

Through lab-based Mu Service Analysis training, carriers, critical infrastructure, government agencies and product developers are learning how to minimize their product or service attack surface. Mu Dynamics is already assisting end-users and product developers in using a process-oriented, proactive approach to service, security and robustness analysis and vulnerability isolation throughout product development and deployment lifecycles. Hands-on use of the Mu Service Analyzer provides unbiased metrics for real management of service, security and robustness with significant expedience in fault remediation.

Service Provider, Critical Infrastructure and Enterprise End Users

Hands-on training teaches participants how the Mu Service Analyzer plays a critical role in the product deployment lifecycle. Unprecedented and unbiased security and robustness metrics allow Security Engineers to better evaluate products. Operations executives learn how early identification of unique attack surfaces and respective disruptive vulnerabilities can prevent costly service downtime, revenue loss and ultimately customer turnover. Training provides developers with clear methods for effective fault remediation to reduce the "mean time to repair" and use regression to easily validate vendor fixes.

Product Developers

Theory and labs demonstrate how to use the Mu Service Analyzer as a customized, process-oriented approach to building service, security, and robustness analysis into the product development lifecycle. QA teams and Lab Managers discover how to quickly isolate and reproduce faults in their local environment before adversely impacting the end-user. Training participants will become familiar with the export and use of actionable remediation tools and reports that help accelerate the fault elimination process. Developers learn how to use regression to verify effective remediation efforts and to ensure that previously discovered faults don't creep back into a product.

Training Topics

Training topics include the primary service platform training using three types of analysis (SLTV Analysis, Published Vulnerability Analysis, and DoS) and attack modes (Endpoint and Passthrough). For more information about the Mu Service Analyzer and more training resources go the the Mu Dynamics web site:

<http://www.mudynamics.com>

SOLUTIONS	IPTV	VoIP	IMS	Industrial Control
MODULES	Denial of Service Analysis			
	Published Vulnerability Analysis			
	Service Level Traffic Variation (Mutation) Analysis			
	External Analysis			
PLATFORM	Mu Service Assurance Platform			

TRAINING MODULES

PLATFORM

Service Analyzer Introduction

- The Dangers of Service Disruption and Degradation
- Rigorous, Automated, Repeatable Processes
- Detailed Reports, Interactive Charts, Packet Captures GUI-Driven Solution

System Components

- Anatomy of the Mu Service Analyzer
- MGMT and AUX Ports
- Console Ports
- Attack Ports
- Power Relays
- LCD Screen

GUI-Driven Solution

- Supported Browsers
- Exploring the Homepage
- Initial Setup (MGMT and AUX ports, NTP, and Users Administration), Licenses, Updates, and Backups
- Support: Basic Troubleshooting, Inline and Online Help

Analyzer Features

- Templates
- Test Bed
- Restarters
- Monitors
- Event Actions
- Remote Automation
- Reporting
- Remediation
- Regression

SLTV

Service Level Traffic Variation VoIP and SLTV

What is Fuzzing?

- Similar structures = similar vulnerabilities
- Code “optimization” leads to exception faults
- Variant Nomenclature (position/method)
- Random vs. Directed Mutation
- “How long will this take?”

Methodology

- Protocols, Suites, Variants, and Vectors
- Surface Scan vs. Deep Dive
- Protocol Configuration and Instrumentation
- Debugging with Explorer
- Test Bed Design (client vs. client & server modes)
- Includes and Excludes (Manual vs. Dynamic)

Interpreting Results

- So what is a “fault?”
- Remediation toolset - Pcaps, Engine Logs, Monitor Logs, Response Time Charts
- How can Monitors help disambiguate results?
- Chain of Custody

Tips & Tricks

- Use mutations as DoS payloads to “turn up the heat”
- Use DoS to generate load while using SLTVs

DoS

Denial of Service IMS and DoS

Exhaustion Profiles

- Service-level DoS Modeling
- Batting Cage Analogy

Methodology

- Test Bed Considerations
- Random Field Fun
- Building Custom Payloads
- Selecting a Health Monitor

Interpreting Results

- Setting Realistic QoS / QoE Expectations
- Rerun with different service Monitors
- Try a different pattern - Tweak, Retest, Repeat

Tips & Tricks

- Use MAC flooding to turn a switch into a hub
- Simulate DDoS attacks

PV ANALYSIS

Content Playback/Published Vulnerabilities

IPTV and PV Analysis

Vulnerability vs. Exploit Testing

- Fighting the Last War
- The How and the What
- Failures of Imagination

Methodology

- Test Bed Design - Addressed vs. Transparent
- Filtering options - Dates, affected products, CVE #s
- Evasion Techniques

Interpreting Results

- Report Generation
- What does the report tell us?
- Researching a Published Vulnerability
- Sample packet captures, external source validation
- Bakeoff Differentiators - Response Times, Resource Monitoring

Tips & Tricks

- Use DoS to create load while running PVAs
- Use SLTV's against management protocols (weakest link)



web: www.mudynamics.com | email: 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