

White Paper

Security Applications and Technologies for IP Communications Networks

Dialogic White Papers

This white paper is brought to you by Dialogic Corporation as part of a continuing series on important communications topics.

Dialogic Corporation is a leading provider of world-class technologies based on open standards that enable innovative mobile, video, IP, and TDM solutions for Network Service Providers and Enterprise Communication Networks. Dialogic's customers and partners rely on its leading-edge, flexible components to rapidly deploy value-added solutions around the world.

Security Applications and Technologies for IP Communications Networks

White Paper

Executive Summary

This white paper briefly highlights past network security issues, examines the shortcomings of existing security architectures that do not address the future's security requirements, and presents possible approaches that can solve them. Notable among these approaches are those for security applications and technologies that go beyond the basic need to control "access" to the network to those that can actually securely control the network and its content, and are likely to become prevalent in the world's current evolution toward IP communications networks.

Table of Contents

Introduction	2
Applications for Security Technology	3
Communications Security	3
Enterprise Security in a Telephony Network	4
Border Control Services in the Mobile Network	5
Legal Intercept	5
Video Ring Back Tone and Video Spam	6
Security Technologies Overview	6
Network Topology Hiding	6
Authentication, Access Control, and Session Admission Control	7
Denial of Service Attack Prevention	8
Signaling and Media Control, and Validation	8
Network QoS Monitoring	9
Signaling and Media Encryption SIP Message Compression/Decompression	9
Content Scanning and Filtering	9
Summary	10
References	10
Acronyms	11

Introduction

In the early days of data networking, security was limited to passwords on sensitive servers and mainframe accounts. As networks evolved, new methods of attacks surfaced in the form of viruses, Trojans, and worms that often were not just focused on gaining access to sensitive information but also on destroying the information to cause economic harm. Soon after came the next wave of attacks, called Denial of Service (DoS), which do not destroy so much as disrupt service, producing long downtime periods that also can cause economic upheaval. DoS and infections remain the biggest concern of the Enterprise network when it comes to outside attacks on a company's assets.

Fraud and intrusion happen so regularly that a large percentage of attacks on Enterprise services actually come from people who have inside knowledge of the corporation, sometimes by employees who are either trying to bypass network restrictions to gain free services or to engage in simple espionage [Phoenix]. Today, toll fraud in a Voice over IP (VoIP) network is actually far easier than it was in a circuit switched network. Fraud and intrusion are the biggest issues driving the security needs of the data networks today. In the near future, VoIP spamming is poised to become a major issue, attacking VoIP mailboxes as well as exploiting the cheap rates to perform long distance direct calling [Korzeniowski].

To combat these issues, the Enterprise network manager employs network data firewalls, and, for the most part, can rely on a robust ecosystem to provide for the corporate needs to counter infections and intrusion. However, many corporations do not have secure circuit switched capabilities, and oftentimes their IP-gateway lies inside their "demilitarized zone" — the "safe" side of their firewall. This portal leaves a back door of sorts for fraud and intrusion that companies will eventually have to secure.

The telephony Service Provider and broadband data network carriers have many more points of access to secure than the typical Enterprise, yet until recently, network security from an IP telephony service perspective had been more of an afterthought. This is evidenced by how the IP Multimedia Subsystem (IMS) — the architectural framework for delivering Internet Protocol (IP) multimedia to mobile users originally designed by the wireless standards body 3rd Generation Partnership Project (3GPP) — can be seen as largely unprepared to provide the necessary security measures. Very little information can be found regarding security in the sense of fraud, DoS, intrusion, or infection prevention in the early 3GPP specifications.

The concept of a "session" in telephony came with the emergence of Session Initiation Protocol (SIP) call control in VoIP communications. Sessions gave rise to the need for new security methodologies, which in turn gave rise to Session Border Controllers (SBCs) as a common solution for access control issues in the next generation networks. SBCs can handle security, manage network address translations, and translate VoIP signaling between two incompatible networks. However, without a formal definition in the IMS, SBC features and functionality are inconsistent, leaving large variations in their capabilities. As a result, Security Solutions are often left up to network managers, who, when attempting to secure their data networks, just tend to add a separate piece of equipment — an external "box" — at the access areas of the network edge. This approach may not always be a sound idea because it:

1. Adds more expense by introducing another "box" to the network architecture.
2. Is not covered in the service provisioning utilities that are supposed to make everything so much simpler in IMS.
3. Introduces performance issues for IP-related media traffic by adding latency to a delay-sensitive path.

In some ways, grafting standalone SBCs onto an evolving network is a stop-gap approach. Another option for securing networks is to identify and integrate the security features to the access servers and gateways so that network managers have the necessary protection they need without having to add a separate firewall for the voice and SIP traffic.

Integrating the media and security functions can:

1. Eliminate the extra “box,” thereby reducing CAPEX and OPEX.
2. Integrate provisioning capabilities with more mainstream equipment.
3. Eliminate the additional latency in the network.

Despite these approaches, the need for security technology nowadays goes beyond just controlling access to the network, and this white paper discusses the security applications and technologies that could become prevalent in the world’s IP communications networks.

Applications for Security Technology

This section discusses several applications for security technology. While these applications may not appear to be related, they employ many of the same core technologies, which is useful when examining opportunities to apply them beyond their current use in network security.

When discussing the applications, it is worthwhile to consider two fundamental communications security areas: the ability to secure the networks and the ability to secure the content in the network.

Communications Security

Communications security is divided into two categories:

1. **Pre-connection establishment** — Performed for the typical Network Address Translation (NAT), authorization, authentication, and admission control functions.
2. **Post-connection establishment** — Performed when the bulk of data is transferred (as well as some additional signaling). It becomes important to filter, shape, scan, encrypt, and control data and signaling such that it meets the QoS contract of the subscriber. It is this post-connection functionality that many of the SBCs seem to lack.

For the most part, issues relating to securing the networks (“network security”) fall within the pre-connection establishment functions, but some are involved with post-connection functionality as well.

Issues relating to securing the content in the network (“content security”) always fall within the post-connection establishment category.

Networks need security for the following access points (see Figure 1):

1. **Access** — The most common network security component; it is located between two disparate (hierarchical) networks.
2. **Interconnect** (also known as the Peering SBC) — Sits between two peer networks to connect one operator’s core network to another operator’s core network.
3. **Enterprise** — Essentially the same as access, but geared more toward the needs of the business data center. These solutions can sometimes contain content-aware capabilities, such as virus scanning.

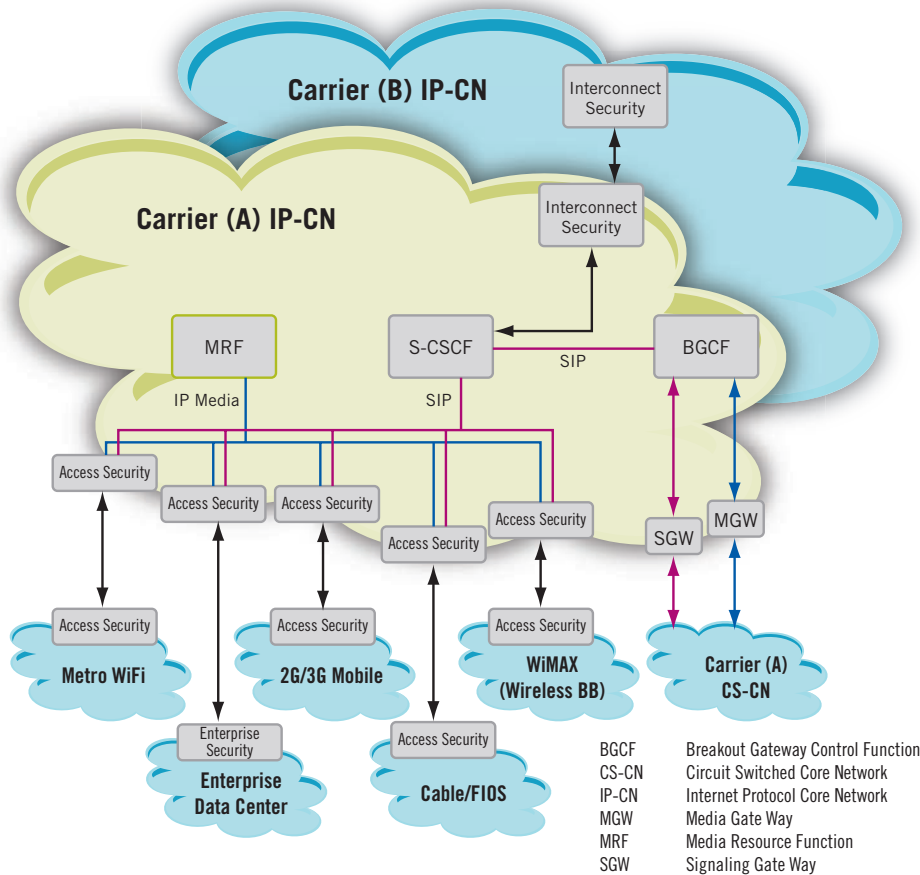


Figure 1. Where Security Plays a Role in the IP Networks of the Future

Ultimately, traffic can be made to route through the SBCs, but this does not mean that the SBCs are “big iron” boxes. Generally, the security functions of an IP network (firewalls, etc.) are a distributed function. This is crucial in a packet network, as it balances the load across numerous peer servers and reduces the impact of DoS attacks, packet storms, and other statistical phenomenon that can bring down centralized gear. Nearly every SBC vendor provides an “appliance-like” rack-mount server box as a solution.

Enterprise Security in a Telephony Network

The Enterprise opportunity for enhanced security technology focuses on the IP gateways. Store chains and businesses of all types could take advantage of security functionality integrated into the gateways. When customers deploy an IP gateway to circuit switched interfaces, they will need the ability to monitor inbound/outbound calls, identify DoS attacks, authenticate signaling traffic, rate limit or shape traffic, and enforce corporate policies.

A firewall capability provided by NAT and a routing capability in the gateway make a powerful Integrated Access Device (IAD) for small- to medium-sized Centrex service markets.

Some simple usage scenarios for the Enterprise that may be addressable with a secure IP gateway device would be:

- An employee is hijacking an IP link to enable dial-up services so that he can access his computer from a remote location.
- An employee is using a fax line to place a long distance voice call.
- An outside entity is attempting to conduct a Distributed DoS (DDoS) attack on the company PBX.
- A large number of employees are attempting to place IP-enabled calls at the same time, threatening to overwhelm the gateway capacity.
- An employee is attempting to use the IP gateway as a path to conduct a DoS attack on an external target.

Border Control Services in the Mobile Network

Every carrier has its own access network, and the core network itself is a collection of the major network carriers. It is important to understand that between every network, some sort of regulation must occur. The following is a list of some features that exist at the border between two networks:

- Network topology hiding
- Authentication and access control
- DoS attack prevention
- Signaling/media control and validation (includes Deep Packet Inspection [DPI] and policy management)
- QoS control, Call Detail Recording (CDR)
- Virus scanning, content filtering, malicious URL scanning
- SIP message compression/decompression, and signaling and media encryption
- Load balancing, traffic shaping, and filtering

These features can be found in the SBC, but the reality is that very few of these features ever show up in one “box.” In fact, many companies that claim SBC capability often only provide rate limiting, authentication, and NAT. By integrating the more advanced functions into the media and signaling gateways, a more comprehensive service solution emerges.

Legal Intercept

Moving beyond the security of the network itself, the content of the media traffic can be analyzed for legal reasons. Wire tapping is nearly as old as the telephone network. It can allow law enforcement agencies to monitor the phone conversations of “persons of interest” to help determine if they are plotting illicit activities. This law enforcement technique became much more challenging with the introduction of wireless phones, and is even harder for VoIP conversations because no specific circuit exists over which the call flows. Every call needs a CDR that contains the information to identify the calling and called party so the call can be located if billing issues arise, but access to the signaling that carries the CDR is required to monitor it. Once monitored, the call may need to be decrypted as well.

Scanning for and monitoring the number of calls needed to perform this service requires a large amount of processing. As a minimum, the call information must be tracked continuously because it is difficult to know when, or from what subscriber device, the person of interest is going to make the call. Once it is located, the call must be conferenced into the monitoring service, decrypted (if necessary), and recorded. In a more automated environment, content can be streamed in real time through a DPI process that looks for keywords of interest and flags suspect content. This DPI process is best co-located with the gateways or servers designed to process the media path to begin with, scaled with the service, and managed in the same fashion as the media resources.

Video Ring Back Tone and Video Spam

Content can come from a variety of sources, some trusted and some circumspect. Being able to protect consumers from unwanted material is a logical function for a security element.

Video Ring Back Tone (VRBT) involves playing a video message to callers' handhelds while they wait for called parties to pick up their phones. It is the same principle as the popular audio Color Ring Back Tone service, with added potential.

VRBT can be used by businesses to present an image to their customers and perhaps inform them of their products and services while the customers are waiting for their calls to be answered. However, VRBT goes beyond just this; it could actually transcend into an entertainment source, such as trivia questions or video shorts that could be played for customers while they wait for a representative to come on-line. Instead of "on-hold" music or a voice script on an infinite loop reminding the customers how important their call is, a VRBT could actually entertain customers while they wait. Such applications would be most useful in call centers, but could also be used for quick market polling of customers for a business.

However, personal video ring back tones and video SPAM are a different matter. One of the things holding back the market is the fear of objectionable material being displayed to an unsuspecting audience. That would be a very challenging protection to implement, but performing DPI on image content before it is displayed might lead to the identification of objectionable material, which could then be filtered.

Security Technologies Overview

Moving beyond the application areas, this section explores the basic functions of the traditional SBCs so as to better understand what makes them unique in the network. Not all of these functions will exist in every Border Controller, nor will they necessarily all be integrated into the media or signaling gateways; however, they need to exist to some degree, so they can be addressed from a network solution perspective.

This section is divided into multiple subsections, each highlighting the value of the notable services that could be found in a secure access gateway or edge server, as well as providing some insight as to what is involved with implementing these technologies.

Network Topology Hiding

Network topology hiding is a fundamental role of a firewall or edge security device. If a hacker understands the topology of a network, then specific nodes can be singled out for attack, allowing the hacker to re-route messages and services to the hacker's advantage (theft of service) or to create more successful DoS or viral attacks on specific services or content.

Every home cable or DSL modem has a network hiding topology service built into it called a Network Address Translation (NAT). NAT exposes only one IP address to the outside world, regardless of the complexity of the network behind it. NAT does this by mapping services directed at the externally exposed IP address to private IP addresses in the network behind NAT. In a simple translation, the TCP or UDP port number contained in the layer 3 protocol header (the layer above the IP layer) is used to map to a specific IP address and port number of a service on the network behind the NAT function. In a more complex example, the contents of the packet itself could be examined and routed according to a set of rules established for the NAT function.

NAT itself is not highly complex, and is actually a feature that can be included in most operating systems. The provisioning and managing of a NAT function is a more complicated affair because it requires web-based servers that are easier to navigate by an operations person or can be automatically provisioned by a network provisioning application.

Authentication, Access Control, and Session Admission Control

Authentication is the function that verifies whether the users initiating traffic coming into the gateway or server are actually who they claim to be. Since signaling and media are broken into different boxes in the IMS network, it requires some additional consideration as to how security is maintained.

In a digital world, a system can never truly prove that a user is who he or she says. To combat this issue, a system can challenge the user with one or more tests, which, if passed, grant the user access. Access is granted and, therefore controlled, based on one or more classes of access verification methods:

1. **Capability-based** (using encryption keys) — An encryption key is a capability-based access mechanism that can be granted to a class of users on an individual basis. Users seeking authorization to access certain network services subscribe to that service and are given an authentication key that is typically associated with a Virtual Private Network (VPN) tied to that service.
2. **Access Control List (ACL)** based — The ACL is analogous to a registration list where a user's session credentials are compared with values stored in a data base. If the credentials (username, IP address, service type requested, etc.) match the expected parameters, then access can be granted.

Control within a network can be managed in several ways. One way is to establish a VPN within the normal access network. A VPN can be a simple overlay network allocated to users of a service who have been granted access. However, Point to Point VPNs (PPVPN) can be provisioned as a number of different service classes over which specialized protocols or flags are set that provide a certain quality of service defined by the Service Level Agreement (SLA) for that application. These PPVPNs can use protocols such as Virtual Local Area Network (VLAN) tagging, Psuedowire Emulation (PE), or Multi-Protocol Label Switching (MPLS). A method of establishing QoS to the Enterprise that has become more popular recently is SIP Trunking, which allows the service to incorporate not only SIP call control traffic but data and media as well. Enterprises are using SIP Trunking as an extension of the IP-PBX, thereby extending their "private" IP telephony network across the public network to interconnect branch offices in a secure manner.

The corollary to this is intrusion detection. Intrusion detection in a network-based gateway is the ability to identify that a session has violated or bypassed the rules of authentication and access control. In essence, an intrusion includes network attacks against services data (typically stored) and applications, as well as host-based attacks such as modifying access rights, unauthorized logins, and access to data files. Also, intrusion can lead to the insertion of malware (viruses, Trojans) into the secure network. A Network Intrusion Detection System (NIDS) [Northcutt] is constructed of sensors, monitoring agents, and event logging engines. The sensors contain the significant data that distinguishes the quality of the NIDS. Running these operations in real time can take up a significant amount of processing power and can add latency to the data path.

Session admission control monitors usage for a particular client in a given session and relies heavily on Access Control Lists. This is a policing function that limits calling activity based on thresholds set administratively for parameters such as total session count, total bandwidth utilization, QoS metrics, etc. This function requires call logging and real-time session monitoring, as well as instrumentation of the session parameters and access to account privileges.

Denial of Service Attack Prevention

The essence of a DoS [Houle] attack is to deny service to one or more network entities by overwhelming their resources and causing economic harm. Common attacks include such actions as:

- Smurf attacks that use Internet Control Message Protocol (ICMP) broadcast messages by substituting the victim's address as the source address of the ICMP request. This tactic amplifies the attack as the network equipment attempts to respond to the ICMP bogus requests.
- Ping attacks that occur when several machines send a continuous stream of PING messages to the victim. The messages overwhelm the victim machine as the Medium Access Control (MAC) device in the server's network interface card cannot respond to the requests.
- SYN flood attacks that send continuous connection requests to the victim, substituting bogus source addresses. The victim opens up a half connection for each request and sends a response to the bogus address. Eventually, connection resources are exhausted, preventing the victim from taking on legitimate traffic until the attack stops and the connections time out.

Many variations exist for these attacks, and new ones are still surfacing. Several techniques can be used to slow down the onslaught of a DoS attack, provided the network is equipped with the necessary mechanisms to begin with. One technique retains an auxiliary set of IP addresses and a load balancing system. In the event of a DoS attack, the Border Element (BE) would need to recognize the attack is taking place and perform alternate routing using the load balancing mechanism. Trusted servers and network equipment can then be alerted to the route change, leaving the DoS to attack a non-existent site.

Signaling and Media Control, and Validation

Fraud is often conducted on a network via the introduction of bogus information that allows an attacker to gain access to services. Signaling control and validation requires an understanding of the signaling protocols and how to validate their authenticity. Subverting signaling is a technique used by attackers to steal services. In order to prevent this, the security function at the application layer (OSI Layer 7) performs an analysis of the signaling content or even Deep Packet Inspection (DPI). DPI is a very processor-intensive operation that requires the bit-by-bit analysis of the actual packet header and contents. In a standard server solution, DPI is accomplished first by streaming the packets to a storage disk or a large memory, then processing. This adds significant latency to the traffic. Silicon components containing acceleration logic can be employed to do DPI on the fly, minimizing the latency through the system. Although most packets can be evaluated on their own, some sessions must be monitored for trends, requiring many packets before a result can be determined.

At the application layer, the packet contents are evaluated for their format and meaning (syntax and semantics) to verify that the packets will do what the session expects them to do.

In addition, policy management must be conducted on each session such that the signaling detected is authorized to be passed in this session. This technique may be important for the Service Provider as a means by which it can control Peer to Peer (P2P) traffic, for which it may not otherwise get revenue.

Just like signaling control and validation, the media control inspection process is evaluated in terms of syntax and semantics; however, since media is controlled by its associated SIP messaging, an additional factor is available that ensures media sessions between SIP user agents are the same as the sessions that were originally negotiated during the session setup.

As mentioned in the *Authentication, Access Control, and Session Admission Control* section, the IMS has a synchronization problem with validation and authentication between media and signaling channels when each is terminated on a separate box. This problem needs to be solved in order to eliminate the requirement for a front-end (standalone) SBC.

Once the session is confirmed, it still must be authenticated against the policies in place for that service and the SIP user agents. This information is often available via a database access to the Home Subscriber Server (HSS).

Network QoS Monitoring

The security concepts can be extended into network quality as well. Managing the QoS requires further instrumentation of the packet stream to watch for things such as packet latency, jitter, and lost or malformed packets. In addition, a BE may be required to help ensure the SLA of a given service by managing the priority queuing policies of real-time signaling and media streams. It is quite common for these priorities (established with tags in the protocol headers) to be reset when traffic is passed between networks, especially when the traffic arrives from another operator's network. The BE must provide the ability to be aware of the SLA established with the other network for traffic associated with the session type and re-assign or re-prioritize the traffic accordingly. Much of this functionality lies in the application layer services, but is a natural fit for the type of processing discussed so far.

This quality information can be stored in the associated CDR. In addition to the CDR, equivalent session-level accounting allows for more policing and monitoring of the actual session. Session Detail Recording (SDR) allows the OA&M facilities to track the usage of SIP-based services for accounting, billing, regulatory, and legal intercept (see CALEA compliance at <http://www.calea.org>).

These features provide a secure external policy and control interface that allows administrators and administrative applications to manually or automatically change the way traffic is handled on a per-session basis.

Signaling and Media Encryption SIP Message Compression/Decompression

As noted previously, since the media and signaling gateways and servers were already processing the contents of the session, it was natural to perform other services on the content so as to avoid multiple "touches" of the session. Some of these additional functions can involve encryption and compression.

Multiple signaling and media encryption techniques are in use today. SIP signaling employs a technique known as Transport Layer Security (TLS) (see <http://www.ietf.org/html.charters/tls-charter.html>). TLS (and its predecessor, Secure Sockets Layer [SSL]) is a cryptographic protocol used in web browsing, email, and internet fax. The BE must provide a mutual authentication protocol (where both ends of the session are authenticated), which requires a Diffie-Hellman or Phase-Shift Keying (PSK)-like key exchange along with a 3DES or AES cipher and an HMAC-MD5 or HMAC-SHA cryptographic hash function. These functions can be run in several cryptographic acceleration processors, as well as in host-based solutions.

Media encryption requires Secure Real-time Transport Protocol (SRTP), which is a much simpler security protocol. SRTP helps secure the content itself from unwarranted eavesdropping. While this standard is not widely deployed yet, demand is growing.

SIP messages can be (and often are) compressed in the network in order to reduce bandwidth demand and improve response time of these messages across the network. Being able to perform real-time compression and decompression of the SIP signaling is not a difficult technology, but nonetheless puts demands on the processing power.

Content Scanning and Filtering

In order to stem the ever-increasing flow of unwanted content in the network, techniques may be employed that scan the content streams and filter undesirable content from the network before they arrive at the attacker's intended destination.

When it comes to the ability to perform real-time content virus scanning, the emphasis is that it be done in real time on the traffic flow because if it cannot, session traffic must be stored to the hard disk (or an extremely large and possibly expensive memory disk).

Being able to scan in real time is the notable aspect of the video content scanning technology mentioned in the *Video Ring Back and Video SPAM* section. In order to perform this in real time, sufficient processing power must be applied. While this is not difficult in a low-density application, it could become quite intensive for a Service Provider application.

For example, one way to scan for video content in real time could be to employ enhanced versions of the algorithms used to identify a value proposition for a customer's logo displayed on the boards during a hockey game. In this case, each time the logo is clearly visible, the application registers the "hit" to determine the value of the logo position to the customer. By using a more advanced version of this algorithm, running in real time, specific content or generally suspect content can be looked for that may need to be filtered. This could be done through a series of correlation algorithms that could either run in parallel or successively over a segment of the video.

Content filtering is pretty straightforward, but scanning in real time for malicious URLs is a bit more demanding. A malicious URL is used to intentionally misdirect traffic as a means of fraud or attack upon a network server. It requires the attacker to alter the content of the protocols in order to fool the network. To prevent this, each data packet must be inspected against known methods of spoofing. If the URL is "malformed," then the entire packet must be discarded. This technique requires a fair amount of processing power, but is consistent with many of the other methodologies discussed so far (such as DPI) and fits well within the scope of the gateway or BE.

Summary

This white paper introduced the need for security in the network and its content, and highlighted the various places in which this functionality could be incorporated. Also presented was the option to go beyond deploying independent SBC boxes (as a front-end to the normal IMS network) to consider solutions that could incorporate the security functionality inside the edge components of the network to reduce traffic latency, operational and capital expenditures, and network complexity. Finally, some of the applications for security in the IP communications network and the security technologies that could be found in a secure access gateway or edge server were discussed.

References

[Houle] Kevin J. Houle, George M. Weaver, "Trends in Denial of Service Attack Technology," US-CERT Coordination Center, October 2001.

[Korzeniowski] Paul Korzeniowski, "VoIP Emerging as Next Spam Entryway," TechNewsWorld, August 2005
<http://www.technewsworld.com/story/45518.html?welcome=1209481825>.

[Northcutt] Stephen Northcutt, "Intrusion Detection FAQ: What is network based intrusion detection?," SANS Institute, http://www.sans.org/resources/idfaq/network_based.php.

[Phoenix] Trusted Strategies, L.L.C. commissioned by Phoenix Technologies, Ltd., "Network Attacks: Analysis of Department of Justice Prosecutions 1999-2006," August 2006.

Acronyms

3GPP	3rd Generation Partnership Project
ACL	Access Control list
BE	Border Element
CALEA	Commission on Accreditation for Law Enforcement Agencies
CAPEX	Capital Expenditure
CDR	Call Detail Recording
DDoS	Distributed DoS
DoS	Denial of Service
DPI	Deep Packet Inspection
HSS	Home Subscriber Server
IAD	Integrated Access Device
ICMP	Internet Control Message Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
MAC	Medium Access Control
MPLS	Multi-Protocol Label Switching
NAT	Network Address Translation
NIDS	Network Intrusion Detection System
OPEX	Operating Expenditure
P2P	Peer to Peer
PBX	Private Branch eXchange
PE	Psuedowire Emulation

Acronyms *(continued)*

PPVPN	Point to Point VPNs
PSK	Phase-Shift Keying
QoS	Quality of Service
SBCs	Session Border Controllers
SDR	Session Detail Recording
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SRTTP	Secure Real-time Transport Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VRBT	Video Ring Back Tone
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network

www.dialogic.com

Dialogic Corporation

9800 Cavendish Blvd., 5th floor
Montreal, Quebec
CANADA H4M 2V9

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH PRODUCTS OF DIALOGIC CORPORATION OR ITS SUBSIDIARIES ("DIALOGIC"). NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

Dialogic may make changes to specifications, product descriptions, and plans at any time, without notice.

Dialogic is a registered trademark of Dialogic Corporation. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 9800 Cavendish Blvd., 5th Floor, Montreal, Quebec, Canada H4M 2V9. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

The names of actual companies and products mentioned herein are the trademarks of their respective owners. Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement their concepts or applications, which licenses may vary from country to country.