DATA SHEET

EXata Cyber Attack Emulator Library

The Cyber Library for the EXata Live-Virtual-Constructive Simulation Platform

The Cyber Library for EXata provides the ability to evaluate a network design for resiliency to cyber attack.

Security elements from the library can be added to EXata network models, and scenarios can be run that use attack elements that cause the network information flows to degrade as if the network was under cyber attack.

Using the system-in-the-loop emulation capabilities of EXata, the behavior of live applications across a simulated virtual network under attack can be determined and analyzed.

The Cyber Library for EXata enables you to gain unique visibility into how a network and the applications that use it will respond during a cyber attack.

Each of the models in the Cyber Library for EXata operate at one or more of the OSI network layers. The following sections describe the various models, grouped into categories:

The EXata sof tware (EXata) provides ultra high-fidelity simulated representations of large-scale wireless, wired, and mixed-platform network performance and behavior. Using the system-in-the-loop emulation interface, these virtual models can be seamlessly integrated with live equipment and applications to create sophisticated live-virtual-constructive (LVC) environments. EXata network models allow you to explore and analyze live early-stage device designs, application code response, and overall communications effectiveness in a highly realistic synthetic network at real-time speed.

MAC Layer Models

Wired Equivalent Privacy (WEP)

WEP is a MAC layer security protocol that provides security for wireless LANs, equivalent to the security provided in wired LANs. The WEP model is based on IEEE standard 802.11i-2004.

CTR with CBC-MAC Protocol (CCMP)

CCMP (CTR with CBC-MAC Protocol) is an RSNA data confidentiality and integrity protocol. WEP is known to be insecure and is replaced by CCMP. CCMP is based on the CCM of the AES encryption algorithm. The CCMP model is based on IEEE standard 802.11-1997.

KEYSIGHT TECHNOLOGIES

Network Layer Models

Certificate model: IFF Certificate

The certificate model is based on WTLSCert certificate defined in WAP WTLS WAP-199-WTLS Wireless Application Protocol Wireless Transport Layer Security Specification.

Information Assurance Hierarchical Encryption Protocol (IAHEP)

IAHEP is an encryption protocol that allows two or more secure enclaves to exchange data over an untrusted network.

MODEL NAME	MODEL TYPE
Adversary model	Multi-layer
ANODR model	Routing protocol
Certificate model	Network layer
CPU and memory resource model	OS resource
Denial of Service (DoS) attack model	Attack
Firewall model	Network layer
Information Assurance Hierarchical Encryption Protocol (IAHEP) model	Network layer
Internet Protocol Security (IPSec) model	Network layer
Internet Security Association and Key, Management Protocol with Internet Key, Exchange (ISAKMP-IKE) model	Network layer
Public Key Infrastructure (PKI) model	Network layer
Secure neighbor model	Network layer
Signal Intelligence (SIGINT)	Model attack
Virus attack model	Attack
WEP and CCMP model	AC layer
Wireless eavesdropping attack model	Attack
Wireless jamming attack model	Attack

* Annotation: Below body copy, table, or figures.

Firewall model

The firewall model is a packet-based stateless software firewall. It is a software process that inspects each packet to determine if the packet should be allowed or denied access. The firewall model is stateless in that it does not retain state once a packet has been processed by the firewall.

The firewall model is based on the iptables packet filter software found in Linux/Unix-based systems.

Internet Protocol Security (IPSec) model

The IPSec model is based on the RFC 2401, RFC 2403, RFC 2404, RFC 2405, and RFC 2406. Internet Security Association and Key Management Protocol with Internet Key Exchange (ISAKMP-IKE) provides a general framework to other security protocols for creating and maintaining Security Associations (SAs) in an Internet environment. The ISAKMP host negotiates SAs (ISAKMP SA) with other ISAKMP hosts and other security protocol, and services use these ISAKMP SA to create their own SAs.

Public Key Infrastructure (PKI) model

A PKI is an infrastructure that uses digital certificates as an authentication mechanism and is built to better manage certificates and their associated keys. A digital certificate is itself a way to reliably identify the user or computer claiming to be the owner of a specific public key.

Secure neighbor

In secure neighbor authentication (SNAuth), every mobile node establishes an authenticated neighborhood on the move. Periodically, every mobile node X broadcasts its identity packet <SNAuth-HELLO, X> to its neighborhood.

Routing Protocols

Anonymous On-Demand Routing (ANODR) Protocol is designed to provide a network-centric anonymous and untraceable routing scheme for mobile ad-hoc networks. It is based on table-driven AODV; therefore, any EXata simulation scenario using AODV can also use ANODR to implement anonymous routing.

Multi-Layer Models

Adversary model

The adversary model comprises an active adversary model wormhole attacker and a passive adversary model eavesdropper. A wormhole attacker tunnels messages received in one location in the network over a low-latency, high-bandwidth link and replays them in a different location. Wireless traffic can be intercepted by any eavesdropping entity in the network, particularly as mobile wireless nodes of the adversary.

Attack Models

Denial of Service (DOS)

A denial-of-service (DOS) attack is the act of overwhelming the resources of a victim computer or network so that the victim cannot service requests from other clients. The clients, therefore, are denied service from the victim computer or network. The DOS attack typically targets the memory or computational resources of the victim computer (or both) by sending a large volume of traffic.

Signals Intelligence (SIGINT)

The SIGINT model provides a basic framework and API upon which advanced intelligence gathering algorithms may be developed.

Virus attack model

A virus attack is modeled as the attacker node sending packets with payloads that contain signatures of some well-known attacks. These packets do not contain any actual virus payload, only their signatures. It is expected that any intrusion detection systems (IDS) or anti-virus software can detect the signature of these packets and classify them as malicious.

Wireless eavesdropping attack model

An eavesdropping attack is modeled as the eavesdropping node's MAC layer operating in promiscuous mode, enabling it to promiscuously listen to nearby wireless communication.

Wireless jamming attack model

Radio jamming, or simply jamming, is the transmission of radio signals at sufficiently high energy to cause disruption of communication for nearby radios. The signals transmitted by jammers interfere with other legitimate signals in the vicinity of the jammer, causing the signal-to-noise ratio of the latter signals to drop significantly, resulting in the corruption of those signals.

OS Resource Models

CPU and memory resource model

The CPU and memory resource model monitors the allocation, consumption, and depletion of resources for a node. This model is used in conjunction with the DoS attack model. The DOS attack model attempts to consume the resources at the victim node, causing the victim node to fail when the resources are completely depleted.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications, or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES