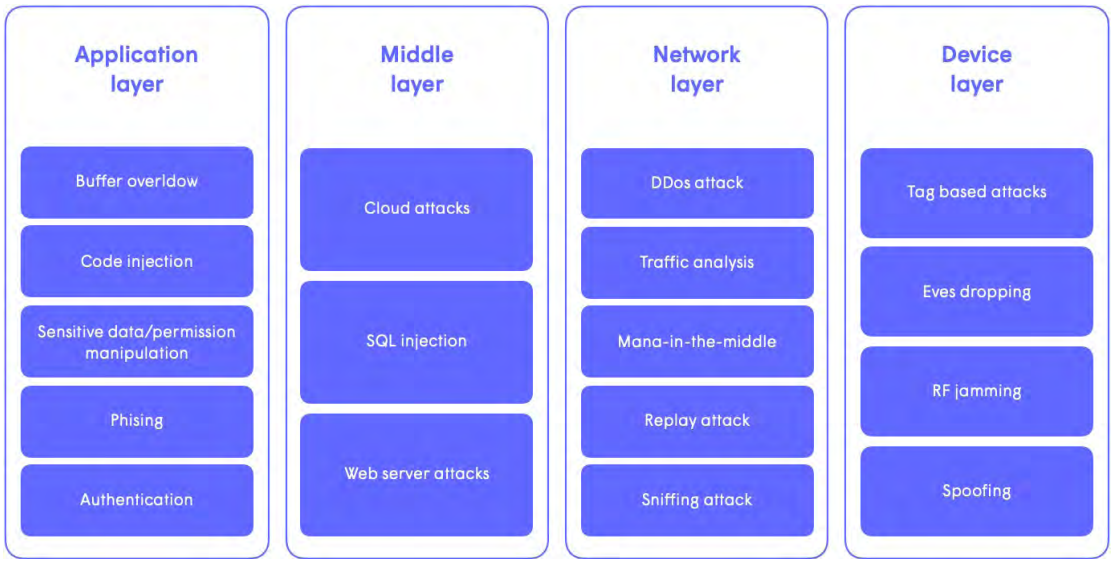

Figure 14—IoT reference model taxonomy

IoT attack flow

Use-case of ransomware

According to leading analysts' reports, the use of ransomware is on the rise, with an average of 144% increase in demands. Attackers use multi-extortion techniques including encryption and name-shaming.

Ransomware is emerging as a productive business model enabling even a novice attacker with little to no technical knowledge to rapidly launch an attack. There are ransomware kits and services available to cybercriminals that remove technical hurdles and lower the bar for participation.

Software vulnerabilities are the primary attack vector for ransomware. In 2021, attackers exploited multiple high-profile vulnerabilities to gain a foothold in homes and small businesses. The duration between vulnerability disclosure and exploit availability has reduced considerably. If vulnerabilities are available, attackers will exploit them and launch attacks. This has made it challenging for organizations and security solutions. Security solutions need to detect and remediate vulnerabilities rapidly.

Log4J is an example of how vulnerabilities are weaponized and exploited at a rapid pace. The following vulnerabilities were exploited in a ransomware attack path.

Figure 15—Vulnerabilities exploited in Log4J

Table 3—Vulnerabilities exploited in ransomware attack path

Vulnerability identified	CVE-2021-44228, CVE-2021-45046, CVE-2021-44832, CVE-2017-5645, CVE-2021-45105, CVE-2019-17571
Vulnerability category	Remote code execution, denial of service

Figure 16—Log4J attack timeline

Taxonomy of ransomware

A ransomware attack typically follows a path with three stages. In stage one, it tries to gain access to the home or business. This is done using internet-facing devices, vulnerable devices, and devices with default credentials. In the second stage, it moves laterally, infecting other devices and scanning for business-critical, sensitive, or personal data. In the last stage, the attacker launches the attack by stealing, locking, or destroying data.

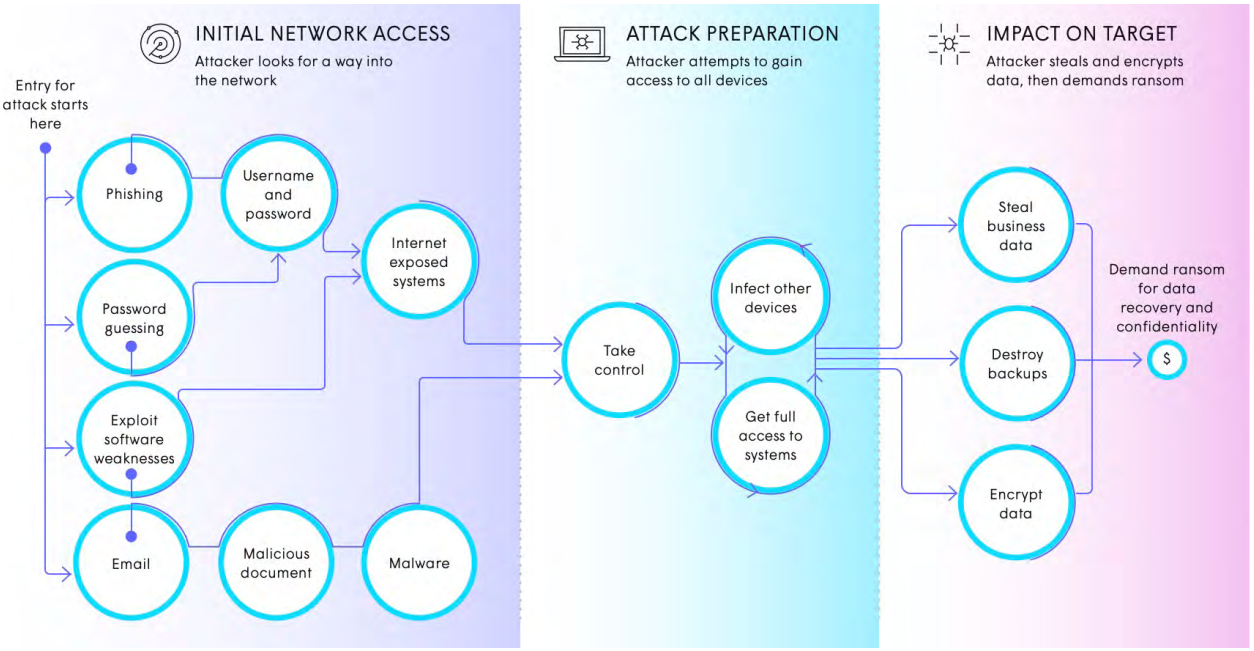

Figure 17—Ransomware attack path

Solution

In the ITU IoT (Figure 13) reference models, different layers have different security requirements:

- Application layer—This layer needs the authorization, authentication, application data confidentiality, and integrity protection, privacy protection, security audit, and anti-virus.
- Network layer—This layer needs authorization, authentication, user data and signaling data confidentiality, and signaling integrity protection.
- Device layer—This layer need authentication, authorization, device integrity validation, access control, data confidentiality, and integrity protection.

Specific security capabilities are closely coupled with application-specific requirements, for example, mobile payment and security requirements.

When designing the security for IoT devices, Plume considers it important to take custom security procedures into account in addition to conventional security procedures. It would be best if the solution assures device security, network security, and the overall security of the IoT architecture and system.

Top analysts rate software vulnerabilities as the most popular attack vector among the cybercriminal community. The following section describes how CSPs can solve many of the problems associated with insecure IoT by providing proactive and continuous vulnerability protection.

Vulnerability detection and protection

Vulnerability insight is part of a multi-layered security strategy and improves the overall network defenses and zero-trust. It is a preventive strategy, and its job is to proactively inform users of known vulnerabilities in devices and help them fix the issues by taking proactive, preventative action.

The solution should protect routers and other devices in the network that are subject to attacks from open ports (capable of infiltrating network defenses) putting user data, finances, and privacy at risk.

A vulnerability management solution has three key components: Detection, protection, and reporting. The section below discusses them in detail (Figure 18). Asset discovery and inventory is a pre-requisite for this solution. Organizations can leverage their existing methods—the details of doing that are out of the scope of this paper.

Figure 18—Vulnerability detection and protection solution

Detection

Visibility and an accurate picture of the network is the key to helping CSPs provide an effective solution. The detection phase is critical to identifying, exposing, and prioritizing the possible threats and weaknesses in the network.

Discovery scan

Detection requires continuous scanning and monitoring of the devices inside the home and small business network. The goal of this scanning is to generate insights about the security posture of the home or business. This is achieved by detecting the device characteristics like firmware, OS, open ports, the services running on those ports, and any port forwarding (UPnP) configuration. All these characteristics should be analyzed and mapped to the known vulnerabilities on the devices. Then vulnerable devices can be automatically blocked from accessing other devices on the home and business network.

Vulnerability scan

Detect if the open ports and the services running on them are vulnerable to brute force or password stuffing attacks. To do this, CPS should be able to find out if the OS running on the devices has any known vulnerabilities. Use opensource or homegrown network scanning tools, like nmap to identify the ports open on the devices on the network and the service versions running on them. Leverage the vulnerabilities databases like NIST and MITRE to identify any known vulnerabilities reported in the discovered services.

In addition, scan the services to detect if the service login credentials are weak or default. Any services running with weak passwords are vulnerable to brute force attacks.

Prevent and protection

Protection approaches can vary based on the technical knowledge and capability of the user. They can range from a complex patch update to step-by-step guided remediation. The goals resolve the issue with minimal user engagement. The following are the possible remediation methods that a good vulnerability protection solution should provide:

Vendor advisory or patch

Provide the link to the vendor advisory or patch where available. The user can follow the advisory and resolve the issue themselves. Example: Firmware upgrade steps, a password change, or temporarily removing a device from the network.

Credential brute force protection

Alert the user if the credentials on the devices are default, weak, and easily hackable. Alert users if the same username/passwords are used for multiple devices/services.

Best practices and guidelines

Provides device-type-specific and a well-curated list of best practices. Provide password hygiene guidelines like a reminder to enable 2FA on the devices, a reminder to change passwords periodically, and a reminder not to repeat passwords for multiple devices.

Virtual patch - continuous protection

The complete vulnerability detection and protection life cycle is very long. It includes the following vulnerability:

Exploitation factors → patch availability → patch application.

The system is vulnerable to attacks during this phase. The virtual patch is a concept that provides vulnerability-specific rules to prevent malicious traffic from targeting the device.

- Pre-patch protection—Detect and prevent traffic exploiting the vulnerability
  - IDS/IPS rules for the vulnerabilities found on the device.
  - Alert when the rule triggers to update the user that they have been protected against the vulnerability.
- Post patch protection—be on the lookout for the vendor patch availability and update the user when the patch is available.

Enhanced security level

Create and deploy a security policy for enhanced and stricter controls for vulnerable devices and homes. Possible policies include:

- Full DPI-based malware protection.
- Block malicious IP/domains.
- Prioritize DOOR alerts for the impacted devices.

Limit device internet exposure

Alert the user if the vulnerable device is exposed on the internet. Proactively limit network access paths to the device and consider disabling UPnP on the vulnerable device.

Internal honey pot

Install a passive detection system in the network. This creates a virtual IP with the most common ports open. Any connection attempt to these services will throw an alert to flag a potential threat. Users can blacklist the connecting IP to proactively protect the network.

Chatbot

Provide a specialized and trained chatbot to guide the user through the remediation steps.

- Provide the user with the unique problem with reference to the vulnerability. E.g.: for CVE-2020-25687, ID is "Vuln-2020-25687".
- Problem specific guidelines—The user can use the chatbot with the given ID and get step to resolve the problem.

Call support

Solution providers should provide a support center where the user can get help resolving issues. Customers can choose to call vendor support directly or the solution provider. Alternately, CSPs can partner with the vendor support and report issues on behalf of the end user.

Reporting

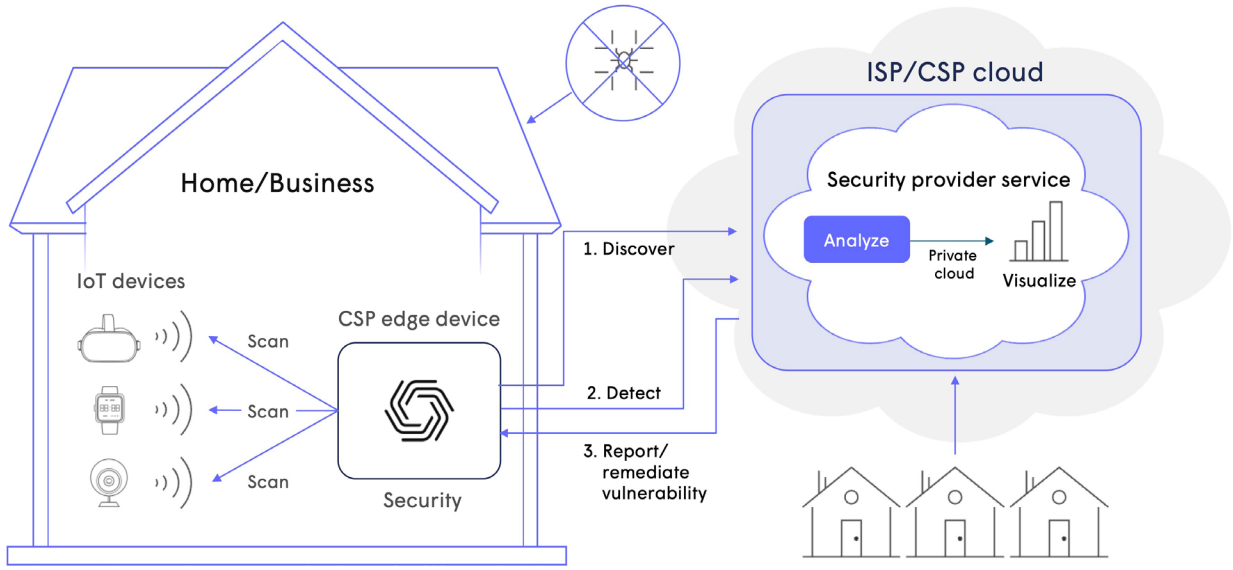

Figure 19—Reporting as part of the vulnerability protection solution

Reporting is a critical part of the vulnerability protection solution and should focus on providing an actionable, prioritized subset of vulnerabilities to the user or administrator. An overall threat score would give a consolidated view of the security posture of the network. The security score would comprise of several factors to measure the security state i.e., number and severity of vulnerabilities, exploitability, time of exposure to a vulnerability, and more.

Conclusion

IoT for homes and small businesses has its merits, but also comes with significant security challenges due to rapid technology transformation and a lack of knowledge. IoT is like an open door with lucrative low-hanging fruit for attackers. Openly available attack kits are further lowering the bar for attackers. Software vulnerabilities, weak passwords, and open ports are the primary attack vectors. It is possible, however, for CSPs to provide value-added security services and safeguard consumers against cyber threats. This is a win-win scenario for both CSPs and users. We need an intelligent vulnerability detection and remediation solution that can continuously scan and flag vulnerabilities and well scan for weak passwords and provide remediation guidance to users. Considering the evasive nature of attacks and the short time spans within which they take place, we need to invest in an AI-based behavioral solution that will provide proactive alerts when a device exhibits malicious behavior and take action to protect the network.

Let's use IoT safely and improve our productivity. Let's close the door on attackers before they close your business.

Abbreviations

AI	artificial intelligence
CSP	communications service providers
CVE	common vulnerabilities and exposures
CVSS	common vulnerability scoring system
DNS	domain name system
IoT	Internet of Things
IT	information technology
ITU	International Telecommunication Union
MITRE	Massachusetts Institute of Technology Research and Engineering
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
TV	television
WFH	work from home

References

1. 1 in 3 Employees Don't Use Vpn to Connect to Company Network While Working from Home: CISO MAG Survey, 2020, CISO MAG

2. 2022 Unit 42 Incident Response Report, 2022, Palo Alto Networks, Inc

3. Babel of IoT Authentication Poses Security Challenges, 2020, Dark Reading, Robert Lemos

4. BotenaGo Malware Targets Millions of IoT Devices, 2021, IOT World Today, Callum Cyrus

5. CosmicStrand: The Discovery of a Sophisticated UEFI Firmware Rootkit, 2022, SecureList by Kaspersky, Global Research & Analysis Team at Kaspersky Lab

6. Current CVSS Score Distribution for All Vulnerabilities, ongoing, CVE Details

7. CVE, ongoing, The Mitre Corporation

8. Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review, 2019, Journal of Computer and Communications, Arbër Beshiri (University "Ukshin Hoti" Prizren) and Arsim Susuri (University "Ukshin Hoti" Prizren)

9. How and When the Chip Shortage Will End, in 4 Charts Fabs Using Older Process Nodes Are the Key, 2021, IEEE Spectrum, Samuel K. Moore

10. IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges, 2020, IEEE, Pooja Anand, Yashwant Singh, Arvind Selwal, Mamoun Alazab, Sudeep Tanwar, and Neeraj Kumar

11. IoT Vulnerability Assessment of the Irish IP Address Space, 2020, F5 Labs, Leona McNulty

12. Known Exploited Vulnerabilities Catalog, ongoing, Cybersecurity and Infrastructure Security Agency

13. National Vulnerability Database, ongoing, National Institute of Standards and Technology

14. Nmap, ongoing, Nmap

15. Report: 57% Of IoT Devices Vulnerable to Severe Attack, 2020, CEPro, Amy Rock

16. Requirements and Reference Architecture of the Machine-To-Machine Service Layer, 2015, International Telecommunications Union

17. Shodan Dashboard, ongoing, Shodan

18. Smart IotT Devices in the Home: Security and Privacy Implications, 2018, IEEE Technology and Society Magazine, Vijay Sivaraman, Hassan Habibi Gharakheili (UNSW Sydney), Clinton Fernandes, Narelle Clark, and Tanya Karliychuk

19. Stop Ransomware, ongoing, Cybersecurity and Infrastructure Security Agency

20. The Mirai Botnet Explained: How Teen Scammers and CCTV Cameras Almost Brought Down the Internet, 2018, CSO, Josh Fruhlinger

21. UEFI Firmware Rootkits: Myths and Reality (Revisited for Black Hat Asia), 2017, Black Hat Asia 2017, Alex Matrosov and Eugene Rodionov

22. UPnProxy: Blackhat Proxies via NAT Injections, 2018, Akamai Technologies

23. UPnProxy: Eternal Silence, 2022, Akamai Technologies, Chad Seaman

24. Vulnerability Metrics, ongoing, National Institute of Standards and Technology