

Mu-4000 DATASHEET

Mu Security is pioneering the product category of Security Analyzers, whose purpose is to reverse the growth of vulnerabilities in all networked hardware and software applications. Security Analyzers enable a thorough and proactive scrutiny of systems for known and previously undetected security flaws, resulting in the reduction of vulnerabilities and therefore exploits. Security Analyzers accomplish this in an efficient and repeatable manner, identifying product vulnerabilities to be eliminated prior to deployment – without requiring access to product source code. The net result of the Security Analyzer system and process is to increase product security.

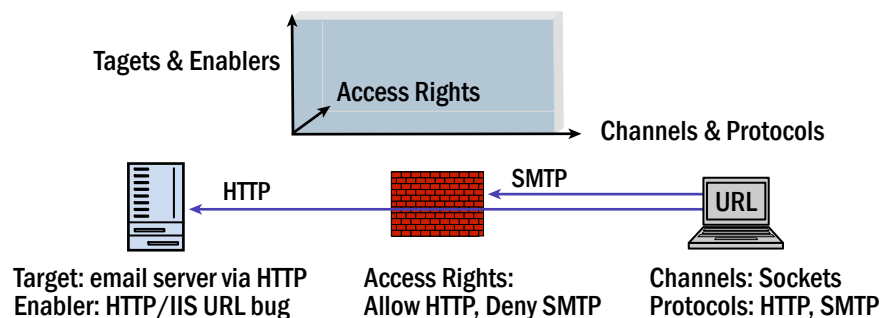
The Mu-4000 is the industry's first Security Analyzer that allows for a systematic and comprehensive analysis of the security of any networked device or application. By identifying known and unknown vulnerabilities, it establishes itself as the security litmus test for any IP-based device or networked application.

The Mu-4000 Security Analyzer subjects the target under analysis to a very large numbers of attacks (mutations), closely monitors and captures the state of the target under analysis, and presents the results of an analysis in a useful actionable way. When used by a service provider or enterprise, the Mu-4000 Security Analyzer helps to immediately identify vulnerabilities in a precise and reproducible manner, and guides the developer to rapidly fix the vulnerabilities uncovered. When used by an enterprise customer, the Mu-4000 Security Analyzer allows the IT staff to measure security vulnerabilities for their specific configuration. The ability to provide vendors with specific, actionable vulnerability details results in quicker vulnerability remediation with the device or application vendor.

Attack Surface Analysis

Network and application protocols have complex design and implementation dependencies that create more opportunities for exploitation. The attack surface approach methodically characterizes the “attackability” of a networked application or device. There are three dimensions that model the attack surface (see figure 1). There are “targets and enablers” that provide admittance according to “access rights” via a set of “channels and protocols.” For more information about attack surface, please see: <http://www.cs.cmu.edu/~pratyus/as.html>.

Figure 1. THREE VECTORS DETERMINE THE RISK OF A VULNERABILITY



SYSTEMATIC ASSESSMENT

As part of your development process, is there a method by which you can comprehensively and systematically assess the security quality of your product?

If the answer is no, consider the use of a Security Analyzer as part of your product development and/or vendor selection and deployment processes.



The Mu-4000 Security Analyzer uses Attack Surface Analysis to identify a target's vulnerabilities by exercising only the relevant portions of code with no platform or programming dependencies. According to Secunia, protocol abuse represents over 80% of vulnerabilities (http://secunia.com/advisory_statistics/).

Mu Security has invented an approach to resolving protocol vulnerabilities through the constructive use of hacking techniques. This approach is called Protocol Spidering™ and it offers a thorough and methodical analysis of the complex inter-dependencies that exist among any and all protocols being attacked. Embedding such capabilities within a platform approach allows such analysis to be comprehensive, efficient, and repeatable.

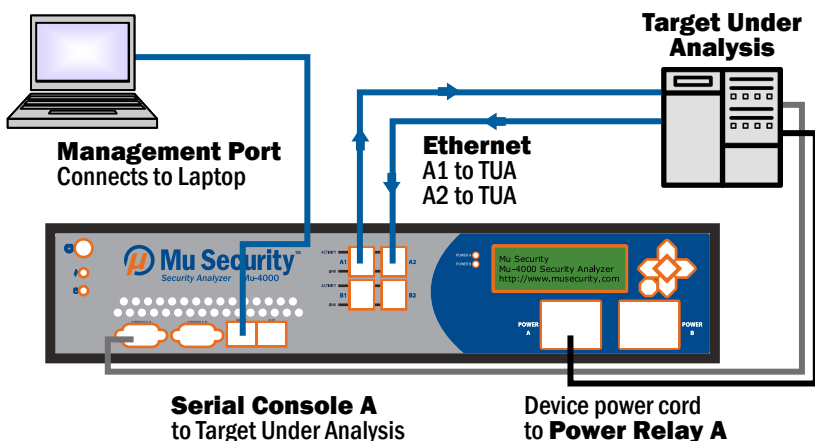
Vulnerabilities and Exploits

Hackers generate exploits by identifying vulnerabilities in their targets. Finding a vulnerability is a prerequisite for creating an exploit. By identifying both known and unknown vulnerabilities early and eliminating them, the security of the device or application is greatly increased. Further, given that most exploits are derivative in nature, the Mu-4000 Security Analyzer provides a way to methodically test many thousands of attack variations derived from a single vulnerability.

Accountability through Proactive and Measurable Security

By incorporating the Mu-4000 Security Analyzer into the development process, equipment and application vendors proactively eliminate vulnerabilities and generate comparative security metrics for their products from release to release. This approach helps service providers and enterprise customers ultimately meet their goal of vendor accountability for reduced vulnerabilities in their products.

Figure 2. EASY ANALYSIS CONFIGURATION



KEY DIFFERENTIATORS

- Support for a wide range of Attack Vectors – millions of internal (Mu generated) attack vectors, end-user developed Attack Vectors, and third party-developed Attack Vectors
- A powerful platform for Security Analysis rather than a narrow solution to a small piece of the problem
- No access to source code required
- Usable by a service provider, enterprise customer and vendor
- Enables simple reproducibility of problems and maintaining of fault trend information
- Support for analysis of a variety of product architectures
- Enhances accountability by supporting simple handoffs between testers and developers, and end-users and vendors

WIDE RANGE OF PRODUCT USAGE FOR SECURITY ANALYSIS

For Equipment Vendors:

- Creation of security profiles
- Pre-release product certification
- Patch verification
- Comparative testing across releases
- Protocol hot-spot identification
- Platform for customer-generated tests and scripts

For Service Providers and Enterprise Customers:

- Product Selection, benchmarking and bakeoffs
- Security profiling of new releases as part of change control process
- Patch verification
- Configuration-specific testing
- Policy Change Verification
- Auditing of network security devices and applications
- Internal application security testing

Breadth of Coverage

The Mu-4000 Security Analyzer supports analysis of the industry's widest range of protocols with millions of mutations across these different protocols. Mu uses its security and engineering expertise to construct analysis suites in a methodical fashion.

- Mu Security blends extensive expertise and a broad set of tools to generate new mutations and support new protocols.
- Comprehensive monitoring and management capabilities provide excellent granular information to remediate potential exploits for both Mu-generated mutations and existing customer-generated attack scripts.
- Each security analysis process leverages institutional knowledge of prior successful attacks, such as the use of trailing blanks to trigger a buffer overflow.
- The Mu-4000 system ensures careful analysis of the underlying protocol and its data types, both to compare against extremes of valid input and to contrast against examples of unexpected input.
- The Mu-4000 Security Analyzer captures hacker techniques, generalizes those techniques, and converts them formally into a comprehensive set of vulnerability probes for the development organization.

The Mu Process

Once the scope of the security analysis has been constructed, the Mu Attack Surface Analysis process is simple:

Step 1: Mutate.

Select the protocols to be analyzed and the variations of the attacks to be used.

Step 2: Monitor.

Configure the mechanisms used to monitor the target; e.g., SYSLOG, SSH, a custom CLI script, or running the target inside a debugger.

Step 3: Manage.

Specify the actions to take based on the observations made using the monitors; e.g., power cycle the device, restart a process, etc.



These three steps are configured using a simple web-based GUI. The UI is designed for different levels of user expertise. Non-expert users configure a comprehensive security analysis session easily, with little understanding of the underlying protocols. Alternately, a security expert selects specific variations within each mutation suite to allow for a fine degree of control. The entire platform is designed for simple integration into the Quality Assurance process flow.

Once an attack surface analysis is configured and launched, there is no further requirement for human monitoring or intervention. The entire security analysis session runs to completion and detailed reports of all faults discovered are available at the end of the process. Mutations that triggered faults can be rerun at any time and the exact sequence of packets that generated the fault can be exported from the system. All details of the attack surface analysis are stored in the on-board database for later analysis and reporting.

AT A GLANCE

- Proactive security
- Comprehensive and measurable platform for security analysis
- Reproducible and actionable
- Support legacy attack vectors and their alternatives
- Minimal external infrastructure required
- Usable by both experts and non-experts
- Provide simple handoff between testers and developers, and customers and vendors

MU-4000 PRODUCT SPECIFICATIONS

PLATFORM FEATURES

Mu-generated Attack Vectors

Generates millions of mutations (attacks) based on Mu Security's deep understanding of security, hacker methodology and secure programming techniques.

Customer-generated Attack Vectors

Support for customer developed attack scripts to allow continued leverage of their installed base of attack vectors with Mu Security's extensive set of Monitors and Managers.

Monitors

Monitors the target under analysis using a variety of methods including SSH, TELNET, Console, SYSLOG, Custom CLI and running inside a debugger. The monitors can work with targets with monolithic or process-based architectures.

Managers

Takes action based on information discovered by Monitors to reset the target to a state that allows for root cause discovery and continued testing with no human intervention – these include hardware managers for device restarts, software managers for power-unit-based restarts.

Reporting

An on-board database coupled with sophisticated report generation tools helps generate reports meeting a wide range of audiences and needs. Summary reports for engineering management, detailed reports for security experts and fault reports for developers are generated with ease. Extractable executable files are also available to quickly reproduce a vulnerability – all without access to source code.

External Vulnerability Triggers

The Mu-4000 Security Analyzer can generate an independently executable program for reproducing faults without needing access to a Mu-4000 system.

Load-Balanced Testing

Attacks can be distributed across multiple Gigabit Ethernet attack ports to speed up the analysis process.

Parallel Testing

Multiple hardware and software platforms can be analyzed in parallel to allow for comparative security analysis.

HARDWARE

Chassis

2U, 19" rack-mount 3.5 x 17 x 14.5 in. (8.6 x 43 x 36.6 cm.)

Weight

22 lbs. (10 kilograms)

Power

100 – 240V AC, 50/60Hz, 4.5A auto-ranging

Environmentals

- Operating temp: 32 to 104°F (0 to 40°C)
- Storage: -4 to 158°F (-20 to +70°C)
- Operating or storage relative humidity: 5 to 95%, non-condensing ports
- 2 Gigabit Ethernet management ports; auto-negotiating, RJ45 connectors
- 2 Serial Console interfaces (RS-232 DB9 connectors)
- 4 Gigabit Ethernet attack ports; auto-negotiating, RJ45 connectors
- 2 power relay connectors on front panel, 2 on rear panel

Annunciators

LCD panel with selector switch panel

Storage

Dual on-board hard drives and CD-ROM drive

Agency Approvals

CE Mark, FCC Part 15 Class A



1153 Bordeaux Drive, Suite 102, Sunnyvale, CA 94089, USA
phone: (408) 329-6330 | fax: (408) 329-6317 | web: www.musecurity.com

PROTOCOLS

The following is a list of protocols supported. Please check with your Mu Security representative for the latest and complete list of supported protocols.

- ARP (Address Resolution Protocol)
- BGP4 (Border Gateway Protocol)
- CDP (Cisco Discovery Protocol)
- FTP (File Transfer Protocol)
- HTTP (Hyper Text Transport Protocol)
- ICMP (Internet Control Message Protocol)
- IGMP (Internet Group Management Protocol)
- IMAP (Internet Message Access Protocol)
- IPv4 (Internet Protocol version 4)
- IPv6 (Internet Protocol version 6)
- ISAKMP (Internet Security Association and Key Management Protocol)
- LDAP (Lightweight Directory Access Protocol)
- PIM-DM (Protocol Independent Multicast – Dense Mode)
- PIM-SM (Protocol Independent Multicast – Sparse Mode)
- POP3 (Post Office Protocol v3)
- RADIUS (with Cisco, Juniper and Microsoft Extensions)
- RTSP (Real Time Streaming Protocol)
- SIP (Session Initiation Protocol)
- SMTP (Simple Mail Transfer Protocol)
- SNMP (Simple Network Management Protocol) and SNMP Traps
- SSDP (Simple Service Discovery Protocol)
- SSH (Secure Shell)
- Sun RPC (Remote Procedure Call) and Portmapper
- TCP (Transmission Control Protocol)
- TFTP (Trivial File Transfer Protocol)
- TLSv1 (Transport Layer Security version 1)
- UDP (User Datagram Protocol)