

Performance Intelligence Center

Security Management KPI Service Package

Benefits at a glance

- Track interconnect traffic
- Detect bypass schemes
- Combat fraud
- Monitor content downloads
- Support Sarbanes-Oxley (SOX) reporting



Business Requirement

Security remains one of the top concerns of executives worldwide. Any time a network is out of service, the end result to the service provider is significant. Customer trust is lost, revenues could be lost, and network integrity is questioned.

Challenge

Most of the investment in security has occurred at the transport layer with IT departments employing various network tools, utilities and security appliances designed to mitigate attacks. These tools are geared to individual sessions and do not have the visibility of details taking place at the network level. Many service disruptions go undetected with a transport layer view since calls or sessions can masquerade as normal traffic. The call control protocols, SS7 and SIP, provide vital details that, when viewed from a network perspective, can be critical in identifying the characteristics and source of an attack.

Solution

When a network is out of service, the end result to the service provider is significant and impacts the bottom line. Revenues could be lost and network integrity is questioned. Tekelec's Security Management solution provides network visibility and alarm analysis by identifying security breaches and unauthorized access enabling timely corrective action. Utilizing the company's core expertise in call control (SS7 & SIP), the solution combines alerting, intrusive firewalls (SS7 and IMS), and SMS firewall.

Benefits

- **Track Interconnection Traffic.** A major source of revenue loss, non-billable interconnect traffic has become an increasing concern for operators of all types. Tekelec's solution provides the tools operators need to capture available data, determine jurisdiction and properly bill for calls. The Security Management KPI Service Package provides "pre-canned" reports that focus specifically on tracking interconnect traffic revenue. Detailed records support bill-back efforts and furnish concrete evidence in the event of litigation.
- **Detect Bypass Schemes.** Operators cannot afford to allow large amounts of unbillable traffic to congest the network. With Tekelec's Performance Intelligence Center (PIC), they can detect traffic patterns related to schemes such as GSM and VoIP bypass, and request compensation using detailed records.
- **Combat Fraud.** Operators can proactively identify suspect subscriber or call patterns, which may indicate subscription, pre-paid, call-selling, International Premium Rate Service (PRS), and other types of fraud. The call data of each subscriber is mapped and analyzed to furnish accurate alarms and generate comprehensive reports.
- **Monitor Content Downloads.** Operators can use Tekelec's PIC solution to monitor customer downloads for ring tones and other services from third-party content providers, and pay only for successful downloads. Content providers are able to audit their revenue streams for accurate royalty payments to authors and publishers.

- **Support Sarbanes-Oxley (SOX) Reporting.** Control of electronic records is imperative to properly support government regulations such as Sarbanes-Oxley.
- **Comprehensive Security Solution.** When deployed with both Tekelec's industry-leading EAGLE® signaling platform and SMS, the Security Management KPI Service Package provides a comprehensive security solution.

USE CASE 1 – BLOCKING PING CALLS

Problem

Ping Calls are events where the attacker places a large number of calls into the network and then releases the call. The network becomes flooded with millions of calls causing congestion and sustained outages. The receiver of such calls receives a false call back number in their missed call list. When the calling party number is used to return the call, the victim is routed to any number of sites.

In the US, calls are routed to telemarketers. In Europe and Asia, calls are routed to premium rate service (PRS) providers charging \$300+ per minute. In the case of the PRS services, the operator ends up paying for the charges.

Solution

Tekelec's Security Management KPI Service Package solution provides applications that give service providers an alarm report identifying the ping activity. Because the solution is capable of providing end-to-end network usage data, service providers will be able to identify the source of network attacks.

Tekelec's PIC can create filters that look for characteristics of a ping call, identify large volumes of calls from one or more sources where all calls were released by the originator and call durations were under two minutes.

The PIC can monitor traffic levels on any route or trunk identifying sudden spikes in traffic levels and create alerts when ping calls occur.

Benefits

- Network protection at the call control layer.
- Reporting capability provides full visibility and alarming when attacks occur.
- Proactive identification and troubleshooting.

USE CASE 2 – SMS SECURITY

Problem

SMS can create several issues, all related to SPAM. SMS Faking is the spoofing of SS7 Signaling Connection Control Part (SCCP) addresses in an effort to gain unauthorized access to an operator's SS7 network. This access is then used to route SPAM into the network. SMS Spoofing is the spoofing of the SMS sender, in an effort to get victims to react, many times creating panic among the population and as a phishing or pharming exercise, to gain personal information about the victim. SMS SPAM is the sending of "junk mail" to many recipients usually through a broadband account. SMS Flooding impacts several areas of the network. SMSC congestion occurs, blocking all SMS messaging within the network (or the portion of the network managed by the affected SMSC). Cell site congestion occurs, blocking all calls and messaging at the affected cell site (blocks all of the available control channels).

Solution

Tekelec's Security Management solution monitors the origin of all messaging traffic and identifies the top originators of SMS that have broadband accounts. The solution sets thresholds on messaging volumes from any one originator, and creates an alarm anytime this threshold is exceeded.

Benefits

- When combined with Tekelec's EAGLE platform and the SMS Firewall, protection from hostile spam attacks, including advanced techniques like spoofing are provided.
- Reporting capability provides full visibility and alarming when attacks occur.
- Proactive identification and troubleshooting.

Tekelec Global Headquarters
 +1.919.460.5500
 888.628.5527
 sales@tekelec.com

EMEA +44.1784.437000
 APAC +65.6796.2288
 CALA +1.919.460.5500

Tekelec has more than 25 offices worldwide serving customers in more than 100 countries. Addresses, phone and fax numbers are listed on the Tekelec website at www.tekelec.com/offices.

© 2010 Tekelec, Inc. All rights reserved.
 The EAGLE and Tekelec logos are registered trademarks of Tekelec. All other trademarks are the property of their respective owners. TKLC-SB-021-NA-01-2010

This document is for informational purposes only, and Tekelec reserves the right to change any aspect of the products, features or functionality described in this document without notice. Please contact Tekelec for additional information and updates.