

# Security and Robustness Testing Maximizes Triple Play Uptime

## Problem: Growing Security Concerns for VoIP Networks

The rate at which Voice over Internet Protocol (VoIP) is growing opens many network security concerns. NIST recently issued Special Publication 800-58 entitled "Security Considerations for Voice Over IP Systems," focusing on VoIP security problems and recommendations, and highlights the current level of concern.

In-Stat predicts business VoIP deployments will grow from 9.9 million in 2006 to 45.8 million deployments in 2010. Yet, the company notes that more than 40 percent of the businesses surveyed do not have specific plans for securing their VoIP deployments. Additionally, when In-Stat asked them to rate their VoIP security knowledge, most enterprise managers characterized themselves as being only "somewhat knowledgeable" – the lowest rating offered. Likewise, Frost & Sullivan predicts that VoIP revenue for service operators will grow at more than 40 percent to over \$8 billion by 2008. Since building and deploying VoIP systems is very complex, security and robustness weaknesses are an unfortunate reality that must be dealt with proactively in order for the growth to develop as predicted.

## Solution: Mu Dynamics Enables More Robust VoIP Deployments

Both VoIP equipment providers and their end-user service provider, cable operator and large enterprise critical infrastructure customers now have a new testing and analysis tool to isolate and document VoIP weaknesses. These tools, called Security Analyzers, ultimately help product developers and end users alike by baselining and reducing their respective attack surface exposures. Mu Dynamics is the innovator of this new marketplace with the Mu-4000 analyzer. Security analyzers ensure the highest quality implementation of SIP, MGCP, H.323 and IMS are among key factors in the successful ongoing deployments of these technologies.

Designing, deploying, and securely operating a VoIP network is a complex effort that requires careful preparation and ongoing testing with any network modifications. The integration of voice and data in a single secure and robust VoIP and data network is a complex ongoing process that requires greater effort than required for data-only networks. VoIP easily overburdens existing data networks, creating serious problems for the organization. Until Security Analyzers arrived, there was no practical way to determine VoIP's security and robustness issues. NIST recommends several key steps to ensure VoIP security, performance and robustness including:

1. Develop appropriate network architecture.
2. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems. Both product developers and their end users should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.
3. VoIP-ready network equipment (e.g., firewalls, IPS devices) and other appropriate protection mechanisms should be employed.

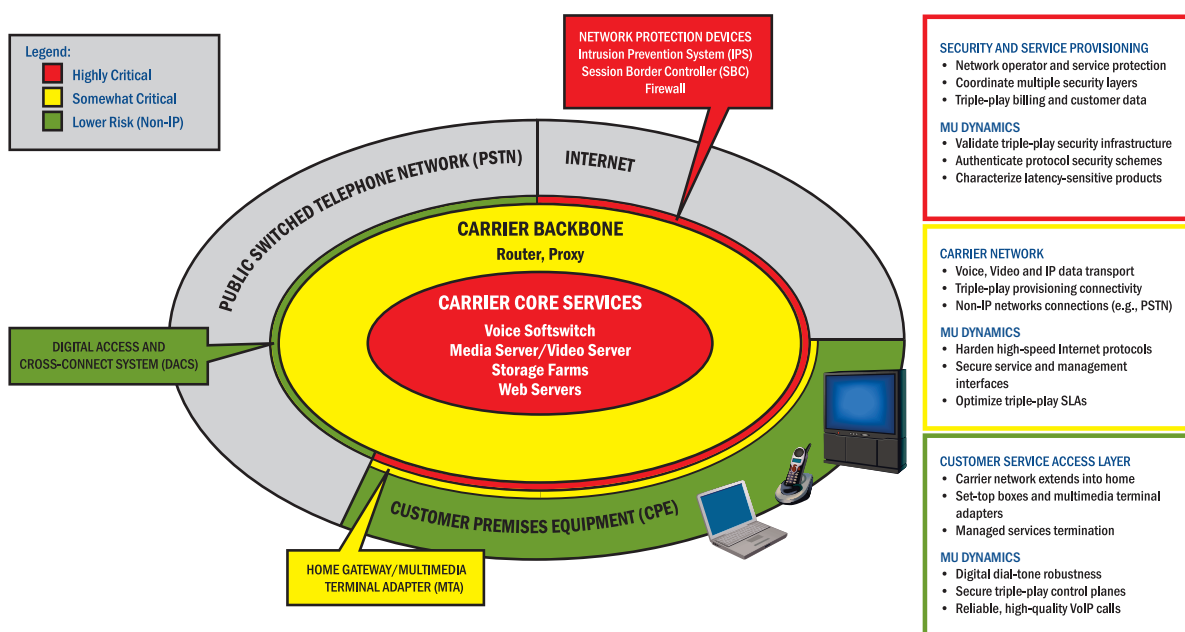


Figure-1. Extended Triple-Play Provisioning and Service Environment

VoIP test and measurement must enable, use, and routinely stress product resiliency and security features that are included in VoIP systems. Microsoft and Carnegie Mellon University developed the concept of “attack surface” for quantifying the exposure of systems to attack. Large network suppliers are already reporting VoIP product weaknesses including intelligent denial of service conditions in VoIP gateways. These exploits include call redirection, eavesdropping and accessing networks and machines that run VoIP products, facilitating theft of service among other issues.

## MU-4000 ANALYZER



InfoWorld magazine notes: “Network vulnerabilities are rampant, worm writers are looking for the next server application to exploit, and malicious hackers are breaching the moat and climbing up the castle’s walls.” Security Analysis is about a baseline of the attack surface, a methodical way of identifying service availability issues for any exposed protocol.

### **Benefits: Profitable, More Reliable and Less Vulnerable Triple Play Applications**

Service Providers, cable operators and their network product providers share a common goal of reducing customer downtime, support costs, and building customer loyalty. As end users roll out IP voice offerings, they must address a host of new issues concerning quality of service – partly because they need to prove to customers that what they’re offering is equivalent to, or better than, traditional phone services. The use of new technologies calls for extra ongoing engineering vigilance including the use of Security Analyzers.

End users previously had limited visibility into a product’s true attack surface, security or robustness metrics of any IP-based products they were purchasing or upgrading. A security analyzer provides an unbiased means to measure a product’s security readiness, robustness, and resiliency before production deployment, conferring the ability to hold vendors accountable for insecure or non-robust products.

Broadband Service Providers, including DSL and Cable Operators, are now using Security Analyzers for:

- **Product Selection:** Security readiness is a key metric to support purchase decisions or upgrades, in addition to robustness, functionality and performance.
- **Product Deployment:** Securely deploy product features or introduce configuration changes into the network architecture, end-users proactively identify and remove robustness issues or vulnerabilities before deployment.
- **Change Control:** Analyze new software or firmware releases or bug fixes before production use, ensure that no published or previously eliminated issues or vulnerabilities are inadvertently used in the network
- **Threat Assessment:** Security crisis management and problem reporting to a vendor is streamlined with Mu-4000’s ability to automate and “operationalize” the auditing and vulnerability remediation processes.

Triple Play Security/Robustness Testing enables customers to proactively discover the true extent of their vulnerabilities, and to take preventive measures and validate signatures before applying them. Product vendors get actionable feedback from end user customers about which issues are “hot” and can tailor their signature development or patch processes to the hottest bugs among their customer base. Full documentation including reporting, packet capture and a software applet replicating the test findings are standard on the Mu-4000. VoIP equipment providers now are using Security Analyzers for:

- **Design and Development:** Vendors use their QA and development teams to repair security flaws as early as possible in the development process, measurable reduction in staffing and support costs.
- **Testing and Customer Problem Resolution:** Issues isolated and information captured by the Mu-4000 bring quick focus to remediating customer-reported problems. No more struggles to reproduce issues.
- **Product Upgrades:** Assessment of configuration changes, software updates and patches ensure security regressions or robustness issues like memory leaks or CPU utilization spikes are not inadvertently introduced.
- **Threat Assessment:** Every network has unique settings but vendors focus their testing on the most common configurations, Mutation Analysis with Published Vulnerability Analysis provides unprecedented threat assessment coverage.



### **Wide Ranging Applicability of Triple Play Product and Service Security and Robustness Testing**

Using a Mu-4000 analyzer offers end users greater service uptime, achieving more profitable services through higher reliability and robustness. The Mu-4000 helps both triple play product developers identify and expedite the remediation of VoIP robustness and vulnerability issues.

With its cost-effective test suites, Mu Dynamics addresses all major VoIP protocols including SIP, H.323 and MGCP, as well as equivalent functionality for IMS implementations. Security Analyzers are an essential and easy-to-deploy way to enable security as a process of continuous improvement.



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