VIRTUAL EXPERIENCE
OCTOBER 11-14

2021 Fall Technical Forum
SCTE • NCTA • CABLELABS

Security Strategies in the Wake of Nation-State Attack Evolution

A Technical Paper prepared for SCTE by

Emma Rochon
Security Architect 2
Comcast Cable
1800 Arch Street, Philadelphia PA 19130
215-262-3275
emma_rochon@comcast.com

Nancy Davoust
VPII, Security Architecture, Identity and Access
Comcast Cable
1800 Arch Street, Philadelphia PA 19130
303-862-0143
nancy_davoust@cable.comcast.com

Table of Contents

List of Figures

1. Introduction

Over the past decade, private businesses have increasingly been the victim of nation-state cyberattacks, which are defined as attacks carried out by a hacker, or a group of hackers, working with adversarial government to commit cybercrime against another country. Notably, there has been an 100% increase in nation-state incidents from 2017-2020. Specifically, nation-state attacks rose from 17% of all known attacks to over 40% during the last 3 years [3].

In this paper, we will highlight some of the issues with nation-state attacks and provide some guidance on how to defend against these attacks on a regular basis. There is no one way to defend against attackers, but there are strategies that can be implemented to prevent an attack from being catastrophic.

2. Nation-State Attack Background

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) and other government agencies continue to post warnings about nation-state attackers and their techniques to attack as they continue to advance. Many of these attacks could be applied to the cable industry. The cable industry has evolved significantly in the past 20 years with the rise of Internet and connected services to become a prized attack surface for nation-state actors.

Who are these nation-state attackers? Often these are known as Advanced Persistent Threats (APTs) because they are constantly working to come up with new attacks and they never go away. The largest groups of APTs come from Russia, China, North Korea, Iran and the U.S. [4]. The attacks are becoming more impactful, with posturing around government influence and even threats of physical war. Additionally, economic damage caused by nation-state attacks impact its citizens. The pipeline attack earlier this year in the U.S. caused fuel shortages for cars in the impacted areas which impacted people getting to work and school [10].

Just like all hackers, nation-states take advantage of known issues. Unlike the general hacking community, nation-states have political goals as well as financial goals. These nation-state attacks include theft of political or military data, advancing foreign policy, disinformation campaigns, or financial motivation. The nation-state attackers profile includes larger targets, more financially rewarding targets, and targets that will bring damage to other countries [4].

And most importantly, nation-states are well organized, funded, and very patient. It is not always directly obvious that a nation-state is sponsoring a cyber-attack, and many attacks do not have confirmation on their origin yet are heavily suspected to be a nation-state attack. If nation-states are going to make their goals, they will be persistent. Once attackers get into systems, they try to stay in them. A key activity for nation-states is to perform reconnaissance once in a system and prior to striking, so they have a good inventory of all the attack methods and damage they can cause before they strike. However, some attacks are very much predicated on timing of new zero-day attacks being found. Zero-day attacks are serious software vulnerability exploits, which the developer or vendor may not be aware of. It is always a race to exploit a new zero-day attack before a patch can be applied to fix the issue [5].

To make matters worse, on July 14, 2021, SecurityWeek reported that China has passed a new law that any zero-day vulnerability discovered by anyone in China is required to be shared with the CCP, and is prohibited from being shared with anyone, or any government outside of China. Product manufacturers may learn of vulnerabilities in their products, but this is not completely clear. This will make it more

difficult to gather information. Until then, security researchers around the world shared information about zero-day vulnerabilities they found.

As we look at how to best secure access from people and software to software resources storing and using sensitive data on various types of devices, we need to understand how to best apply our time and resources to protect against these nation-state attacks. Nation-state attacks have evolved from political statements to other types of attacks such as military intelligence, election interference, resource interference and ransomware. Protections include doubling down on security overall, and especially ensuring there are strong authentication, access management and authorization systems to protect against attacks like phishing, and escalated privileges.

There are many exploitable attack surfaces and nation-states understand how to take best advantage of many of these. One well known path is using supply chain weaknesses to plant malware which may propagate into other systems or provide access and visibility once implanted within a company. There have been cases of malware being included in devices or software specifically in products destined for the country they desire to attack. Therefore, when a device is powered on, software is now running inside the country and company they are trying to attack, and it does not appear to be an attack from the outside. Some security experts recommend not to buy devices or software from countries in question.

3. Past and Current Cyberattacks

Analysis of past and current cyberattacks is among the best tools when it comes to understanding where to apply more security to defend your systems. Knowing what occurs in those successful exploits can shape updated guidelines on what to consider when defending your own systems. Often, security requirements present as clinical, general statements and theories that take effort to apply to systems. And while those statements and theories are critical to system security, they fall into the category of security hygiene and overall best practices. Ensuring that data is using NIST-approved encryption mechanisms is a best practice, since any deprecated encryption practices could be broken by attackers, if they were able to breach the data in the first place. Best practices come from the assumption that attackers are already present. And zero trust principles require continuously questioning trust, aligning with the thinking that attackers are already present in systems. That doesn't mean every system has an attacker in it, it just means that we must assume that attackers can break past the first layer of security and are able to gain access to systems.

As was introduced earlier in this paper, nation-state attackers take advantage of undiscovered zero-day software vulnerabilities. Many of us receive notifications daily which ask us to update software. Outdated software is where exploitable vulnerabilities lay, and without updating software often and consistently, systems are more vulnerable to common attacks. When systems choose to release software patches, they often release patch notes on what was changed. Attackers often use these patch notes to create exploits for systems running the vulnerable version and will use these exploits to target unpatched systems. Possibly the most notable ransomware, WannaCry, originated from outdated software. Attackers used the exploit on the SMB protocol to create WannaCry, a ransomware that successfully attacked over 300,000 devices [9]. Ransomware has affected everything from gas prices to meat production and it is expected that it will continue to grow [10].

A recent attack that occurred using zero-day vulnerabilities was to a popular email, calendar, and collaboration tool [2]. In this situation, attackers had discovered four zero-day vulnerabilities within this server. Patches for this vulnerability were released about a month and a half later. The four vulnerabilities, when used in tandem, can lead to remote code execution (RCE). Remote code execution is

how attackers can hijack servers, create backdoors, steal data, and further any malicious code deployment. This attack was traced back to an APT group from China. APT groups, or Advanced Persistent Threats, are threats that originate from nation-state attackers, and often consist of an attacker gaining entry to a system and lying dormant for an amount of time. Although an update and security patch have been released to remediate these vulnerabilities, that does not mean the threat is gone. Anyone using the affected software versions is vulnerable to future attempts of the exploit. Furthermore, current systems may have been compromised even with the patch, and techniques such as an undetected backdoor or a time bomb file that will execute on a certain date may still exist on the patched server. This attack demonstrates the capability of nation-state attackers.

Another malware attack that occurred in 2020 offers insight into how nation-state hackers operate. In this situation, attackers were able to use forged tokens to obtain privileged access in a system used for IT administration throughout many organizations. Attackers then used this elevated privilege to access whatever software they wanted to within the organization by using the forged token. Forged tokens can only work if they are not cryptographically secure tokens, if the keys to secure the tokens were stolen or the applications validating the tokens are susceptible to replay attacks and do not validate the signatures with unique data for each transaction. These types of compromises provide unauthorized access to data and software.

In the past two years, we've seen an increase in ransomware, effectively making some systems completely unusable. From 2019 to 2020, ransomware attacks rose 62% worldwide, and an incredible 158% in North America [10]. Ransomware infects a system and encrypts the system data against the user's will. Then, the user is presented with an option to pay a ransom, which will hypothetically decrypt the user's data. Ransomware is complicated to resolve. In the past, ransomware victims were warned not to pay the ransom, as that would encourage other attackers to go down the ransomware route. There is also never a guarantee that paying the ransom will unlock your system. In some ransomware, it was easier for the program to wipe the system instead of encrypting it, so that by the time the ransom was paid, the data was already gone. Many of the new ransomware infections require multiple payments, the first to unlock your encrypted data, the next to avoid selling data to others. There may be a third payment set up as a monthly fee, to avoid any re-locking of data. In most cases of ransomware, it is unlikely that the targeted system will be able to recover normally, or that the organization will recover financially.

Nation-state attackers, as well as individual hackers, are seeing the current landscape of how organizations respond to ransomware attacks. The popularity of ransomware is partly due to how many organizations are paying out the ransoms. Statista surveyed over more than 600 IT organizations found that most of them had been infected with ransomware in 2020, and 68% of those infected paid the ransom [6].

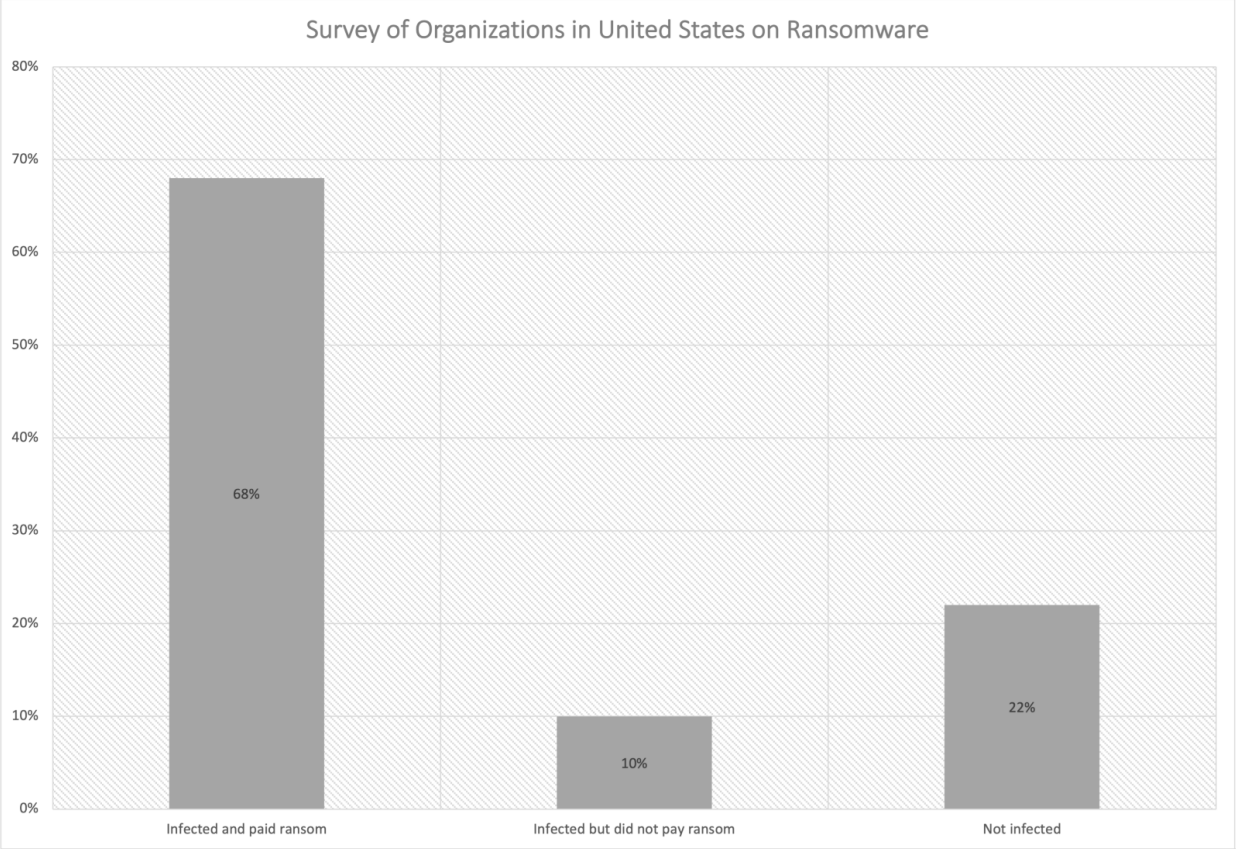

Figure 1 - Organizations on ransomware response in 2020

The effect of ransomware is two-fold. First, the ransom itself generates financial gain for the attackers. Second, the ransomware takes the system offline. Other attacks for taking systems offline include denial-of-service attacks, where a system is flooded with requests, too many to handle. Ransomware can take a system offline, as well as generate significant money for the attackers, which a typical denial-of-service attack cannot do. As more organizations continue to pay out the ransom, more ransomware attacks will happen. Instead of waiting for a ransomware attack to hit a system, it's better to plan.

The best defense against ransomware is to ensure that your system can be re-built, and re-instated, without touching the infected portion of the system. Often, this is done by building a disaster recovery (DR) environment, that replicates the production environment of the system. However, if a disaster recovery system is on the same network, or attached to the production environment in some way, it is useless. The disaster recovery environment should be geographically and logically separated from the production environment. The DR plan needs to include a back-up copy of any needed data, that is located off-site and stored in a separate way than other data. Many ransomware systems attempt to discover automated backup systems first, then ensure to lock both the original and the backup. Ensure your business-critical systems are equipped to deal with ransomware appropriately, to avoid unwanted payments and unwanted outages for your business.

4. IoT Device Security

Nation-state attacks can use any possible method to achieve its goals. One area that has been overlooked in the nation-state conversations, but could become an issue, is IoT devices. According to Juniper

Research, over 46 billion IoT devices will be attached to networks around the world by the end of 2021. That is a lot of potential attack surfaces.

IoT devices, even though small in processing power, can still propagate malware or overwhelm a network with traffic, especially if tens of millions start to chat all at once. Additionally, many IoT devices openly communicate with various back-office systems for software updates, configuration changes and service level monitoring. Many IoT device manufacturers have yet to appropriately implement security, because of resource constraints on the device, yet the device is able to connect to networks using various protocols. If an attacker could compromise the "right" (unprotected) IoT devices, they could be used to deny service, lock or steal data, and more. Some of the connectivity challenges are not only issues with specific protocols, but, just like software, which version of protocol is supported on the devices. Some more popular protocols include WiFi, Bluetooth, Bluetooth Low Energy (BLE), LoRa, RF, NF, Zigbee and others. Each protocol is created by a different organization at different times over the last 10+ years to help connect devices to a network. Even the protocols that start out with some security have a difficult time keeping up with new versions that are secure since IoT software stacks are difficult to update.

The Zigbee organization has changed its name to the Connectivity Standards Alliance (CSA) and now includes Matter (its newest secured protocol), Zigbee, Green Power, Smart Energy, JupiterMesh, RF4CE and Dotdot. We are happy to see the newer protocols evolve security protections. The Professional Service Association (PSA) organization certifies security principles for IoT devices for a unique identifier, security lifecycle, PKI certification, secure boot, secure updates, anti-rollback, secure storage and trusted cryptographic services. Earlier in 2021, they had certified 30 chips/SOCs, 14 software platforms and 10 OEM devices to date. Wi-Fi improved security with WPA3 which includes a QR code with a public key you can scan with your phone instead of using a password and has stronger cryptographic algorithms with forward secrecy and updated keys.

While we are making progress, it is not enough to rely on external organizations to provide all the necessary security for devices attaching to our networks. One thing we can do is participate more in setting standards and enforcing compliance from manufacturers. We can learn, from the many security standards on other products and services that have emerged from International Standards Organization (ISO), National Institute of Standards and Technology (NIST), Payment Card Industry (PCI), Health Insurance Portability and Accountability Ace (HIPAA), various privacy laws (GDPR, CCPA & CPRA, and many others), Financial Industry Regulatory Authority (FINRA) and others to help mold where we are today. We can certainly take many lessons learned from across the spectrum and apply as many as possible. Then where there are gaps, we need to step-up and lead innovative solutions.

To help understand how to best mitigate issues, study and understand past and present attacks. A good source of attack information is available from the U.S. CERT vulnerability advisory, which provides information on discovered vulnerabilities every day. A surprising number of vulnerabilities are published on a regular basis. As you learn about new security vulnerabilities, you can assess your environment, applications, devices, services and resources for issues. Some issues can be mitigated with workarounds or additional protections applied to help protect your company and your customers before formal patches can be released.

For IoT devices, let's apply the normal baseline security practices for larger devices. There are 5 major areas to ensure device security. Most of these are currently inadequate, which means they do not exist at all or are highly immature:

1. Standards to which IoT devices should comply
2. Designs which allow for improvements in features, including security updates over time -- which is more difficult to implement but necessary to resolve

3. Testing and compliance measures to ensure implementations meet laws and standards
4. Ongoing operational support for scanning and patching.

The real trick with an IoT device is to ensure it can be as secure as a server, but with very little resources. Many manufacturers' margins are thin because of tough competition and rising costs for resources and labor. Manufacturers have little incentive to increase spending on security unless other manufacturers are investing as well. Most people do not understand security well enough to know what look for, and have no influence on manufacturers of IoT devices. After all, if an IoT device breaks due to a security issue, the consumer must buy another appliance. That seems counter to the cycle we'd like to see created, where manufacturers are required to build security in to keep devices, people, and networks secure.

Part of a secure IoT device architecture could depend upon being behind a secure gateway in the home, however not all ISP connections and gateway products will be at the same level of security. Additionally, IoT devices may respond to a myriad of protocol announcements to join a network or be discovered and accessible and may never traverse on a path that is secure to the Internet. And then there are exploits which could take advantage of these devices that may not be able to discriminate against the signals from a secured gateway vs a rogue device.

Some basic tenants for device security include but are not limited to having secrets encrypted in storage, and obfuscated when in use. These secrets include a hardened identity that cannot be spoofed. One way to do this is to only put identity into hardware and secure it with an x.509 certificate, where the private key is also only available in hardware. Having a hardened identity prevents spoofing and evil twin attacks as well as serving as the basis for strong authentication against a trusted identity.

Devices also need to include secure boot up sequences and operational status to ensure integrity and authenticity of the hardware and software. Secure boot needs to include an unbroken chain of trust between the different layers of components and software, to ensure hackers cannot introduce new software between layers of different authentication keys that are not tied to a root of trust or authentication processes. Authentication is best when it is a cryptographic series of functions that cannot be interrupted when software is first being loaded for use during the boot process.

Devices must include a way to receive secure configuration updates as well as secure software updates. When devices do not include security on configuration interfaces, this leaves security entirely to the environment in which the device is run to ensure that only authorized configurations are allowed. The device must include protections against malware, which include automated software updates, without customer intervention.

Devices must ensure that unnecessary hardware and software ports are not available, which could be an open hole for attackers to exploit. Having open ports and unnecessary protocols or APIs is a common issue. Attackers will learn how to reach devices using these protocols and open ports. Additionally, ensuring security is turned on for the necessary open ports is critical. Using common or global secrets to protect ports is no longer an acceptable practice. Each port needs to use unit-unique public key cryptography to ensure access only comes from legitimate users in the ecosystem and is only destined for that specific device.

One of the most common issues is the inclusion of a default password in devices. This should be prohibited. Many people do not change default passwords. Attackers count on getting into devices this way. Additionally, passwords are easy to crack and should never be used without including multifactor authentication. People needing access can use mobile apps to manage multifactor authentication, or

a QR code with public key cryptography. Logins could use common sign-in systems such as Google, Microsoft or Apple. These are trusted authentication systems.

With the increased use of zero-trust principles which include micro segmentation, the blast radius for compromises can be reduced. Micro segmentation ensures that each resource should only be reachable by other authorized resources, and is accomplished by isolating network access. Authentication of resources is required, in addition to authorization as will be discussed. Another best security practice is to ensure that only things that need to reach the Internet, do. Many people accidentally configure public cloud accounts to be publicly accessible. Additionally, IPv6 addresses can be a source for common access mistakes, such as when people use a public address rather than a private address for internal applications.

One common question that comes up in security is how to assess if a device is healthy, meaning, not currently compromised. We not only need to know if a device is heathy as a part of normal monitoring, but also whether it is healthy upon first configuration for service – a clean start. For IoT devices today, we generally don't know. For IoT devices in the future, without overburdening the necessary hardware and software for an IoT device, it should be mandatory to have device security state, software versioning and file integrity. Creating a virtual device architecture for monitoring device health could improve our ability to contain attacks.

Using common security frameworks, such as the NIST Cybersecurity Framework, to map out all the components of IoT devices for its entire lifecycle is a good way to cover the necessary security protections. The NIST Cybersecurity Framework provides guidance on identification, protection, detection, response and recovery. For example, identification includes visibility into where and what systems or devices are in your ecosystem and how they are lifecycle-managed and governed. How will you able to respond to an attack if you don't know where or how to reach devices, systems or applications? In conjunction with traditional security frameworks, technological maturation processes need also to be assessed and anticipated. Consistency in security processes and operational monitoring need to be applied with good ways to measure against risk for your company.

Continuous scanning and immediate patching are both critical to keeping down the number of vulnerabilities on your devices and in your software. There are great scanning tools available for things like Windows servers, but when it comes to homegrown applications, IoT devices and industry-unique solutions, scanning leaves much to be desired. Each team responsible for building and operating devices and software can keep up their operational excellence metrics with weekly reporting on any known issues and remediation status. Operational excellence is a requirement to ensure there are no outages. Too often, software teams are focused exclusively on new release cycles at the cost of spending cycles to lower technical debt -- which includes security vulnerabilities.

Additional scanning techniques can look for static passwords, which should be immediately replaced with strong authentication mechanisms, managed by automation where possible. Also very important is scanning for certificate expiration dates and replacing certificates before they expire. For example, if a certificate is expired that is used for TLS authentication, TLS leaves a wide-open security hole by failing the connection open with no security. Be sure to configure TLS sessions to prohibit failing open, and monitor and replace certificates before they expire.

Monitoring for the previously mentioned device health, as well as activity such as communications paths are important to understand. If communication should only be happening with a back office system on your corporate network, but you can see communication messaging over APIs exiting your corporate network, that is an alert. It may represent a security issue related to data that may be leaking; access may

be compromised; malware may be propagating, etc. Monitoring should also include using data analytics and machine learning to access patterns for people as well as applications. Understanding what the normal operating model looks like can be key to blocking lateral movement, if access or device software is compromised.

Monitoring file integrity and approved configurations matters. If an attacker changes configurations and plants malware, you want to be able to detect and respond right away. Having a way to roll back or rebuild clean code quickly to remove malware is very important. Often the difference between a small incident and a large compromise is time. If good monitoring techniques are not in place, small issues can go undetected for a long time. Combinations of small issues may fall under the radar of detection and then can be executed together to perform a larger exfiltration, such as a "golden" pile of data being moved, or denying access to services or devices.

Concentrating on all points of network access is also important. That said, monitoring can only be as good as the data it is getting. If unauthorized access is happening in a vendor network or off-shore facilities, is there anything monitoring the network that will trigger unusual activity? This activity could appear to come from a legitimate vendor connection, but the fact that the traffic came at an unusual hour could be a tipoff.

Examining source IP addresses (if you can get them) can tell you if there are connections coming from geolocations that are unacceptable. Collecting context-rich data, containing information such as source IP address, can enable a system to separate legitimate traffic from unacceptable traffic. More systems and services are using location, connecting to compromised data sets for comparison and getting information from government agencies to help identify issues, such as known malicious source IP addresses. Also, security level protections for connections with outside businesses or facilities should be verified to ensure malware protections are in place before accepting traffic from that new connection. DDOS and malware-sourced verification is common.

Using good Secure Development Lifecycle (SDL) management practices is also mandatory. Ensuring every device make and model has gone through a threat model to identify attack surfaces and identify how to best protect them is important to do as a part of the design phase. When threat modeling, review not only the architecture, features and functionality of the product, but also the code build pipeline. Additionally, ensure all APIs and protocols are being designed for secure use. Data encryption and privacy also need to be reviewed as a part of a good threat model. Then ensure pen testing is conducted, in an environment like where the device will actually operate, to provide the right level of operation security configurations. There are many other aspects to the SDL, including scanning for bugs in code, and the previously mentioned monitoring aspects.

5. Authentication and Authorization

So how can we secure access? By using strong authentication, access controls and authorization for users, software, and devices. Authentication and authorization are often confused with one another, but in the scope of system security, it is critical for the two to be implemented and assessed separately but designed together to ensure no security gaps. Authentication is the process of confirming a subject's identity, and authorization is only allowing that identity access to information and systems they are allowed to access. Authentication and authorization are most associated with human users, but modern practices include authentication and authorization of machine access as well.

Secure your front and back doors as well as your windows into your systems, applications, resources, devices and services. Secure your workforce users, workforce admin accounts, workforce

service accounts, guest and vendor accounts, and all customer accounts. If nation-state attackers get their hands on any kind of credentials, they will use them. Work within the zero-trust model, to create checkpoints throughout the system to ensure users, and machines, are not only who they say they are, but that they also have the correct access. Following this model can prevent attackers from taking advantage of authentication and authorization in a system.

Evaluating the system's environment is the first step in considering authentication and authorization. A common solution to insecure connections is to require the use of a VPN, or a Virtual Private Network. The use of a VPN verifies that the user is on a private, usually encrypted, connection. However, before the connection to a VPN can be established, a user must authenticate to the VPN and prove their identity. Access to the VPN may be needed to access sensitive or confidential data, so it is important to use a strong method of authenticating users to the VPN. VPNs generally don't take care of any authorizations beyond hooking into authentication systems such as SSO to ensure they have active user credentials that are authenticated.

Ten years ago, a simple username and password combination would be enough to access sensitive data and critical systems. Today, multi-factor authentication is the industry standard. In fact, multi-factor authentication has a 99.9% success rate in protecting against compromised credentials [5]. The purpose of multi-factor authentication (MFA) is to first, enter your username and password, but as a second step, to prove user presence through a second device.

However, MFA is not invincible, and as it becomes widely adopted, we will see more and more attacks on systems protected by multi-factor. Older MFA solutions such as SMS-based MFA have shown to be easily hacked, which is why SMS-based MFA is becoming less popular and is being replaced by multi-factor that depends on an authenticator application, such as Duo Mobile or Microsoft Authenticator. These authenticator applications provide another level of security that SMS-based MFA does not. The difference between SMS-based MFA and application-based MFA is that it is easier for an attacker to compromise a user's text messages, but a significantly more difficult task at hand if they need to get to an application in the user's device and compromise secure APIs. However, there are even potential vulnerabilities with these authenticator apps, such as user error. If a user gets too comfortable accepting authenticator requests, they have the chance of accepting a false authentication request and approving an attacker's request. Therefore, many authenticator apps have begun implementing multi-factor requests that force the user to engage with the request, and in process, confirming that they are the one who made the actual request.

Passwordless authentication is making its way through the technology world [5]. At the root of authentication, there are three ways a user can prove their identity: something they know, something they have, or something they are. Something they know would be a password, or a security question. Basing user authentication on something they know is no longer considered secure. Multi-factor authentication, as well as SMS-based two factor authentication, depends on something the user has. This is usually a phone but can also be a hardware token. With multi-factor authentication, the first step of authenticating is to enter a username and password combination, and then approve a request on another device. The password is still in use during this authentication mechanism. With something that the user is, however, passwordless authentication is making a rise. This is authentication that is based on user presence, as well as user validation in the form of biometrics.

Passwordless authentication does not only consist of user biometrics. In fact, there are a handful of ways that users can authenticate into a system without using a password. However, biometrics have become one of the most popular ways a user can authenticate, without a password. The different technologies

behind passwordless authentication include, but are not limited to: FIDO2, Windows Hello, and Microsoft Authenticator passwordless authentication.

These forms of multi-factor authentication, app-based or passwordless, are acceptable options for gaining access to a network. However, once a user is authenticated through single sign-on using a specific device, that authentication can carry over to more resources, including other applications, without requesting to sign back in. This is accomplished by using technologies like OpenIDConnect (OIDC), SAML, and OAuth. These technologies rely on cryptographic tokens and keys to be passed from machine to machine. These technologies can be used to identify and authenticate human users as well.
Creating a secured identity for machine access may not be an obvious solution, but attackers have been able to use machine identities to gain entry to a system. How do we prevent attackers from spoofing machine identities? One solution is PKI, with a signature over unique data in the transaction which shows current proof of possession of the private key associated with the public key inside the certificate. The certificate contains the device identity, and the certificate is also signed by the trusted certificate authority.

Authorization ultimately arises from the principles of least privilege, which essentially states that users should have access only to the resources they need, and no more. Authorization is often overlooked, as it requires specifying explicit access to specific resources and tasks as named in an attribute or role-based access control policy. However, it is critical for access to be defined per user, such as a general user role with least permissions and then only giving specific users elevated privileges. Abusing excess privileges is an integral part of how attackers navigate through a network, and access control is how one can prevent an attacker from leveraging them.

While an attacker can certainly leverage excess privileges, an employee can as well. Insider threats are a real concern and make up a significant portion of privileged access attacks. This is especially concerning if an individual has unfiltered access to systems, and their credentials are not revoked after termination. Real-time ability to revoke credentials is crucial in preventing abuse and compromises. If an individual leaves the organization, or does not need access to a resource anymore, the immediate revocation of their credentials or access is critical. This includes not only employees, but also contractors and business partners. Vendor access is another area of user access that often is overlooked. Vendor access must follow the same policies as regular users within the environment, potentially with less access to base resources.

Following a zero-trust model, as well as authenticating and authorizing users for resources by using modern technologies will assist in preventing stolen, forged, or abused credentials from causing a catastrophic incident. Nation-state attackers are resourceful and will take what they can. Minimizing their blast radius from compromised credentials is essential.

6. Conclusion

There is no guaranteed way to prevent attackers from exploiting your systems. However, best practices can be applied, as can a bit of innovativeness about how to thwart unauthorized access into systems, and prevent unwanted events. As described in this paper, nation-state attackers will try any method possible to circumvent system security. Defending against potential attackers requires time, energy, and money. However, it is no longer possible to ignore security when building systems and networks. Using the methods outlined in this paper can help prepare a system to defend against attackers.

Attackers, especially those representing nation-states, will continue to evolve their attack methods as technology evolves. Underestimating these attackers will result in a security posture unprepared to deal

with evolving attacks. As we know, there is no one magic fix for defending against hackers. They are resourceful, unpredictable, and relentless. Instead of a one-time fix, system security involves an ongoing process of evaluating, building, testing, re-evaluating, re-building, re-testing, and repeating. The purpose of this continuous evaluation is to keep up with the attackers, as they are continually and constantly attempting to gain access to cable provider systems. Following the practices in this paper will help create a security posture for cable providers in the modern age.

Abbreviations

API	application programming interface
APTs	advanced persistent threats
BLE	bluetooth low energy
CISA	Cybersecurity and Infrastructure Security Agency
CCP	Chinese Communist Part
CCPA	California Consumer Privacy Act
CPRA	California Privacy Rights Act
CSA	Connectivity Standards Alliance
DR	disaster recovery
FBI	Federal Bureau of Investigations
FINRA	Financial Industry Regulatory Authority
GDPR	Global Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability
IoT	internet of things
ISO	International Organization for Standardization
MFA	multi-factor authentication
NF	near-field
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OIDC	OpenIDConnect
PCI DSS	Payment Card Industry Data Security Standard
PKI	public key infrastructure
RCE	remote code execution
RF	radio frequency
SDL	secure development lifecycle
SMB	server message block
TLS	transport layer security
VPN	virtual private network

Bibliography & References

[1] "*Cybersecurity Framework*", NIST, https://www.nist.gov/cyberframework

[2] *"Microsoft: Multiple Exchange Server Zero-Days Under Attack by Chinese Hacking Group"*, Ryan Naraine, SecurityWeek, https://www.securityweek.com/microsoft-4-exchange-server-zero-days-under-attack-chinese-apt-group, March 2 2021

[2] "*Nation-state cyberattacks see huge rise in 2020*", Sead Fadilpašić, TechRadar, https://www.techradar.com/news/nation-state-cyberattacks-see-huge-rise-in-2020, April 8, 2021

[3] "*Nation States, Cyberconflict and the Web of Profit*", HP Wolf Security, HP, https://threatresearch.ext.hp.com/web-of-profit-nation-state-report/, April 8, 2021

[4] "*New Law Will Help Chinese Government Stockpile Zero-Days*", Kevin Townsend, SecurityWeek, https://www.securityweek.com/new-law-will-help-chinese-government-stockpile-zero-days, July 14, 2021

[5] "*One simple action you can take to prevent 99.9 percent of attacks on your accounts*", Melanie Maynes, Microsoft, https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/, August 20, 2019

[6] "*Share of organizations in the United States that experienced a ransomware attack and paid the ransom in 2020*", Joseph Johnson, Statista, https://www.statista.com/statistics/701282/ransomware-experience-of-companies/, March 5, 2021

[7] "*Technical Deep Dive Into SolarWinds Breach*", Parmanand Mishra, Qualys, https://blog.qualys.com/vulnerabilities-threat-research/2021/01/04/technical-deep-dive-into-solarwinds-breach, January 4, 2021

[8] *"WannaCry Ransomware Campaign: Threat Details and Risk Management"*, John Miller and David Mainor, FireEye, https://www.fireeye.com/blog/products-and-services/2017/05/wannacry-ransomware-campaign.html, May 15, 2017

[9] "*Why ransomware attacks are on the rise – and what can be done to stop them*", Lynsey Jeffery and Vignesh Ramachandran, PBS, https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them, July 8, 2021

