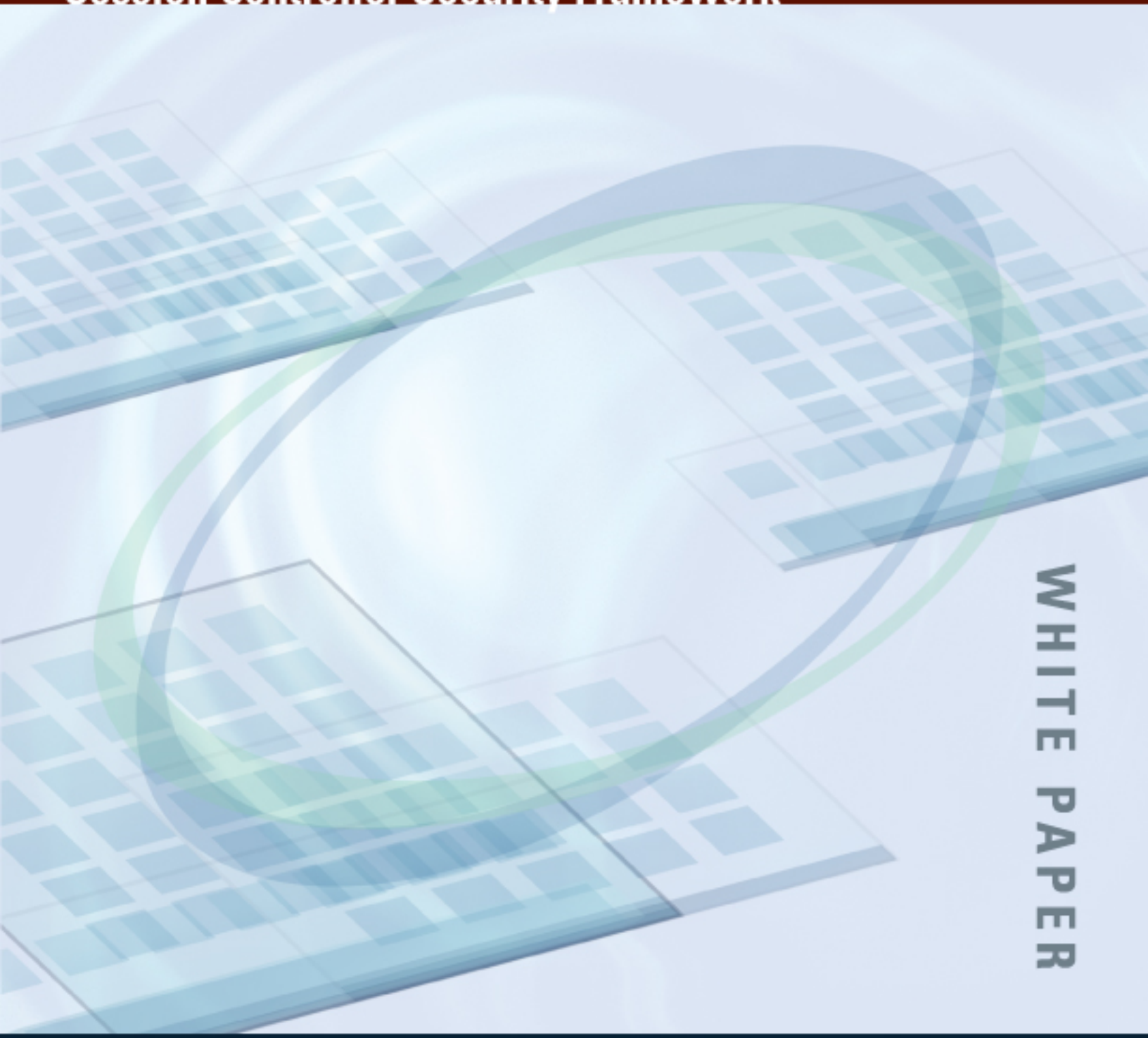
Session Controller Security Framework



WHITE PAPER

CONNECTING the WORLD'S VOICE

NETRAKE

Overview

The continued growth of the Internet has opened new opportunities for consumers, businesses and service providers. But at the same time, the open nature of the Internet has created new and potentially disastrous risks from network-based intrusion, fraud and attacks.

Current-generation network security technologies are based primarily on fixed-parameter access controls. In today's increasingly robust and dynamic communications environment, traditional firewalls simply cannot provide the needed levels of performance, privacy and network integrity.

In this Netrake white paper, we will examine the growth of Internet usage and the stress this traffic has placed on previous-generation security systems. The document also analyzes detail a new generation of hardware-based, session-oriented security technologies designed specifically to provide dynamic protection in carrier-class environments.

Internet Growth and Online Threats

The booming popularity of the Internet continues to place growing performance and security demands on provider networks.

In December of 1995, IDC estimated that the total number of worldwide Internet users at approximately 16 million. By 2005, based on statistics compiled by a range of Internet research groups, the global number of Internet users had grown to more than 880 million. According to the Internet Society, there were just 111 hosts on the Internet in 1977, yet by 2002 the Internet was home to more than 200 million systems with registered IP addresses, and the group estimates that by 2010 fully 80 percent of the planet will be on the Internet.

While there is no single comprehensive and definitive source of information on the size and growth of the Internet, conservative studies indicate that the traffic and capacity of the public Internet continues to grow at a rate of about 100 percent each year.

That explosive growth has created significant new opportunities for consumers, network operators and service providers. Yet at the same time, the very open architecture that has enabled the success and growth of the Internet has also made it vulnerable to a growing number of increasingly sophisticated on-line threats. In fact, the Internet's direct peer-to-peer communication has presented an open invitation to hackers to try to disable servers and user endpoints.

While organizations once had to deal with little more than hackers and viruses, today's enterprise is confronted by a far broader and increasingly dangerous set of network-

based risks. From the network operator perspective, two of the most common and difficult threats are Denial of Service (DoS) attacks and email viruses.

Today's increasingly sophisticated hackers take advantage of the fact that traditional network equipment cannot scan across the entire stream of data in real-time. DoS attacks can be used to stress and overload Intrusion Detection Equipment, thus increasing the probability of a successful attack. Email viruses propagate by replicating messages to all directory addresses. These floods of incoming data disrupt service and enable hackers to send malicious files to remote hosts.

The cost of these and other Internet threats is huge and growing.

In 1998, The CERT Coordination Center affiliated with Carnegie Mellon University recorded just 262 specific Internet vulnerabilities and fewer than 5,000 security incident reports. Just five years later, in 2003, CERT/CC had recorded more than 4,000 vulnerabilities and recorded more than 80,000 separate security-related incidents. In 2004, the Computer Security Institute reported over $140 billion in damage from Internet-related security breaches in the U.S. alone.

Unfortunately, traditional network security systems do not provide the carrier-class protection needed to thwart today's Internet threats.

Current Security System Limitations

Most previous-generation network security was provided by brute force firewalls that typically acted to deny all unsolicited traffic.

These older solutions depended on fixed parameter access control and delivered only static management of session-based traffic. But these traditional security systems simply do not provide an acceptable level of protection against the robust attacks and unauthorized access attempts that are common in today's real-time, peer-to-peer communications environment.

In an effort to avoid address exhaustion on public IP networks, private address ranges have been used to pool several devices through the use of network address translation (NAT). Unfortunately, current NET devices cannot handle the new generation more sophisticated applications and communications services, like Voice over IP (VoIP), that often require dynamic port assignments for peer-to-peer communications.

This situation creates a two-fold problem. First, firewalls that block unsolicited traffic across IP boundaries will not work with dynamically assigned port ranges. And second, inbound calls do not have visibility to the private address of the phone they are attempting to reach. As a result, the phone will not even ring, and work-arounds that attempt to address this problem risk compromising network integrity.

As providers have overcome historic “last mile” bandwidth constraints, and as consumers have enthusiastically bought into higher bandwidth, always-on (which are often poorly secured, and thus higher risk) endpoint products, these security concerns have multiplied. As Voice over IP grows, and as networks prepare for the emergence of IP television, video and multicasting services, the limitations of current security solutions will become increasingly evident, particularly at the network level.

A New Security Approach

Fortunately, a new and far more powerful generation of security applications has now emerged.

While older systems offered only static management of session-based traffic, today’s more capable security measures are application-aware and provide true dynamic authentication and admission control. Security systems that depended on fixed parameters for access control are now being replaced by solutions that can examine and recognize variable-length signatures and patterns, in real-time and across control and media sessions.

These more powerful and adaptive security systems allow network operators to strike an appropriate balance between the protection of user privacy and the lawful interception and monitoring of suspect traffic. By delivering real-time signature recognition and policy-based responses to IP traffic, these processing systems ensure optimum network integrity.

These hardware-based security solutions provide the access needed to support peer-to-peer communications, while at the same time protecting and preserving network integrity.

Today’s most capable systems examine the payload of a control session to determine the private address of a called device, and then coordinates with the firewall to establish a session-based “pinhole” for that media flow. Once the session in complete, the pinhole is closed, and this operation is completed from inside a carrier network with little or no impact on private networks.

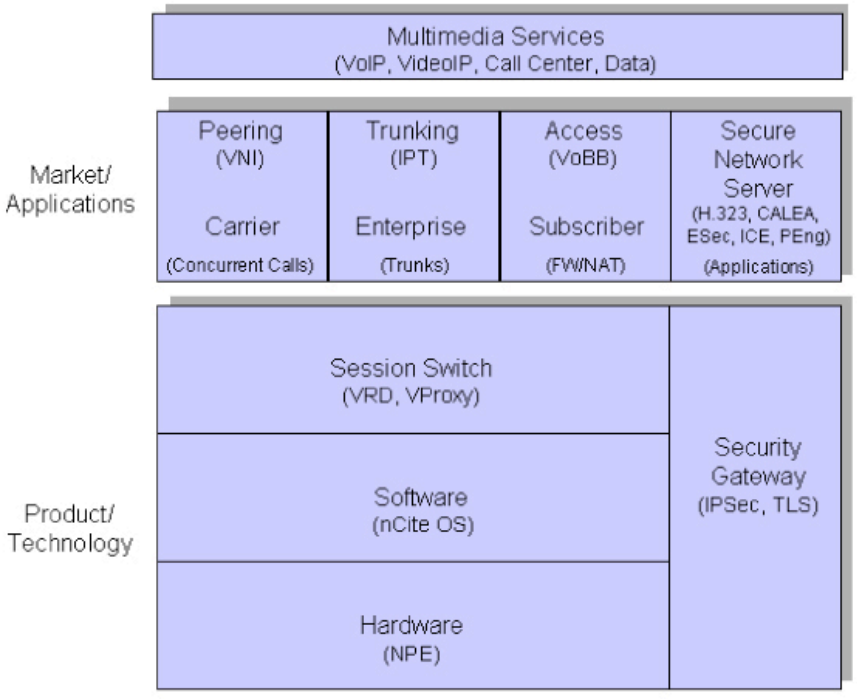
Using this approach, all traffic is scanned at wire speeds and examined for patterns across packet boundaries to discern legitimate sessions and to identify and shut down security attacks. Illegitimate session attempts can thus be filtered out before they disrupt network traffic. Because this method scans across packet boundaries, the security system can also be programmed to recognize messages with viral attachments, and then to overwrite the virus, in effect inoculating the network against that threat.

Session-Based Security Framework

The session-based security approach provides a data-plane-based DoS protection framework incorporating self-aware security features. Advanced features integrated within this architecture can include early rouge detection (ERD), late rouge detection (LRD), customer authentication and authorization, protocol and media validations, signaling rate throttling, topology hiding and intrusion prevention.

Within this framework, every session passes through authentication (customer identification) and authorization (within customer-defined service subscription) before a session is admitted to the network.

Authentication is managed through an operator-controlled process, in which customers are identified by defining an IP address or a range of IP addresses, or an ingress 8021.Q tag that a legitimate customer might use for session origination or termination. Any call that originates from this domain is classified as belonging to this customer, and any call that terminates to a device within this definition is classified as terminating to this customer.



A session border controller (SBC) is used to defend the service provider's infrastructure from attack and overload, since it provides the first point of communication and defense at the edge of the network. The framework identifies the requirements that a session border controller must satisfy to protect the SBC itself, including protection of the

service infrastructure (such as SIP servers, softswitches, application servers, media servers or media gateways), and to provide both security and privacy/confidentiality protection to the subscriber, the enterprise and the service provider.

The types of traffic that can be allowed and logged by an SBC include:

ARP response and request
RIP 2
BFD message
SIP/UDP REGISTER message
SIP/UDP INVITE message
SIP UDP response message
SIP/UDP other methods
SIP unrecognized
SIP/TCP
ICMP

Areas of Protection

This hardware-based, session-oriented approach can be implemented to erect a true network shield capable of providing comprehensive, real-time security. The broad areas of security coverage can include:

DoS prevention. Designed specifically for DoS protection for Service Provider infrastructures, this approach provides deep packet classification for signaling and media streams at Layer 2 through Layer 7. Transaction rate limiting is used to ensure that SIP devices on the secure side are not flooded with valid SIP requests from unauthorized sources. The SBC is self-protected at Layer 3 and Layer 4 against signaling floods. Early rouge and late rouge detection methods protect against fragmented and malformed messages.

Topology hiding. This framework also provides complete infrastructure topology hiding at all protocol layers for confidentiality and for the prevention of service attacks. Industry-standard encryption methods such as TLS and IPSec are used to provide privacy support.

Access control. The framework described here can also be deployed to deliver session-aware access control for signaling and media using static and dynamic ACLs based on threshold limits on Layer 3 and Layer 5.

VRD separation. This approach can also deliver support for Virtual Routing Domains (VRDs) with full inter-VRD topology hiding and separation, ability to create separate signaling and media-only VRDs.

Fraud prevention. The framework can also support a wide range of fraud prevention, including session-based authentication, authorization, and contract enforcement for signaling and media and service theft protection.

Monitoring and reporting. More advanced security solutions can also deliver network monitoring and reporting output, including audit trails, event logs, access violation logs and traps, management access command recording, Call Detail Records (CDRs) with media performance monitoring, raw packet capture ability and lawful intercept capability (CALEA).

Netrake nCite Security

Netrake has pioneered session based security management for VoIP networks and provides a solution to shield and secure service provider networks. The Netrake network shield allows VoIP traffic traversal across network boundaries while providing subscriber and application awareness. This network shield is a fundamental aspect to the design and implementation of the Network session border control platform.

The Netrake hardware-based approach is designed specifically to handle large, line rate, wire speed attacks.

The Netrake SBC is based on a carrier grade, highly scaleable foundation with the ability to provide session management for millions of subscribers. Netrake's SBC security framework identifies the requirements that a session border controller must satisfy to protect itself, the network infrastructure and the subscriber. Secure session management based on deep packet inspection and built on high-speed hardware must dynamically sense and deny services to unauthorized subscribers.

Netrake nCite security capabilities include:

- Media validation to prevent DoS attacks, including malicious RTP. The nCite allows the discarding of packets of inappropriate size, and ensures the size of packets does not change during a valid session. The nCite also performs RTP header validation by monitoring the RTP Sequence numbers and RTP version numbers. The solution also ensures that media packets are arriving at a valid rate and discards packets with known attack signatures.

- Signaling rate throttling and filtering to police the amount of transactions per second forwarded to an element in the service providers network preventing DoS attacks such as INVITE flooding.

- Topology hiding within signaling packets to ensure the service provider's VoIP infrastructure is not advertised.

- Intrusion prevention through the detection and blocking of overflow buffer attacks. The nCite has passed the CERT Advisory CA-2003-06 test suite for SIP signaling vulnerabilities.

- Protocol validation though the use of protocol syntax checking, formatting, and proper sequencing of IP protocols. Protocol validation can be used to prevent IP fragmentation attacks, SYN resource starvation attacks and ICMP floods.

Benefits of Hardware-Based Security

- Carrier-class protection against all major classes of network security threats, including fragmented traffic, malformed requests, DoS attacks, properly formed requests from unauthenticated sources, DDoS attacks and SNY floods.
- Packet-level scanning of all traffic at wire speeds.
- Real-time dynamic authentication and admission control across control and media sessions.
- DoS detection for various traffic types o the in-band (Gigabit) ports. Traffic admission based on configurable values and on SIP and H.323 signaling traffic.
- Robust protection schemes, including: deep packet classification, traffic shaping and management, alarms, logging, static/dynamic ACL methods and transaction limiting.
- Specifically designed to counteract large, line-rate, wire-speed network attacks.
- Robust, highly scalable session border management for up to millions of subscribers.
- Comprehensive security protection for softswitches, media servers and gateways, SIP servers, application servers and the SBC itself.

Conclusion

The open, peer-to-peer nature of the Internet has created exciting new opportunities for consumers, businesses and network operators. Unfortunately, that same openness poses serious risks to subscriber privacy and network security. Current-generation firewalls provide only fixed-parameter access control and cannot adequately cope with the dynamic, high-volume traffic requirements of carrier-grade networks.

Now a new generation of hardware-based, session-oriented security solutions has emerged. Based on the capabilities of Session Border Controllers, this more advanced approach delivers measurably higher levels of network performance, privacy and integrity. The Netrake nCite SBC solution is ideally suited to deliver optimum protection against large line-rate, wire-speed network attacks.