Threat Assessment
THREATEX NETWORK ATTACK TESTING SOLUTIONS

In today's hostile computing environment, companies are justifiably concerned about suffering attacks from malicious entities: Distributed Denial of Service (DDoS), CodeRed II worm, MyDoom, Nimda, SQL Slammer, WiFi attacks, e-mail viruses, VoIP vulnerabilities and their endless variants.

ThreatEx emulates thousands of attacks and variants including:

- DDoS
- Worms
- E-mail attacks
- Viruses
- VoIP attacks
- Wireless attacks (802.11 a/b/g)
- Expanded protocol fuzzing for finding unknown vulnerabilities
- Application penetration
- Advanced protocol fuzzing
- Additional emulations become possible with the continuous release of new exploit definitions and threat updates

IT professionals understand that defending against these attacks is a difficult proposition and the price of failure is higher than most companies are willing to admit.

ThreatEx is a complementary solution to Spirent Communications' Avalanche load-testing appliance. As a next-generation solution that provides visibility into essential areas of network security, ThreatEx enables Spirent customers to move beyond measuring the network's capacity for normal traffic. Customers can now emulate and analyze the effects of corrupt traffic and other impairments on their networks.

By using ThreatEx, network security professionals can identify vulnerabilities through realistic attacks on individual devices or entire networks. The ability to run sequences of controlled attacks greatly accelerates the task of closing system vulnerabilities and setting the right security policies. Continuously updated exploit definitions in the ThreatEx knowledge base assist in the prevention of malware surprises.

DON'T FACE THE THREAT ALONE

ThreatEx is a powerful ally in the ongoing battle to defend your network against malicious traffic. The ThreatEx solution offers a range of key benefits:

- Provides a proactive threat-containment strategy, reducing the risk of costly network downtime
- Closes the window of vulnerability while reducing the need for in-house research, since threat updates are released when new outbreaks occur
- Enhances lab-based vulnerability testing by injecting hostile traffic into a highly controlled environment
- Enables IT personnel to confirm vendor performance claims by assessing network defenses against known and unknown threats
- Features diagnostic, assessment and reporting capabilities highlighted by real-time displays
- Allows testing of robustness for next generation UTM (Unified Threat Management) Systems, verifying their capability and performance
- Provides native security testing on 802.11 a/b/g WiFi implementations

THREATEX KNOWLEDGE BASE AND UPDATE SERVICE

To ensure you are fully protected against the latest threats, Spirent offers a subscription-based threat definition update service for the ThreatEx system. Subscription to this database ensures your QA and IT staff have immediate access to the latest threat signatures, delivering zero-day testing capabilities. ThreatEx knowledge base updates can be downloaded at the end of each business day or pulled down as needed.

THREATEX DESIGNER

ThreatEx Designer enables IT and QA staff to modify existing threats or to create customized threats in minutes – without time-intensive programming. The intuitive point-and-click graphical user interface enables threats and exploits to be developed simply by describing them. The software then generates exploits using a patented TDL (Threat Definition Language) format. Users can also import specific traffic via Pcap files and replay or modify unique protocols or other transactions. Threat files can be executed directly by the ThreatEx System or stored in a central database for future use.

THREATEX PROTOCOL FUZZER

ThreatEx is a powerful system for creating actual threats that will affect real systems and security devices. Now with the optional ThreatEx Protocol Fuzzer application, millions upon millions of fuzzing variants can be created to find unknown vulnerabilities in devices or host systems quickly and easily. This is in combination with ThreatEx's powerful attack generation that pinpoints content delivery and security equipment devices' breaking points that otherwise would go unseen. ThreatEx Protocol Fuzzer provides specific suites that cover a broad range of protocols in economical packages for Internet, VoIP and IPTV including:

| Internet	VoIP	IPTV
HTTP	SIP	IGMP
BGP	SDP	PIM
CDP	H323	SCTP
EIGRP	RTSP	
MPLS uni + multi	IGMP	
OSPF		
PIM		
RIPng		
RIPv2		
UDP		
TCP		
IPv6		
STP		
SMTP		
FTP		

AUTOMATION

To streamline and automate the testing process, the ThreatEx platform includes ThreatWalker, a complete Tcl scripting environment for automating and developing test plans in Windows, Linux or Sun environments. QA staff can select an existing test plan or develop an entire test through the API. This automated approach simplifies the process of re-testing the network each time a new threat is detected.

Script developers will benefit from ThreatWalker's streamlined approach to creating regression tests for executing exploits sequentially. Developers can configure test parameters, threat parameters and statistical monitoring techniques through an intuitive GUI, and automatically generate Tcl scripts to be executed immediately or quickly customized using the Tcl templates. ThreatWalker includes templates, integrated exploits, test plan attributes and ready-to-execute threats. It is supported on Linux, Sun and Windows platforms.

A COMPLETE SOLUTION

The ThreatEx system delivers a complete vulnerability testing assessment solution to protect your network from hostile attacks. By selecting ThreatEx, your company gains more than access to the market-leading testing platform for malicious attacks. You also get a full and active partner constantly on the alert for new threats. Don't go at it alone – deflect hostile network threats by using the ThreatEx solution.
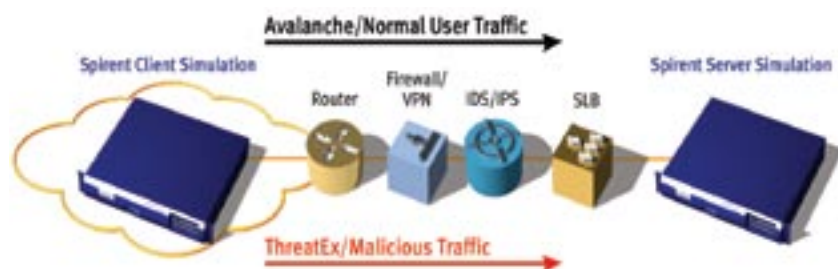
Testing with Avalanche and ThreatEx: Enables IT and QA staff to use mixtures of both positive and negative traffic to test the security infrastructure under load.

MULTI-PLATFORM SUPPORT

ThreatEx is designed to operate on multiple hardware platforms to address various testing needs. ThreatEx will run on either a ThreatEx/2700 appliance or the Spirent TestCenter™ multi-slot chassis for maximum versatility. The ThreatEx/2700 appliance delivers maximum performance in a varying fashion and includes support for both copper and fiber interfaces. The ThreatEx/2700 is equipped with a built-in pass-thru port.

Stateful and stateless threats can be combined with external traffic streams to create any number of test scenarios. For added flexibility and complete assessment capabilities, ThreatEx will also run on the multi-slot Spirent TestCenter chassis. Doing so expands the test bench to include threat capabilities to the many other applications supported on the Spirent TestCenter, including the Avalanche L4-7 application performance assessment tool.

For further information about the Spirent TestCenter chassis, refer to the Spirent TestCenter Brochure (P/N 79-000902) available at www.spirent.com on the Web.

Supported Spirent TestCenter modules include EMB-2003B, CPR-2001B, BND-0005, FBR-2001B, and EDM-2001B.

THREATEX APPLIANCE SPECIFICATIONS

When sold as an integrated hardware and software package, ThreatEx includes a 3U, 19-inch rack-mountable infrastructure stressing appliance.

- Dimensions: 5.25" H x 16.53" W x 19.75" D fits standard 19" rack, 3U high
- Weight: 31 lbs. (14 kg)
- Operating environment: 5° C to 40° C
- Relative humidity: 10– 90%, non-condensing
- Power requirements: 115 – 230 V, 50/60 Hz
- Maximum power consumption: 460 W
- Regulatory approvals: FCC Class A, CE, UL-1950, GS Mark

ORDERING INFORMATION

ThreatEx for 2700 Appliance	
TE-0001	ThreatEx Network Attack appliance with copper interfaces
TE-0002	ThreatEx Network Attack appliance with fiber interfaces
TE-0003	One-year subscription to Standard ThreatEx Knowledge database
TE-0004	ThreatEx Designer
TE-0006	Provides native WiFi 801.11 a/b/g attacks and WiFi NIC
TE-0007	Provides extended e-mail attack suite
TE-1001	ThreatEx Bundle – Appliance (copper), ThreatEx Designer, 1 Yr Knowledge Base
TE-1002	ThreatEx Bundle – Appliance (fiber), ThreatEx Designer, 1 Yr Knowledge Base
TE-0008	ThreatEx Protocol Fuzzer applications and VoIP Protocols (User must have a basic ThreatEx system at a minimum)
TE-0009	ThreatEx Protocol Fuzzer applications and IPTV Protocols
TE-0010	ThreatEx Protocol Fuzzer applications and Internet Protocols
TE-0011	ThreatEx Protocol Fuzzer Software Bundle (requires Threat Basic Platform at a minimum)
ThreatEx for Spirent TestCenter 2u Chassis	
BPK-1064A-2U	THREATEX NETWORK ATTACK BASE PACKAGE for 2u TestCenter Chassis: Series 2000 Modules Does NOT include Knowledge base update subscription (Use SUB-0001)
SUB-0001	THREATEX NETWORK ATTACK KNOWLEDGE BASE UPDATE SUBSCRIPTION 1 YR for STC 2u and 9u Chassis – One Year subscription to ThreatEx Knowledge database
BPK-1065A-2U	THREATEX NETWORK ATTACK DESIGNER TOOL KIT
TPK-1021-2U	THREATEX NETWORK ATTACK E-MAIL VIRUS SUITE
TPK-1022-2U	THREATEX NETWORK FUZZING SUITE FOR VOIP PROTOCOLS
TPK-1023-2U	THREATEX NETWORK FUZZING SUITE FOR IPTV PROTOCOLS
TPK-1024-2U	THREATEX NETWORK FUZZING SUITE FOR INTERNET PROTOCOLS
ThreatEx for Spirent TestCenter 9u Chassis	
BPK-1064A	THREATEX NETWORK ATTACK BASE PACKAGE for 9u TestCenter Chassis: Series 2000 Modules Does NOT include Knowledge base update subscription (Use SUB-0001)
BPK-1065A	THREATEX NETWORK ATTACK DESIGNER TOOL KIT
TPK-1021	THREATEX NETWORK ATTACK E-MAIL VIRUS SUITE
TPK-1022	THREATEX NETWORK FUZZING SUITE FOR VOIP PROTOCOLS
TPK-1023	THREATEX NETWORK FUZZING SUITE FOR IPTV PROTOCOLS
TPK-1024	THREATEX NETWORK FUZZING SUITE FOR INTERNET PROTOCOLS
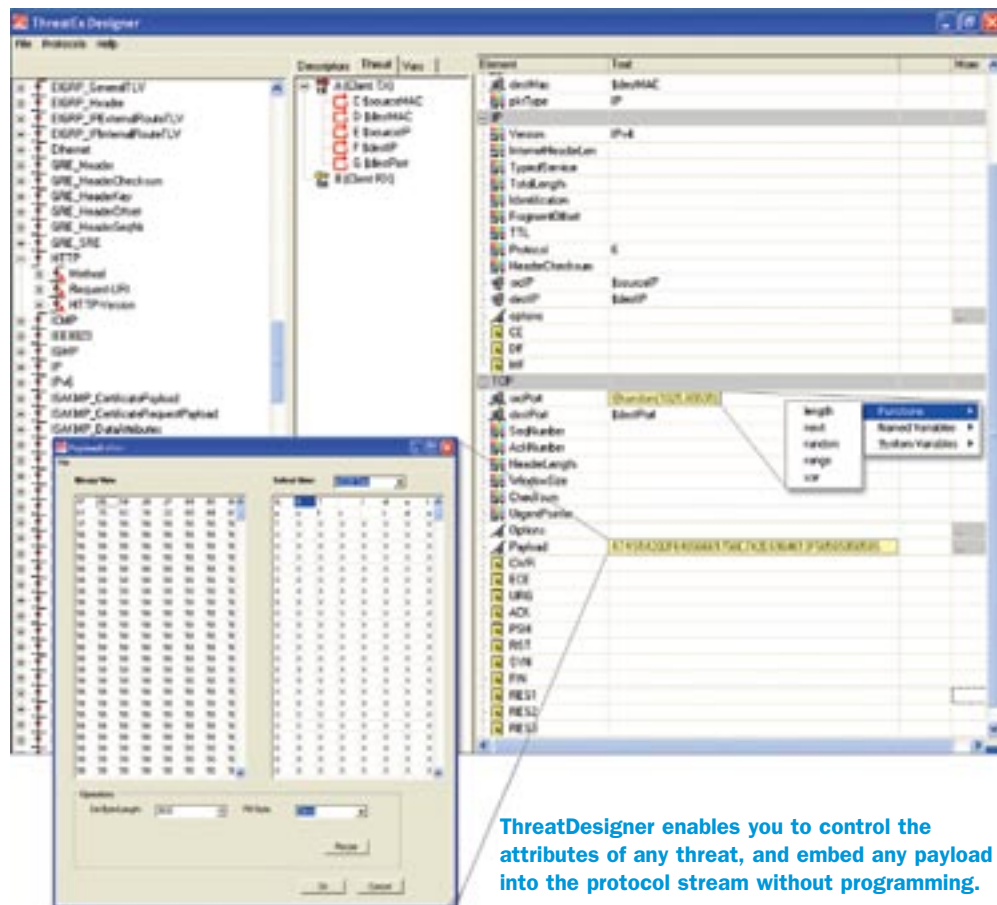
ThreatDesigner enables you to control the attributes of any threat, and embed any payload into the protocol stream without programming.

SPIRENT
Communications

SPIRENT GLOBAL SERVICES

Spirent Communications understands that internal resources for managing complex testing programs may not always be available. Our Global Services engineers enable your business to quickly implement field-proven solutions, instead of spending time and resources to develop them in-house. Further information can be found at www.spirent.com/gs.

■ ThreatEx Implementation Service: Spirent can help you manage all facets of installing the ThreatEx solution into your test bed – from site readiness analysis to physical installation and systems configuration. Knowledge transfer services are also available to help your staff perform critical testing tasks without delay.

■ Network Security Assessment: Experienced engineers from Spirent Global Services are available to assist in network vulnerability and performance assessment. Regulatory compliance can be established, and costs can be controlled by right-sizing your network security infrastructure.

■ Engineering Services: In-house access to ThreatEx product experts can reduce your company's overall risk and accelerate the delivery of custom functionality. Additional resources translate into quick ramp-up, development, testing and deployment of customized attacks and protocols.

Spirent Communications
1325 Borregas Avenue
Sunnyvale, CA 94089 USA

SALES AND INFORMATION
sales-spirent@spirent.com
www.spirent.com

Americas
T: +1 800.SPIRENT
+818 676.2683

Europe, Middle East, Africa
T: +33 1 6137.2250

Asia Pacific
T: +852 2511.3822