# IPTV Migration Strategies

## Part 1: Security Primer

**Mark Millard and Susan Crouse**

**White Paper | March 2016**

alticast

# Contents

# Executive Summary

Cable Operators have built up sophisticated systems for delivering media services to the home. They have been through complex infrastructure transitions in the past -- for example, moving from analog to digital to HD. Now many are considering or have even begun their next revolution for media delivery, the transition to an all-IP or hybrid IPTV infrastructure.

The motivations for this change are multi-faceted. Some operators are negotiating content rights that would broaden their footprint to allow them to deliver content in a true TV Everywhere model. This also may allow some to deliver content in both a managed and unmanaged network including out-of-geography content delivery. This provides the opportunity to engage a larger viewer base and increase revenue through device support models while delivering to a multitude of both MSO devices and consumer devices. With the new FCC NPRM opening retail markets for STBs, there is more impetus to consider new delivery systems to support the possible influx of retail STBs offered directly to consumers, while continuing to add value to the operator's leased box offerings.

*…the new behaviors of millenials for consuming video on their own devices, creates a challenge for MSOs to consider how they can reposition themselves as innovators*

In addition, moving to IPTV delivery may increase the demand for faster broadband services, so this could alone drive revenue on the broadband services side of the MSO business.

Another motivation is to design an infrastructure that allows for services expansion. This might be through Internet of Things Household Automation, or it could be by providing other applications to users, whether via additional Video Solution partners or via applications from the MSO that enhance the media or home automation experience.

With Amazon, Google, Roku and Apple already providing IPTV media solutions, MSOs may see these as challenges to change their own methods. There is an innovation perception particularly by cord-nevers, that devices like HDMI dongles and small footprint pucks that deliver video "over the top" are new and better technology. As well, cord-nevers are less willing to lease HW for video consumption. This perception and the new behaviors of millenials for consuming video on their own devices create a challenge for MSOs to consider how they can reposition themselves as innovators. Part of the challenge is content packaging. The cord-nevers also trend towards OTT services because they can buy specific content offerings. MSOs are beginning to address this by unbundling their content and allowing users to design their own content packages. This ability is often based on renegotiating contracts with their

content providers and adding new content by partnering with new media services.

To enable this new business opportunity and take advantage of business expansion, operators need to consider developing an IPTV ecosystem. Building an IPTV delivery system is a complex undertaking. There are many things to consider when creating a viable, reliable, robust architecture. This also provides an opportunity for operators to innovate in the overall solution not only for the architecture, but for service, support and business rules. While developing this new solution, operators can consider how to save costs with the dynamic nature of a cloud architecture for growth and redundancy, as well as premises installation, services and monitoring and maintenance of both operator and user devices.

## The Challenges of Moving to All-IPTV

When considering development of an IPTV delivery solution, the system needs a fresh approach filled with opportunity for cost savings, delivery optimization and innovative solutions for the subscribers. This extensive list of questions below covers issues that should be addressed:

- What legacy infrastructure is still meaningful?

  MoCA, QAM, Switched Digital Video, DTA, CAS, DRM, Transcoding, DOCSIS.

- What new infrastructure and operational processes are desired?

  Private/Public cloud infrastructure, content ingest and management, content transcoding, content delivery network, DOCSIS, DRM, centralized vs. distributed operations (some change, some remain same), billing/payment/packaging options (millennials leading way for no long term contracts, etc…), integration with “Big Data” systems for operations and revenue-generating services such as advertising.

- How is DOCSIS 3.1 optimally used in an IPTV delivery system?
- What does the household ecosystem look like?

  - Gateway, user devices, STBs/dongles, wireless vs. wired, the mixture of in-home (e.g., multi-room DVR) vs cloud-based services.

- What formats do we need to support to deliver the media (both for storing and streaming)?
  - HLS, V9, MPEG-DASH, RTMP, RTSP, etc.
  - H.264, HEVC, etc.
- What are the pros and cons of Adaptive Bit Rate Streaming (ABR)?
- What will be the proper mixture of multicast vs unicast services?
- How are UI and video streaming guaranteed as consumers update software on devices and acquire new devices?

  (What is the best way to deliver multiple UIs for the variety of devices that need to be supported?)
- How is quality of service (QoS) ensured for video delivery in and out of the home?
- Will there be new methods for in-home Broadband Network management?
- How is integration designed for other services like sVOD, cDVR, dvertising ?
- What does the high level architecture look like, including DVR and Advertising?
- Should Internet-like payment systems, for example PayPal for shopping applications, be considered for integration? (“one-click purchases”)
- How is content protected to all devices in and outside of the home? How are multiple types of encryption (multi-DRM) handled?
- Do we need to use multi-cast to maximize video delivery efficiencies?
- What about 4K?
- Are there new analytics that should be monitored and managed and how is that done?
- What are the support challenges?

- What opportunities exist for simplification of our current system?
- Is this a good time to consider different approaches to billing, backoffice SW, transcoding, storage and other system components?
- How much will this cost and how long will it take?
- What should be considered when selecting an Application/Services ecosystem:
    - Whose apps? Any apps? Whether allied with a particular application ecosystem like Google, or with a private ecosystem?
    - Industry solutions (e,g., RDK) vs. global marketplace solutions (e.g., Android).
    - Need for services outside of the operator to add functionality (i.e., Google managed services) or providing access to services (i.e., IoT collection and backhaul).
    - Security, operations vs. development – Selecting a framework for development and more importantly deployment and operations, as well as securing customer information within the box, the network and the cloud.
- With all these issues and questions, the examination of an IPTV system can be broken down into a few key categories.

  Video Delivery Architecture: HeadEnd to the Last Mile

  Businesss Infrastructure

  Device Ecosystem

  E2E Ecosystem Security

  Service and Support

  Future Proofing the Solution (4K VR IoT)

To cover the plethora of issues, IPTV Migration will be broken down into a series of papers. This first part covers E2E security for IP services.

# End-to-End Ecosystem Security

*With the increasing number of apps used for personal data, such as health monitoring and home monitoring, overall security is coming to the forefront of any new STB conversation.*

## *IP Security Considerations*

Beyond content protection, there are a number of security requirements for an IPTV delivery system. These include account protection, user data protection, application data protection, potentially a 'household firewall' for IoT operations and more. With the increasing number of apps used for personal data, such as health monitoring and home monitoring, overall security is coming to the forefront of any new STB conversation. Some new apps coming to STBs include pairing or operation from consumer mobile and tablet devices. Those connections usually are bound over wireless networks using various communication protocols, for example WiFI, Bluetooth and LTE.

When developing this new infrastructure can bring an abundance of opportunities beyond video consumption, all areas of security should be considered. The operator can consider addressing security holistically for the home using a variety of services and as a pathway of those services to cloud operations, including asset and data storage.

Operators need to consider end-to-end security solutions that address the following scenarios:

- Account protection and access to users' credentials.
- User data protection such as access to users' profile meta data and billing details. Operators should protect their subscribers against fraud, malware, spyware, hacker attacks and identity theft.
- Application data stored both locally on the CPE as well as managed in the cloud.
- Securing a range of devices that may or may not be managed by the operator.
- **Zero day attacks** where hackers exploit security holes before the operator or device vendor becomes aware of them.
- Threats to operator managed devices (i.e. gateways) that include shutting down or bricking a device (including Blackmail).
- WiFi security from gateways to CPE on the home network (LAN).

End-to-end security solutions should provide the operator with the following benefits:

- Minimize operator liability through threat detection and mitigation in a timely fashion.
- Enable collection, monitoring and storage of security data such that operational requirements (DevOps) are less demanding on operator resources.
- Introduce security analytics, providing expertise that may not reside in-house.
- Allow active controls and tools that facilitate dynamic end-to-end managed service and device management.
- Increase levels of quality of service (QoS) protection and business continuity (minimize disrupted services).
- Enable operator confidence on device behavior and reaction to threats in a deterministic and predictable manner.

With these considerations in mind, there are three broad categories of security that should be addressed in the IP ecosystem: securing the device, securing the network, and securing the cloud.

## *Securing the Device*

Operators must ensure that the IP set-top and gateway devices placed on the customer's premises don't threaten their network infrastructure or the customer's home network. For devices managed by the operator, the software stack employed by the OEM vendor (i.e. OS, middleware, application utilities) must be hardened against known avenues of attack and threats. Likewise, software distributed by the operator (i.e. UX/UI applications and services) must face the same level of security as the stack. If third-party applications are available to the operator's managed device, then the operator must vet the application for security risks prior to deployment.

Technological approaches towards hardening the OEM and operator software against security threats include:

- Hardware Root of Trust
- Secure Boot Loader
- Role-based Access Control (RBAC)
- Buffer Overflow Protection
- Return Into libc Attack Protection
- Secure Program Execution
- Address Obfuscation

- Code Injection Attack Protection
- SELinux
- Application Sandboxing
- Detection and Prevention of Memory Corruption Attacks
- TLB-miss Corruption Blocking
- Process Footprint Wiping
- Secure Dynamic Module Loading (Kernel and User)

These topics are beyond the scope of this overview. However, they introduce the complexity of the solution required to safeguard the operator's device and client applications.

## *Securing the Network and Customers*

Network security is already of principal concern to operators having deployed millions of set-top boxes and gateway devices for QAM- and DOCSIS-based platforms. Moving to an IP ecosystem will not minimize this challenge. The operator must adopt policies and technologies to prevent and monitor unauthorized access, misuse and modifcation of their services. This includes threats that leverage techniques for denying customers access to a computer network (WAN or LAN) and network accessible resources such as the Internet or operator specific services.

Network adminstration and DevOps control the authorization of access to data on a operator's network. Tools must be put in place to monitor device and back office server activity and enforce the access control policies for these network components. Even if the attacker obtains root access, they should not be able to change the policy, therefore disabling the security mechanisms in place.

As threats are detected and identified, the operator must be able to dynamically respond and control security settings and policies from the headend. Both client and server components in the IP ecosystem need to provide ways to actively modify these security policy changes in real tme.

The operator must protect against both passive and active attacks on the network. Passive attacks occur when a network intruder intercepts data traveling through the network between the IP ecosystem/headend servers and the CPE. Active attacks occur in which an intruder initiates commands and software to disrupt the network's normal operation[1].

[1] See reference to *Computer and Information Security Handlbook* below.

Passive attacks include:

- Wiretaps
- Port scanners
- Idle scans

Active attacks include:

- Denial-of-service attacks
- DNS spoofing
- Man in the middle attacks
- ARP poisoning
- VLAN hopping
- Smurf attacks
- Buffer overflows
- Heap overflows
- Format string attacks
- SQL injections
- Phishing
- Cross-site scripting
- Cross-site Request Forgeries (CSRF)
- Cyber-attacks

Again these topics are beyond the scope of this overview. However, operator's must become aware of these threats in order to instrument policies and solutions to protect their customers and brand reputation.

## *Securing the Cloud*

Additional threats are introduced by the IP ecosystem employed to deliver the operator cloud-based services. As more services are implemented in the cloud outside the controlled operator environment, the potential for data to be compromised increases. The cloud service may or may not be managed directly by the operator; for example, when it is a CDN or third-party media service. The failure to address security threats with the cloud service provider will put the data's availability and integrity at risk.

Software as a Service (SaaS) and/or Platform as a Service (PaaS) have unique security challenges. In SaaS environments the cloud service

provider is responsible for security controls that target the application space such as the content delivery, billing management system, and customer account management. In PaaS solutions, the cloud service provider and operator are both responsible for addressing security threats since the application is most likely a custom solution implemented and managed by the operator. Note that the security issues are the same regardless of whether the deployment model is a private, public or hybrid cloud infrastructure.

One way to mitigate security threats in the cloud is to adopt security standards when determining an operator's security policy. Standards are based on different approaches for security, system development, financial reporting, IT service delivery, or control environments. ISO, the International Standards Organization, publishes an audit standard for Information Security Management Systems (ISO/IEC 27001). NIST, the National Institute of Standards and Technology, publishes papers related to information security that may be useful for determining policy. Also, the United States Federal Government has created standards for categorizing information and systems that offer minimum security solutions (FIBS Pub 200). A cloud service provider may offer certification in ISO, NIST or FISMA standards; this certification should be considered by the operator while investigating cloud-based solutions.

In addition to standards, an operator must consider the following:

- Assessing risk based on available resources for monitoring and managing their network and data.
- Reviewing traditional security mechanisms already in place such as firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) or Network Access Control (NAC) products.
- Adopting new tools and processes that target virtualization solutions as opposed to legacy utilities that only work well for services located on physical premises under the operator's control.

## End-to-End Security Testing

As a system is designed and developed, a test plan needs to be created that focuses on the operator's security policy. Implementing a security policy can be one of the more difficult tasks. It is challenging to ensure that all possible attacks on a system are vetted. As well, there are often standards that must be met, either published standards or specific requirements by constituents like content owners. In addition to developing and executing an internal test plan, an operator may consider using an outside consulting expert in cyber attacks to attempt to break into the services.

Approaches to testing for secure systems is a broad and specialized topic. Much of this is addressed directly for content through approved methods – in particular when hardware like cable cards are part of the system. The move away from cable cards in IPTV creates a different testing environment. Test plans should be integral parts of the complete system design.

## Conclusion

Security for IPTV is a broad issue, as apparent from both the areas that need protection, standards to be met, the various ways infrastructures can be attacked and the testing necessary to ensure success. When developing an IPTV delivery solution it is paramount to make security a top priority in system design.

Early on, operators primarily addressed content security as mandated by the content owners. With the fast growth in broadband services, combined with media content protection, security demands for data over broadband become even more critical. As IPTV becomes prominent for delivering media, even more information is traveling on these networks. With 4K emerging as the next video format, content security requirements from content owners are evolving to be more robust. The variations of networks, systems and data are putting security at the forefront of operator service requirements as they need to be vigilant about both media and data protection for their subscribers. Designing security into the architecture up front is important to ensure all the bases are covered.

# References

Androidauthority.com Rob Triggs Dec. 2014

Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257

Wikipedia contributors. "Network security." *Wikipedia, The Free Encyclopedia*. Wikipedia, The Free Encyclopedia, 18 Mar. 2016. Web. 19 Mar. 2016.

Cloud Security Alliance, https://cloudsecurityalliance.org

# Contact Alticast

For more information
please contact one of our regional offices or
visit www.alticast.com
or email info@alticast.com

Alticast Corporation
Seoul, South Korea
Tel +82 2 2007 7827
info@alticast.com

Alticast Inc.
Colorado, USA
Tel +1 720 887 1700
us@alticast.com

Alticast BV Amsterdam.
Amsterdam, Netherlands
Tel +31(0)20 240 31 90
eu@alticast.com