WHITE PAPER

Secure All-IP Telephony

Network protection is serious business. *Anywhere* there's a hole in a network security "fence" or "gate" some snooper, hacker or toll-fraud thief is going to find it. A good, solid network protection strategy builds a series of security "gates" at multiple layers within the OSI model.

PATTON®
Let's Connect!™

Contents

Authored by

W. Glendon Flowers
Product Marketing Manager
Patton Electronics Co.

Marc Aeberhard
Product Line Manager,
Patton Electronics Co.

Patrick Ramer
Chief Software Engineer,
Patton Electronics Co.

Printed in the USA.

Introduction

Voice-over-IP technology has given birth to several daughters: unified communications, SIP trunking, hosted (IP) PBX and cloud telephony. These developments offer features that boost workforce productivity along with streamlined, flexible network architectures and reductions in capital expenses (CapEx) and operating costs (OpEx). Unfortunately, the ALL-IP revolution has a downside. Converged communication networks widen the attack surface for malicious players on the Internet. IP telephony opens the enterprise network to such vulnerabilities as toll fraud, denial of service (DoS) and distributed denial of service (DDoS) attacks, among others.

> *"Ultimately, it's the very flexibility that makes VoIP systems so appealing that also makes them vulnerable; businesses that adopt VoIP as a communications standard need to consider implementing additional security practices to keep business data secure."*
>
> – *Larry Alton*

With toll fraud, the company may never notice the intrusion until the exorbitant phone bill comes in. With DoS/DDoS the loss of network resources is quickly apparent, yet the disruption of business operations is costly, and may take hours or days to resolve.

Network protection is serious business. You want to secure your ALL-IP network systems against all manner of hackers, snoopers, malicious intruders and the like. That's what this white paper is about: *network security for enterprise-class IP telephony*.

This paper proposes an enterprise network security solution for SIP (session initiation protocol) based VoIP telephony with SIP trunking service delivered by an Internet telephony service provider (ITSP). The solution relies on an enterprise session border controller (eSBC) installed as customer premise equipment (CPE) at the subscriber location.

The eSBC reduces the attack surface of the enterprise network systems by creating a "choke point" that prevents intruders from sending unauthorized data or extracting valuable or sensitive data from a network.

> *"The attack surface of a software environment is the sum of the different points (the "attack vectors") where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment. Keeping the attack surface as small as possible is a basic security measure."*
>
> — *Wikipedia*

To ensure the enterprise local area network (LAN) is protected against security threats, we need mechanisms at various layers of the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) model for network communication (see figure 1). Because, *anywhere* there's a hole in a network security "fence" or "gate" some snooper, hacker or toll-fraud thief is likely to find it.

Trojans

For starters, you don't want any Trojans hiding in your VoIP equipment. Recently, the news has been about gear from "certain countries" contains backdoors that allow snooping and hacking into your network. *We don't like that*. So, let's start with choosing reliable, high-quality manufacturer located in a trusted country. No Trojans.

Multi-Layered Strategy

A good, solid *network protection strategy* builds a series of security "gates" at multiple layers within the OSI model. Each and every sender must clear all the gates before being admitted to the enterprise LAN and VoIP network.

So, as we outline our network-protection (security) strategy, which will be implemented in an eSBC device, let's start at the bottom of the seven-layer OSI model and work our way up.

As figure 1 shows, the Access Control List (ACL) provides security/firewall functions that span three of the OSI layers: 2) Frame, 3) Packet, and 4) Transport, which we will discuss in layer-by-layer detail below.

"Phone fraud is a multi-million dollar industry that crosses international and industry borders. Attackers target call centers, as well as consumers, in attempts to gain access to funds, steal merchandise, and phish for identities. Phone fraud is now so prevalent that the average enterprise call center is exposing more than $9 million each year to fraud."

– Pindrop Security

Layer One: Physical

Interface Activation/De-activation. At the most basic level unwanted access to the network via a physical interface must be prevented. This means any ports on the eSBC that are intended for future activation (not currently intended for active use) should be disabled—that is configured as out-of-service. The eSBC must provide such configuration capability.

Layer Two: Frame Layer

ACL MAC filtering. One aspect of the ACL is filtering on the Media Access Control (MAC) address. The MAC address is a device identifier at the Ethernet frame layer. Defining known and trusted Ethernet devices—hardware SIP phones, software SIP phones on PCs and laptops, skype-for-business (S4B) endpoints and other unified communications (UC) clients endpoints—provides a way to block unknown (suspicious) devices from entering the enterprise LAN and wreaking havoc.

Layer Three: Network (IP/Packet) Layer

ACL IP filtering. The access control list supports filtering by Internet Protocol (IP) addresses. Trusted (friendly) and suspicious or known malicious IP addresses are called out and either blocked or allowed accordingly.

ACL call initiation filtering. Another ACL feature that may be configured involves blocking voice traffic associated with calls that were not initiated by a SIP endpoint within the enterprise LAN or the trusted remote peer, the ITSP Domain or IP.

Trusted Networks. Only trusted networks are allowed: Using virtual private network technology (VPN), remote networks can securely be granted access to the phone service provided by the ITSP.

Overload protection. To prevent DOS/DDOS attacks, the maximum packet volume threshold

7 Application: Encryption	SIP-Trust-Remote—Only allows SIP messages from trusted peer User Agent header check Call Routing—Reject calls with odd destinations or source ID
6 Presentation: CODECS	RTP CODEC restriction—Reject calls with odd CODECS
5 Session: SIP/B2BUA	SIP Authentication—Username/Password authentication SIP-Peer-Flood prevent—Rejection of SIP messages in case of DoS attacks
4 Transport: RTP/TCP/UDP	ACL—TCP or UDP port filtering SRTP—Encrypt network signaling (SIP header encryption) TLS—Encrypt digital media (voice encryption)
3 Network: IP	ACL—IP filtering ACL—Allow traffic only for connections set up from inside (LAN to WAN)
2 Frame: Ethernet	ACL—MAC filtering
1 Physical: Media	Device—Unused ports can be disabled

Figure 1: eSBC security gates presented according to OSI layer

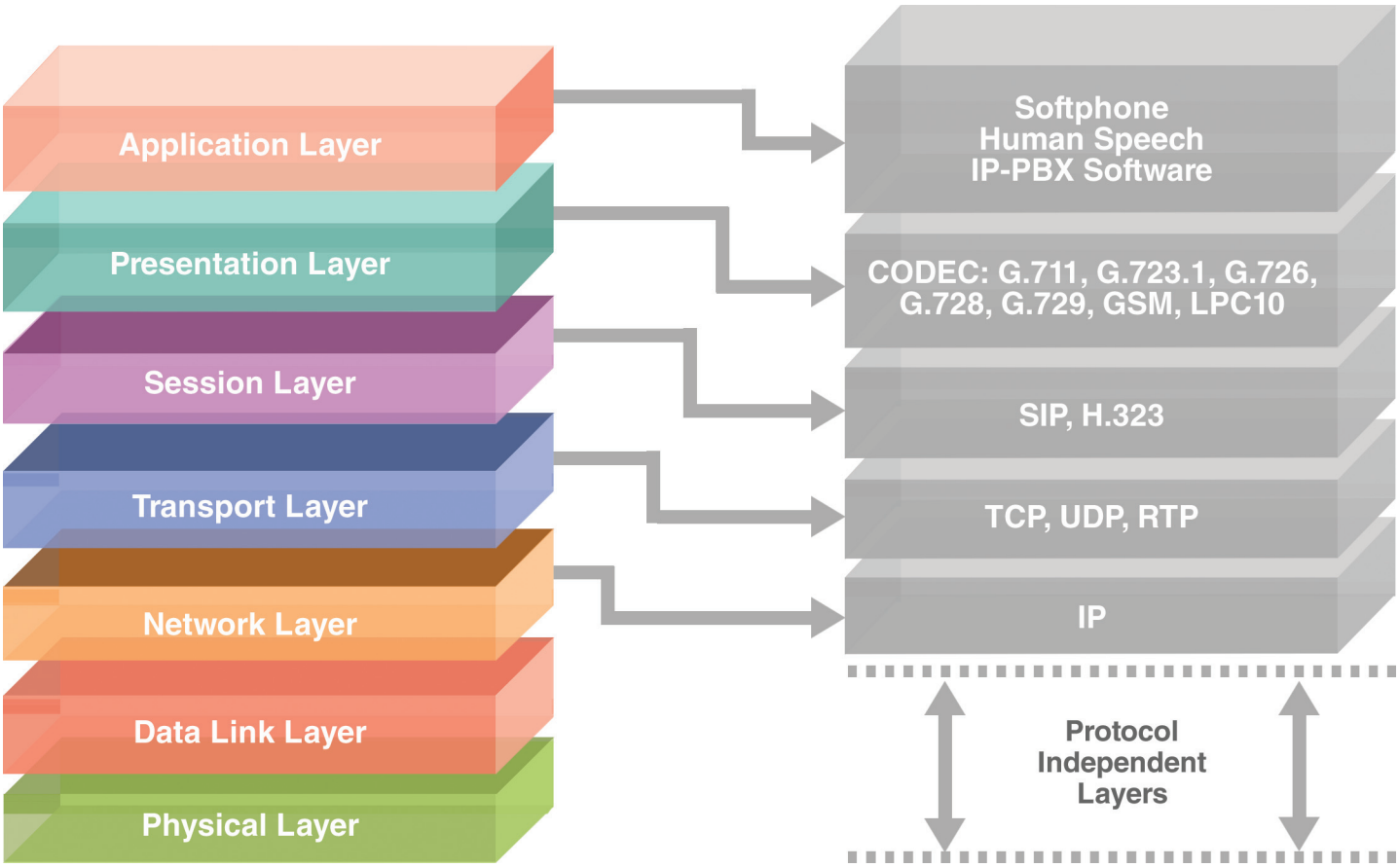

Figure 2: Mapping VoIP protocols to the ISO OSI Model

can be specified in the eSBC device configuration. When the threshold is exceeded, further incoming traffic is blocked until the volume returns to a normal expected level. This function prevents a total breakdown of the enterprise network.

Layer Four: Transport Layer

Port Blocking. For voice over IP (see figure 2), we're talking about the session initiation protocol (SIP) protocol data unit (PDU), which is encapsulated in a User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) in the transport layer. UDP or TCP ports exploited by malicious entities (notably 5060 and 5061) can be blocked. Attackers often use these ports to locate a weakly-configured IP PBX system and brute-force SIP passwords. Once the attacker has access to the account, they may use it to make or resell unauthorized calls. The attacker may also use the access to conduct a voice phishing (vishing) campaign. Port blocking can obviate such attacks.

> *"Toll fraud, which is sometimes called VoIP fraud, is when a hacker is able to access your phone system and make fraudulent long distance calls from your account. Long distance per-minute charges add up fast. According to a survey conducted by the Communications Fraud Control Association (CFCA), a whopping $46.3 billion in losses were attributed to toll fraud in 2013 alone."*
>
> — *Bruce Brownlee, Callforwarding.com*

Encryption: A fully secure eSBC solution employs data encryption for both the signaling information and the encoded media (voice).

- **Transport Layer Security (TLS)** encrypts the signaling (header information) of the SIP PDU. The encryption prevents invasive parties from capturing calling or called party information for malicious purposes. The encryption also aids in preventing address spoofing.
- **Secure Real-time Transport Protocol (SRTP)** encrypts the digital media enclosed in the RTP PDU (RFC 3550). The encryption prevents snooper and hackers from listening in on sensitive voice calls and exploiting that information. SRTP uses two types of keys: session keys for the content and master keys like the lock on your door.

Stateful Firewall: This function ensures incoming traffic is only accepted once the connection has been initiated. Your business is your castle. Who wants to come in? Is your drawbridge up or down? Traffic may be allowed or disallowed based on the state of the transport connection. Connection Established? Gate open. Connection Terminated? Gate closed.

With the help of a B2BUA this functionality can be leveraged at the application level. See B2BUA in section Layer Seven: Application.

Layer Five: Session Layer

The SIP protocol per se (RFC 3261) lives in the session layer. There is a rich set of mechanisms defined with in the SIP standard that can be leveraged to prevent toll fraud and DOS/DDOS attacks.

- **SIP Authentication**—Username / Password authentication ensures only valid and legitimate callers can initiate a SIP call. Here's how the process works:
  1) A User Agent Client (UAC) sends a SIP message to a User Agent Server (UAS)
  2) The UAS responds back with a 4xx challenge response
  3) A UAC uses data in the 4xx challenge response to encrypt his or her identity credentials (e.g. telephone password)
  4) The UAC resends the SIP message with the encrypted credentials

This four-step process ensures that only authenticated messages are sent to SIP applications for processing. Messages that don't pass authentication are discarded.

- **SIP-Trust-Remote**—A list of trusted remote peers can be configured for each SIP interface on the eSBC device. The trusted peers list may be specified using IP addresses or fully qualified domain names (FQDNs). When this mechanism is set up, connection requests from peers not included in the list will be rejected. Requests sent from not trusted hosts receive a SIP 503 Service Unavailable response from the eSBC.
- **SIP-Peer-Flood prevent**—When a DOS/DDOS attack is indicated by the network layer, SIP messages are rejected until the threat is cleared.

Layer Six: Presentation

This is where the coder-decoder (CODEC), which converts analog voice to ones and zeroes (digital voice packets(/RTP), is specified. Common codecs, such as G.711, G.722 and G.729, are well known. Part of a good security policy at this layer involves blocking as suspicious any traffic that employs an "odd", unusual, or unrecognized CODEC.

Layer Seven: Application

Provisioning/Configuration—Access to the CPE device for provisioning and configuration is restricted to known and approved customer accounts with authenticated credentials. User names and passwords are encrypted. In addition, TFTP and Telnet access to the device can be enabled or restricted to prevent unwanted penetration.

A state-of-the-art eSBC ensures only secure access is granted using HTTPS for the web interface or secure provisioning with mutual authentication of client and server. For CLI access SSH is required, while Telnet and TFTP access are not secure and should be disabled.

B2BUA*—In addition to standard SIP protocol functions, a software entity known as a back-to-back user agent (B2BUA) may also be employed in the application layer. At this level, call routing protections can be set in place. Using deep-packet inspection, source and destination addresses can be examined for any anomalies in the address format. Protocol Data Unit (PDU) headers, including calling and called numbers can be validated for correct format and content. Non-conforming call requests are rejected to prevent any suspicious traffic from penetrating the enterprise network. In other words, throw out the garbage.

Call Routing—number format, number range are inspected and validated against know and trusted callers. Call blocking may be implemented against calls coming from suspicious or unwanted sources, such as certain countries or call centers.

Operating System Security

Additional security features that protect the SmartNode Trinity operating system include the following:

- **Signed Software Images**—To prevent any maldware, virus, or other malicious manipulation of the software upgrade image, Trinity-based devices only accept software images that are signed by Patton during software upgrade.
- **Boot-Loader Security**—This mechanism protects SmartNode devices against root access or access to file systems.

Conclusion

Many vendors of VoIP CPE products offer some of the VoIP security mechanisms described in this paper. Patton's SmartNode line of eSBC products has implemented *ALL* of them, at every layer of the OSI schema—in a single customer-premise device.

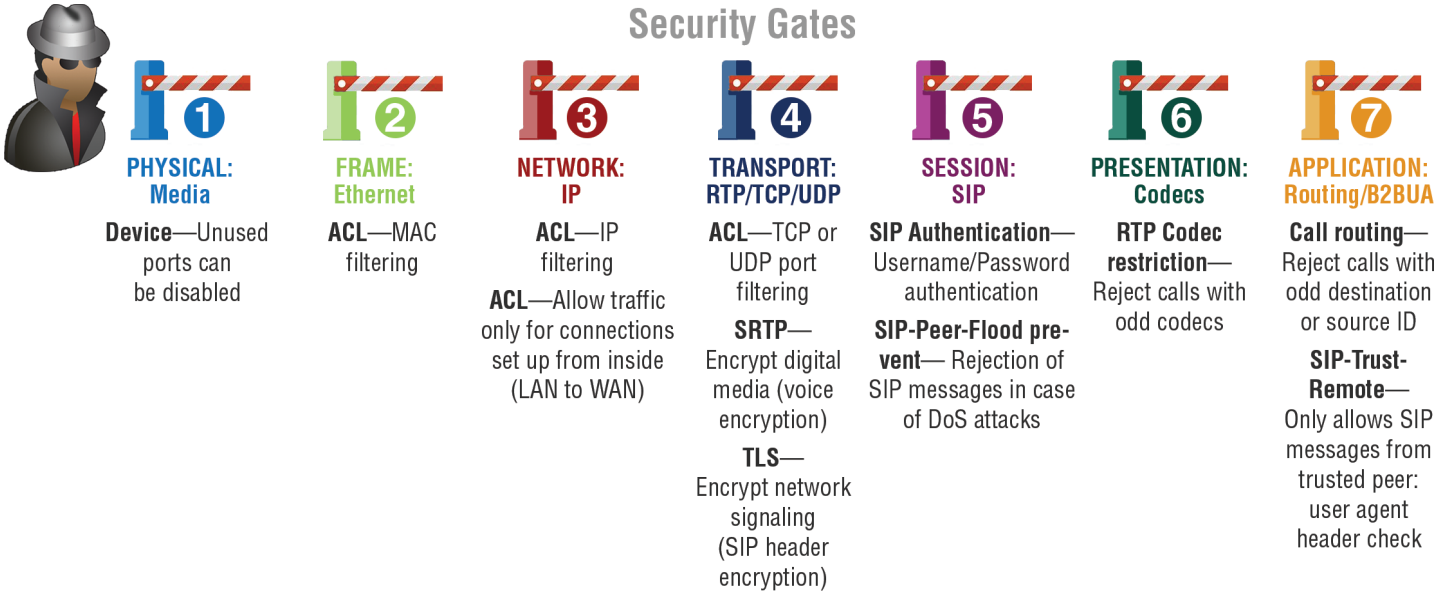

Figure 3: Security gates implemented in SmartNode eSBCs

*[RFC3261], Section 6 defines the following terms:

- UAS: a SIP User Agent Server.
- UAC: a SIP User Agent Client.
- B2BUA: a SIP Back-to-Back User Agent, which is the logical combination of a User Agent Server (UAS) and User Agent Client (UAC).

About Patton

Patton is all about connections. It is our joy and mission to connect real-world customer challenges with high-quality, right-priced solutions—complemented by unrivaled customer service and technical support. Incorporated in 1984, Patton has built everything from micro-sized widgets that connect "this-with-that," to carrier-grade Telecom gear that connects subscribers to service-providers. Patton's specialty is interconnecting legacy TDM and serial systems with new-generation IP-based voice, data, and multimedia technologies.

Headquartered in Gaithersburg, MD, USA, Patton equipment—including VoIP, Ethernet extension, and wireless router technologies—is up-and-running in carrier, enterprise and industrial networks worldwide. Patton works in connection with a growing network of technology, business, and sales-channel partners. To connect with local-market requirements, Patton operates training and support centers in Switzerland, Hungary, Lebanon, Australia and the USA.

Patton… Let's Connect!

About the authors

W. Glendon Flowers
Product Marketing Manager,
Patton Electronics Co.

Glendon is responsible for creating corporate marketing and technical content including press releases, web copy, white papers, case studies, educational and tutorial pieces as well as other publications. He serves as editor in chief for Patton's email newsletter and other outbound communications. He holds a Bachelor of Science in Computer Science from UMUC and a Bachelor of Music in percussion performance from UMCP.

Marc Aeberhard
Product Line Manager,
Patton Electronics Co.

Marc is SmartNode Product Line Manager at Patton, based in Switzerland. He is a specialist in business administration and technical management and holds a Swiss federal diploma. He is involved in telecommunication technology for close to 20 years and is with the company for more than 10 years where he previously was leading the technical support team in Western Europe.

Patrick Ramer
Chief Software Engineer,
Patton Electronics Co.

Patrick is leading Patton's software engineering team that is responsible for the Trinity and SmartWare operating systems running on a wide range of Patton products including the SmartNode product line. He holds an MSc degree in Microengineering and has been designing and developing software for 20 years. He has lead software projects in various industries such as telecommunications, security alarm systems, industrial and building automation with a strong focus on protocols.

PATTON®
let's Connect!™

7622 Rickenbacker Drive
Gaithersburg, MD 20879 USA
tel: **+1.301.975.1007**
fax: **+1.301.869.9293**
web: **www.patton.com**
email: **marketing@patton.com**

Document: 07M-SECALLIPTEL-WP