

CASE STUDY: Bolstering the Reliability, Availability and Security of IP Multimedia Subsystem (IMS) Rollouts by Security Assurance

The Service Availability Challenge

IMS is being quickly elevated in carrier spending priorities for its promised ability to transform the telecom industry. Telcos, mobile operators and other service providers want to deliver multimedia services across next-generation packet-switched networks and traditional circuit-switched networks, including mobile networks (e.g., GSM 3G, LTE, WiMAX, etc.). Service providers expect and require that their significant investments in IMS will quickly reap new business opportunities and lower operational costs without placing existing services at risk. But before new multimedia services become a strong revenue contributor, service providers and network product providers alike must have strong confidence in the reliability, availability and security of the underlying IMS infrastructure.

One major international service provider is well on its way to reaping the rewards of IMS. This Tier 1 service provider is piloting IMS-based services, including VoIP, presence and other advanced applications. Based on the success of its pilot, an aggressive schedule is underway for interactive push-to-talk, multimedia conferencing and other multimedia applications.

High Cost of Downtime

Customers expect dial-tone when they pick up their phone (be it a handset, a smartphone or a softphone), and they will not dismiss reliability for the pleasure of cool multimedia applications. If service providers want to maintain loyal subscribers and protect their brand, they need to meet the wireline carrier industry's gold standard of 99.999% uptime, regardless if services are traditional or cutting edge.

Absolute failures continue to be of major concern, but service providers must also contend with partial failures or service degradations, where a service performs more slowly than usual, even to the point of end user frustration. Downtime in IMS-based services can result in significant lost revenue for the providers because of:

- customer churn,
- increase in avoidable support costs,
- decreased average revenue per user (ARPU).

Loss of Service Revenue

This service provider estimates that, in a small metropolitan area with 100,000 subscribers, downtime in its residential service areas costs more than \$8,300 per hour and that downtime in business service areas costs more than \$11,500 per hour. Across all its service areas, the cost of downtime quickly adds up to **tens of millions of dollars per year**.



EXECUTIVE SUMMARY

CHALLENGE

- Capture new revenue opportunities and reduce operational costs by transitioning to next-generation network architecture and IMS;
- Offer VoIP, presence-based applications, multimedia conferencing and other advanced services that are reliable, available and secure;
- Identify and eliminate sources of potential service degradations before they impact the customer experience and service-level agreements;
- Select high-quality IMS products free from service-affecting vulnerabilities that may result in downtime.

SOLUTION

Mu-4000 Analyzer

RESULTS

- Met service availability requirements for VoIP and rich media applications;
- Met aggressive rollout schedule for IMS applications and pilot of next-generation network architecture;
- Verified that IMS products are free from security or reliability weaknesses before products are purchased and deployed into the production network;
- Automated and conducted comprehensive testing of highly complex IMS applications and equipment, and integrated into regression testing across the whole deployment life cycle.

business-critical voice service. If an attacker used SIP to disable a security enforcement device, the service provider's entire perimeter defense system is compromised and the attacker may access the service provider's core network to inflict further disruptive behavior. Loss of these services will negatively impact providers' service availability and revenues.

Improving Service Availability and Security with Mu

The Chief Architect of IMS Services at this service provider is keenly aware that delivering a useful, profitable service to customers also means protecting the IMS against attacks and service abuse. Verifying that IMS products are free from zero-day and known vulnerabilities is a vital step in this protection. The Chief Architect demanded that all gear deployed in the IMS pilot meet the company's same high standards for reliability, availability and security as the traditional circuit-switched network. The solution was the Mu-4000 appliance and its SIP protocol mutation modules for comprehensive service assurance. Figure 2 shows a simplified network diagram of this service provider's IMS architecture. Table 1 summarizes the network elements that the Mu solution analyzes and the benefits for the service providers. Please refer to the "Use Case Details" section for more information.

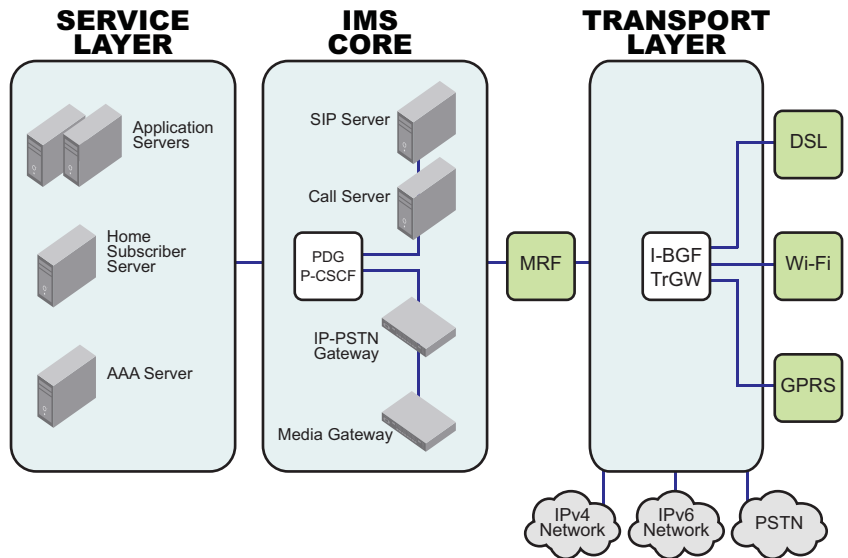


Figure 3. A leading service provider's IMS architecture.

Business Benefits from Using Mu

After using Mu's solution for nine months, the service provider achieved significant business benefits. With comprehensive service assurance incorporated into the entire life cycle of its IMS deployment, the provider met its goals for service uptime and avoided service disruptions or quality issues that would otherwise impact revenue, customer retention rate and overall customer satisfaction.

Key results include:

- Minimized system downtime and associated customer churn.
- Rolled out IMS applications met or exceeded customers' expectations as well as internal metrics for service availability and quality.
- Reduced cost in several operations areas due to taking a proactive approach to problem resolution before IMS network infrastructure was production deployed.

Reducing Total Cost of Ownership

Gaining cost efficiencies are especially important, given the investment required to build-out an IMS infrastructure.

CapEx | The provider saved on capital equipment expenditures with Mu's solution. Mu helps this service provider ensure the IMS products and applications it purchases are resilient, which prevents wasting valuable CapEx on low-quality products, also avoiding OpEx penalties due to higher-than-planned field fire drills of lower-quality equipment in production deployment. Mu provides an automated analysis approach, so the service provider does not need to buy multiple point solutions providing only one component of the necessary service assurance analysis capabilities of Mu.

Layer	Network Elements	Mu Tested	Benefits from Using Mu
Service/ Applications Layer	Application Server	☑	<ul style="list-style-type: none"> • Harden IMS Service infrastructure • Protect against vulnerabilities that may result in voice spam, denial-of-service attacks and malware.
	Home Subscriber Server	☑	
	Authentication Authorization Accounting (AAA) Server	☑	
	Media Resource Function (MRF) Server	☑	
	Security Gateway	☑	
IMS Core (Control) Layer	Call Session Control Function (CSCF)	☑	<ul style="list-style-type: none"> • Reduce TCO by addressing product vulnerabilities early. • Characterize system responsiveness to identify problem spots.
	Packet Data Gateway (PDG)	☑	
	SIP Server	☑	
	Call Server	☑	
	Media Gateway	☑	
	IP-PSTN Gateway	☑	
Transport Layer	Interconnection Border Gateway Function (I-BGF)	☑	
	Translation Gateway (trGW)	☑	
	Router	☑	

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

Loss from Customer Churn

The service provider further estimates that, in the average small metro area, dissatisfaction with the quality of an existing service increases the customer churn rate by up to 5 percent. Service reliability is even more important when piloting new services, since users are forming their first impressions and the success of the broader business is at stake. So for the IMS pilot, the service provider estimates that customer dissatisfaction will increase the churn rate up to 8 percent.

The service provider conservatively estimates that the cost of churn per subscriber ranges from \$400 to \$600, based on time-based replacement costs. Figure 1 shows just how expensive it is for the service provider when customers become unhappy to the point that they leave for an alternative carrier. The average cost of churn for this small metro area would range from \$1.6M to \$4.8M per year. Again, across all the regions serviced by this provider the cost of customer churn quickly grows to **hundreds of millions of dollars per year**.

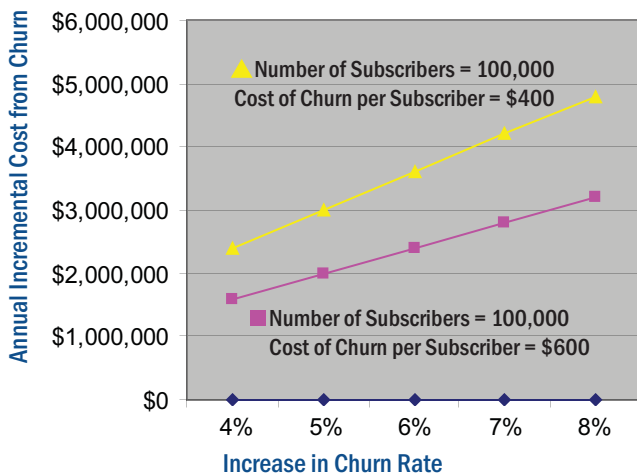


Figure 1: Cost of customer churn as a result of IMS quality issues in a small metro area of 100,000 subscribers.

Difficulties in Testing IMS Networks

Due to these high costs, service providers are motivated to reduce network downtime and maintain high IMS service quality. However, assuring the reliability, availability and security of emerging IMS services is an unprecedented challenge. Balancing the economic and competitive pressure to deploy new services at traditionally high subscriber expectations over a rapidly changing infrastructure is like nothing that has been attempted by the carriers. Addressing the challenge requires expertise and solutions previously unavailable in the industry. These solutions must methodically measure and assure the service availability of an IMS network and its associated applications, from transport to core to application services. This service provider understands firsthand that the inherent complexity and immaturity of IMS create ample opportunities for interoperability and robustness issues.

New and Complex

IMS is comprised of dozens of new protocols specified by many standards bodies, including the 3rd Generation Partnership Project (3GPP), Internet Engineering Task Force (IETF), European Telecommunications Standards Institute (ETSI), International Telecommunication Union (ITU), the IMS Forum, and CableLabs. Any new protocol or protocol extension may have many interpretations and carries the risk of being fragile (and causing operator network downtime) until hardened in the real world.

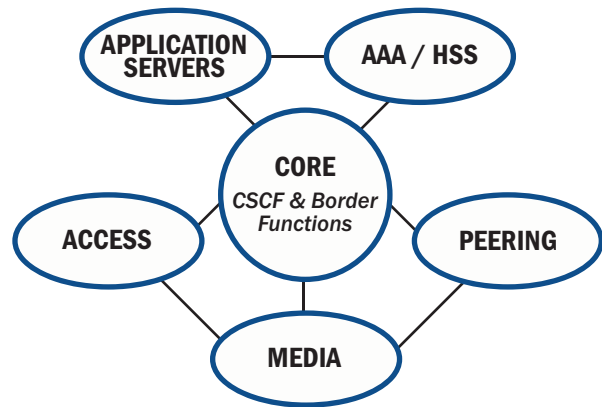


Figure 2: Generic IMS architecture. The number of protocols required by IMS networks is exponentially multiplied by many different types of equipments and applications. The variety of deployment scenarios further adds to the complexity.

In addition, IMS leverages many IP-based protocols, each of which has its own dependencies and vulnerabilities. For delivering voice [over IP] service, IMS uses the Session Initiation Protocol (SIP) to control communications. SIP is known to have a large number of acceptable implementations, which creates unforeseen security weaknesses and makes it challenging for network equipment manufacturers to build interoperable products. SIP itself leverages many of the mechanisms developed for HTTP and SMTP/MIME, thus inheriting those protocols' weaknesses and vulnerabilities as well.

Fragile and Vulnerable

VoIP communications from subscribers' PCs, smartphones and other SIP endpoints on a next-generation network are far more exposed than traditional analog communications. Attacks may originate from the Internet, wireless LANs or GPRS networks.

Attackers potentially compromise applications using IMS and SIP, such as presence-based applications, to bypass traditional perimeter network defenses and spread spam/spit (spam over Internet telephony), denial-of-service (DoS) attacks, malware or worse. Malicious traffic, including DoS flooding attacks can severely impact voice quality, as VoIP is far more sensitive to network latency and jitter than "best-effort" data-oriented applications. If any IMS vulnerabilities are exploited, attackers could knock out a media gateway, voicemail, or other

OpEx | The provider also saved on operational expenses after leveraging the automation and ease of use of Mu's solution. Resolving vulnerability and bug fix issues with vendors now involves less finger-pointing and is quicker, because of Mu's full range of remediation tools, interactive charts and detailed reports, highlighting the issues in detail. The testing staff accurately verifies bug fixes from vendors with Mu's regression testing feature. The service provider also reduces costly SLA penalties using Mu's Response time Charts for highly actionable information about system response time and availability statistics available.

Use Case Details

Testing IMS Transport, Core and Services Layers

This service provider uses the Mu-4000 analyzer to test the reliability, availability and security of gear used in the IMS transport, core and services layers. Comprehensive test coverage across all involved IMS network elements is essential because any single protocol vulnerability can expose the entire network to attack.

With Mu, the service provider's engineering team detects zero-day, DoS and published vulnerabilities in VoIP and IMS products. Mu is an integral part of the service provider's life cycle for IMS product purchase, development, roll-out and change management. When vulnerabilities or product weaknesses are identified through use of the Mu system, the onboard Mu remediation suite is essential for efficient problem resolution. Automated testing with Mu saves the engineering team considerable time, which enabled the service provider to roll out IMS applications to customers on schedule.

The Mu-4000's Dynamic Stateful Fuzzing engine subjects the target IMS system to many combinations and permutations of protocol attacks in a controlled environment. Fuzzing, combined with an advanced monitoring and fault isolation capability, uncovers problems that are often overlooked by conventional testing methods but are particularly important for voice and real-time multimedia applications. These issues include:

- buffer overflows,
- memory leaks,
- CPU utilization spike,
- performance degradation, and
- other latency issues.

IMS Core Layer

The engineering team uses the Mu-4000 to test the Proxy Call Session Control Function (P-CSCF), which acts as a centralized SIP routing engine, policy manager and policy enforcement point for the delivery of real-time IMS applications. Protecting the [P-]CSCF from accidental misuse or intentional attacks and is a priority, because attackers can use subscriber devices to attack the IMS edge with DoS attacks, carefully crafted exploit code or malicious packets.

The engineering team also uses the Mu-4000 to test the IP-PSTN gateways, media gateways and perimeter security devices. The Interrogating Call Session Control Functions (I-CSCF's) that serve as the SIP peering point between service providers are also a point of potential exposure. One service provider may inadvertently pass malicious traffic across the SIP peering links or even everyday network packet corruption could impact service availability. The engineering team uses the Mu-4000 to assure that the I-CSCF's are robust.

Application Layer

The team also uses the Mu-4000 to test availability and robustness of various IMS services, including application services for VoIP, push-to-talk and multimedia conferencing. Engineers use the Mu-4000 to test interactions between the Serving Call Session Control Function (S-CSCF) in the control layer and the Application Server functions. Developers' ability to test XML and HTTP/HTTPS protocols is also essential for applications that use web services to take advantage of IMS network functionality, such as call control, conferencing and user interaction.

Transport Layer

The provider's test suites using the Mu-4000 typically include SIP with IMS extensions, MGCP, possibly with the NCS profile, H.248 with IA profile, HTTP, XML and RTP. The engineering team uses the Mu-4000 to test the core infrastructure, including routing protocols, LDP, MPLS, and other lower layer protocols. The engineering team also uses the Mu-4000 to test SIP implementations used in the various endpoint devices. Furthermore, the Mu solution is used to test the H.248 protocol implementations used in the Media Gateway Controller to support voice and fax calls between the PSTN and IP networks, as well as RTP protocols that carry the data encoded with the codecs that digitally represent audio and video traffic.



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