

CASE STUDY: Service Provider Tunes in IPTV Service Reliability and Security with Thorough Security Analysis

The stakes are nothing less than the future of entertainment and communications. It is a battle to be the company that brings video, voice and data services to homes and businesses in the United States and across the world. Telecom, ISP, cable and satellite companies are competing fiercely to earn their share of Internet Protocol Television (IPTV) revenue.

An estimated 55 million people will subscribe to IPTV services by 2010, according to the Open IPTV Forum. But before any service provider can tap into new revenue streams from IPTV service delivery, it must make a massive investment necessary to build a robust, secure digital TV infrastructure.

A leading service provider is piloting IPTV service to consumers in several communities in the United States. For this Tier 1 telecom service provider, delivering high quality IPTV will generate new revenues that will offset declining voice revenues. IPTV will enable the company to more effectively compete with the cable industry's successful triple-play services. It also hopes that IPTV will help it create long lasting customer relationships, which will ameliorate the industry's pervasive issues with customer churn.

Seizing the IPTV Opportunity

To achieve this promising future, the Chief Architect of IPTV at this service provider is overseeing a massive overhaul of its network architecture. IPTV is predicated on an intelligent, next-generation network infrastructure with advanced security that can deliver IP-based broadcast and video-on-demand (VoD) as well as other rich content. 2008 is a promising year for IPTV, given the early popularity of the service among elite users. The service provider hopes to capitalize on events such as the Beijing Olympics, which are ideal for IPTV, and spread the demand for IPTV among the broader population.

The service provider delivers broadcast TV as well as video-on-demand today in its IPTV pilot in several communities in the United States. Subscribers can order content on demand, so they can choose entertainment they want to watch when they want to watch it. The service provider plans to add the ability to interact with scheduled programs, such as the ability for viewers to vote with their remote controls.

Based on the success of on-demand ad delivery on Internet sites, the service provider has high hopes that targeted customized advertising can be a significant revenue stream. By delivering more relevant advertising to consumers, the service provider can charge advertisers a premium.



CHALLENGE

- Offer broadcast TV, video-on-demand, interactive TV and targeted advertising to consumers as part of an IPTV pilot, which will generate new revenue streams and offset declining voice revenues;
- Compete more effectively against triple-play services from cable companies;
- Identify potential sources of service degradations before they impact the customer experience and service level agreements;
- Ensure that IP-based video can share the next-generation network without impacting the availability of other revenue-generating subscriber services, including VoIP;
- Verify that IPTV network equipment is free from zero-day and known vulnerabilities.

SOLUTION

Mu-4000 Analyzer

RESULTS

- Successfully piloted IPTV services to consumers in several regions in the United States, paving the way for future rich content service rollouts;
- Met massively high service availability requirements for IPTV without impacting VoIP and other services that run on the same next-generation network infrastructure;
- Verify that IPTV products are free from vulnerabilities that may affect security or robustness before products are purchased and deployed into the production network;
- Automate and conduct comprehensive testing of highly complex IPTV applications and equipment to meet aggressive service rollout schedule.

The service provider has aggressive plans for other IPTV services. Integration with other communication services, such as phone or the PC, will allow subscribers to interact with friends and other people while watching TV. With presence and text messaging, subscribers can see which of their friends are online and chat about the show they are watching. Users can receive on-screen notifications about incoming calls or requests for video chat. Integration with mobile devices means that subscribers can download content to their mobile devices. A parent away from home can use a mobile phone to approve and unlock pay-per-view content that the children ordered.

The High Cost of Downtime for IPTV

Any market shift creates the potential of huge rewards and risks, and IPTV is no different. This service provider's IPTV pilot is backed by the build-out of a next-generation network architecture that can scale to handle the massive quality of service and availability demands of digital TV. Although this is a pilot, consumers will nevertheless expect that their IPTV service will "just work" -- without hiccups or hitches.

To meet those expectations, the service provider must proactively plan to deal with service degradations as well as service outages. Poor video quality or repeated outages for video services, especially for broadcast, will no doubt result in dissatisfied customers and customer turnover. It will also increase customer and network support costs, which is particularly concerning given the massive investment required to build the IPTV infrastructure. Negative customer feedback and bad press associated with a failed pilot puts future revenue streams at risk and could damage the company's brand.

IP network video is inherently intolerant of packet loss. IP network video is highly compressed and the video codecs don't recover from packet loss at the network layer, which means that losing a single packet of IP-encapsulated video can result in visibly degraded video quality. The quality of service challenge is compounded when considering that IP video will run on the same network with VoIP, best-effort Internet traffic and over-the-top video. Availability of these other subscriber services may be impacted by the robustness and security of IPTV services.

The service provider must also protect the IP infrastructure that carries the video signals. It has seen some of its Tier 2 competitors roll out IPTV services without the necessary attention and been hit by cyber-attacks and industry backlash. As a Tier 1 provider, a poorly planned rollout could cause long-lasting damage to the company's brand.

IPTV is subject to the same hacker attacks, threats and vulnerabilities that plague other network-based services such as the Internet. Attackers are often quick to exploit services in their early phases of adoption on the assumption that the service is not fully hardened.

Denial-of-service (DoS) attacks are of particular concern for IPTV. The nature of direct subscriber interaction makes the video serving infrastructure more susceptible to attacks. Video servers must be highly protected, as they are vulnerable to DoS, TCP and application-level attacks. Even if a DoS attack doesn't cause a service outage, network performance may degrade, which can impact video quality. Many other IPTV infrastructure elements and application services are at risk. For instance, an attack on a server that handles channel switching may overload that server and leave consumers without the ability to change the channel with their remotes.

Another risk is the subscriber's home network itself. IPTV may be carried over a subscriber's home network, along with Internet traffic, gaming sessions, and VoIP calls. A security breach on one of the subscribers' computers may open up the opportunity for attacks on the service provider's IPTV infrastructure, which also creates risk. The service provider must be assured that set-top boxes and other home equipment are free from vulnerabilities and security weaknesses.

Protecting IPTV Robustness and Security with Mu

Ensuring the robustness and security of the IPTV infrastructure is a multi-faceted undertaking, requiring the protection of the video serving infrastructure as well as the network infrastructure. Success was predicated on building IPTV system that can deliver high quality services and survive attacks. Given the unprecedented complexity and the aggressive rollout schedule, the Chief Architect knew he needed find efficiencies to accelerate the process of assuring that the IPTV elements will meet the company's standards for robustness and security.

The Chief Architect turned to Mu's security analysis solution for comprehensive security and robustness testing. With Mu analyzer, the engineering team test IPTV video serving and network infrastructure equipment for known and zero-day vulnerabilities prior to purchase and deployment into the network. With Mu, engineers validate the network's ability to defend itself against attacks and verify the performance of IPTV services when under attack, thus minimizing the risk of service degradation and outage. Refer to the "Technical Details" section for more information about use cases.

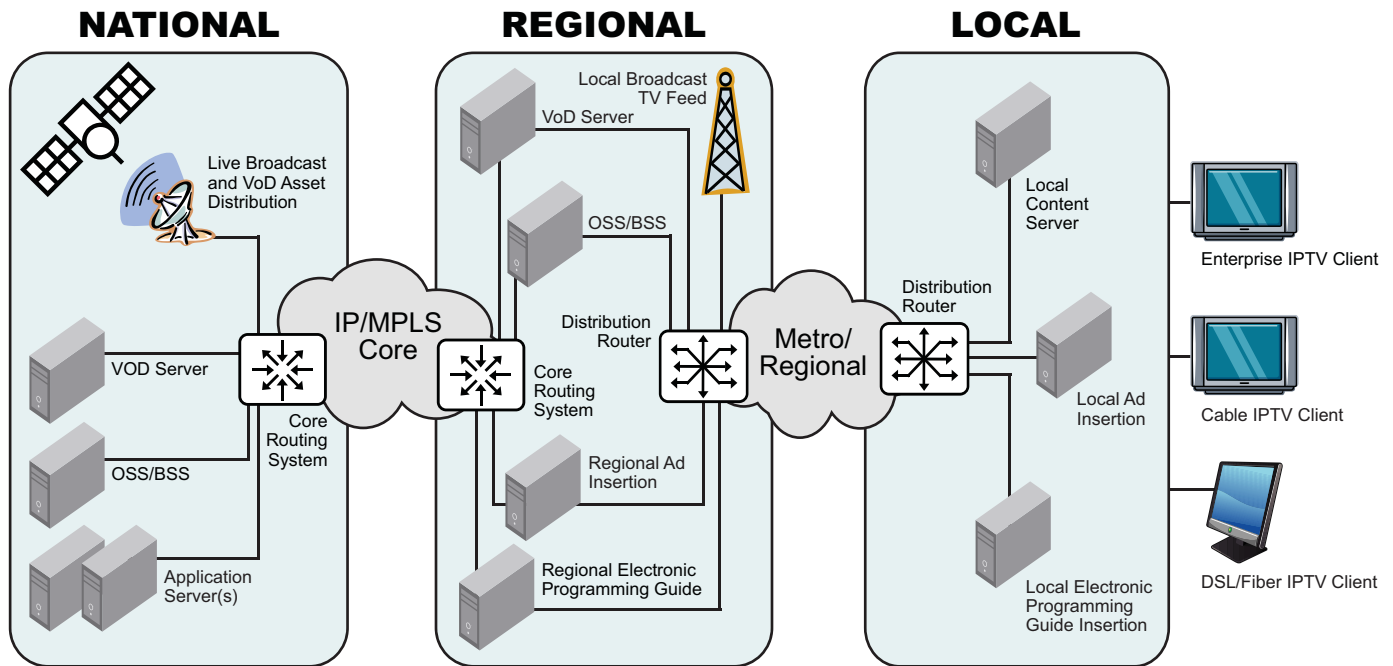


Figure 1. A leading service provider's IPTV architecture.

Business Benefits from Mu

The service provider has achieved measurable business benefits with Mu. Comprehensive security and robustness testing is incorporated into the IPTV deployment lifecycle, from product purchasing to deployment to product updates. The service provider has met its goals for IPTV service uptime and has avoided unplanned service disruptions or quality issues that can negatively impact revenue, customer retention rate, customer satisfaction and the public perception of its IPTV service.

Key results include:

- Rolled out IPTV pilot that met its customers' expectations as well as service level agreements for availability and quality.
- Reduced cost due to a proactive approach to problem resolution.

Reducing Total Cost of Ownership

Lower total costs contribute to a faster ROI, especially considering the significant investment required for a digital TV infrastructure. Firstly, the provider has saved on equipment outlay, lowering its capital expenditures (CapEx). Mu provides an integrated analysis approach, so the service provider does not need to buy multiple point solutions that provide a fraction of the analysis capabilities of Mu.

It has also reduced operational expenses (OpEx) for the IPTV infrastructure, due to cost savings in problem resolution and avoidable support costs. With Mu's full range of remediation tools, interactive charts and detailed reports, resolving issues with vendors has become easier and less time-consuming. The engineering team uses Mu to find bugs before service roll-out and upgrade, so the frequency and severity of downtime has been reduced. Customer service and network support staff spends less time resolving downtime-related customer issues.

Layer	Network Elements	Mu Tested	Benefits from Using Mu
National	Core routers	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> • Harden IPTV infrastructure • Reduce TCO by addressing product vulnerabilities early • Deliver high quality video
	Video Servers	<input checked="" type="checkbox"/>	
	CMTSs	<input checked="" type="checkbox"/>	
	Subscriber Management System	<input checked="" type="checkbox"/>	
Regional	Core routers	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> • Minimize quality issues, including packet loss and jitter • Characterize system responsiveness to identify problem spots
	Video Servers	<input checked="" type="checkbox"/>	
	CMTS	<input checked="" type="checkbox"/>	
	Subscriber Management System	<input checked="" type="checkbox"/>	
Local	Edge Routers	<input checked="" type="checkbox"/>	
	L2 Switches	<input checked="" type="checkbox"/>	
	Home Gateways	<input checked="" type="checkbox"/>	
	Set-top Boxes	<input checked="" type="checkbox"/>	
	Multimedia	<input checked="" type="checkbox"/>	
	Terminal Adapters	<input checked="" type="checkbox"/>	
	DSLAMs	<input checked="" type="checkbox"/>	

Table 1. Mu's Solution Provides Comprehensive Service Assurance for IPTV Network Elements and Applications.

The service provider delivers IPTV over the same infrastructure as VoIP and other IP services without impacting those revenue-generating services. It has been able to achieve its SLAs, which means it has avoided penalties. Mu's Response Time Charts provides detailed,

actionable information about system response time and availability statistics, making it easy for the service provider to audit its SLA conformance and avoid SLA-related penalties.

The service provider has improved its software patch process as well as its ongoing security operations. Mu's regression testing feature enables its testing staff to accurately verify bug fixes and software upgrades from vendors. Mu's run-to-completion analysis capability does not require human intervention once started, and automatically pinpoints flaws. Mu's analysis templates help disseminate scarce security knowledge, and establish security analysis best practices across the entire organization. The provider finds it easier to train new analysts and provide professional development in security analysis for existing staff.

Technical Details

Thorough Attack Surface Coverage

Mu-4000 analyzer provides comprehensive coverage of protocols used in IPTV. The engineering team subjects IPTV elements and protocols to rigorous attack mutations to discover service availability weaknesses that result from protocol vulnerabilities. The team uses Mu to test IPTV gear, including multimedia terminal adapters, CMTS, set-top boxes, home gateways, subscriber management systems, edge and core routers, L2 switches, intelligent DSLAMs and video services. The Mu can test across a broad array of IPTV protocols, including IGMP, RTSP, SIP, H.248, MGCP, PIM, SNMP, SSH, HTTP and IPv6.

The engineering team uses Mu to detect zero-day and published vulnerabilities in IPTV devices prior to purchase and deployment. Mu's Dynamic Stateful Fuzzing technique subjects the target system to many combinations and permutations of protocol abuse attacks. Fuzzing uncovers problems that are overlooked by conventional testing methods, including buffer overflows, memory leaks, CPU utilization and latency issues, which are critical for video, voice and multimedia applications.

Comprehensive Support for Analyzing IPTV Deployments

Pinpointing vulnerabilities prior to product purchase or deployment clearly improves the network's security posture. With Mu, the service provider can also establish a baseline for the IPTV product security and robustness, which is essential, given the rapid evolution of IPTV protocols and products occurring today.

The engineering team uses Mu as part of its remediation processes. It uses Mu to verify new patches and releases as part of its change management process.

Automation Improves Efficiency

Assessing robustness and security is an inherent part of this service provider's operational best practices and given the massive complexity of IPTV, test automation is a foregone conclusion. The time savings enabled the service provider to roll out IPTV services on budget and on schedule. With automation, they can cover more mutations than would be humanly possible with scripting or manual efforts. They use Mu-4000 appliance to automate other toolsets, including the open-source vulnerability analysis tool Nessus. Another time-saver is the ability to automatically re-run any test with one-touch regression testing, which allows them to validate that a vendor's patch truly fixes the issue.

Ease of Use

The security team also appreciates Mu's GUI for ease of use. As a Web-based appliance, Mu-4000 is easy to install and is intuitive to use. Wizards and templates guide the engineers through the analysis process. Creating and using a template is a step-by-step process that allows the engineers to define attack types, monitor events and take action in response to events. Test-center staff simply selects any of Mu's protocols and then configures the comprehensive variety of custom attack parameters in each template.

The XML-based templates are also portable using Mu-4000 for any aspect of the analysis. Templates further a "Best Practice" approach that is easily shared organization-wide and with the engineers that have complementary skill sets. Monitors allow engineers to capture additional information on the target, so they can capture exactly what was happening at any moment to trigger automatic fault isolation.

Ongoing Analysis

By verifying that vulnerable IPTV products are not deployed into production, this Tier-1 service provider avoids most significant problems down the road, including service degradations and downtime. Mu-4000 is used across the entire deployment lifecycle from the initial product purchase to subsequent upgrades.



web: www.mudynamics.com | email: info@mudynamics.com
address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA
phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317