



Contact:  
Kevin Gallagher  
Gallagher Group Communications  
925-831-1041  
[kevin@gg-comm.com](mailto:kevin@gg-comm.com)

## **WEST COAST LABS DEMONSTRATES MU SECURITY LEADERSHIP IN STATEFUL FUZZING & NEGATIVE TESTING**

### **Mu-4000 Commercial Fuzzing Engine Demonstrates Superior Depth, Fault Count, and Fault Severity Advantage Uses Popular SIP Implementation in Asterisk® PBX Baseline**

**Sunnyvale, CA – February 20, 2008** – Mu Security, a pioneer in the new security analyzer market, today announced the completion of a six-month West Coast Labs (WCL) independent report and hands-on commercially-available fuzzer engine comparison documenting [Mu-4000](#) industry leadership. WCL found Mu’s appliance offers superior negative testing effectiveness that helps [VoIP service providers](#) and their [suppliers](#) detect and remediate vulnerabilities and product weaknesses that would otherwise result in costly downtime or customer churn. Moreover, WCL found that negative testing demonstrates sufficient maturity for mainstream use by carriers, enterprises, and anyone deploying mission-critical IP-based services like VoIP and SOA.

[Download WCL’s Product Test Report, “Mu-4000 Security Analyzer: Reliability, Availability and Security \(including Negative\) Testing Study” by clicking here.](#)

WCL created, documented and implemented this repeatable negative testing baseline of protocol fuzzing engines using comparisons in actual testing of real target protocol implementations to compare results for various negative testing tools. Mu commissioned WCL to develop and publish the methodology so any service provider, carrier, cable operator or network product vendor can independently replicate the test bed and findings first-hand. During the report, WCL demonstrated Mu’s superior depth of protocol coverage for the emerging [Voice over IP protocol \(VoIP\), Session Initiation Protocol](#)

[\(SIP\)](#), which was chosen for this evaluation due to its complexity, number of faults found, and severity of those faults.

“West Coast Labs found the Mu-4000 appliance demonstrated superior results in our industry-first Negative Testing benchmark, and moreover showed clear leadership in ease-of-installation and ease-of-use,” said Chris Thomas, operations director, West Coast Labs, based in Cardiff, UK. “Our goal was simply to define a consistent evaluation methodology that Service Providers and their suppliers could replicate for their own selection of negative test and protocol fuzzing tools.”

### **VoIP Applications Selected Due to Wide Deployment, Increasing Service Revenues**

WCL’s benchmark methodology is applicable to any of [Mu’s 50-plus protocols](#). To create an interesting and meaningful comparison, Mu asked WCL to evaluate a complex stateful application like VoIP requiring hundreds of thousands, or millions, of dynamically-created test cases. For [VoIP and IMS, SIP](#) is increasingly commonly deployed and its complexity means that it must be thoroughly tested before providers depend on it for high-growth revenue generating service offerings. Many global service providers and suppliers currently leverage multiple open source negative testing products for SIP – often these are static or unsupported hand-built packages created during the last five years.

Once SIP was selected, a suitable and commonly-deployed open-source target was needed. [Asterisk VoIP servers](#) provide a very popular SIP implementation—a so-called “soft PBX.” Asterisk implements many SIP “methods” essential for complex and stateful call processing. The Mu-4000 appliance’s SIP protocol attack suite matched Asterisk’s SIP code complexity shining a spotlight into the many different dark corners of the code. Asterisk also offers significant configuration flexibility for testing many different real-world scenarios.

WCL’s test bed using a complex Asterisk configuration offered maximum possible exposure of the protocol fuzzing engine’s attack vectors for commercial negative testing

tools. This comparison ensured identical Asterisk configurations for each test to ensure results could be meaningfully compared, and to ensure repeatability.

### **Metric Baseline of Results Demonstrates Mu Leadership**

Final results of the WCL benchmark clearly demonstrate that code coverage by itself was less useful as a comparative metric than originally thought. Code coverage is not a complete metric by itself because if two different test tools each measure 40 percent code coverage, users are simply unable to prove coverage of the same 40 percent or how much of that 40 percent overlapped.

As a result, WCL identified objective, relevant tiebreakers. For instance: How many faults (crashes) does the negative test suite isolate and document? How severe are these product weaknesses or faults? Severity and Quantity are a minimum set of comparison criteria for commercial protocol fuzzing engines that must be used alongside depth (code coverage).

“We are pleased that West Coast Labs built a reproducible and insightful comparison to aid businesses in their selection of commercially-available negative testing systems,” said Adam Stein, vice president marketing, Mu Security. “This benchmark is especially helpful to any Service Provider or developer building SIP-based VoIP or IP Multimedia Subsystems (IMS) applications including mobile network operators. In less than two years time, Mu has demonstrated SIP negative testing superiority in a scientifically designed, open test process that validates the firm’s Protocol Spidering™ methodology at the heart of the Mu-4000’s protocol analysis engine.”

### **About West Coast Labs**

West Coast Labs is one of the world's leading independent test facilities providing a range of technical services for testing a range of technologies including UTM, Malware - including Anti-Virus, Trojan, Worms, Exploits and Spyware - Spam, URL, Web and Email Filtering, Firewall, VPN, IDS, IPS and IPD.

## **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 has 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>.

###