

SPIRENT LANDSLIDE

IMS SECURITY TESTING

A key aspect of IP Multi-Media Subsystem (IMS) and Multi-Media Domain (MMD) is built-in security independent of the access technology. As a result, service providers must be able to test IMS security regardless of the type of network in which it is deployed.

Spirent Communications' Landslide™ IMS Security option, with the Dynamic IPSec, IP Data Application, and IPSec accelerator card options, provides the ability to perform lab tests for performance and accuracy of secure access to the IMS. The Landslide also allows for modeling the customer experience for secure transmissions regardless of the access technology used. The IMS Security option can be used with all Spirent wireless packet data test applications.

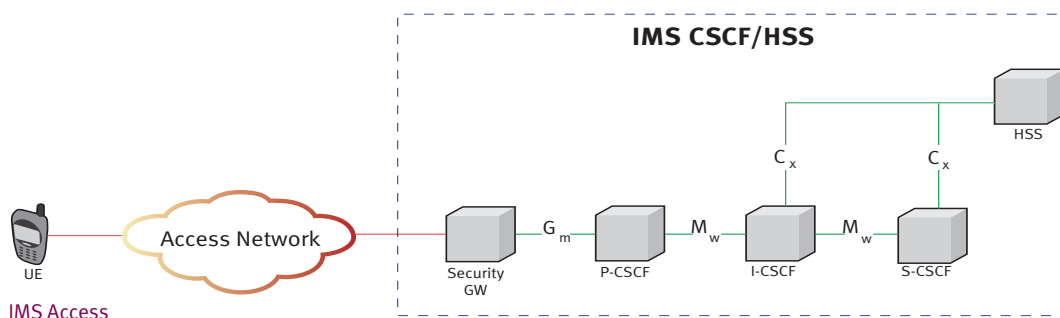
In the IMS/MMD, access to IP services is not allowed until a security association exists between the mobile node and the network. The security association is negotiated using the SIP protocol. Additionally, mutual authentication of the user and network must occur before IP services are allowed. In IMS/MMD this is done via IMS AKA. The Landslide IMS Security option supports SIP signaling with IMS AKA for mutual authentication of user and network. Additionally, the Landslide supports IPSec for secure access.

APPLICATIONS

- Validate system scalability and identify capacity limits
- Measure call/data performance
- Characterize system before trial/delivery
- Identify performance ceilings
- Enable accurate capacity planning

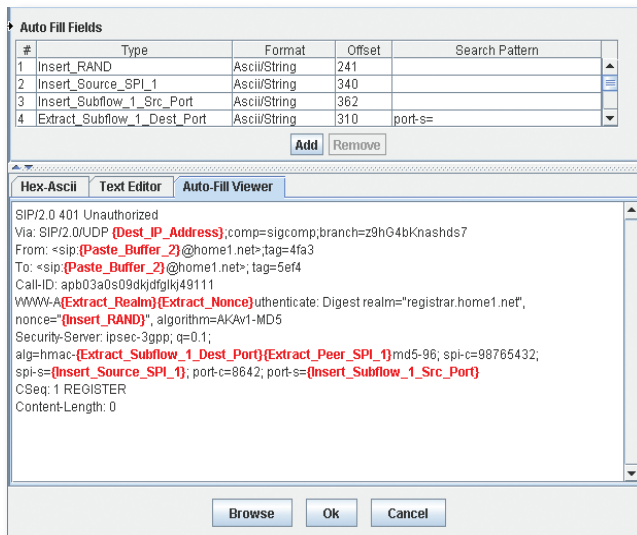
FEATURES & BENEFITS

- Realistic, real-world simulations allow equipment vendors to accurately specify the performance characteristics of their equipment under real-world conditions
- Simultaneous control and user plane allows service providers to measure the performance of their network and to validate new features and services in the lab
- Unmatched scalability for the user to simulate subscriber loads ranging from a small rural town to the largest metropolitan city
- Standard Web browser interface means there is no need to load software onto user equipment
- Emulation of multiple network elements for the user to test in a variety of network topologies providing more effective utilization of lab equipment and reducing capital expenditure and ongoing support costs associated with a test lab



FEATURES & BENEFITS (CONTINUED)

- Automation control so the user can run many test cases simultaneously or serially on multiple Landslide test servers, creating real-world scenarios for heavy load and long duration stability tests
- TCL Interface for the user to control/monitor the Landslide from a higher level management system, making it possible to compile specific test reports for both the emulation (Landslide) and the device under test
- Security Gateway Testing—Landslide emulates the UE, P-CSCF, I-CSCF and S-CSCF, isolating the security gateway for testing
- P-CSCF Testing—Landslide emulates the UE, I-CSCF and S-CSCF so that a security gateway/P-CSCF can be tested
- End-to-End Testing—Landslide emulates the UE endpoints to test all of the elements involved in IMS Security
- Customized IMS Testing—The IMS Security option is easily modified to meet the specific test needs of the user. By using the Landslide’s powerful Advanced Data editing capabilities, the user may modify any SIP messaging and authentication parameter as well as search, copy and paste data to and from both sent and received messages. This capability makes it easy to make required changes that will accommodate the specifics of a particular implementation.



Landslide Data Message Editor

TECHNICAL SPECIFICATIONS

- Landslide Test Server (without performance accelerator)
 - 200,000 simultaneous tunnels without per session certificates
 - 100,000 simultaneous tunnels with per session certificates
 - Up to 4 tunnels per emulated node
 - Up to 200 SAs per second using pre-shared key
 - Up to 100 SAs per second using certificates
 - Up to 1.5 Gbps of encrypted traffic
- Referenced Standards
 - 3GPP2 S.S0086-B: IMS Security Framework
 - 3GPP2 X.S0013-004: IP Multimedia Call Control Protocol Based on SIP and SDP
 - 3GPP 33.102: 3G Security; Security architecture
 - 3GPP 33.203: 3G Security; Access security for IP-based services
 - RFC 2617: HTTP Authentication: Basic and Digest Access Authentication
 - RFC 3310: Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)
 - RFC 3329: Security Mechanism Agreement or the Session Initiation Protocol (SIP)

The listed specifications were used as reference material in the development of this application. This does not necessarily imply full implementation of all requirements within the referenced specifications.

ORDERING INFORMATION	
DESCRIPTION	PART NUMBER
<p>IMS SECURITY TESTING</p> <p>Provides ability to test performance and accuracy of IMS security gateways. Dynamic IPsec/ACC must be purchased separately. Can be used in conjunction with other applications using advanced data. SN/MAC ID of existing Manager required.</p>	L-FT-024
<p>LANDSLIDE IP DATA APPLICATION</p> <p>Adds IP Data Application to an existing Landslide Test system. Serial number or MAC ID of existing Landslide Manager required.</p>	L-APP-007
<p>DYNAMIC IPSEC EMULATION</p> <p>Adds IPsec emulation to an existing Landslide Test System. IPsec accelerator must be ordered separately. Serial number or MAC ID of existing Landslide Manager required.</p>	L-FT-004
<p>LANDSLIDE IPSEC ACCELERATOR CARDS</p> <p>Provide hardware accelerated IPsec processing for Landslide Test Server. Requires L-FT-004 Dynamic IPsec Emulation feature. See sales rep for more information.</p>	L-ACC-003 L-ACC-004

SPIRENT LANDSLIDE
IMS SECURITY TESTING

SPIRENT SERVICES

Spirent Global Services provides a variety of professional services, support services and education services—all focused on helping customers meet their complex testing and service assurance requirements. For more information, visit the Global Services Website at www.spirent.com/gs or contact your Spirent sales representative.

AMERICAS 1-800-SPIRENT • +1-818-676-2683 • sales@spirent.com

EUROPE AND THE MIDDLE EAST +44 (0) 1293 767979 • emeainfo@spirent.com

ASIA AND THE PACIFIC +86-10-8518-2539 • salesasia@spirent.com

© 2010 Spirent Communications, Inc. All of the company names and/or brand names and/or product names referred to in this document, in particular the name “Spirent” and its logo device, are either registered trademarks or trademarks pending registration in accordance with relevant national laws. All rights reserved. Specifications subject to change without notice. Rev. C 07/10

