



Contact:
Kevin Gallagher
Gallagher Group Communications
925.831-1041
kevin@gg-comm.com

MU SECURITY ROLLS OUT NEXT-GENERATION SECURITY ANALYZER, DELIVERING STRONG ROI FOR SERVICE PROVIDERS AND VENDORS

Cox Communications and Redback Extend Analysis Use Cases

Sunnyvale, Calif. – November 5, 2007 – Mu Security, the leader in network security analysis systems, today announced a major new release of its flagship Mu-4000 Security Analyzer appliance. The Mu-4000 improves the reliability and uptime of networked products and IP business services by proactively addressing robustness and resiliency factors before systems are deployed in production environments. As a result, Mu Security’s growing service provider customer base is avoiding service outages and reducing customer churn.

“In order to provide our customers with the highest quality service and reliability, we use the Mu-4000 to ensure the equipment deployed on our network is thoroughly tested prior to placing it into production,” said Paul Farley, director of network intelligence & security engineering at Cox Communications. “Using the Mu-4000 to run virtually every conceivable testing scenario helps us live up to our customers’ expectations as their trusted provider of voice, video, data and wireless services.”

“The reactive spending on perimeter security or managed services has not been effective as network downtime and vulnerabilities continue to grow,” says Analyst Mike Monticello at Enterprise Management Associates. “That's why Mu Security's solution is becoming indispensable to users who want to methodically identify the root causes of robustness shortcomings or deep-seated vulnerabilities lurking within any IP-based product or service.”

What's New in Version 3

Mu Security's third-generation solution maximizes customer ROI with new features including sharable analysis templates, interactive graphical response time charting and dynamic stateful protocol fuzzing as the basis for robustness analysis.

Sharable Analysis Templates Enable Knowledge Sharing and Best Practices

With the introduction of Sharable Analysis Templates, Mu Security is establishing strategic best practices for system testing across organizations. Organizations often find it very difficult to add security metrics or repeatable processes across groups. Typically, only a small, specialized incident response group within a company has security expertise, whereas the larger product certification/testing group often lacks sufficient security knowledge to test for product robustness.

Mu Security's Mu-4000 platform now supports customizable analysis templates that easily transfer between Mu-4000 appliances to help disseminate scarce security knowledge within organizations. By capturing best practices that can be replicated, the new Mu-4000 is greatly simplifying robustness testing, and thereby enabling a repeatable security process as a key competitive differentiator for Mu's customers.

"As a leading provider of products used in the world's largest triple-play networks, Redback assures its carrier customers the highest levels of security for critical applications that require robust performance," said Rod Couvrey, vice president of software engineering at Redback. "Mu Security and their innovative Mu-4000 appliance help ensure that the Redback software engineering team leverages security analysis as a best practice to identify and remediate possible product vulnerabilities or quality issues as early as possible in our development lifecycle."

Response Time Chart Exposes Hot Spots

Latency-sensitive applications unable to process valid data in specific timeframes may not meet response-time goals or service level agreements. Legacy fuzzing tools have never before attempted to measure a target system's ability to process valid traffic while being probed by invalid traffic.

With Response Time Charts, the updated Mu-4000 interactively exposes quality and availability issues to accelerate remediation. Customers can actively gauge a system's ability to maintain control and specific performance levels while processing unexpected inputs. In addition to hard failures (e.g., system crashes), users can now isolate hard-to-detect “soft faults” including memory leaks, CPU utilization spikes and rising latency levels to help service providers maintain SLAs by avoiding costly downtime.

Dynamic Stateful Fuzzing Ensures Deeper Attack Surface Coverage

Most static fuzzers tend to focus only on the protocol specification without any regard to how the target's implemented or deployed. This approach tends to have a least-common-denominator effect, making many static attack vectors irrelevant in the real world.

The new Dynamic Stateful Fuzzing engine overcomes these major limitations by first accessing the target system to map out the target's exact capabilities. After this step, the engine computes a set of attack vectors tailored to the target, and then dynamically executes them. The result is much deeper attack surface coverage with more vulnerabilities being uncovered.

Furthermore, this is the only solution to support user-defined protocol extensions, allowing customers to use their Mu-4000 to dynamically construct attack vectors over and beyond what Mu provides out-of-the-box.

Many protocols have multi-packet exchanges, like HTTP or SIP dialogs. The only way to get deep coverage of the protocol implementation is to exercise it in all its valid and invalid states. Only the Mu-4000's dynamic stateful fuzzing engine can deliver structurally and semantically invalid attacks in all the relevant states of stateful protocols. These attacks include valid packets sent at the wrong time, or packets that are never valid, but are designed to cause damage to the code that implements the protocol's state machine(s). This latest Mu-4000 provides deeper and broader attack surface coverage, and enables customers to significantly reduce service-impacting vulnerabilities.

The updated Mu-4000 feature set is available immediately at no additional cost to existing support customers worldwide.

About Mu Security

Mu Security offers a market-leading security analysis system, delivering a rigorous and streamlined methodology for verifying the robustness and security readiness of any IP-based product or application. Founded by pioneers of intrusion detection and prevention technology, Mu Security is backed by preeminent venture capital firms including Accel Partners, Benchmark Capital and DAG Ventures. The company is headquartered in Sunnyvale, CA. For more information, visit the company's website at <http://www.musecurity.com>.

###