WHITEPAPER

The Challenge of Maximizing Service Availability and Security

Spending on security defense-in-depth has not slowed the growth rate of vulnerabilities and exploits. Protocol-based attacks and existing attack surface weaknesses are increasingly targeted to create an entryway to the end systems, servers and valuable customer information stored within a network. Every production network is unique and developers are unable to proactively analyze and test for every system or application setting. It is nevertheless essential that end users test their networked applications, hardware systems and software products in the configurations they intend to use, and perform regression tests as those configurations evolve.

Organizations of all types have invested significant resources in layered defenses designed to protect network resources and the information within the network itself. However, the very networked products creating these layers of defense are themselves complex and vulnerable to attack. As a result, the network is not fully protected so it is unable to deliver maximum service availability. Ultimately, any weaknesses in product's attack surface may result in potentially costly downtime. Analyzing infrastructure products within the network — including those meant to protect the network — is critical.

Mu Security™
Mutate. Monitor. Manage.

686 W. Maude Avenue, Suite #104
Sunnyvale, CA 94085
866-276-4640 toll-free
408-329-6330 international
408-329-6317 fax

Vulnerability of IP-based products

Nearly every product, service, application and data type is moving to an IP-based infrastructure. As a result, formerly isolated products in homogenous networks (e.g., SCADA) are embedded within heterogeneous deployments (e.g., IPv4, IPv6), resulting in dramatically larger and more complex attack surfaces that are exposed to a wide variety of potential attack sources.

An attack surface ultimately identifies methods by which an attacker can enter and potentially cause damage to a system. Attack surface growth is attributed to:

- Evolution of traditional telephony and video infrastructures to IP-based systems including VoIP, IMS and IPTV;
- Deployment of IPv6 alongside IPv4 with complex coexistence mechanisms
- Substantial code changes in complex multi-function products

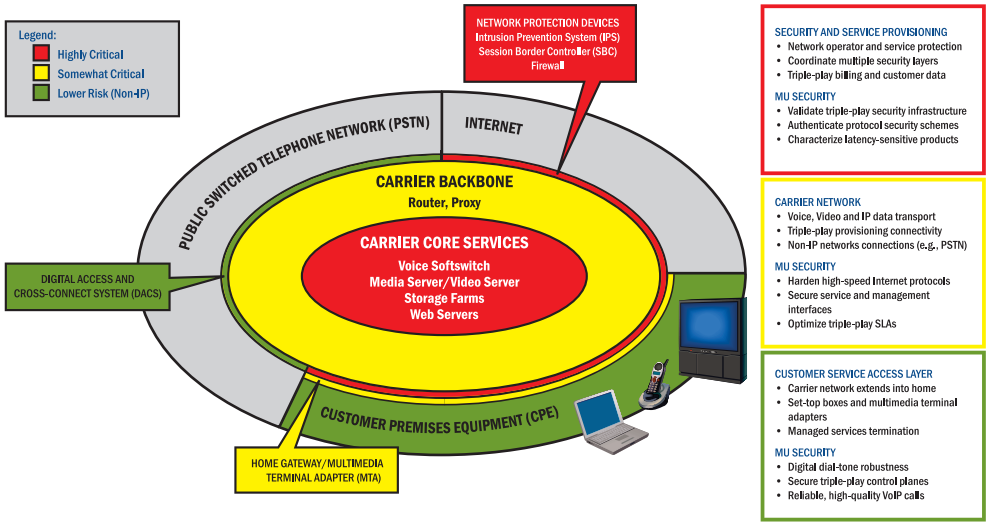


Figure 1. Mu Helps Improve IP Telephony Service Availablity

End user benefits of the Mu-4000

User organizations such as service providers, critical infrastructure operators and large enterprises must understand the attack surface weaknesses within the products they have deployed, plan to upgrade or intend to deploy. In particular, service providers continually find 0-day vulnerabilities that affect their ability to fulfill service availability agreements, resulting in embarrassing and costly penalties, possibly also resulting in loss of customers. Service availability is a key way to build competitive advantage.

Limitations of current security assessment approaches

Most penetration testing or vulnerability-assessment tools only analyze how targets react to known vulnerabilities. While helpful, there is a much larger issue of unknown security or service availability problems. Moreover, most tools available today only search for the subset of known vulnerabilities for which patches exist, since the only remediation these tools can offer is to bring the target up-to-date by applying a patch that promises to fix the issue at hand. Moreover, these tools cannot discover unknown weaknesses in the attack surface (also known as “0-day vulnerabilities”).

Implementation flaws surrounding a protocol implementation’s state, semantics or structure may manifest themselves as service availability issues, including security vulnerabilities that could be exploitable. Despite these issues being a major concern for vendors as well as end users of IP-enabled products, there has never before been an automated, structured and process-oriented approach to discovering (and eliminating!) their root causes.

Spectrum of faults

Security vulnerabilities represent one end of the spectrum of implementation flaws that might be uncovered by applying security analysis. These might be referred to as “hard faults” such as system crashes that can occur in any network-connected software or hardware product.

However, there are many faults of equal concern to a customer that is evaluating or deploying a vendor's products. Some internal issues may not cause a crash but may indicate a lack of robustness that could result in reduced operational availability — CPU utilization spikes, memory leaks, etc. Additionally types of operation availability reductions for products in use on a VoIP network might include reduced throughput, of either signaling traffic or call traffic, of that traffic could experience dramatic swings in latency and jitter, among other undesirable behaviors that affect a customer's perception of service quality.

Hard faults are essential to discover and fix, ideally before a product ships. Despite vendors' best efforts, however, this is not always possible, as there are literally trillions of possible combinations of features in even a modestly complex product, and each of those combinations may behave uniquely in only a small subset of possible end-user configurations. Therefore, end users need tools to uncover such flaws before they impact service availability. Trust vendors, but verify that the products work they way you intend to use them. If you find a flaw, the biggest thing you can do to help your vendor is to give them meaningful remediation hints, like the tools the Mu-4000 generates which help the vendor quickly reproduce the issue in-house.

Requirements for vulnerability assessment

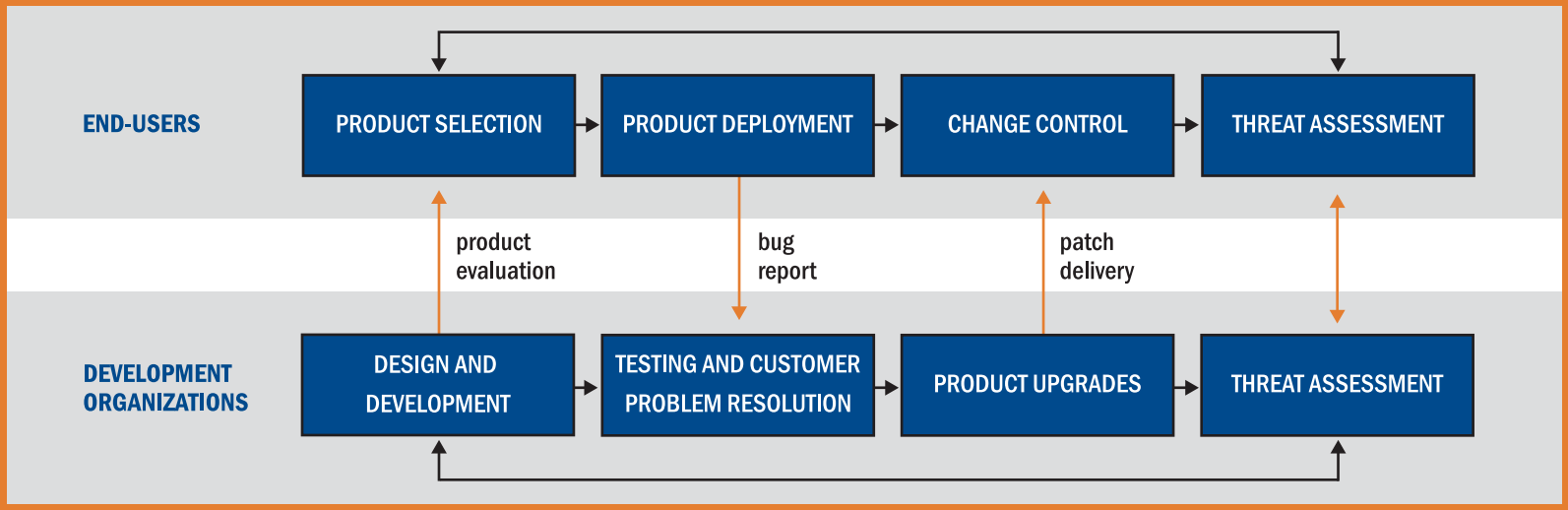
End users — including service provider and IT operations staffs — have lacked an extensible security analysis system that provides a process-enabling framework for automating the testing and measurement of service robustness and security.

Process requirements

End users and service providers require formal and unbiased methodologies to measure an IP-based product's security defects before deployment. Such process improvement requirements include:

- An unbiased metrics-driven process provides leverage by which vendors are held accountable for insecure or non-robust products by scientifically characterizing a product's service availability or security readiness, both before and during production deployment.
- The ability to establish the ability of the systems and the layers of defense to survive or deflect the latest published vulnerabilities.

Security Analysis enhances all stages of the product lifecycle



Vulnerability reduction

To ensure that all new IP-based systems become gradually more robust and secure, users of such products require a security assessment system that delivers:

- Proactive identification and removal of vulnerabilities before and during deployment of systems and applications in production networks.
- Automated regression analysis to ensure prior results can be repeated and that previously discovered issues do not recur.
- Assurance that devices are ready for deployment in a mixed vendor environment by demonstrating that they can survive known attacks.

Essential requirements for the security assessment process

End users require the ability to apply the very latest published vulnerabilities from the real world to discover where they are vulnerable to malicious exploits and to take preventive measures. Organizations require rigorous methodologies to assess an IP-based product's security readiness before purchasing. These requirements impact many IT processes, including theose in the table on the following page:

Core Process	Requirement for Proactive Security
Product Selection	Security and robustness metrics in the purchasing decision process ensure only best-of-breed products are selected for deployment.
Product Deployment	Whether introducing new products into the network or activating new features, it is essential that systems be evaluated before they unwittingly reduce service availability.
Change Control	New configurations or releases must be evaluated for stability before they are deployed. Also, signature-based security features must be verified correct by exposing them to new published vulnerabilities in a controlled setting.
Threat Assessment	End-user operations teams must proactively deliver actionable feedback to their vendors so that fixes can be developed quickly.

The Mu-4000: Protocol-Based Vulnerability Assessment

The Mu-4000 Security Analyzer offers organizations "a tiger team in a box", a self-contained, rack-mountable appliance easily configured and managed via a graphical user interface that uncovers known and unknown weaknesses in network products in a lab environment. The Mu-4000 includes a built-in test harness that actively captures packets associated with user-defined fault conditions for both internally and externally generated attack traffic.

The Mu-4000 uses the structure of protocols themselves and knowledge of vulnerability patterns across protocol implementations to efficiently explore the space of potential vulnerabilities within the protocols implemented by any application or infrastructure device. The Mu-4000 generates millions of unique attacks against any product with an IP address. This emulates a hacker's proactive approach to isolating attack surface weaknesses and finding flaws, as opposed to the reactive stance that has characterized security assessment products to date.

The Mu-4000 reflects Mu Security's deep understanding and core competencies in the following areas:

- System and hardened protocol design, including the diverse attack surface pathways exploited by hackers
- Process automation for the creation of repeatable and customizable test processes for product developers
- Development of intuitive interfaces for non-expert users
- Dynamic modification and changes to attacks
- Proactive testing technologies

Before upgrading any application or infrastructure device, end users can test all upgrade alternatives for vulnerabilities and select the version or configuration alternative with the smallest attack surface. Once a device in the network has up-to-date attack surface analysis baselines that align with its desired configuration, developers can quickly re-test such a device to verify that modifications do not reduce the device's robustness.

Enterprise IT organizations equipped with the Mu-4000 are proactively avoiding service availability issues and security weaknesses before network device purchase or deployment. The result is millions of dollars savings annually in operations budget alone per organization.

The Mu-4000 is the only customizable and comprehensive solution that provides all the following capabilities:

- Broad spectrum of attacks: Mu-generated, customer-generated and published (known) attacks
- Identification of 0-day protocol implementation flaws
- Transmission of published vulnerabilities, with or without obfuscation
- Fully-automated published and 0-day vulnerability analysis, including expedited remediation tools and regression processes
- No source code required for analysis
- Seamless integration with external scripts, tools and third-party applications
- Integrated database for automated regression and trending

Attack categories

The Mu-4000's protocol mutations dynamically encompass millions of stateless and stateful protocol violations based upon the structural aspects of those protocols. It can also leverage attacks against the components abstracted from other protocols with similar functions. The system creates a database of meta-attacks against dozens of common protocol features, enabling the search for generalized vulnerabilities within similar components of dissimilar protocols.

The Mu-4000 constantly enhances its intelligent protocol fuzzing application to discover previously unknown vulnerabilities using patent-pending Protocol Spidering™ technology. The resulting protocol mutations unlock and optimize the structural interdependencies and functional correlations of the protocols under analysis.

The Mu-4000's attack applications are summarized as follows:

Attack Category	Description
Protocol mutation attacks generated by the Mu-4000	The Mu-4000 offers tens of millions of protocol attack mutations that dynamically combine dozens of transport and authentication techniques.
External Attacks	The Mu-4000 supports CLI-based, internally developed, free, open-source or commercial scripts and tools (e.g., PROTOS or Nessus) to leverage, optimize and automate existing tools and testing.
Published vulnerability analysis (PVA)	The Mu-4000 automates vulnerability assessment to attacks since 1-Jan-2004 for signature-based network security enforcement products such as firewalls, UTMs, deep-inspection devices, IPS and other signature-based systems.

The rich protocol analysis capabilities of the Mu-4000, combined with the system's attack modes, enable end user organizations to safely run a wide range of critical applications, including:

- Policy change reviews
- Patch testing
- Identification of flaws in the design, development, deployment of internally developed applications
- Regression testing after vendor fixes
- Network service availability assurance
- Web site testing
- Robustness/Availability analysis
- Triple-play application availability
- Network infrastructure auditing
- Automation of existing scripts/tools
- IPS, AV/Email gateways, DI firewall testing
- Network/DMZ auditing during scheduled downtimes

Key capabilities of the Mu-4000

The Mu-4000 is a comprehensive security analysis system for any IP-based product that offers inline as well as target mode testing capabilities. Key features and capabilities include:

Exploit and analysis databases

Drawing upon a database of thousands of previously discovered published vulnerability exploits, the Mu-4000 generates packets and directs them at up to four targets at a time. Security analysis results are stored in a database and run again or extracted at any time once an analysis is completed. Historical trends and other comparative data can be accessed and studied by pulling up the relevant results in the Mu-4000's intuitive graphical user interface.

Transformation engine

The Mu-4000's built-in transformation engine alters any exploit to evade discovery techniques, a technique frequently used by attackers. These capabilities in the industry are variously known as evasion and obfuscation. Such alterations can include packet fragmentation, target port re-assignment and code misrepresentation, as well as varying the source IP address.

Intelligent protocol fuzzing

Intelligent protocol fuzzing, or generation of specific, unique attacks targeted against specific aspects of protocols (either the state, structure, or semantics). These attacks identify vulnerabilities by creating a system crash or a SmartDoS condition.

Monitoring

Target monitoring capabilities record problematic traffic and verify a target's status and enable test repeatability. The monitoring capability is tightly integrated with the ability to restart a failed target, either via a software restart or a full hardware power cycle.

Test facility deployment

The Mu-4000 is used by a growing number of established industry test labs worldwide to evaluate products in key categories such as multilayer security appliances, government compliance, network routers and switches, IP Telephony infrastructure and streaming media applications. These organizations include publication-oriented labs that provide certification and standalone published reviews as well as private commercial labs that perform paid testing projects and government labs that focus on requirements-based and standards-based certification for worldwide government, federal and state IT purchasing.

Figure 2. Mu-4000 Screen Shot

Benefits of the Mu-4000

The Mu-4000 enables service providers and end-user IT organizations to analyze their unique attack surfaces and proactively remediate a wide range of potentially disruptive vulnerabilities in the following ways:

- Quantification of limitations in reactive, layered-defense security approaches.
- Achievement of security assurance through analysis, assessment, and remediation based upon key security standards and requirements.

Product selection

- Comparison of similar products from competing vendors relative to service availability and security readiness.
- Empowerment of users to hold their application and infrastructure product vendors accountable to higher standards of service availability and security.

Product deployment

- Once a device has up-to-date attack surface analysis coverage that reflects its current configuration, service provider and corporate IT teams can easily re-test such a device as part of the change management process to verify that ongoing modifications do not adversely affect service availability.
- The ability to continually and dynamically apply the latest published vulnerabilities from the real world enables users to validate signatures before applying them and to take preventive measures as determined by demonstrated openings in the attack surface.

Change Control

- Before upgrading any application or infrastructure product, users can evaluate all upgrade alternatives for security vulnerabilities or service availability weaknesses and select the version with the best profile.
- Proposed configuration changes are compared to ensure that there is no newly introduced weakness in the attack surface.

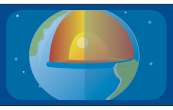
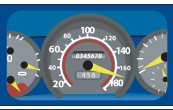
Conclusion

The most effective strategy for proactively defeating hackers and maintaining a highly available service is to eliminate attack surface weaknesses before they cause downtime. The Mu-4000 Security Analyzer enables end user and service provider networking and operations teams to identify the root cause of these weaknesses and enable you to provide the necessary details to the vendor so they can address these issues.

The Mu-4000 provides an effective way to search the enormous space of previously unknown attacks against the protocols commonly implemented across enterprise networks. The capability of the Mu-4000 to test any IP-based application or device, including switches, routers, intrusion detection and intrusion prevention devices, and IP-based applications running on servers enables IT organizations to transition from reactive to a proactive operational stance in the critical area of network security and service availability.

The Mu-4000 also provides external analysis capabilities to vastly improve IT and lab staff productivity by optimizing existing processes, labor-intensive testing and analysis processes. Finally, the Mu-4000 embodies a repeatable and automated published vulnerability auditing framework that can evaluate network infrastructure security enforcement products, ensuring that these devices actually protect the network as promised by vendors.

The following is a partial list of product families covered by Mu-4000 protocol mutations:

	Core:	Operators of network infrastructure devices are likely to need at least these protocols. ARP, BOOTP, CDP, DHCP, DHCPv6, GRE, ICMPv4, ICMPv6, IGMP, IPsec, IPv4, IPv6, L2TP, MPLS, PPPoE, SSL-TLS, TACACS+, TCP, UDP
	Enterprise:	Network operators up to the largest deployments need this set of protocols. FTP, H.323, IEEE 802.1Q, IEEE 802.1X, IMAP, LDAP, MSRPC, POP3, RADIUS, SCTP, SIP, SMTP
	Management:	These protocols facilitate management of networks and devices, in the broadest sense. BOOTP, DHCP, DHCPv6, HTTP, IEEE 802.1AB, ISAKMP, LDAP, LDP, SNMP, SSDP, SSH
	Media:	Media-intensive devices and networks employing these protocols need to be analyzed deeply. H.323, IEEE 802.1AB, MGCP, RTSP, SCTP, SIP
	Metro Ethernet:	Operators of any scale Ethernet networks should ensure that these protocol implementations are robust. IEEE 802.1AB, IEEE 802.1Q, IEEE 802.1X, MPLS
	Multicast:	Devices that employ multicast technology need a well-implemented, solid foundation of these protocols. ICMPv6, IGMP, PIM-DM, PIM-SM
	Routing:	Network operators of all scales must ensure that their routers can tolerate a wide variety of invalid input. ARP, BGP, OSPF, PIM-DM, PIM-SM, PPPoE, RIPng, RIPv1/v2
	SCADA:	Critical Infrastructure operators that perform security analysis know that their network devices are robust. DNP, ICCP, IEEE 802.1AB, MMS, Modbus, OPC
	Storage:	In order to protect valuable data, protocols used to access stored data must be highly robust. CIFS, iSCSI, MSRPC, NFS, SunRPC

About Mu Security

Mu Security is a technology innovator that created a new class of security analysis system. The company's mission is to widely deploy security analysis and reduce product and application vulnerabilities. The security analysis process and the Mu-4000 Security Analyzer platform provide a rigorous and streamlined methodology for verifying and improving the service availability and security readiness of any IP-based product or application.

Mu Security enables enterprises and service providers to evaluate new products and software updates for known and previously undetected security vulnerabilities. In so doing, the company:

- Introduces security readiness as a metric for end-users' product purchase and deployment decisions;
- Allows development teams to efficiently identify security flaws in their products before release;
- Significantly decreases the number of security events in production networks through a proactive methodology that detects security flaws before systems and applications are deployed.

Mu Security was founded in 2005 by experts in intrusion detection and prevention, ethical hacking and network management. The company is headquartered in Sunnyvale, California, and is backed by preeminent venture capital firms, including Accel Partners, Benchmark Capital and DAG Ventures.