

GOVERNMENT WHITEPAPER

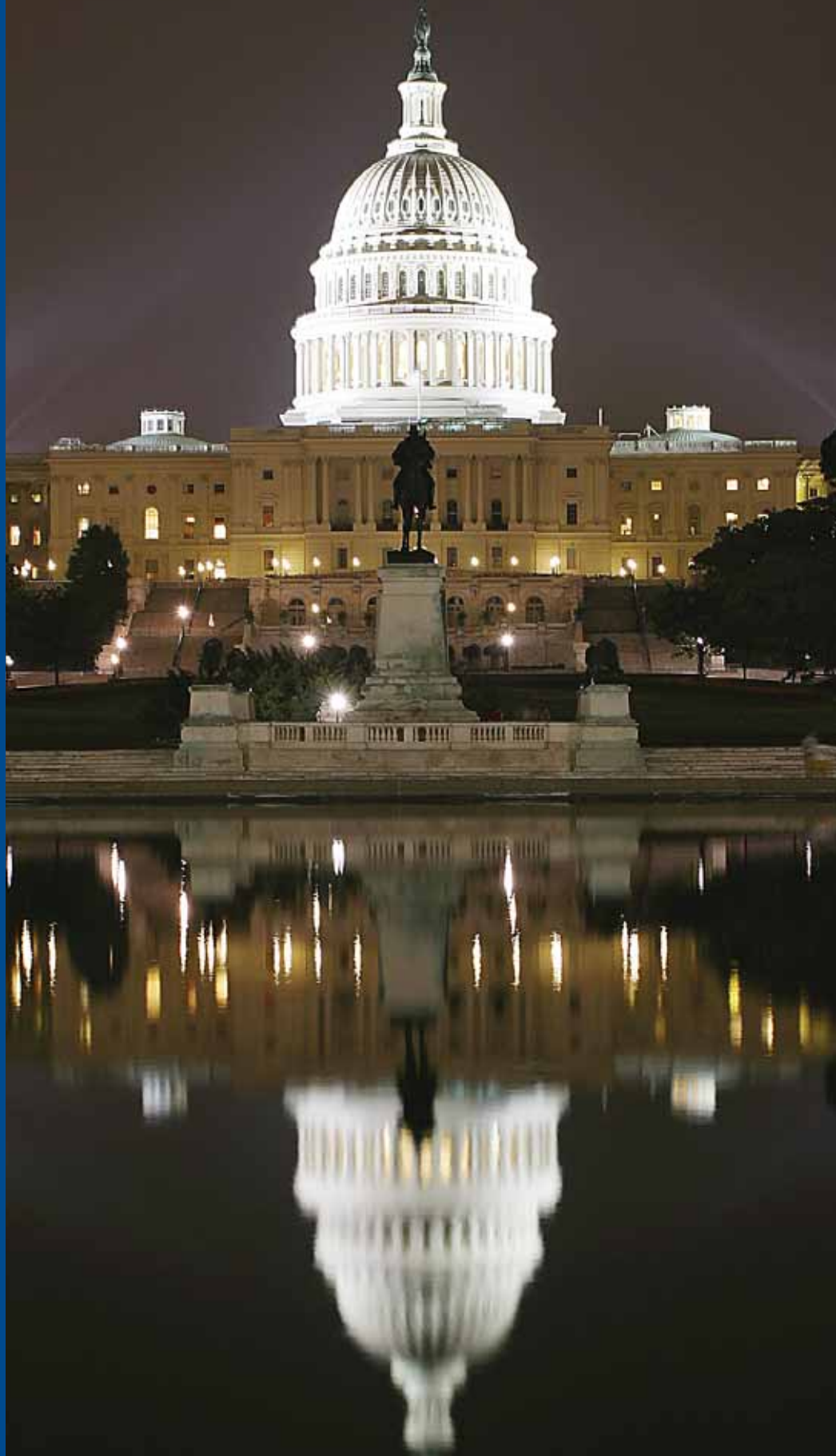
## **AUTOMATING INFORMATION ASSURANCE AND CYBER TESTING**

For government departments and agencies, “mission-critical network” isn’t a throw-away term, it is reality. As a result, applications and networks must uphold a higher standard of performance, reliability and security than in the private sector. The networks that make government run are highly interconnected and are built on increasingly open standards. The security stakes are high, and with the global threat landscape evolving rapidly, national security is literally on the line.



686 W. Maude Avenue, Suite #104  
Sunnyvale, CA 94085  
866-276-4640 toll-free  
408-329-6330 international  
408-329-6317 fax  
[www.mudynamics.com](http://www.mudynamics.com)

# Serve & Protect





“ABB’s use of the Mu Test Suite throughout our software development lifecycle helps us model real world traffic, understand service response time weaknesses and adverse side-effects. It answers questions such as, “If a system is being overloaded by one type of service-level traffic, what is the effect on other unexpected traffic to that system’s processes?”

**Kevin McGrath**  
Scientist  
ABB

## Honeywell

“Without an effective cyber security solution, even the latest and greatest process control technology on the market can be rendered obsolete and become a danger to the plant and plant employees.”

**Kevin Staggs**  
Engineering Fellow and  
Global Security Architect  
Honeywell

### Government agencies face several key technology challenges today:

- **The threat of cyber-warfare is escalating.** Cyber-crime is a global issue that is not only a threat to industry or individuals, but also increasingly to national security. Attacks are sophisticated, well-organized operations conducted for political, military and economic purposes. In April 2009, CBS News reported that the Pentagon spent more than \$100 million within the previous six months responding to and repairing damage from cyber-attacks and other computer network problems.<sup>1</sup> A number of nations have incorporated cyber-warfare and countermeasures into their military doctrines and cyber-attacks on the governments of Estonia and Georgia may well be harbingers of the future state of information warfare.
- **Migration to IPv6.** As IPv6 becomes the mandatory standard protocol for the Department of Defense (DOD), Air Force and other departments, many IT teams are doing the heavy lifting of IPv6 production testing and deployment. Organizations must test the security, scalability and reliability of IPv6 network equipment as well as in a dual-stack environment. IPv6 has some significant implications for security, despite its reputation for strong security. For instance, the larger address space of IPv6 makes scanning certain IP prefixes more difficult than in IPv4, which makes IPv6 more resistant to malicious traffic, but also makes it more difficult to identify unlisted rogue malware machines using distributed attack and spoofing techniques over IPv6.
- **Adoption of commercial-off-the-shelf (COTS) technology.** Government agencies and departments are rapidly converging voice, data and video services on a common IP infrastructure to take advantage of the efficiency and cost savings of a single infrastructure. The use of COTS technology in the network infrastructure is an opportunity for IT modernization and lower costs, but it also creates the need for greater risk management. Commercial products may have software weaknesses or worse, be intentionally compromised, which may lead to reliability issues or put the reliability and security of critical systems in jeopardy. Organizations must assure that they’ve done the utmost to develop and deploy secure and reliable network services using off-the-shelf technology.
- **Massive investments in new technology, including the smart grid.** The Obama Administration’s economic stimulus plan includes \$11 billion for the creation of the smart grid. Some \$40 billion is set aside for developing IT network infrastructure. Utilities in the U.S. expect to have almost 52 million customers outfitted with smart meters by 2015, according to the Edison Foundation.<sup>2</sup> In the rush to take advantage of unprecedented new funding to bring new innovative IT and smart grid technologies to market, software weaknesses and reliability issues may be overlooked until the products are in production use.
- **Critical infrastructure is moving toward IP.** Industrial control networks and critical infrastructure networks supporting energy, communications, transportation and emergency services are migrating from closed, proprietary architectures, to open, IP-based systems. This transition delivers richer capabilities and greater operational efficiency, but concomitant are risks including the introduction of unfamiliar software stacks in new types of deployments and interconnection of formerly isolated networks with non-industrial control system networks.



<sup>1</sup> “Pentagon Bill To Fix Cyber Attacks: \$100M,” CBS News.com, April 7, 2009  
<http://www.cbsnews.com/stories/2009/04/07/tech/main4926071.shtml>

<sup>2</sup> “Utility-Scale Smart Meter Deployments, Plans & Proposals,” The Edison Foundation: The Institution for Electrical Efficiency May 2009  
[http://www.edisonfoundation.net/iee/issueBriefs/SmartMeter%20Rollouts\\_Q509.pdf](http://www.edisonfoundation.net/iee/issueBriefs/SmartMeter%20Rollouts_Q509.pdf)

"By leveraging Mu's Test Suite throughout our product development cycles, our teams have a new and critically important capability to bolster our product reliability and design methodology to ensure SEL products and updates are 'battle tested' and secure well in advance of commercial shipment."

**Rhett Smith**  
**Security Products**  
**Development Manager**  
**Schweitzer Engineering**  
**Laboratories (SEL)**



"Creating an IA Master Plan with a vision, clear goals and objectives to improve the speed of capability for deployment and implementation of newer technologies while ensuring the creation of an IA governance structure and consistent policies."

**Mike Davis**  
**Info Assurance/Security**  
**Technical Authority**  
**US Navy's Space and Naval**  
**Warfare Systems Command**  
**(SPAWAR)**

## Assure Reliable and Secure Deployments with Mu

As federal, state and local agencies fine-tune their information assurance plans and effectively implement an enterprise-wide trusted infrastructure, they must protect the new and improved aspects of their architecture, while also maintaining the technology that is in place. As part of their strategic information assurance plans, IP network equipment and networked applications must be tested extensively to ensure that they are free from software weaknesses and reliability issues that could compromise effectiveness in the field.

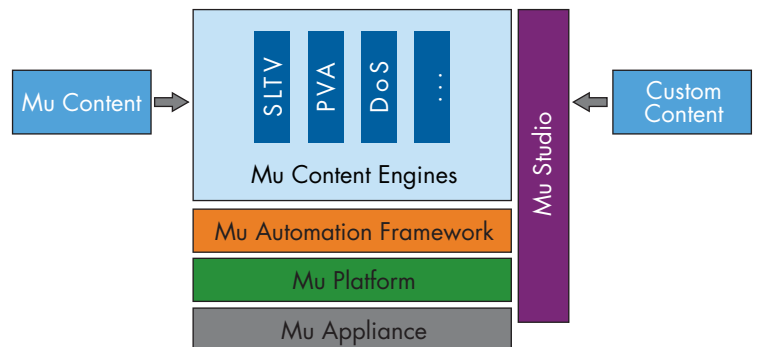
Government and private sector organizations use Mu Dynamics' Mu Test Suite across the information assurance and software development lifecycles to address software weaknesses and reliability issues in network applications and gain actionable metrics. With the Mu Test Suite, organizations can:

- **Identify software weaknesses and vulnerabilities more rapidly.** With Mu Test Suite, developers, QA engineers and security engineers can identify and quantify software weaknesses and vulnerabilities in networked applications that impact security, performance and survivability. With the Mu Test Suite, developers and engineers can quickly determine a thorough and precise attack surface coverage. Mu's unique stateful protocol modeling engine interactively explores complex, stateful targets with millions of dynamically generated variations of protocol traffic tailored to the target's exact capabilities. Adaptive analysis combines Mu's dynamic protocol fuzzing suites with a large number of transport and authentication options.

The Mu Test Suite, developers and engineers can quickly determine a thorough and precise attack surface coverage. Mu's unique stateful protocol modeling engine interactively explores complex, stateful targets with millions of dynamically generated variations of protocol traffic tailored to the target's exact capabilities. Adaptive analysis combines Mu's dynamic protocol fuzzing suites with a large number of transport and authentication options.

Mu's testing approach delivers better test coverage and better ROI when compared with prior approaches, which were very labor-intensive if conducted at all. Development and test cycles are shortened, while boosting overall quality. In addition, organizations reduce costly overhead from fire drills and reduce the lifecycle cost that accrues from shifting the discovery of bugs as early as possible in the product development or deployment lifecycle. In fact, NIST has shown that organizations can gain more than a 10x savings for early adoption of methodologies that reduce the number of service weaknesses.<sup>3</sup>

- **Test proprietary protocols and custom extensions to standard protocols more quickly.** Mu Studio leverages the Mu platform to automate the creation and application of complex, custom and proprietary test case



**Figure 1:** Mu Studio allows customers to define custom tests for a variety of user cases with minimal effort.

<sup>3</sup> "The Economic Impact of Inadequate Infrastructure for Software Testing," NIST. <http://www.nist.gov/director/prog-ofc/report02-3.pdf>

## RAPIDLY DEFINE CUSTOM TESTS WITH MU STUDIO

Mu Studio allows customers to define custom tests in a broad variety of use cases with minimal efforts. Mu Studio takes in user-defined packet captures (pcaps) that represent scenarios of interest to the customer. Pcaps can be of custom protocols, custom extensions, custom multi-protocol exchanges or new functionality exposed or fixed by a vendor patch.

Mu Studio brings formerly static content to life. Each pcap is actually a step-by-step description of how a set of systems interact, and it contains all sides of every exchange. It is similar to a program, or set of instructions, that exercises code when played against a target.

The engine underlying Mu Studio deciphers the packet uploads and figures out which transports are involved and which fields make up the payload. It then auto-generates thousands of test cases from the pcaps and can replay them statefully. Since the Mu engine understands more than 60 protocols and can replace transports in a live, stateful manner, thousands of test cases can be run in a lab environment to test the robustness of almost any exchange between two systems.



IPv6 Case Study

scenarios. Using Mu Studio obviates the need to develop custom test cases or wait months for commercial test vendors to provide a solution. With Mu Studio, once you capture network traffic, you can test it. Mu Studio delivers a robust testing methodology that addresses unique implementations of cutting edge protocols, multi-protocol interactions, vendor-customized extensions of standard protocols, and proprietary protocols.

Mu Studio speeds testing in a broad variety of situations that were formerly difficult to test. For instance, many protocols used in critical infrastructure applications, such as the family of protocols defined under IEC-60870 (such as 60870-5-104), IEC-61850, IEC-61400 and DNP3) tend to have custom extensions, which makes them difficult to test. In addition, SIP, DHCP, RADIUS and OSPF often have custom vendor-specific extensions.

- **Protect critical services with denial-of-service (DoS) test modules.** You can create customizable DoS attacks and detail accidental or malicious impact on critical services. Mu includes pre-defined templates for well-known application-level and protocol DoS attacks, which greatly simplifies testing. You can then put the test results into action, as the Mu can correlate traffic injection rate with faults and outages and identify system recovery time.
- **Ensure the most reliable, available and secure devices are procured – and maintained throughout the lifecycle.** With Mu as part of the testing toolbox, QA and security engineers can mitigate risk by verifying the security and reliability of products prior to procurement. Once products are placed into service, they can use the Mu Test Suite to continually evaluate the products based on the initial configuration. As patches are applied or new versions become available, this baseline can be proactively referenced throughout the product's lifetime. This is particularly critical when services and applications are dependent on cutting-edge services, such as Community Directive Number 503 (ICD-503).

Mu's automated fault isolation and remediation tools provide advanced analysis to pinpoint failures to a single unique attack when possible. Faults are ranked using the industry standard CVSS scoring methodology. Users can easily define faults using criteria such as log output, system load and code coverage. Sophisticated, customizable reports include captured data and configuration templates, which are essential in meeting C&A requirements.

### CASE IN POINT

#### Department Validates IPv6 Readiness with Mu

IPv6 brings the pervasive networking, mobility and security that are necessary to support future combat operations. One branch of the U.S. military is on the leading edge of the transition to a production IPv6 infrastructure. The department has followed extensive certification and accreditation procedures, and it created a rigorous test plan which included verifying that the intrusion detection system (IDS) and firewall products it had procured would work as advertised. The COTS products performed as promised in the IPv6 pilot, but the department needed proof that the IDS/firewalls would scale to meet the reliability and security requirements of a production deployment.

Development, QA and security engineering teams used the Mu Test Suite to identify software weaknesses that could lead to network security, robustness, conformance or survivability issues. The team used the Mu Test Suite to verify simultaneous support for IPv6 and IPv4, including dual stack, automatic tunneling and configured tunneling. It also verified that the IDS/firewall signatures were up-to-date.

In addition, the department used the Mu Test Suite to validate that its security logs correctly identified malicious traffic, so it could meet its C&A requirements, even though the team had limited experience with IPv6 testing. Using the Mu Test Suite

enabled the department to validate that the IPv6 IDS/firewalls were free of security and

reliability issues in a more robust manner and in a shorter timeframe.

### CASE IN POINT

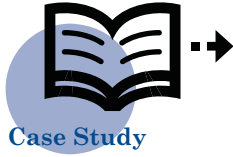
#### Agency Operationalizes Risk Management under ICD-503 Requirements

The Intelligence Community Directive Number 503 (ICD-503) represents an opportunity to shift security from inflexible, policy-based compliance to risk-based protection, in which the missions and business functions define the security requirements and associated safeguards. The end goal is to reduce risk to computer networking systems used by the Intelligence Community by improving reliability, availability and, in particular, security.

bigger win comes from continuous improvement across the product and service lifecycle, including patch management.

The Mu Test Suite is an integral part of the agency's procedures for certification, accreditation and monitoring. By automating testing with the Mu Test Suite, the agency streamlined the evaluation of vulnerability and penetration testing and developed standardized test and evaluation templates. Most importantly, it significantly reduced the time required for testing, which enabled it to reliably deploy new application and network services to support the national security community.

A major U.S. intelligence agency recognized taking an innovative approach to ICD-503 certification would deliver ROI in the earliest stages of product development and service deployment lifecycles, but an even



ICD-503 Case Study

#### Mu Dynamics offers solution bundles for various markets and customers

- Admin
- DMZ
- IMS
- Industrial Control
- IPTV
- LTE
- Mail
- Routing
- Storage
- VoIP

#### Solution bundles from Mu Dynamic include:

- VOIP
- IMS
- Industrial Control/Critical Infrastructure
- IPTV
- Storage
- Data Services
- Routing
- Admin

#### About Mu Test Suite

Since its inception in 2005, the award-winning Mu Test Suite has evolved into a complete network testing solution. The Mu solution offers powerful capabilities to improve reliability, availability and security of any IP-based network applications and services. With constant addition of new features and functions, including Mu Studio, the Mu Test Suite serves an active and growing customer base.

#### Purchasing Mu Dynamics Products

The Mu Test Suite is used at government agencies, leading global service providers, and network product vendors. Mu is listed on the GSA purchasing schedules and through selected resellers.

#### About Mu Dynamics

Mu Dynamics proactively eliminates costly service and product weaknesses by testing for the unexpected. Mu's solution automates a systematic and repeatable process that identifies hard-to-detect sources of potential downtime within IP services and underlying networks. The award-winning Mu solution is deployed at more than 100 locations, primarily at leading global service providers, government agencies, and network product vendors. Headquartered in Sunnyvale, Calif., Mu is backed by leading venture capital firms that include Accel Partners, Benchmark Capital, DAG Ventures and Focus Ventures. Information about Mu Dynamics is available on the Web at [www.mudynamics.com](http://www.mudynamics.com).



web: [www.mudynamics.com](http://www.mudynamics.com) | email: [info@mudynamics.com](mailto:info@mudynamics.com)  
 address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA  
 phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317