SCTE·ISBE CABLE-TEC EXPO 2018 | ATLANTA, GA OCTOBER 22-25

2018 Fall Technical Forum SCTE·ISBE • NCTA • CABLELABS

Preventing Unwelcome Guests in Your Home

Securing IoT Devices Within the Home Network

A Technical Paper prepared for SCTE•ISBE by

Dave Belt
Technology Evangelist
Irdeto
Conifer, Co.
(303) 653-7647
dave.belt@irdeto.com

Table of Contents

Title **Page Number**

1. Introduction

With the explosion of IoT devices within the home network, new challenges are emerging for MVPDs from a device management perspective. In the traditional cable model, Operators had full control of the system from plant to device providing the ability to not only manage system security, but also the end user experience. With the emergence of the TVE experience, operators have slowly been accepting and eventually embracing the presence of COAM devices within the ecosystem.

Herein we will look at the devices and threats within the Home Network with the end goal of understanding these devices and their capabilities and enabling the creation of practical policies for their management. First, we will look at device management models and how this affects our control over their behaviour. Next, we will walk through the type of security capabilities that we expect within trusted devices. Finally, we will look at the types of threats that can occur within these device ecosystems and lay some guidelines for managing them.

2. Devices and Their Management

Home networks are built from devices. These devices collect data, present information and services as well as provide the underlying infrastructure over which the home network operates.

The nature of the threat a device poses is dependent upon its functionality, physical implementation, as well as its management model. A key distinction of the Operator's control over a device is influenced primarily by its management model, in particular Consumer Premise Equipment (CPE) vs Consumer Owned and Managed (COAM) devices.

Ultimately the device is the primary entry point into any ecosystem and the most accessible point to the hacker. The securing of these endpoints is pertinent to ensuring the integrity of the ecosystem as a whole.

2.1. Managed Devices (CPE)

Consumer Premise Equipment is the device model most familiar to the MVPD and has been the backbone for most of their history. By providing the customer with their service consumption devices the operator maintains comprehensive control over the device's user experience, but more important to this discussion, the device security.

Operators have been driving new security requirements into these devices over the last several decades and have the ability to adopt new security technologies quickly in response to emerging threats.

In general, when considering the network as a whole, CPE devices present a lower threat risk simply due to the control the Operator has over them. This of course puts the burden on the Operator to implement the security functionality however the only way to have full control is to own the system.

2.2. Unmanaged Devices (COAM)

Unmanaged devices are produced by CE Manufacturers presumably unrelated to the Operator. These devices are produced for general public consumption but due to an intersection of services, the device needs to interact with the Operator's ecosystem in some manner.

The first encounter between unmanaged devices and Operators was the emergence of OTT video. Consumers had a desire for the TV Everywhere experience and as such the market demands the consumption of Operators' video on COAM devices.

The lack of relationship between the Operator and COAM Manufacturer creates an inherent lack of control over the device capabilities and security. In order to get their service on the device, the Operator must create an app which is frequently subject to the Manufacturer's submission rules. Simultaneously, the Operator may have little visibility into the security controls built into the device at manufacture, leaving the Operator at risk to the limitations of the device.

2.3. Operator Influenced COAM (Hybrid)

A third management model is rapidly emerging with Operators, especially with the deployment of IoT based ecosystems. Operator influenced COAM devices fall somewhere in between CPE and independent COAM.

Increasingly Operators are creating business relationships with existing CE Manufacturers. The Manufacturer gets increased volume due to inclusion and promotion within the Operator's offerings, and the Operator gets some level of influence over the device features.

While not as controlled as CPE, this model provides greater control for the Operator, but is still subject to the whims of the Manufacturer's broader roadmap. Due to the appeal of the CE devices to the consumer, this model is becoming increasingly common.

3. Device Security Features and Their Accessibility

MVPDs through their traditional business model of video delivery have come to expect, and indeed have pioneered many device level security features. These features have since made the jump from STBs to common consumer devices.

While security features may be present on a device, access to those features may vary greatly by platform. Frequently these features are only available at the hardware or OS level. This is done by the manufacturer not to reduce 3rd party integration capabilities, but rather to secure their own device ecosystem.

It is in this context that the CPE vs COAM management models make the difference. In a CPE model, security features are fully accessible to Operator integration whereas in the COAM model, the security features may not even be known to the Operator.

Knowledge and access to available security features is critical to building secure home network ecosystems.

3.1. Application Code Signing

Application code signing consists of applying a secure digital signature to a binary software image. Prior to execution, that signature is verified and on success the application is permitted to run.

Code signing is pertinent to verifying that the intended code is running on the device as opposed to rogue software potentially injected by a hacker. This is a key tool to preventing malware attacks on devices. More advanced architectures implement dynamic code signing, where signatures are checked while the application is running. This prevents runtime code injection attacks on the device.

Many COAM devices have code signing implemented, however it is mostly for the system software running on the device. If an operator is integrating at the application level, they will likely not have access to this security functionality.

3.2. Secure Boot

The secure boot is built on the code signing technology previously mentioned. When a secure device boots up, this boot process first performs a signature check of the OS and firmware image prior to boot.

In order for this boot to be truly secure, it must reside within a secure hardware processor, including the asymmetric public key used for code verification. Exposure of this to the software level allows a hacker to circumvent the signing process and potentially inject rogue code. A secure boot is considered to be a bare minimum for developing secure devices in contemporary embedded devices.

The boot processes for COAM and CPE devices are similar, however on CPE devices the Operator has the ability to have their integrated code signed with the system code.

3.3. Secure Micro

The secure micro consists of an area of the device processor that is very tightly protected. Operations within the secure micro are prevented from being exposed at the software level preventing a hacker from access. All cryptographic and keying operations are then performed within this space. A secure micro is a basic requirement in order to implement a secure boot described previously.

White Box Cryptography is a solution that allows the creation of a secure environment in software, but is best used in environments with no or inaccessible secure micro.

This is the main feature of COAM devices that will likely not be accessible to the application developer. The secure micro is frequently used by CE manufacturers to secure their platform, but access to it requires proprietary APIs from the Si manufacturer.

3.4. Hardware Root of Trust and Device Identity

Utilizing the secure micro described previously, a Hardware Root of Trust consists of a unique key or set of keys programmed into the device. This provides the ability to target a unique device with a secure non-tamper identity.

Within any device management ecosystem, device identity is crucial to the system management. By having a secure unique identity, the ecosystem operator can be assured that the devices attaching to the ecosystem truly belong there. Simple device IDs are easily spoof-able by a hacker but with the use of an Authentication Key Exchange (AKE), the identity can be securely identified.

Using this identity, the device can also be uniquely field targeted with firmware or credential upgrades. A payload package encrypted based on the root is uniquely encrypted for that device and cannot be extracted by others.

3.5. Debug Detection

Embedded devices intended to run a known set of firmware and software, frequently have debug detection implemented. Upon attaching a debugger to the device, the firmware can take various evasive actions from reporting it to completely disabling the device. Debug detection is one of the main tools used to keep the hacker out of the device to begin with.

Penetration of the device itself gives the hacker access to the device's data, its operation and potentially to the ecosystem's back end systems.

4. Device Threats and Their Impact

4.1. Data Privacy

As mentioned early on, home networks are made of devices that collect information, present information and potentially take action on that information. The protection of the consumer's data is paramount to protecting a device-based ecosystem. Failure to do so destroys the consumers trust and subsequently that of the ecosystem.

Likely the greatest concern from a customer perspective is that of in home video. The proliferation of video based IoT devices of late, from security cameras to nursery monitors to even the Ring doorbell which is an outside device, provide the hacker with unprecedented access to the household. On a certain level the customer is more violated by a stranger seeing the inside of their home than if their credit card was stolen.

Access to video content provides a distinct physical threat to the consumer in general. This data is easily used for a potential home attack due to the ability to monitor the comings and goings of the resident of the home as well as being able to map out a home and identify items of interest for theft. Monitoring of minors coming and going within the household provides a useful tool for potential predatory behaviour, as a potential predator can easily establish the day to day patterns of the household.

Digital thermostats provide similar data due to their intended usage. When one leaves the home, the thermostat is turned down and then turned back up when coming home. Analysis of this "Big Data" provides a detailed record of the comings and goings of the household.

Encryption technology over the wire is the obvious way to protects content between devices and servers and TLS/SSL technology has become ubiquitous for maintaining these leaks. Failure to do so is considered a Noob development error in contemporary devices.

Protection of data on the device itself is more complicated and requires a layering of the security technologies discussed herein. The implementation of code signing, and a secure boot ensures the integrity of the device itself. Implementation of debug detection prevents hackers from gaining access and encryption of sensitive data on the device prevents access assuming a hacker has gained control of the device.

4.2. Identity Theft

Not dis-similar to data theft, identity theft consists of the acquisition of personally identifiable information (PII) for the purposes of impersonating that individual. PII has historically been very sensitive for Operators due to regulatory controls built around it.

Increasingly personal devices have one or more login credentials which are subject to compromise. Access to any of these can compromise one or more of the many accounts we all have online including financial, social and digital communication. Simultaneously these devices are caching credit card data within them to allow service transaction with a smooth user experience.

Due to our increasingly connected habits, identity theft is on the rise and will likely continue this trend. Media hype around the topic adds awareness to the issues for consumers, but rarely provides them with the tools to actively combat identity theft.

4.3. Access to Backend Services

If a hacker wants to gain access to an ecosystem's backend services, the first place he will target is one of the devices on the ecosystem. By scraping and disassembling the firmware image, the hacker now has an entire blueprint of how the system operates. Any backend API calls within the system will easily be located within the code along with the access credentials required of them.

Once the calls and credentials are obtained, the hacker can now impersonate the device itself gaining access to the backend systems. Clearly the device has controlled access to the backend systems but at this point the hacker begins to look for vulnerabilities within the server software to dig further into the system.

Access at this level may compromise not only one customer's data, but the entire store of the customer base, effectively magnifying the data privacy and identity theft issued described above.

4.4. Device Disablement

ZigBee devices, which are quite prevalent in the low cost IoT space, have been shown to be quite vulnerable to worms and malware. The nature of their AdHoc network allows one ZigBee device, which is under a hackers control, to affect other ZigBee devices connected to it.

While the interference with the actual functionality of a device frequently results in a bad user experience, many attacks have more nefarious goals. Recent ZigBee attacks have been demonstrated to block communications with home door locks, leaving the home unsecured. Clearly this can be leveraged by brick & mortar hackers to gain entry to the home. The use of these devices to control home lighting systems is a low risk implementation, however they must be used with care when designing safety critical solutions.

4.5. DDoS Attacks

The Distributed Denial of Service attack has been gaining increased visibility in the press of late. In this attack, a hacker targets a specific model of device that occurs in large numbers on the Internet. Malware is installed on all of these devices and they are used as a massive cluster to perform a DDoS attack on some web presence.

While this attack may not, and likely will not be on the Operator themselves, the PR from an attack of this nature is bound to be damaging to the corporate brand. Simultaneously, a DDoS is designed to send out continuous packet streams to take down a web presence. If enough devices are on the Operator's network, this could possibly cause network disruptions.

This is a significant threat in COAM devices due to the lack of transparency of the devices. While many of the security solution discussed herein will prevent this type of device compromise, understanding which are implemented within devices is crucial to managing a secure ecosystem.

4.6. Ransomware

Ransomware has also been gaining press of late, but mainly in PC type environments. In this type of attack, a device's software or data is encrypted by a hacker, preventing access to the actual user. A ransom is charged by the hacker to provide a key for unlocking the device.

This type of attack is now gaining more prevalence within embedded devices but occurring at the ecosystem level. Once one device is hacked within the ecosystem, the hacker now has the ability to hack

all of them if they are identical devices. All devices are disabled with rogue firmware upgrades and the entire ecosystem is held hostage.

Attacks of this nature are interesting to hackers as an individual is no longer being extorted but instead a large organization is. This naturally leads to bigger ransoms and a perpetuation of the business model.

4.7. Theft of Service

Operators are in the business of selling digital media services. Theft of these services has been and continues to be a major undercut to the Operator revenue model.

Theft of service frequently focuses around the edge device as this is where the service is delivered and the hacker has access to it. Types of attacks in the category are quite broad but can consist of everything from password sharing to device cloning in the interest of gaining free access.

Again, a multi-layered security approach is key here to hardening the device and preventing the hacker access to it.

5. Conclusions

Herein we've looked at home security specifically from the device level, in particular management models, security features and finally threats to the home ecosystem. With respect to deployment of these systems, there are some key takeaways that one wants to consider during implementation.

5.1. Know Your Devices

In the traditional CPE model, the Operator has a high degree of control and understanding of the devices deployed within the ecosystem. With COAM devices this transparency is reduced, however not eliminated. It's important for the operator to understand these devices and assign levels of trust based on their capabilities. This categorization can vary from CPE, to devices with strong authentication down to unknown devices with a low level of trust. Once these devices are successfully categorized, permission can be granted based on their level of trust.

5.2. Understand Device Security Features

In order to classify devices into trust categories, it's pertinent to understand the security features implemented within a particular device. When the devices are managed by the Operator, this information is readily available however for other COAM devices this may require additional data sources. The OCF provides a device qualification leading to a strong device authentication certification. Certified devices of this type provide a level of trust that can be used for security profiling. Additionally, databases such as Shodan can be utilized for profiling unknown devices. Clearly, this takes more effort than a CPE based model however it is necessary to provide a secure yet open environment where all devices can play safely together.

5.3. Provide Access Based on Trust

Similar to human relationships, with devices we grant access based on the level of trust within the ecosystem. By categorizing these devices based on what we know about their security capabilities, we have the ability to grant access accordingly. Highly trusted devices may be granted access to Operator resources whereas devices with a lower trust level may only get network access and may even be quarantined based on rogue behaviour.

Abbreviations

CPE	Consumer Provisioned Equipment
COAM	Consumer Owned and Managed
MVP	Minimum Viable Product
MVPD	Multichannel Video Programming Distributor
OCF	Open Connectivity Foundation
TVE	TV Everywhere

Bibliography & References

Open Connectivity Foundation (OCF) - https://openconnectivity.org/

Shodan - https://www.shodan.io/

3 Embedded Hardware Security Features Your Smartphone Needs – Joel Snyder, https://insights.samsung.com/2018/06/22/3-embedded-hardware-security-features-your-smartphone-needs/

How hardware-based technology keeps mobile devices secure – Ben Cade, https://gcn.com/Articles/2018/02/13/hardware-based-mobile-security.aspx

The 7 Craziest IoT Device Hacks – Mike O'Malley, https://blog.radware.com/security/2018/05/7-craziest-iot-device-hacks/

5 Infamous IoT Hacks and Vulnerabilities – Isabel Harner, https://www.iotforall.com/infamous-iot-hacks/

