

Plugged In: The Newsletter of IMS Interoperability & Certification



Securing IMS Networks and Infrastructure Products with Adam P. Stein, Mu Dynamics

IMS Forum Newsletter: What are some areas of IMS where you have found challenges for operators?

Adam P. Stein: For one of our Tier 1 service-provider customers, a cable operator, we worked with them to qualify a number of IMS products about to be deployed in their IMS core. One of them was SIP gateway using the DIAMETER protocol. With the gateway vendor's DIAMETER implementation the customer found numerous problems that would cause both costly downtime and customer churn. The gateway, when subjected to unanticipated input from the protocol-fuzzing engine, rolled over and the OSS billing database was completely exposed.

The issues Mu discovers are not just services going down or latency, but the core security of the service of the network behind it. If network elements and information are no longer protected, you probably want to know about it.

Mu offers more than 50 different protocol modules including a SIP-mutation module. Our SIP suite subjects a product under analysis to everything from buffer overflows to memory leaks to CPU utilization spikes to performance degradation and ultimately latency issues. Each incorrect response is monitored by the Mu appliance and documented, so they can be quickly fixed.

IMS: Are there any special IMS challenges or advantages?

AS: Yes. We see operators using IMS to provision a large number of services centrally that in the past have been deployed separately. That is a huge advantage for service providers to deploy multiple services over one architecture. IMS lowers operation costs and allows them to offer more services using less capital. IMS is a platform for provisioning many services concurrently at a lower cost.

The challenge that goes with that is how to make sure that it is practicable to avoid any downtime issues because of the reliability and security of those services. That's because now, it is not just one service that might be going down with IMS, but many.

IMS: I have heard of situations, such as codec incompatibilities, that can be very sensitive

AS: Yes. An operator may have tested something during purchase, but every network's fingerprint is unique. Operators using a Mu system for service-assurance testing may find a particular codec's latency is unacceptable compared to specifications promised by a vendor's data sheet. Until the operator tests a vendor-specific implementation against their network setting, they simply won't know.

With Mu you can analyze structured communication schema using the protocol-fuzzing engine. It provides an automated and repeatable process to ensure maximum IMS service availability.

It is even more applicable to operators and their network vendors. Codecs are one type of application, but, where Mu really shines is on the protocol side. Whether an operator is working on products in the IMS core or service layers, our approach offers comprehensive analysis. For example, in an IMS core operators can ensure the reliability of their SIP servers or in the service layer make sure their application servers are secure. Mu helps operators detail the interconnected and dependent layers of their IMS architecture.

IMS: Will service providers offer multiple services themselves or just enable them?

AS: What we are seeing is that IMS offers application options. In the Bay Area where I live, there are many wireless service provider choices, but there are only two providers that offer triple-play services. In Europe or Asia, in contrast, it is a horn of plenty of triple- or quad-play services from multiple providers. When there are more than two, the duopoly is gone, and pricing and the variety of applications multiply. You can get all your services from one operator or you can pick what think are the best of breed from different vendors and aggregate them yourself. But, the service provider ultimately gets more choice of applications with real-time IP services.

IMS: Tell me about your products, especially what is Mu's "Security Analyzer and integrated fuzzer engine" system?

AS: Mu today offers an appliance that includes a protocol-fuzzing engine. It generates so-called "unanticipated input." When vendors develop a product for IMS networks, their network-operator customers want to know how it responds to unanticipated input to minimize revenue loss from downtime and customer churn. Any unexpected weaknesses, not only to malicious input, but also if some product feature malfunctions might cause the operator's network to go down.

Many operator network outages, whether caused by misconfigured products or even power failures, can be discovered in an IMS environment. If a product is going to be fragile, you want to identify the root cause behind it going down hard, or, in

latency-sensitive applications such as VoIP, what is affecting user quality. The Mu system automates the ability to pinpoint and document these issues ahead of time.

IMS: How are you different from a session border controller?

AS: Mu has SBC vendors as customers. SBC vendors use Mu to validate that they are reliable and secure against malicious and unexpected traffic. For example, dropping a SIP phone and flooding the network with SIP INVITEs. One Mu product module covers protocol mutations, a second contains more than 1,000 known vulnerabilities, another focuses on software as a service and others will deal with issues, such as denial-of-service (DoS) attacks. Operators and their suppliers use Mu to protect their assets from the unexpected traffic, a perfect storm. Understanding how your network and unique product setting respond is critical, because measuring sheer performance or throughput is increasingly meaningless.

Having the opportunity to work with IMS vendors is a primary reason behind Mu's continued involvement in IMS plugfests. Moving beyond interconnectivity and interoperability is critical for IMS deployment success.

To this end, we just finished working with the IMS Forum on publishing a new white paper ("[Building Reliable, Available and Secure Service Provider IMS Networks](#)") to discuss the baseline required for reliable and secure service-provider networks. How should IMS product deployment and development life cycle be made more secure? What factors should operators and vendors consider and what things they have to reference, such as SBCs, when thinking about reliability.

IMS: Many operators and vendors are concerned about whether malware would overwhelm their networks.

AS: We look at everything from layer 2 to layer 7 with our stateful and dynamic analysis, as well as the IMS control plane and also the transport layer. This is important as many vendors, when building high-quality products, don't adequately separate out the control plane, the data (application) plane and the transport plane. This makes malformed traffic, intentional or innocent, extremely damaging to product resiliency and network uptime.

AT&T and Verizon offer quad plays in the United States and so does Comcast. So actually we are seeing the start of more competition opportunities, and all can be provisioned off an IMS architecture. It has to be reliable, though, or the potential for revenue loss also multiplies. Rather than running three networks, operators use one and realize lower operation costs - but offer the same reliability or better. Mu is valuable here to ensure the operator's network is not adversely affected due to reliability, availability or security weaknesses that often arrive in unexpected traffic. We can measure their service assurance risks and baseline it. When we baseline it, operators compare real life benchmarking in their labs. They can also compare product A to C before purchasing - we have a few customers doing that today.

We work with more than one-third of major service providers today. And that is unique, for a company this size--just 52 people--to serve this many customers in just two years time. And we serve numerous IP service product vendor customers too in Asia, Europe and North America.

Using Mu, a service provider accurately works with a vendor to "trust, but verify" products before deployment in their network. Operators use a security analysis system eliminating the need for vendors to recreate their problems in QA two months later. Mu documents the problem so vendors have an actionable set of information about what went wrong, and what needs be fixed.

Manufacturers use Mu products throughout their secure development life cycle (SDLC) and integrate it into their field development schedule. This is far more cost effective than fixing a reported problem in the middle of a deployment (NIST and NSP Partners state such changes can be 10 times more expensive). A customer might buy another session border controller because it costs too much to get yours fixed and the competitor's product is higher quality.

If a service provider is deploying multiple services on an IMS platform, they want to be sure, like the mainframes in the 1970s, that it has the highest reliability, availability and security. That is what we call service assurance.

IMS: Service assurance is the key?

AS: Yes. With new technology, like IMS, operators want to know costly downtime or customer churn is avoided. The NSP study on TCO/ROI of Security Analysis details this issue. An outage can cost hundreds of thousands per hour, not to mention the customer churn issue. IMS is a great technology, but it is also a service that has to run at the highest possible availability. If that architecture is down or there are latency issues, operators have, not only the cost of the downtime, but there is the cost of customer churn. Mu helps prevent unforeseen issues from adversely impacting the operator.

***Adam Stein**, vice president of marketing at Mu Dynamics Inc., has more than 20 years of marketing expertise focused on hardware for networking and security, software and silicon. He previously led global marketing programs at UTM network security innovator Fortinet. Stein also has led outbound marketing for Cisco Systems Inc., Juniper Networks Inc., Broadcom Corp. and Foundry Networks Inc. Stein has a M.A. in Marketing from Emerson College and B.A. in Sciences from the University of Colorado at Boulder.*