Adapting Proven Technology to Counter IoT Threats

A Technical Paper prepared for SCTE/ISBE by

Petr Peterka
Chief Technology Officer
Verimatrix
6059 Cornerstone Ct. W
San Diego, CA 92121
+1 858-677-7800 x4001
ppeterka@verimatrix.com

Table of Contents

Introduction

The Internet of Things (IoT) is emerging fast from hype to reality across homes, enterprises, cities and infrastructures, creating massive opportunities in multiple sectors. But inevitably, given the associated proliferation in IP connected objects and services, it generates new security threats at different levels from minor nuisances to major national security threats. This has created a view that radically different technologies and strategies are needed to counter threats in this new security landscape. Verimatrix challenges this notion by arguing that although some of the threats may appear novel, they involve many techniques around theft of credentials and denial of service that are already well known. As a result, existing technology well proven in other spheres, especially pay TV revenue protection, can be adapted to counter these threats. While new threats are of course arising all the time and require constant vigilance on the part of security providers to counter, the required innovation is already taking place. Security firms such as Verimatrix are investing in AI, Machine Learning and other advanced techniques designed to provide early warning of emerging attacks so that they can be anticipated in advance, or at worst, countered as they unfold before significant damage has been done. Above all, the key to protecting the IoT lies in renewable security which is essential to stay ahead in the arms race against hackers and pirates.

Not Radically New Technology

1. Education Needed for Secure IoT

1.1. IoT Security Falling Behind Expansion

The IoT is expanding so quickly that security is lagging behind, both in deployment and understanding of the risks. There have already been some high-profile attacks, as well as demonstrations of vulnerabilities by security professionals that are potentially even more serious. Such attacks or demonstrations have varied in seriousness, from causing a nuisance or minor economic damage, to major threats to national security, as in the case of the now infamous hack of the Ukrainian power grid[i].

Even when vulnerabilities are unearthed by security researchers, the “good guys,” it can prove costly for the manufacturers or service providers involved. This was the case for Chrysler when forced to recall 1.4 million Cherokee Jeeps[ii] after they were hacked in 2015 by two researchers demonstrating a complete remote takeover of the vehicles’ digital control systems. Such cases emphasize problems caused by lack of attention to security during design and development of core IoT components or subsystems, or even the whole infrastructure.

1.2. Public Awareness of Threats Growing

Even the general public has become aware of the threats posed by the growing connectivity between objects, including their cars and devices in their own homes. This has been brought on by several well publicized cases, some of which have implications for personal safety or privacy.

Although many of these cases have involved demonstrations rather than actual hacks, experience tells us that where vulnerabilities exist it is only a matter of time before they get exploited. The potential to cause injury or even death by taking over connected cars has already been demonstrated. On the privacy front, one of the most infamous cases involved toy internet-connected stuffed animals manufactured by

CloudPets, which were hacked[iii] in February 2017, exposing personal information of over 800,000 customers to eavesdropping.

Such cases highlight the need to educate the public clearly over the risks and often relatively straightforward measures that can be taken to guard against these threats. At the same time, there is a need for guidance over where responsibilities lie for DDoS or other large-scale attacks launched by recruiting botnets comprising domestic IoT devices.

1.3. Key Players Often Lack Understanding of Threats and Impact on Value Chain

Although there may be growing awareness of IoT security risks in principle, even providers of core components and services often fail to understand the full ramifications. Just as a joined up IoT opens new horizons for adding value and creating new business opportunities, so it also expands the threat landscape. While key players may have a good grasp of security threats to their own products or service domain, they may not appreciate implications for other IoT domains to which they are now connected. A manufacturer of smart talking dolls might address possible risks to children posed by malfunctions but fail to appreciate that a burglar might take it over to instruct a voice-controlled personal assistant such as Amazon's Alexa to open the front door. The main point then is to consider that the joined up connected nature of the IoT presents opportunities for many sorts of wrong doing across multiple domains. This needs to be communicated in particular to relevant IT departments so that the security nuances of the IoT can be taken into full account during software development. Providers of both components and services also need to be brought on board, given that a major factor making the IoT such an attractive target for hackers is that many devices are shipped with insecure defaults and exploitable code. Furthermore, they are rarely upgraded, usually lacking the capability.

1.4. False Perception that IoT Requires Security Revolution

It might seem natural to assume that because the IoT is a new era for telematics, opening up new vistas for existing and emerging players, it must also require radically new security technologies to counter threats that will arise in this different landscape. This is a serious misapprehension because although the IoT does undoubtedly introduce new contexts and modes of transmission, as well as greatly increased scale and opportunity for attack, the underlying methods are fundamentally the same. These include theft of content, hijacking multiple devices to launch DDoS attacks and injection of malware to disrupt activities, eavesdrop data or launch ransomware attacks.

1.5. Proven Methods Can Be Adapted to Counter Many IoT Threats

Although the consequences have the potential to be felt more widely, the IoT has thus far elicited threats that have been similar to previous attacks to the traditional IT infrastructure. This means that methods and technologies already developed in other spheres, including those that have protected of billions of dollars of revenue in the pay TV industry, can be adapted for the IoT and are already being deployed by Verimatrix and others. The great advantage is that such methods are already mature and well proven so that IoT service providers can deploy them with the confidence that they will work in their environment, provided they have been properly adapted. Section 5 explores how pay TV encryption and key management, authentication, entitlement management and other established processes can be adapted for the IoT.

1.6. Some New Tools Needed but Already Under Development

It is true that some new tools and techniques will be needed to counter emerging threats, but again, these are not unique to the IoT. Just about all telematics sectors face the common challenge of having to monitor for threats, some of which cannot be anticipated in advance, and be able to deal with them as they arise. Section 4 describes how Verimatrix designed its approach to counter threats based on four pillars of IoT security, with a fundamental requirement being that it can be renewed as required, not just to keep pace with the evolving threat landscape, but to stay one step ahead where possible.

1.7. Revenue Protection Vendors Well Placed

Given their experience combating piracy, content theft and various forms of attack, revenue protection providers are already armed with many of the tools and technologies needed to protect the IoT. They have long-standing experience securing the IP set-top box (STB), which was an early example of an Internet-connected thing, and more recently have had to adapt to online content distribution. This has required the extension of protection against content and service theft to many other connected devices, including tablets, smartphones, gaming consoles and cast dongles. Upgradeability has become essential for pay TV security, so providers in that field have become skilled not just at keeping their own software up to date through transmission of regular updates, but also other critical third-party components that can be vulnerable to attack if the latest fixes have not been applied.

IoT Threats

2. Four Threat Levels

2.1. Level 1: Nuisance

There are significant variations in impact even within the category of threats that might be defined just as a nuisance because there is no injury, loss of life or disruption on a large scale. It includes attacks on IoT components such as domestic refrigerators, with potential to cause upset and economic loss to individuals. It also includes threats to confidentiality and personal data which, while not causing physical harm, can still lead to significant distress in the event of identity theft, for example. The scope for such low-level threats will increase as the IoT becomes more inter-connected across domains, which is another reason for taking this category seriously.

At the same time, the IoT is attracting new forms of malware designed specifically to exploit the lack of security to cause malfunctions or deny service. A new malware strain called BrickerBot was detected in March 2017iv, targeting IoT devices by corrupting their storage capability and reconfiguring kernel parameters. This can result in permanent denial of service (PDS) since the devices can be crippled to the point they either need replacing or factory restoration.

2.2. Level 2: Threats to Business and Brand

Attacks on businesses have become more common and larger scale as a result of IoT proliferation. This has increased the scale of DDoS attacks and also made them easier to mount by presenting large numbers of unsecured connected devices. This is a particular threat to smaller enterprises for which the economic or reputational damage could be terminal. The DDoS attack on the news site KrebsOnSecurity[v] was such

a case where large numbers of routers and surveillance cameras were recruited, although fortunately that was thwarted by prompt action from CDN vendor Akamai.

Apart from DDoS, the IoT also gives greater scope for malware attacks against businesses, which can be motivated by an individual grudge and are increasingly common for extortion. Ransomware attacks have been encouraged by some large payouts made by firms desperate to restore critical systems in the event they fail to recover compromised systems. South Koran Web host Nayana admitted paying just over $1 million in Bitcoin[vi] after being unable to recover data stored on 153 Linux servers and 3,400 customer websites when it had been maliciously encrypted by ransomware attack.

This category overlaps with level 4 because many large-scale attacks, including both DDoS and malware, target multiple companies as well as national infrastructure. The widespread attacks in late June 2017 involving the Petya ransomware[vii] afflicted both infrastructure and individual enterprises, with victims including the world's largest advertising agency WPP.

2.3. Level 3: Threats to Life or Limb

The third threat level embraces incidents threatening personal injury or death, rather than an enterprise or infrastructure. The connected car is the most obvious target under this category given there are now 112 million vehicles around the world with direct access to the internet, set to more than double by 2025 according to Gartner. There have been no proven attacks against connected cars that have caused injury, but the risks have been demonstrated by researchers under realistic conditions. This has exposed scope not just for targeting individual cars to disable say a braking system, but also for remote commandeering of a large number of vehicles. As fully autonomous driving comes closer, potential for causing serious accidents by taking over a vehicle's electronic control unit (ECU) will increase.

Cars will also be just as susceptible as other IP-connected systems to ransomware from attackers seeking to exploit vulnerabilities in ECUs themselves or infotainment systems to obtain money from the owners. In anticipation of such threats, several industry initiatives have sprung up reaching towards a coordinated approach to IoT security, such as the Automotive Security Review Board (ASRB) launched by Intel, alongside Aeris and Uber, in October 2015. This has staged several workshops in which engineers, cryptographers and security researchers from around the world are collaborating on an Intel and Linux-based in-vehicle infotainment (IVI) simulation platform.

Robotics is another obvious sector where there is potential for causing serious harm through malicious takeover and this field is growing just as fast as the connected car. While the growth is mostly concentrated in the enterprise and particularly manufacturing sector at present, robots are set to enter the domestic realm on a significant scale within the next few years. They too will be IP connected, over Wi-Fi or cellular networks, with optimism over their utility being tempered by fears over security. A recent report[viii] found that robots were just as prone to hacking as other connected systems and noted that there had already been instances of injury and in one or two cases death caused by malfunctions that also demonstrated the scope for malicious damage.

2.4. Level 4: Threats to National Security and Critical Infrastructure

Threats under this category have naturally aroused greatest concern among governments and security agencies. This partly reflects the great potential scale of disruption but also the fact that several major attacks have already occurred. One positive aspect is that these attacks have galvanized coordinated

responses around the world and ensured that from now on, IoT security will be taken much more seriously by makers of components and providers of services, as well as infrastructure companies.

Just as for Level 2, these large-scale attacks can involve DDoS or various forms of malware, which as we have seen are now being tuned specifically to exploit IoT vulnerabilities. The first large botnets recruited for DDoS attacks involved coopting consumer broadband routers but have come to include surveillance cameras, webcams, digital video recorders, cable TV or other connected set top boxes and, most recently, new types of consumer IoT devices. The threat to critical infrastructure was demonstrated by the DDoS attack on US DNS service provider Dyn[ix] in October 2016.

Even greater concern caused by malware and DDoS occurred two months later when the Ukrainian national power grid was subject to its second coordinated attack within a year, leading to a widespread two-hour blackout. The attack, orchestrated by multiple groups working together, was more sophisticated than the first known power outage that happened a year prior and resulted in a blackout for 225,000 households in the capital city Kiev. The event wasn't intended to cause serious damage, but it did serve as a training lesson for future attacks.

Architectural View

3. Three Alternative Architectures

The IoT as a whole covers a huge variety of infrastructures, services, use cases and devices, so it is not surprising that there is a not just one underlying design architecture. Three alternatives have emerged, the first being the case of IoT devices connected to the wide area infrastructure, or cloud, via some form of intelligent gateway/hub. The second option, sometimes considered a variant on the first, still involves an intermediate unit between end devices and the cloud, but in this case, it is dumb and confined largely to aggregation, routing and protocol conversion. The third option is for devices to be connected directly to the cloud so that they participate as end points in an IP network overlaying local radio protocols. The three options are suited to different situations and vary in the security risks they pose. There is no one-size-fits-all approach to IoT security.

3.1. Device to Gateway to Cloud

Under this model, a centralized hub or gateway sits between the IoT devices and the associated service resident in the cloud. These can be regarded as network edge devices converting between local radio protocols on the client side and IP broadband into the cloud where the service is hosted. The gateway should also provide a connectivity layer locally above the radio protocols, enabling devices to interoperate irrespective of which protocol they support. This makes the service seamless, giving freedom to install devices whatever low power IoT radio protocol they support, whether ZigBee, ZWave, Bluetooth, Wi-Fi HaLow or other.

The gateways may also be capable of running applications to perform local actions that may involve coordination between different IoT devices, but which do not need reference to the cloud. Gateways will play a useful function in partitioning IoT services, filtering data, analytics processes and applications to avoid overloading the host in the cloud.

On the security side, the gateway will, to some extent, insulate devices from the cloud and protect the links on that side. It will also play a role preventing rogue devices from disrupting the wider service, with

the ability to shut them down. Crucially though, the gateway cannot provide end-to-end security by dint of its physical and logical position in the hierarchy. Its position as a gatekeeper with processing capability could make the gateway itself a target of attack itself from the cloud. Indeed, by being an edge device between the internet and the local wireless domain the gateway is a logical point of entry for any threat vector. Therefore, the service may require overlying security above the gateway to ensure end-to-end security at the application level.

3.2. Device to Bridge to Cloud

This model still imposes a form of gateway between devices and the cloud but here it is dumb and so best defined as a bridge, which will be confined largely to protocol conversion and aggregation. This model has emerged for situations in which local intelligence is not required, but when there is a need for operation at longer range than in a typical home. As with the device-to-gateway-to-cloud model described in 3.2 this connects devices by short range radio to an IP end point of the cloud, in this case a dumb bridge. The function of the bridge is to translate protocols that are low bit rate but often longer range than say ZigBee to a higher capacity wide area network. A typical scenario could be in agriculture in which multiple sensors may send data on environmental variables such as temperature or humidity intermittently to a dumb bridge or aggregator up to a few miles away, which, in turn, would forward these into the cloud for processing.

Protocols suited to this model include low-power wide-area network (LPWAN), which in turn is based on the LoRa chirp spread spectrum (CSS) radio modulation technology, optimized for very low power and bit rate but intermediate range.

This bridge model has also been proposed for some forms of home and factory automation using another protocol, 6LoWPAN designed specifically for IPv6 over Low Power Wireless Personal Area Networks. This, in turn, underpins the Thread protocol designed primarily for the home which may become more prominent with ongoing roll out of IPv6 replacing the original IPv4 which has address space that is all but exhausted. The argument here is that IPv6 also brings other benefits, including auto-configuration and end-to-end routing, which eliminate the need for an intelligent gateway. This makes it possible to implement a distributed approach based on dumb bridge devices just performing low level protocol conversion within the home.

E-health is another possible use case for the bridge model when mobile monitoring devices may connect to the service via the user's smartphone. In this case, the smartphone would act as a bridge between diagnostic sensors and the cloud-based center where data would be stored, monitored and analyzed. E-health is also a candidate for the full gateway model residing on a more powerful laptop or tablet, which would then perform the data preprocessing and even potentially diagnosis in less critical cases. Security of the data to ensure confidentiality would of course be critical, calling for full end-to-end tunneling, possibly using the HTTPS (secure protocol) between each sensor and the cloud server through the bridge or gateway.

3.3. Device to Cloud

There will be many instances when the best model will cut out an intermediate gateway and connect IoT devices directly to the cloud. This could be the case for services for which devices are not contained within the range of a static gateway, as in the connected car or container monitoring. In the case of the connected car, there will be some form of gateway, protocol converter or aggregator within the vehicle;

however, this could be treated as an IoT end point from the service perspective, usually communicating over cellular networks.

This model will also be favored for some IoT services within homes or enterprise premises where the direct communication with the cloud could will be via narrowband IoT (NB-IoT). This has been designed primarily for indoor coverage as part of the 3GPP suite of protocols within the LTE spectrum and is capable of running an IP protocol stack. It allows mobile network operators (MNOs) to allocate some of their existing spectrum to these IoT applications.

A key point about this model is that it runs the full IP protocol set end to end. This makes end-to-end security more straightforward to deploy. The service can exploit the security and privacy features already provided by the mobile network, including user confidentiality, device authentication and data integrity.

3.4. Pros and Cons of Three Models

The three models have evolved to suit different IoT services or use cases in terms of mobility, device capability and requirement for local computation or data analysis. Security has not really been considered and must adapt to the architecture as well as the varying levels and nature of the threats.

3.4.1. Intelligent Gateway

The intelligent gateway approach has an obvious advantage where there is a need for local decision making and processing of data that could overwhelm both the network and centralized resources if offloaded to the cloud. Such a dedicated IoT gateway can provide extra storage and processing services, allowing the end nodes to be as power efficient and cost-effective as possible. The gateway can also participate in link level security within the local IoT domain.

On the downside, there is uncertainty over optimal design of the gateway, which if dedicated could become an obstacle to rapid IoT innovation, just as legacy STBs can be in pay TV. The gateway can also be a single point of failure, as has already become apparent to users of smartwatches and wearable fitness or health monitors that are paired with the user's smartphone and cannot communicate when that is unavailable. For that reason, various architectures that allow devices to pair with any smartphone or other mobile connected device within range have been proposed, but these bring obvious security concerns, especially for domain services such as E-health where data confidentiality is critical. Dedicated gateways also present targets for attack, by virtue of their computational resources, which can be vulnerable to physical tampering, extraction of private keys, spoofing and even "man in the middle attacks." These can all be countered through strong end-to-end security but deter some service providers from this model.

3.4.2. "Dumb" Gateway

The bridge or "dumb gateway" model lends itself more to sensor networks where little more than polling and aggregated data collection are required. It may also be applicable for IoT in the home for monitoring domestic appliances such as freezers, fridges, toasters, kettles and water meters as communication may be intermittent and the level of processing required is small enough to be handled in the device itself or the cloud.

One advantage is that a simple bridge is less of a hostage to fortune than a dedicated gateway, which is partly why hybrid models recruiting smartphones, tablets and other mobile devices as intelligent hubs have been proposed. Such hybrid models can score by providing the processing required for edge

computing as is enabled by the dedicated gateway model, while avoiding single points of failure or reliance on a static device that may not scale well or adapt to future IoT services. The dumb gateway model fails to provide the local intelligence and data filtering that will be essential for many IoT scenarios.

3.4.3. Device-to-Cloud

The direct device-to-cloud model offers the big advantage of running a full IP protocol stack end to end, avoiding need for protocol translation and bringing a richer set of tools at the network level. End-to-end application level security can be deployed readily on top of the stack with less concern over vulnerabilities associated with intermediate gateways. This approach is well suited to applications for which roaming is required without a need for local intelligence beyond the end device itself. It is also applicable to a range of applications that can be served by suitable protocols that work within the mobile spectrum, such as NB-IoT.

Technology View

4. Four Pillars

IoT security should be built around four pillars that cover all aspects and components of IoT services, including devices, data, the service and the network infrastructure. The pillars do not define particular threats because these are constantly evolving and cannot be countered by any specific measures. The point is that the four pillars provide a flexible framework that can be expanded and renewed in the field to keep up with the evolving IoT security landscape and be ready to counter new threats as they emerge. These pillars have not come out of thin air and have their roots in well proven security in pay TV and other sectors. This section examines how each of the pillars maps onto recognized security practices, including the CIA Triad (confidentiality, integrity and availability), not to be confused with the U.S. Central Intelligence Agency sharing the same acronym. Another widely recognized and now venerable model is the IEEE AAA, for authentication, authorization and accounting.

4.1. Device Integrity

The first pillar of IoT security ensures that devices and the software they are executing have not been compromised by any means at any stage in their lifecycle. This corresponds closely with the “I” of the CIA Triad detecting attempts to hijack the device in some way and preventing pirates from succeeding. It requires firstly ensuring integrity of the bootstrap process by which devices or their users obtain key material and configuration information, among other parameters, to allow them to be authenticated for operation within an IoT domain.

Secondly, integrity of the updating process must be assured to avoid devices being subsequently compromised during operation. It is Verimatrix’s contention that integrity of both bootstrap and update can be safeguarded by existing proven mechanisms.

4.2. Device Authentication

The second pillar is essential to protect the wider IoT network or service from intrusion by unauthorized clients or users. This requires assurance that only devices explicitly or directly identifiable are allowed to join a given IoT network. That, in turn, prevents entry of spurious data into the IoT collection network or

access to systems requiring authorization. This can be achieved by embedding unique authentication keys into protected areas of a chip. However, simple cryptographic solutions will be needed for small IoT devices such as sensors that operate at low energy with minimal computational capabilities.

On the other hand, some IoT devices will be operated by users, in which case authentication may be better associated with the individual concerned, who may have multiple clients accessing a given IoT network. In such situations, there is growing interest in the concept of virtual device authentication with ideas such as transferrable credentials like virtual car keys that can be carried around on mobile phones. The underlying point is that IoT device authentication is important but requires a flexible approach to take account of the highly diverse hardware and use cases involved. It maps naturally to the first A of the IEEE AAA, but goes further than what was envisioned at the time that model was developed to cater for the vast uncharted scope of the IoT. Device integrity and authentication, as well as integrity of communication, contribute to DDoS attack prevention and thus to availability of the overall service.

4.3. Integrity of Communications

Integrity of the communications between devices and the IoT network or hub is the third pillar of security and protects data from interception or alteration during transit. Rather than physically protecting a link, this involves the creation of secure tunnels to avoid eavesdropping or corruption of data. This should also prevent spoofing through falsification of data to masquerade as an authorized device or user.

Since the secure tunnel is enforced by encryption, communications integrity clearly relies on the first two pillars, device integrity and authentication, as well as security within the cloud hosting an IoT service, to be sure that it really does offer end-to-end protection of an IoT data path.

This pillar derives directly from the “C” of the CIA Triad for confidentiality, achieved by encryption, and can be built from proven technologies in pay TV for which integrity is essential to prevent theft of video assets during transmission. In fact, communications integrity and confidentiality have become even more critical for video service providers as they expand into analytics and rely on sensitive customer data for decisions relating to quality of service. As a result, they depend increasingly on their customers’ trust to obtain personal information and this is also becoming a requirement for many IoT-related services.

4.4. Security of Data

Security of the data collected by a connected device is the fourth pillar of IoT security. Similar to the third pillar, the objective is to protect against the corruption or faking of data, along with other possible malfeasances. The difference is that the focus is on the whole data lifecycle rather than just transmission. At this level, policy rules and privacy regulations should be enforced since they are intimately bound up with the data being collected. This pillar relies on the other three to protect against threats to data posed by rogue devices or events during transmission.

This relates to the C of the CIA Triad and also to the “accounting” component of the IEEE AAA because both of these rely on end-to-end security of the data. If the data is compromised at any stage, there can be no guarantee of confidentiality and the veracity of information to generate billing is uncertain.

4.5. Pillars to Extend Entitlement Management

Entitlement management is one vital aspect of security that builds on the four pillars and is applicable in most security domains, including pay TV where it evolved in the context of digital rights management

(DRM,) as well as many parts of the IoT spectrum. It equates to the "authorization" component of the IEEE AAA model by defining precisely what end devices are allowed to do through access control lists.

In the pay TV context, it could mean determining which channels a particular user can watch on a particular device, or which on-demand content can be accessed. The IoT is moving towards a similar model because it is becoming clear that devices on the network cannot generally be trusted and therefore must be restricted in their wider capability. In pay TV, this separation between local and remote access has long been executed in the context of the STB. Users are allowed to view channel guides for example but only the pay TV operator can change that guide's contents.

Similarly, in the IoT, a surveillance camera can be configured to only be accessed remotely by designated members of the household or, perhaps, to grant temporary access to the fire department during cases of emergency and then revoke that access immediately thereafter. In the case of systems that have potential for serious harm in the event of malicious intervention or takeover, as in the case of autonomous cars or domestic robots, restrictions could be imposed on the actions taken. Cars could be prevented from taking actions that would risk injury to all parties, including occupants of other vehicles and pedestrians. Ramifications of this are discussed further in Section 5.5.

4.6. Renewability and Upgradeability Critical to Counter Emerging Threats

The ability to renew security remotely and almost transparently to the user has become well established across multiple telematics domains, including enterprise data centers, personal computing and pay TV. It is just as essential for the IoT, where clearly security must keep pace with evolving threats without requiring devices such as sensors or light bulbs to be returned to base for upgrades. This raises some new challenges given the very limited processing and storage resources available in many IoT devices and involves matching the renewability process to the use case. Remote environmental sensors do not pose the same threat as connected cars and so obviously do not require the same level of security. In that case, it may be sufficient to keep the aggregating bridge or gateway up to date on their behalf with the focus on the integrity of the data. For most use cases though, it will be imperative that security of end devices can be renewed directly, including electric domestic appliances that can be switched on or off with potentially adverse consequences, at the very least unnecessary consumption of power.

Renewability has played a fundamental role in the arms race against piracy in pay TV since the dawn of digital transmission with the focus on protection of the STB. With IP connectivity, scope for upgradeability has increased, with the aim of ensuring that pirates cannot get at the video content directly by first circumventing the box in which decoding occurred.

Such measures begin with secure boot and other techniques to make sure that when the system starts up, it is loading known authenticated software and not some malware or Trojan invading from the internet. Revenue protection vendors have developed technology for updating the software securely during operation.

Such techniques have also been deployed on PCs and have been carried across to connected devices for secure video delivery. Meanwhile, these techniques have been extended to cater for the fact that these connected devices, unlike STBs, do not have security components like DRM and now watermarking pre-integrated in the factory because they are not built for a single pay TV service. This has been addressed with the help of device makers and their system-on-chip (SoC) providers by deploying trusted execution environments (TEEs), enabling more vulnerable aspects of a pay TV service to be isolated from the underlying operating system and therefore from the apps running on top.

It is becoming possible to replicate the secure software updating, long available for the STB, on mobile devices such as smartphones, via standards for TEEs such as the GlobalPlatform TEE management framework (TMF) and the open trust protocol (OTrP.)

4.7. Extending Connected Security and Renewability to Lower Power IoT Devices

By itself TEE technology does not address the problem of protecting many IoT services because it requires significant processing power not available in small devices like sensors. Such devices will tend to run on small embedded chips like ARM Cortex M cores rather than, for example, the powerful quad-core processors found in many smartphones.

To bridge this gap in processing and storage capability, the OTrP was formed in July 2016. OTrP is really more than a protocol since it extends the security techniques already proven on smartphones and tablets to IoT devices, incorporating the same sort of trusted code management. Verimatrix supports OTrP and believes it provides the foundation for extension of code isolation and secure update to low power and resource-limited devices.

Although this still leaves important issues to resolve, these concern consumer awareness, assigning responsibility for breaches and financing of IoT security in general, rather than the underlying technology. The key point here is that the work now being conducted around the OTrP is leading towards a framework in which IoT can be shielded by the same protection as pay TV services for which there is also a need to satisfy third parties over security, in that case rights holders. Indeed, it is because the experience of pay TV security transfers naturally to IoT that Verimatrix has identified this as an important sector for its technology in years to come.

4.8. Security Options for IoT Protocols

Most IoT services will require end-to-end security at the application level to ensure there are no points of weakness. It is true that many of the components of a given IoT service will have some level of security built in, but this cannot be relied on to provide comprehensive end-to-end protection against all possible threats.

There is also security embedded in some of the IoT wireless protocols themselves, which can play a useful role in protecting the link between components and bridges or gateways as part of the overall solution.

Mapping Pay TV Security to IoT Threats

5. Adaptation of Existing Methods to IoT

The thesis of this paper is that new security challenges for telematics as a whole are often just old ones exploiting different vulnerabilities that arise in given domains. It is true the IoT does introduce some novel threats and uncertainty where the future security landscape looks highly unpredictable. But when the threats are peeled down to reveal the points of vulnerability that allowed them to arise as well as the attack vectors used, they are remarkably similar to those already experienced in the pay TV world, especially more recently as video services have embraced web and IP delivery. So although the future of IoT threats is unpredictable, that holds equally for other domains including pay TV. Indeed, it is precisely

because the future landscape is uncertain that renewable security has been developed firstly for the STB and then other connected devices for viewing video services.

As a result, methods developed for pay TV revenue and service protection can readily be adapted to the IoT. This section explains how the principle threat categories in pay TV map onto the IoT and can be met by adapting proven methods.

5.1. Encryption and Key Management

Encryption and key management have a vital part to play in many IoT domains, with the common theme being protecting data, whether from eavesdropping, deletion, theft or tampering. Data can be of different types, comprising valuable content as in video services, measurements as in environmental monitoring, or control of critical functions as in robotics as well as many other domains. On the surface, threats may look different and yet all involve similar techniques for attacking data beneath the bonnet.

In pay TV, encryption and key management are absolutely essential for protecting valuable video assets against piracy or theft of service, while in the IoT, the focus may be on protecting data during transit, whether from end devices to gateways or within the cloud. There may be a privacy aspect, as in medical applications where a user would not want an unauthorized third-party access to data about personal health, for example. There will also be safety considerations in the eHealth sector, given the potential to take over remote control of pacemakers, insulin pumps and internal units designed to administer a drug at a controlled level.

Another big and fast-growing area common to many sectors is big data analytics, harnessing information from multiple sources, some of which is confidential. Exploiting such data relies on building trust with consumers, whether in pay TV for serving recommendations, or domestic appliance monitoring to gain valuable information about usage. In all such cases, encryption and key management can protect data against interception and unauthorized access.

In pay TV, revenue security vendors are uniquely placed not just to protect analytics data but also obtain it by virtue of their privileged position as custodians of the service. Similarly in the IoT arena, they will be able to assist service providers in this dual role of data protectors and generators.

5.2. Authentication and Protection of Software Integrity

Many attacks on IT systems and more recently IoT devices have involved infiltration with viruses or malware that cause alien functions to be executed that are very different from those for which the system was designed. This has been the cause of most incidents to date involving the IoT, primarily DDoS attacks resulting from recruitment of Botnets in this way. Such attacks are not new, but the IoT, by making unprecedented numbers of devices available, is increasing their scale and potential for disruption greatly. The IoT enables much greater data volumes to be focused against individual targets with the ability to cripple even the web sites of major enterprises for up to several hours in some cases before the attacks are defused.

Techniques already widely deployed, including secure boot, download and upgrade, ensure that sources and software integrity are verified before any execution is allowed. In such a controlled environment, it should be difficult to install any unauthorized software on the devices and therefore hard for viruses or malware to come in and cause chaos.

5.3. Protection Against Cloning Attacks

Cloning attacks are common to pay TV and the IoT, while having different motivations. In pay TV, cloning emerged soon after the introduction of smart cards as the device holding the user's credentials for decrypting authorized content in the STB. By creating a clone that looks like it belongs to a paid subscriber, it was possible to access channels free of charge.

In the IoT world, cloning might have different motives, to mimic a device that enables certain actions to be performed or to give a service the false impression that it is operating normally to disguise malicious actions. A lot of attention has already been paid to cloning of radio frequency identification (RFID) devices widely used for inventory control, object tracking during transportation and security badges for employees to enter work premises. This has brought obvious risks of unauthorized access to buildings as well as theft of valuable items in transit by cloning relevant RFID tags. As a result, various schemes have been proposed to identify and counter RFID cloning.

However, RFID only supports one-way wireless communications and a greater concern for the IoT might be the cloning of systems which support near-field communication (NFC.) This operates at a shorter range than RFID at distances up to just 4 inches but with two-way communications.

It is possible that NFC will become a major medium for configuring IoT devices via smartphones, given that these are already internet-connected and have security built in. By tapping a device, a smartphone could automatically configure a new IoT device via NFC and admit it to the service.

Many applications will require somewhat longer range than NFC but still local communications, such as virtual keys for opening cars and possibly gaining access to buildings as well. This may well use Bluetooth Low Energy for the exchange of credentials, which makes that a possible target for cloning attacks to steal a car for example. There are tools readily available on the web that claim to enable such attacks.

However, such attacks can be countered by methods already well deployed in pay TV where this has been an issue for two decades.

5.4. Extending Entitlement Management to Pay TV

Even when devices have been verified and checks have been made to ensure they are not running any malicious software, it is still possible for them to perform unexpected actions as a result of direct physical access, malfunction or misconfiguration. That is where entitlement management comes in by defining exactly what each device can and cannot do. In pay TV, entitlement management has long been deployed for DRM to restrict access to given channels, often since device, location and time of day. It can also control actions such as storing a piece of content on a personal video recorder (PVR).

Entitlement management can be carried across to the IoT for a wide range of functions, some relatively trivial but still important like ensuring that your own light bulbs but not your neighbor's are connected to your network. It can also bear down on DDoS and other attacks by applying business rules to data flows to and from devices. For example, it can ensure CCTV data is just transmitted to local DVR or cloud video storage and avoid it being sent to unknown web sites. It can also discriminate between devices according to their security capability. It may be that some devices have the full-blown protection of a TEE while others with less computational resource just have an embedded key. In that case, the former device

may be allowed to access external services while the latter is confined to communications within the local IoT domain.

6. What New Technology is Needed

6.1. IoT Increases Uncertainty

As previously distinct and isolated IoT domains become connected, well-defined security boundaries will break down, making it even harder than before to predict how threats will emerge. A threat that might appear to be confined to one domain can affect others. The case of the smart toys discussed in Section 1.2 demonstrated how an IoT device could have unintended consequences by threatening privacy—something the developers probably had not envisaged.

Such cross-domain security risks will extend well beyond privacy and become almost impossible to spot in advance. They have already been quite widely discussed in the context of voice-driven personal assistants like Amazon's Alexa and Apple's Siri as they increasingly interact with various IoT domains, including home environmental control and indeed security for operating doors and windows. The prospect of malicious takeover of such assistants to wreak mischief or even perpetrate a crime such as a break in is no longer just speculation but presents real threats that can be demonstrated.

6.2. IoT Security Must Be Proactive and Adaptive

Given this unpredictability, IoT security needs two qualities—renewability and intelligence. The role of renewability in upgrading security to address emerging threats was discussed in Section 4.6, but on its own, it is not sufficient because in some cases the damage will already have been done. It is essential that attacks can be anticipated as they unfold through recognition of associated unusual patterns of activity. This is particularly vital in attacks exploiting unexpected vulnerabilities that have not been covered, when it may be necessary to take some emergency action like temporarily shutting down a particular server or segment of a network.

Machine learning and AI come in by providing the capability to recognize and respond intelligently to unusual patterns. These have already been deployed in pay TV and again can be adapted for the IoT in different contexts. For example, a water meter registering a sudden massive increase in consumption might indicate a leak or a hack. Application of AI might help distinguish between the two by analyzing the precise pattern of consumption data.

6.3. Need for IoT Device Birth Certificate

Apart from cross domain threats, another unintended consequence of the IoT could arise when devices are redeployed or relocated, or even when there is a change in homeownership. In such cases, an IoT device could end up under new ownership, and if it has not undergone a proper factor reset, there is the possibility of unauthorized access to personal or confidential information. In the absence of a full inventory of all IoT devices ever built, which is unlikely to happen, there is a need for some form of birth certificate associated with each to track its lifetime history. This would identify where the device was manufactured and certified, as well as which service providers deployed it during its lifetime and with which customers.

The blockchain system has been suggested as a possible solution given its increasingly wide deployment. Although designed to secure financial transactions and most closely associated with the internet Bitcoin

currency, its operation as a distributed peer-to-peer ledger resistant to data modification makes it ideal for inventory management and for logging the life history of IoT devices.

In fact, these same properties look likely to involve blockchain in many IoT services that require tracking and traceability either of transactions or objects. Real-time tracking to monitor equipment in the field or packages in transit can be implemented over a distributed blockchain network, allied to public key infrastructure (PKI) to facilitate secure information transfer between components. This will enable a range of new applications, some of which are already being trialed.

Blockchain can combine security with distributed operation and time stamping, which will enable the traceability essential for many IoT sectors, including the lifecycle management of devices themselves.

6.4. Responding to Successful Attacks

One golden rule of security is that it cannot succeed in blocking all attacks because there will always be some new or undiscovered points of weakness that can be exploited. Inevitably, there will be some attacks that get through all perimeter defenses and the measure of a good security system lies in how well it can cope with these and minimize damage.

Pay TV revenue protection specialists such as Verimatrix are already deploying machine learning and AI to protect customers' video services and are extending these to the IoT both for proactive monitoring and post-attack response. For example, machine learning can be applied to detect unusual patterns that indicate a potential hack. A well-trained machine learning model should be able to identify connections or nodes where unusual activity or data traffic patterns are occurring and shut those down, while leaving others open so as to minimize overall impact on a service. While at present, machine learning in cyber security is often confined to providing warnings upon which human analysts then act, in time they will take over more and more of the ultimate decision making. This is important for the IoT whose proliferation will expose even more the shortage of skilled human security analysts, as well as the lack of time available to make decisions. In the end, a machine can process information and act much faster than a human, provided it has acquired the contextual intelligence.

Indeed, as monitoring becomes more sophisticated, it will be more likely to pick up attacks early or even sniff them out before they occur. The potential for this was demonstrated by the case of the Cherokee Jeeps hack discussed in Section 1.1. The two security researchers pointed out it had taken months of trial and error before they succeeded in taking over the vehicles. This would have left traces detectable by an intelligent monitoring system.

Conclusion

Two key take home messages can be extracted from this paper.

1) When the application and service specific aspects of the IoT are stripped down, the same fundamental threats and attack vectors common to many telematics domains are revealed, including enterprise data centers and pay TV services. These threats can be countered by security tools and services that are already mature and well proven in these sectors (e.g. secure boot and upgrade, device authentication, secure protocols, etc.).

2) Advanced techniques based on AI and machine learning are being developed by existing security specialists and these will be applicable in the IoT. They will be increasingly capable of detecting attacks either before they occur or very quickly afterwards by identifying unusual patterns of traffic or activity. They will enable much faster diagnosis of such activity, which may result just from a faulty device but could indicate that an attack is unfolding. As these techniques mature, they will become capable of taking over from human security experts in making critical decisions such as shutting down parts of a service in response to attacks. This can save vital time in handling incidents as well as freeing up human experts to take more strategic roles in IoT security.

Abbreviations

ASRB	Automotive Security Review Board
CSS	Chirp spread spectrum
DRM	Digital rights management
ECU	Electronic control unit
IoT	Internet of things
IVI	In-vehicle infotainment
LPWAN	Low-power wide-area network
MNO	Mobile network operators
NB-IoT	Narrowband internet of things
NFC	Near-field communication
OTrP	Open trust protocol
PDS	Permanent denial of service
PKI	Public key infrastructure
PVR	Personal video recorder
RFID	Radio frequency identification
STB	Set-top box
SoC	System-on-chip
TEE	Trusted execution environment
TMF	Trusted execution environment management framework
ISBE	International Society of Broadband Experts
SCTE	Society of Cable Telecommunications Engineers

Bibliography & References

[i] https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/

[ii] https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

[iii] http://www.huffingtonpost.com/entry/cloudpet-hack-recordings-messages_us_58b4aef0e4b0a8a9b7857b45

[iv] https://www.bleepingcomputer.com/news/security/new-malware-intentionally-bricks-iot-devices/

[v] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
[vi] http://www.nayana.com/bbs/set_view.php?b_name=notice&w_no=961

[vii] http://www.wired.co.uk/article/petya-malware-ransomware-attack-outbreak-june-2017

[viii] https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf

[ix] http://www.computerweekly.com/news/450401576/Dyn-DDoS-attack-highlights-vulnerability-of-global-internet-infrastructure