



***Building Reliable, Available and Secure Service Provider
IMS Networks***

February 4, 2008

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.

IMS Forum Contact Information:

IMS Forum Headquarters
211 Summit Place #292
Box 10,000
Silverthorne, Colorado 80498
USA
www.IMSForum.org
Email: 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.

Thank you,

Michael Khalilian
Chairman & President
IMS Forum
Mkhalilian@IMSForum.org

Contributors

The IMS Forum would like to thank the following contributors:

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

Adam Stein, Vice President of Mu Security, Inc.

Mu-info@musecurity.com

About Mu Security:

Mu Security 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 Security 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.musecurity.com>

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 study¹ 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.

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

2. 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.

3. 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