



# Building Reliable, Available and Secure Service Provider IMS Networks

## **Legal Notices:**

All contents copyright © 2008 by the IMS Forum®. All rights reserved. No part of this document or the related files may be reproduced, stored in a retrieval system, or transmitted in any form by any means (electronic, photocopy, recording, or otherwise) without the prior written permission of the IMS Forum.

**Limit of Liability and Disclaimer of Warranty:** The IMS Forum has used its best efforts in developing this document, and the information provided herein is provided “as is.” The IMS Forum makes no representation or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose and shall in no event be liable for any loss of profit or any other commercial damage, including but not limited to special, incidental, consequential, or other damages.

IMS Forum, IMS Plugfest and IMS Certified are trademarks of the IMS Forum Inc. All other trademarks and service marks are the property of their respective owners.

## **About the IMS Forum:**

The IMS Forum® is a global, non-profit industry association devoted to interoperable IP Multimedia Subsystem services delivery architecture and solutions. The IMS Forum mission is to accelerate the interoperability of IMS revenue-generating services, enabling enterprise and residential consumers to fully benefit from the delivery of multimedia mobile and fixed services over broadband cable, wireless, wireline and fiber networks. The IMS Forum is the creator and organizer of the IMS Plugfest™, the industry’s only event focused on IMS service interoperability, verification and certification through the IMS Certified™ program.

Through its organized Plugfests, working group interactions and other activities, forum members develop cost-effective technical frameworks for converged IP services over wireline, cable, 3G, WiFi and WiMAX networks. For additional information, or to join the IMS Forum and the IMS Plugfests, please visit [www.IMSForum.org](http://www.IMSForum.org).

## ***IMS Forum Contact Information:***

IMS Forum Headquarters  
211 Summit Place #292  
Box 10,000  
Silverthorne, Colorado 80498  
USA  
[www.IMSForum.org](http://www.IMSForum.org)  
Email: [Info@IMSForum.org](mailto:Info@IMSForum.org)  
Telephone: +1 970-262-6100

## **Foreword from IMS Forum Chairman and President:**

We are in the midst of the convergence of Internet and broadband over cellular, WiFi, WiMAX, cable, fiber, power lines, and increased consumer expectations of enhanced services and applications. Investors world-wide accept that “content is king,” however at the end of the day, the “consumer is king.” Consumers are forcing service providers to deliver bundled services, with the right quality of service at the right price, and with reach features tied into mobility and multimedia. These expectations are the main drivers for the implementation of the IP Multimedia Subsystem (IMS) services architecture.

The IMS Forum focus ensures that IMS architecture is tested and certified through a rigorous process. We work with service providers, vendors, regulators as well as other industry groups to inform, educate and promote interoperable IMS services working across all types of broadband networks.

The IMS Forum issues two types of documents, white papers and best practices. The white papers focus upon information dissemination, education and promotion of IMS services. The best practices focus upon clarifications and methodologies for implementation of IMS applications and services

Thanks to IMS Forum members and industry partners for their contributions to this document.

To participate in IMS Forum projects, including technical working groups, the IMS interoperability, please visit [www.IMSForum.org](http://www.IMSForum.org).

Thank you,

Michael Khalilian  
Chairman & President  
IMS Forum  
[Mkhalilian@IMSForum.org](mailto:Mkhalilian@IMSForum.org)

## Contributors

The IMS Forum would like to thank the following contributors:

Russ Daigle, Director of Engineering at Mu Dynamics, Inc.

Adam Stein, Vice President of Mu Dynamics, Inc.

[Mu-info@musecurity.com](mailto:Mu-info@musecurity.com)

### About Mu Dynamics:

Mu Dynamics offers a new class of security analysis system, delivering a rigorous and streamlined methodology for verifying the robustness and security readiness of any IP-based product or application. Since Mu's debut of its flagship Mu-4000 analyzer appliance in early 2005, the company's achieved significant customer traction. One-third of the world's 15 largest service provider and cable operators now use Mu; Mu's customers represent one-half of the revenue in the global network, application and security infrastructure market; and Mu's customers represent one-third of the revenue in the global industrial control manufacturer market. Headquartered in Sunnyvale, CA., Mu is backed by preeminent venture capital firms that include Accel Partners, Benchmark Capital and DAG Ventures.. More information is available at <http://www.mudynamics.com>.

# TABLE OF CONTENTS

<b>1. Executive Summary</b> .....	<b>1</b>
Figure 1: Worldwide Revenue Forecast .....	2
<b>2. How does a Robustness Testing System or Security Analyzer work?</b> .....	<b>2</b>
Figure 2: Visualizing how Robustness Testing and Negative Testing Works .....	3
Figure 3: Charting Response Time and Latency with Robustness Testing.....	4
<b>3. What analysis and testing should vendors and users perform on IMS products?</b> .....	<b>5</b>
<b>4. Which IMS protocol implementations should be tested? Why?</b> .....	<b>6</b>
Figure 4: IMS Architecture User, Control and Application Planes All Subject to Robustness Weaknesses .....	8
Figure 5: Protocols that require Robustness Testing .....	9
<b>5. Conclusions</b> .....	<b>10</b>
<b>6. Glossary</b> .....	<b>11</b>

## 1. Executive Summary

Who is responsible for the reliability, availability and security (RAS) of IMS Services? IMS vulnerability exploitation could have devastating results, especially if a media gateway, voice mail, or other mission-critical, voice-related resources are impaired. In fact, the entire perimeter defense could be compromised if an attacker is able to use SIP to disable a security enforcement device.

To proactively protect their investments and revenue-bearing network services, Broadband Service Providers, including DSL, wireless and Cable Operators, are now using negative testing and robustness analysis for:

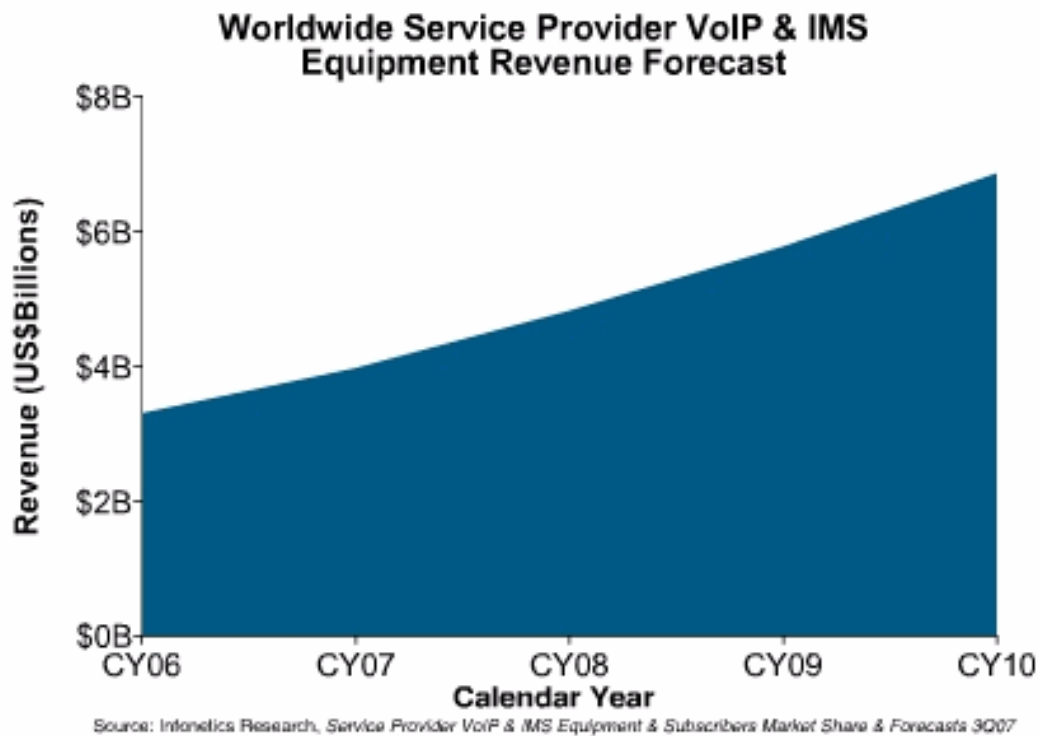
- Product Selection: RAS readiness is a key metric to support purchase decisions or upgrades, in addition to robustness, functionality and performance.
- Product Deployment: By securely deploying product features or introducing configuration changes into the network architecture, end-users proactively identify and remove robustness vulnerabilities before deployment.
- Change Control: Analyzing new software or firmware releases or bug fixes before production use, ensuring no published or previously eliminated issues or vulnerabilities are inadvertently deployed in the network.
- Threat Assessment: Security crisis management and problem reporting to a vendor is streamlined with a negative testing system's integrated ability to automate and "operationalize" the auditing and vulnerability remediation processes.

IMS users, including service providers, continuously strive to enhance service availability by reducing system downtime that results in the costly loss of either existing customers or confidential information. Negative testing works with these users to baseline their wide-ranging IMS product security and robustness during the initial purchase or upgrade to help ensure maximum uptime. This approach also maximizes network services against disruption or malicious activities that are likely to become more widespread with the growing VoIP and IMS equipment market space. Potential robustness weaknesses in IMS systems, and the use of negative testing, is unique from other product analysis areas such as Routing, L2 switching, SCADA or even storage. Still, there exist a few commonalities in the management interface protocols commonly supported in IMS systems that represent an often overlooked attack surface vector.

Many service providers interviewed in an NSP Partners study<sup>1</sup> noted unacceptable levels of downtime or customer churn due to network robustness issues. Survey participants found that integrating product robustness analysis to discover and eliminate weaknesses and vulnerabilities reduces downtime and customer churn. In more than one instance, participants noted that the integration of robustness negative analysis into their deployment and development processes paid for themselves in less than a month by reducing customer churn or field fire drills.

---

<sup>1</sup> NSP Partners LLC, November 1, 2007; The Business Case and Return on Investment for Deploying Robustness Testing



**Figure 1: Worldwide Revenue Forecast**  
*Source: Infonetics Research*

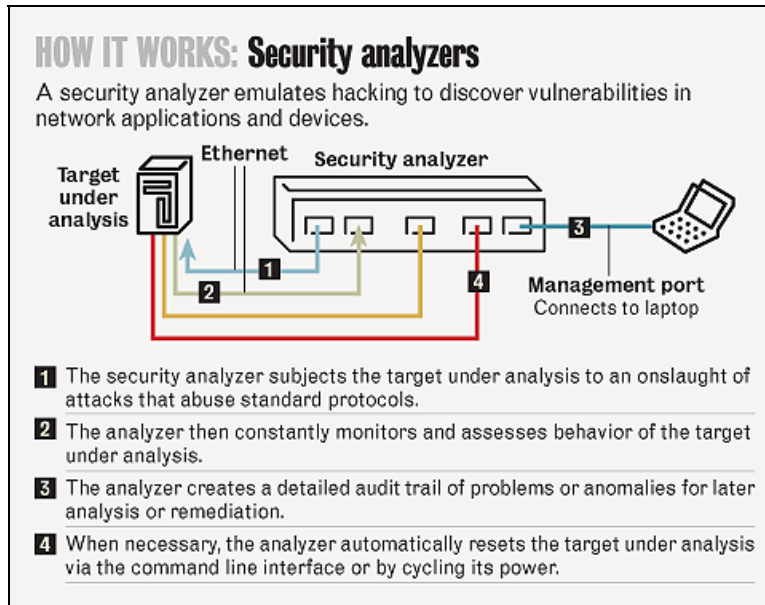
The NSP study found that with existing analysis techniques, many network robustness issues go undetected until the worst case scenario happens, and network downtime or malicious access occurs. Simply put, existing analysis techniques provide limited value. Most cover only the “shallow end” of the product’s communication attack surface “pool” through homegrown scripts, use of commercial stateless protocol fuzzing software and other open-source tools to test for security weaknesses. The problems found with manual testing are relatively obvious; many subtle system weaknesses and security flaws went undetected.<sup>2</sup> VoIP or IMS system flaws—for example, in Session Initiation Protocol (SIP)—would have resulted in serious denial-of-service conditions in the production Internet telephony networks, equating to opportunities for expensive network service outages.

IMS product developers use robustness testing to ensure their products are free of both 0-day and published vulnerability defects that would cause users to suffer negative public consequences, lost revenue or customer turnover. The increasing complexities of triple play service deployments, security product rollouts or 3G/Wireless services can quickly outpace existing resources in the IMS testing ability to isolate the attack surface of any product deployed within the entire network.

## 2. How does a Robustness Testing System using a Security Analyzer work?

Robustness testing subjects IMS implementations to rigorous attack mutations that discover service availability weaknesses resulting from protocol vulnerabilities, and document how organizations can secure IMS-based applications. Potential weaknesses of IMS applications usually require many ports to be opened on the network infrastructure allowing signaling and media related to incoming access requests. This is the antithesis of a firewall’s normal function of monitoring the IP and UDP/TCP layers and keeping unused ports closed.

<sup>2</sup> NIST [Cost of Poor Software Quality](#), May 2002



**Figure 2: Visualizing Reliability, Availability and Security (incl. Negative) Testing**

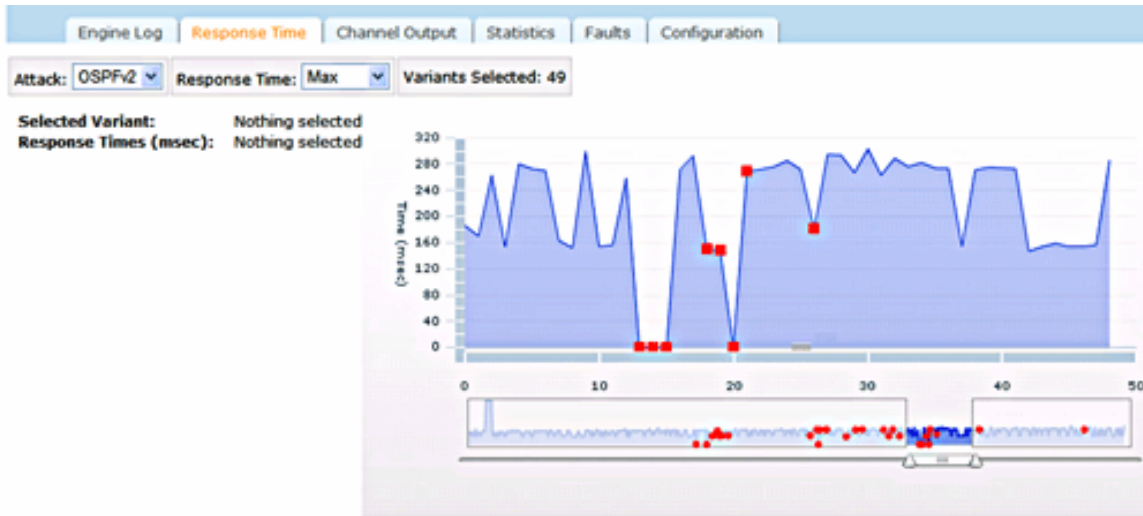
*Source: Network World*

Protocol abuse targets vulnerabilities in many types of devices and applications, from firewalls, VoIP controllers and VPN gateways to intrusion-prevention systems and other perimeter defenses. Despite the considerable investments made in security infrastructure, many vulnerabilities remain undetected. To alleviate protocol abuse, robustness testing helps IT departments assess the security of IP-based products, services or applications. This rigorous process, complete with an audit trail and remediation scripts, finds and fixes IMS or VoIP system vulnerabilities before deploying these systems and software into production networks.<sup>3</sup>

Negative testing systems work by connecting to a system and emulating hacking by generalizing techniques hackers employ and applying these as a comprehensive set of protocol attack vectors in a systematic, repeatable fashion. Unlike source code analyzers and vulnerability assessment tools, negative testing is used by non-experts to assess systems and applications in a lab environment.

Robustness analysis, including the protocol fuzzing technique, detects known and unknown zero-day vulnerabilities by subjecting the target system or software to many permutations and combinations of protocol abuse attacks. To analyze for unknown vulnerabilities, maximum protocol abuse is achieved through extremes of valid, invalid or unexpected inputs that violate the protocol's specifications. Examples of these extremes include formatting a field's type, length or value incorrectly, inserting illegal characters and adding trailing blanks. Resulting problems detected include buffer overflows, memory leaks, CPU utilization and even latency issues often missed by conventional testing.

<sup>3</sup> Network World, May 15, 2006; Security Analyzers target vulnerabilities by Kowsik Guruswamy, CTO and co-founder Mu Dynamics



**Figure 3: Charting Response Time and Latency with Robustness Testing**

*Source: Mu Dynamics*

The key to finding protocol vulnerabilities and IMS system weaknesses is in understanding a protocol's potential weak spots. GSM mobile operators that are evolving their 2G/3G networks towards the IMS architecture are especially interested in proactively finding and removing these weaknesses before production service deployment. Comprehensive coverage is critical because, just as the failure of a single part can cause an airplane to crash, a single protocol vulnerability can expose an entire network to attack. But to be truly effective, the robustness testing system must also operate efficiently with a finite and well-conceived set of protocol attack vectors.

Negative testing, including dynamically-compiled protocol fuzzing within a robustness testing regime, subjects the target system or application to a large number of attacks—potentially millions. During this onslaught, the state of the target is continuously monitored. Details on any anomaly or unexpected result are logged in a database that provides a complete audit trail to establish baselines and historical regressions that are useful when comparing products, releases or configurations. A testing system also creates a self-extracting, executable file capable of replicating the exact state, structure and semantics for each vulnerability. This “virtualized” attack file can be shared with the vendor or development team to expedite the remediation effort.

The ability to pinpoint vulnerabilities in a stand-alone system or application provides a practical way to compare competitive product offerings, possibly against a benchmark, before making a purchase decision. Additional post-purchase applications include alerting the vendor to weaknesses or vulnerabilities to assist with the remediation effort, verify patches or profiling new releases as part of a change management process, and evaluate and contrast specific system configurations. A robustness system can assess the effect of changes in the Service Provider IMS service security policy, evaluate internally developed software for vulnerabilities, and also perform on-demand security audits.

In order to provide a minimum level of security for environments using IMS applications, organizations must implement an IMS-aware defense in depth or translation gateways. IMS awareness adds significant complexity to these firewalls, NAT, and other security perimeter defenses, and this complexity can make them less robust, to the point of reaching vulnerability to exploits.

### 3. What analysis and testing should vendors and users perform on IMS products?

In addition to existing IMS and VoIP reliability or security testing solutions available on the market today, complete reliability, availability and security testing offers IMS providers significant technical advantages and functionality not available elsewhere. The range of IMS Testing options available to both service provider users and their varied suppliers includes these six aspects below. Each testing aspect can be used independently, though combined they are strengthened.

- **Stateful Dynamic Fuzzing:** Integrated and extensive protocol coverage available today builds complete protocol state machines that enable robustness testing deep within the target protocol's software layers and state transitions. While competing solutions only test the "first PDU" of a protocol interaction, robustness testing supports stateful fuzzing throughout every message exchange and transition that a protocol supports in a real operating environment. This means that IMS users will be better positioned to identify more robustness-related issues and bugs using negative testing.
- **Test-bed flexibility:** Negative testing can function as either a protocol client or as both the client and server (or equivalent) in order to test pass-through devices such as routers, proxies and SBCs. The analyzer acts as a variety of protocol entities, in order to test the robustness of every critical service enabled on a given device, including core protocols (MGCP (with NCS), H.248, SIP/IMS), as well as the often-overlooked management protocols (SSH, HTTP, Telnet, SNMP) that can also introduce risk and cause an outage. For example, during past IMS PlugFests, robustness testing identified a number of critical robustness issues in existing IMS supplier products triggered by both application and management protocols that cause the entire device under test to crash and reboot.
- **Automation:** Robustness testing systems apply a scientifically repeatable process of what it takes to incorporate robustness testing into the business process. For example, if the target device crashes during a test, the analyzer appliance automatically detects the failure and recovers the device so that the testing can continue through to completion. Robustness testing also monitors what is going on inside the device under test (DUT), and correlates cause and effect between the specific negative test case(s) and the isolated fault(s). For every fault identified, the integrated analyzer performs automated data collection, alerting and reporting. Negative testing also needs to interoperate with, and automate, other test tools in IMS-based service deployment environments. Without these capabilities, robustness testing would not be practical or efficient for any IMS, VoIP or Triple Play environment.
- **Soft-fault Characterization/Documentation:** While robustness testing solutions only detect hard crashes, negative testing has been very capable of finding and isolating hard faults (e.g., crashes), service availability and degradation is just as critical to MSOs and our customers. For example, a normally benign event such as a CPU utilization spike or memory leak can have disastrous consequences on a VoIP infrastructure device. Security Analysis isolates and documents these "soft faults," and records response-time (latency) for critical service availability through the analysis.
- **Information Sharing:** Robustness testing system fault reports are designed to be actionable in the business environment. A fault report indicating that one out of thousands of attacks caused a service to crash at some point in time is not useful and, unfortunately, that is where most robustness testing tools stop. In contrast, mobile operators quickly benefit from a clearly documented robustness analysis that fully automates the verification and isolation process, captures critical details from the DUT during the fault event or crash, and provides actionable remediation tools including packet captures (PCAPs) and Linux-based software replays of the

entire weakness or fault. By rapid and broad sharing of key documented insights and best practices via XML templates, many non-experts benefit from the knowledge of a single expert.

- Regressions: Without accurate tracking of key findings, it would be very difficult to eliminate the risk of a robustness issue regressing back into a vendor's protocol implementation and the IMS deployment environment. Service Provider engineering teams would spend many hours manually tracking and storing key fault details, software updates, test case updates, and analysis results. It is necessary for robustness testing to address this by providing a built-in version control system to track updates to its test cases and enable one-click regression/verification tests.
- Service Availability: Just as important as uncovering hard faults (i.e., crashes), is tracking the availability and responsiveness of the device under test. It has been observed that even non-load attacks affect the responsiveness of a DUT. For real-time architectures like IMS, this is just as important to measure as hard crashes.

To ensure network service reliability, the component IMS products must keep running even when conditions aren't perfect—more often than usually noticed. Any test tool that will do a credible job of characterizing the behavior of a target device must be comprehensively covering the space of potential negative test cases. As the product's attack surface is mapped, it is important to do more than just observe the absence of negative results. If we want to see how the target reacts when exposed to extremely toxic traffic, users can also measure how well it continues to handle the traffic customers are paying for. Robustness testing ensures providers plan for the unexpected.

#### 4. Which IMS protocol implementations should be tested? Why?

The 3GPP/TISPAN IMS network architecture has no shortage of functional components or standardized interfaces between those functions. It is precisely these interfaces between the different functions that we are interested in here, as it is the sum of these interfaces that form the attack surface of the IMS Network.

Traditionally, service providers and larger enterprises assumed denial of service resulted from large quantities of packets being continuously presented to a device. Those packets may attack a protocol specifically, or seek to overwhelm a device overall with traffic. The net result is that the device becomes unavailable, or a Denial of Service (DoS) occurs.

However, denial of service also results from the attack of a device with relatively low quantities of malicious packets. Single path architectures, such as security devices, where all packets are handled through a common processing task, are vulnerable to spending excessive amount of processing cycles on malformed packets. Complex IMS product and resulting service architectures, where control and exception packets are handled differently than data packets, are susceptible to malicious packets compromising the ability to process more important control traffic, such as routing updates. Vendors who focus on feature and performance testing frequently leave unexplored the ability of the system to properly deal with the impact of low throughput denial on service attacks.

The attack surface consists of the set of interfaces into a system or network that an adversary can use to disrupt service or gain unauthorized access to. The larger the attack surface, the more opportunities an attacker has to wreak havoc. Minimizing and measuring a target's attack surface is an active area of research and discussion (by CMU, Microsoft, and others). For our purposes, we are assuming a given set of protocols/interfaces as defined by the IMS architecture, and are not considering how to reduce the attack surface. In addition to considering interfaces exposed externally by an IMS core network, we also consider internal interfaces. Attacks not only originate from insiders, but also from outsiders becoming insiders by exploiting (known or previously unknown) vulnerabilities to externally visible interfaces to gain unauthorized access to the internal network elements.

The IMS network can be broken down into a number of layers: the transport layer, the core IMS (or control) layer and the service/applications layer. (The access network is not considered here, although it is just as important to test the attack surface of such network elements.)

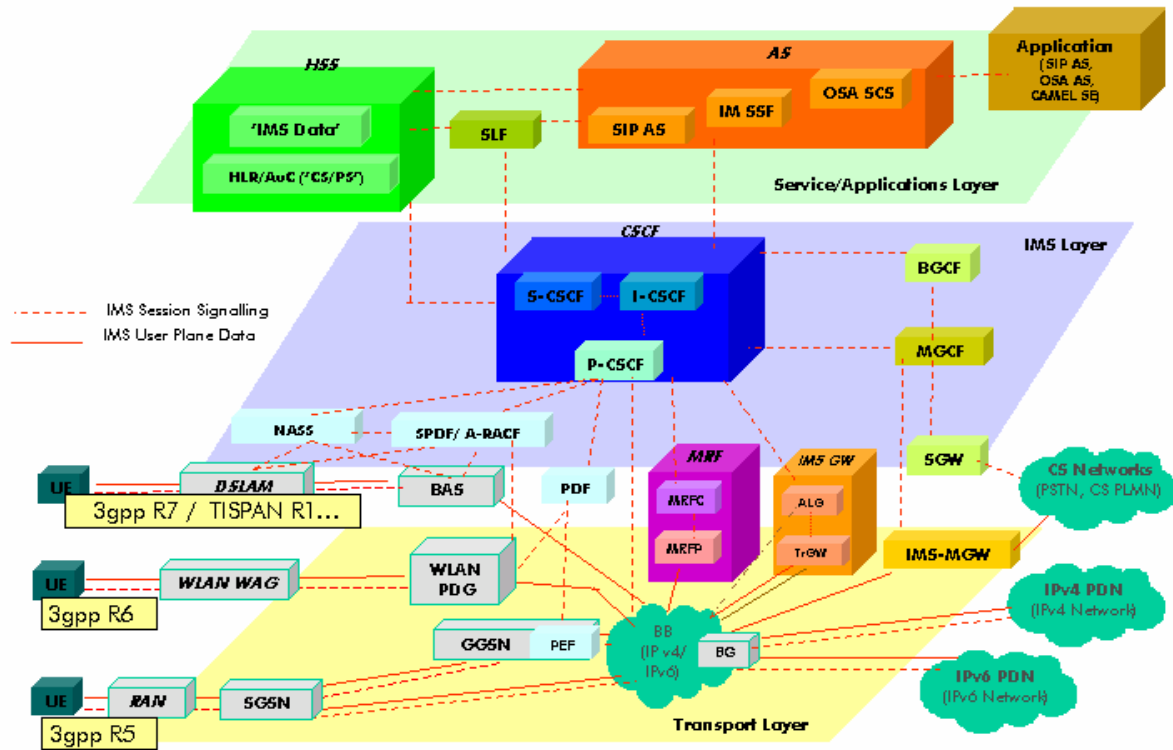
The transport layer covers the standard L2-L5 protocols that will be supported by most devices, and are solely used to transport/encapsulate high-level protocol messages. These are certainly part of the attack surface, and need robustness and negative testing. This includes IPv4, IPv6, ICMP, ICMPv6, UDP, and TCP. In addition, some of the IMS functional components also support and need testing for SCTP, IKE, IPSEC, and TLS. It is easy for IMS equipment vendors to discount or forget this category since they may not have developed these protocols. However, that would be a mistake as new vulnerabilities are still uncovered in these areas. Since each device in the network could have a different implementation of a given protocol, or even the same implementation but on different machine architecture (i.e., MIPS processor versus Intel), or a different Operating System, this implies that each protocol should be tested against each device it is present on.

Next comes the control layer, or the IMS core. This layer has the call/session control servers and proxies at its core (aka P-CSCF, S-CSCF, and I-CSCF), surrounded by ancillary control providing other functions such as BGCF, MGCF, MRFC, \*GW, etc. This layer performs basic services and control such as authenticating users, routing/load-balancing calls, policy enforcement, generate charging records, passing calls on to the appropriate servers for higher level services (i.e., in the service/application layer), topology hiding, etc. This layer is dominated by the SIP protocol for signaling and Diameter for interfacing with permanent stores (such as authentication info, user profiles, and the like). It also generates offline charging records. SIP (and any application protocol) should be tested separately over each transport the protocol supports, namely UDP, TCP, SSL/TLS, SCTP, and allover IPv4 and IPv6; not only do the different transports exercise different code in the transport/application, but some vulnerabilities target protocols over specific transports.

The service/application layer hosts and executes higher level services via application servers (AS). The S-CSCF in the core layer figures out the services to be applied to a call/transaction, and interfaces with the appropriate set of AS server(s) using the SIP protocol. Examples of such application services include third party call control (3PCC), instant messaging, conference calling, call waiting, busy call ring-back, presence, news push services, sponsored call, automatic conference call setup and phone calls at predefined times, voice mail, location based services, push-to-talk, group management, voice call continuity (as a mobile phone moves between circuit switched and packet switched radio domains), sending accounting info to charging functions, and others. Protocols involved in this application layer includes SIP (key for interaction between the S-CSCF in the control layer and the AS functions), and CAMEL Application Part (CAP) signaling protocol and OSA API (from AS to Camel Service Environment and OSA AS respectively) for non-SIP based services such as legacy services. An AS can also use the Mobile Application Part (MAP) protocol for providing services to mobile phone users via GSM/UMTS/GPRS access core networks. In addition, OSA/Parlay X web services (over SOAP via HTTP/HTTPS) can be used to enable web service application developers to make use of network functionality (for call control, conferencing, user interaction, charging, 3PCC, SMS and terminal location, etc.).

Parallel to the above three layers is the media layer. Devices and sets of protocols involved in transferring actual audio/video media between endpoints. Unique to IMS implementations, robustness analysis and testing should include the protocols that encapsulate and transport the digitally encoded audio and video, including RTP, RTCP, SRTP, and SRTCP. In addition, the actual codec used to digitally encode the audio and video are also part of the attack surface that should be included in testing; this includes both sampled and framed codecs.

Not to be forgotten are a number of other miscellaneous protocols supported in a number of the devices across all IMS layers. This is why it is important for service-specific test coverage in multi-service IMS networks. There may be any number of services that these devices support, for which a tool (such as freely available nmap) could be used to expose which IMS services are enabled on each of the devices. Each such exposed IMS service component is part of the attack surface and, as such, needs unique reliability and robustness negative testing performed upon it. A network is only as secure as its weakest link. And the complexity of many IMS multi-service products and service offerings requires dynamic negative testing attack suites to cleanly isolate and document these areas of potential attack surface coverage weaknesses like Diameter or IKEv2.



**Figure 4: IMS Architecture User, Control and Application Planes**  
**All Subject to Robustness Weaknesses**

*Source: Wikipedia<sup>4</sup>*

Many IMS products are complex systems, often leveraging unrelated protocols that open up attack surfaces— analogous to a car having a flat tire though nothing is wrong with the actual car mechanics. Attack surfaces already seen in IMS products include SNMP (v1, v2c, v3) as it is frequently used for network and device management. Link Layer Discovery Protocol (LLDP) is found in IMS products for device discovery. Telnet, SSH, HTTP/HTTPS, and FTP is present in IMS systems for remote access and management. Routing protocols are often part of IMS products including RIP, OSPF, IS-IS, and BGP used for routing within and between domains. And many more...

<sup>4</sup> Wikipedia IMS Page [http://en.wikipedia.org/wiki/IP\\_Multimedia\\_Subsystem](http://en.wikipedia.org/wiki/IP_Multimedia_Subsystem)

Reference/ Interface Point	Involved Entities	Protocol
Cr	MRFC, AS	HTTP, SCTP
Cx	I-CSCF, S-CSCF, HSS	Diameter
Dh	SIP AS, OSA, SCF, IM-SSF, HSS	Diameter
Dx	I-CSCF, S-CSCF, SLF	Diameter
Gm	UE, P-CSCF	SIP, IKE, IPSEC, TLS
Go	PDF, GGSN	COPS (Rel 5), Diameter (Rel6+)
Gq	P-CSCF, PDF	Diameter
ISC	S-CSCF, I-CSCF, AS	SIP
Ma	I-CSCF, AS	SIP
Mg, Mi, Mj, Mk	MGCF, I-CSCF, S-CSCF, BGCF	SIP
Mm	IBCF, I-CSCF, S-CSCF, any other IP device in IMS core	SIP, H248, IKE, IPSEC, TLS, HTTP
Mn	MGCF, IMS-MGW	H248
Mp	MRFC, MRFP	H248
Mr	S-CSCF, MRFC	SIP
Mw	P-CSCF, I-CSCF, S-CSCF	SIP (as used to interface with external IMS networks)
Sh	SIP AS, OSA SCS, HSS	Diameter
Si	IM-SSF, HSS	MAP
Sr	MRFC, AS	HTTP
Ut	UE, AS	(SIP AS, OSA SCS, HTTP, HTTPS, TLS IM-SSF)
Most	Most	ARP, IPv4, IPv6, UDP, TCP, ICMP, ICMPv6
Misc.	Misc.	RTP, RTCP, SRTP, SRTCP, LLDP, SNMP, SSH, TelNet, HTTP/HTTPS, SSL/TLS
AS interfaces	SCS, IM-SSF, IP	CAMEL Application Part (CAP), Open Service Architecture (OSA) API, (same as Ut for Parlay X), Mobile Application Part (MAP), OSA/Parlay X Web Services

*Note that all attacks are supported over a diverse set of transport protocols  
where applicable: IPv4, IPv6, UDP, TCP and TLS.*

**Figure 5: Protocols that require Robustness Testing**

## 5. Conclusions

Several IMS Forum members are now leveraging IMS robustness analysis. As evidenced by the superior economics of finding product weaknesses prior to development, these fellow IMS Forum members are actively improving their product quality in addition to reducing downtime in any service provider customer application deployment.

IMS users benefit with maximum product and application uptime and reduced downtime cost savings. In fact, many of the largest Tier 1 service providers and cable operators are automating their product deployments, selection and upgrades through specified negative testing to analyze potential system flaws and weaknesses. Protocol mutations, directed against any products that implemented a specific protocol, can cause systems using it to perform poorly and/or crash. Negative testing systems, their protocol mutations and documentation suite, are not your average scanner, nor are they penetration tools. Instead, this approach performs a full range of vulnerability analyses on everything from a firewall to an IMS Soft Switch element, represented by the Media Gateway Controller (MGC) element, to a piece of VoIP software. In a nutshell, the testing system performs a wide variety of vulnerability tests from simple scans to protocol mutations.

Protocol mutations are everything from malformed packets to dangerous payloads to state-machine violations and beyond. The analyzer's application of dynamically-generated protocol mutations tells you quickly and positively how your IMS system will behave under a wide variety of attacks and security-related failures or errors. If the protocol mutations provided (and updated periodically) are not enough for you, write your own. And, if the system under analysis crashes as a result of the testing, the analyzer will restart it automatically and resume testing. So, if the software is not implementing the protocol correctly—and, by extension, may be subject to exploitation—you'll know it.

The relatively new nature of IMS development and deployment immediately benefits through the elimination of mobile operator service downtime including malicious zero-day exploits. As carrier networks have become more essential to the operation of businesses worldwide, they are becoming more complex. Many service providers interviewed in a recent NSP Partners study found themselves facing unacceptable levels of downtime or customer churn due to network robustness issues. These participants found that integrating product robustness analysis to discover and eliminate weaknesses and vulnerabilities reduces downtime and customer churn. In fact, NSP analyst Peter Fetterolf found that, in more than one instance, participants noted that the integration of robustness negative analysis into deployment and development processes paid for itself in less than one month by reducing customer churn or field fire drills.

With sophisticated, mission critical testing to do on a large scale network, IMS developers are finding that the old paradigms of running a scanner and calling it a day are gone. The primary business risk associated with a robustness testing solution is to not move forward with the deployment. If IMS-based service providers fail to act now, they will experience unplanned downtime, customer churn and continue to operate without the knowledge of where the most likely service-affecting robustness issues exist in our environment. Meanwhile, competing MSOs and carriers who do leverage security analyzers will enjoy the benefits of a thoroughly tested and highly robust operating environment with reduced customer downtime or service latency issues. A single outage of a critical IMS-based customer-facing service will dramatically outweigh the costs associated with acquiring and deploying a Security Analyzer system. Customers have zero tolerance for poor-quality VoIP or triple play services, and it is very difficult and costly to regain a lost customer.

## 6. Glossary

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
API	Application Program Interface
AS	Application Server
ARIB	Association of Radio Industries and Businesses (ARIB)
ATIS	Alliance for Telecommunications Industry Solutions
AVP	Attribute-Value Pair
CAMEL	Customized Application Mobile Enhanced Logic
CCSA	China Communications Standards Association (CCSA)
CDF	Charging Data Feature
CN	Core Network
COPS	(Common Open Policy Service)– RFC 2748
CS	Circuit Switched
CSCF	Call Session Control Function
Cx	Diameter interface for interactions between HSS and CSCF
DIAMETER	Successor to RADIUS – RFC 3588 – Need for Mobile IP
DSL	Digital Subscriber Line
ETSI	European Telecommunications Standards Institute
FMC	Fixed/Mobile Convergence
FTTH	Fiber to the Home
GSM	Global System for Mobile Communications
HSS	Home Subscriber Server
I-CSCF	Interrogating Call Session Control Function
IPSec	IP Security Protocol
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem

IP	Internet Protocol
MGCF	Media Gateway Control Function
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
MSF	MultiService Forum
NAT	Network Address Translation
OSA	Open Services Architecture
PRACK	Provision Response Acknowledgement (SIP Message)
P-CSCF	Proxy-Call Session Control Function
PSTN	Public Switched Telephone Network
PDF	Policy Description Function
QoS	Quality of Service
RADIUS	RFC 2865 – Remote Authentication Dial In User Service
SBC	Session Border Controller
SCS	Service Capability Server
S-CSCF	Serving-Call Session Control Function
SEG	Security Gateway
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
Sh	User profile interface between HSS and AS
TTA	Telecommunications Technology Association (TTA)
TTC	Telecommunication Technology Committee
UE	User Equipment (IMS Terminal)
VCC	Voice Call Continuity
WIFI	Wireless Fidelity (IEEE 802.11)
WI-MAX	Worldwide Interoperability for Microwave Access, Inc (IEEE 802.16)
XCAP	XML Configuration Access Protocol