ribbon

Voice Network Vulnerabilities in the Enterprise: How to Address Them

White Paper

Contents

Introduction

As the core enabler of IP-based communications, Session Initiation Protocol (SIP) is the de-facto standard to support solutions for voice, video, unified communications, and more. SIP services are used to connect both cloud -based communication services (Microsoft Teams, Zoom, Ring Central, etc.) as well as IP-PBXs (Cisco, Avaya, NEC, Mitel, etc.). Despite its advantages, SIP-based communications inherently introduces additional security issues that need to be understood and systematically addressed by IT organizations.

Firewalls alone are not enough to provide a secure network. Instead, enterprise customers need a complete, seamless approach to network security—one that encompasses the unique vulnerabilities of real-time communications systems—to preempt issues and protect the organization as a whole.

Without the necessary expertise, monitoring, and management, companies could be leaving their network vulnerable to exploitation through their VoIP communications.

This whitepaper will discuss:

- **Threats That SIP/IP Communications Face:** Hackers use many tactics to exploit the vulnerabilities of IP-based communications. Understanding their tactics and motivations can help IT organizations fend off common attack vectors.
- **Barriers to Security:** Many enterprises simply lack the expertise required to defend themselves or have gaps or inconsistencies in their defenses, between voice and data networks.
- **Preparing a Defense:** Once an organization understands the threats and plans for them, what are the tools required to safeguard SIP-based communications.

Understanding the Threat

Since cybercriminals look to exploit SIP vulnerabilities, IT professionals need to know what their motivations are. Depending on the hackers' goal, whether it's to make money using toll fraud, deploy a blackmail scheme, or to steal sensitive information, their actual tactics may differ. Based on these tactics, it's essential the organization understands the effect a successful attack could have not only on its communications network, but also on its network at large.

For instance, attackers will often send specially crafted SIP messages to a customers' network looking for a response that indicates an unsecured port. Sophisticated hackers craft multiple messages with different SIP variables to test how the system under attack responds.

Once a response is received, they usually try to perform a set of SIP registrations to authenticate a remote SIP user agent on the network. Because many hackers also have detailed specifications on the default user accounts for multiple vendor PBX and UC offerings, they have successfully breached and exploited corporate communications systems worldwide.

Full Network Breach via the Voice Network

Fraud, theft, or disrupted network performance is one thing, but a full security breach is another matter altogether. Often, hackers use attacks to probe network vulnerabilities and find a way into the company's internal systems Common SIP attack techniques include registration hijacking, server impersonation, and tampering with message bodies. Once the hacker is inside, the enterprise is opened up to theft of financial data or system shutdowns or lockouts for blackmail.

Service Theft and Espionage

In theft of service cases, bad actors will break into an organization's communication systems (IP PBXs, voice mail systems, IP to PSTN gateways, IP phones) to make outbound calls to premium numbers using the compromised equipment as a proxy or relay. Here the hacker can resell the premium calling access and generate illicit revenue. The price of this type of fraud can be quite high — estimated that it costs corporate customers $4 billion annually[1].

Other bad actors are focused on corporate espionage and will try to eavesdrop on important conversations by tapping phone-based and video conferencing systems. This type of fraud can become quite costly as hackers become privy to private communications with senior executives, suppliers, R&D groups, and strategic customers.

Denial of Service (DoS)

With a DoS attack, hackers will try to flood a company with a crushing amount of useless traffic to overwhelm the network's "business as usual" management rules and security protocols. These attacks can be severely disruptive for the company under attack, as the added traffic strains bandwidth and limits the number of resources available to support legitimate corporate communication activities. Many times the attacks are blackmail attempts – once the enterprise pays the ransom, the network returns to normal.

Even if the DoS attack is controlled, maintaining network quality becomes a challenge particularly if specialized equipment is not in place to thwart it. This degradation can impact revenue and damage customer relationships.

[1]A New Breed of Criminal, AT&T

Barriers to Defense

Because hackers are very sophisticated and their work is difficult to trace, most companies don't realize they are under attack until it's too late. Even enterprises with significant investments in security tools and staff can find themselves secretly being taken advantage of. The tools at the hacker's disposal enable them to cast a wide net and probe vulnerabilities across a swath of organizations.

Many companies believe that a firewall is all the protection they will ever need, and they write off voice/video quality issues as just another run of the mill technical problem. Even those groups that use monitoring software on their firewalls and network are still vulnerable. For instance, if a server returns a locator message to find out where the attack originates, the attacker will shut down that IP address and switch to a different one, continuing to attack.

Despite the need for better security measures, many enterprises still fail to adequately secure their voice and video infrastructures completely. TechTarget explains the barriers that may be keeping them from adopting more secure implementations:

> **" It is not that IP cannot be secured as much as the implementations are weak from a security perspective. One of the reasons may be that securing a VoIP network can be difficult and requires a lot of specialized expertise. Many organizations do not want to accept the expense of hardening the security around their VoIP networks, and many more do not understand the measures that must be taken to prevent security breaches."**

Preparing a Defense

Providing an adequate defense to the voice network requires a variety of techniques and tools. For instance, a simple reset all default usernames/passwords for vendor supplied communication elements (PBXs, UC systems, voice mail, etc.) will greatly help repel initial attacks from cybercriminals across the board. While this is an obvious first step, other elements should be brought into the picture to make the security perimeter more formidable.

SBCs – A Requirement for Secure Real-time Communications

Suffice to say that a Session Border Controller (SBC) needs to be the central component in protecting your voice network, and by extension, your overall network topology. An SBC, at its most basic level, is a SIP-aware firewall that inspects every SIP voice/video packet, deciding to admit or deny access to the organization's network. The SBC constantly looks for suspicious content and unauthorized users while thwarting attacks. It relies on known information (e.g., an authorized user base) and from automated processes such as a security analytics platform to make decisions on entry or denial.

For example, the SBC may recognize that an overwhelming amount of traffic is originating from a specific IP address or is aimed at a particular phone extension. It may find that a set of similar machines are all trying to request the same server. Here, the SBC will automatically step in and initiate protection protocols—blocking traffic and creating alerts for further analysis.

In the case of Ribbon, our SBCs provide a suite of security components that include:

- **B2BUA/Network Topology Hiding:** The Ribbon SBC hides the network topology by acting as a back-to-back user agent (B2BUA), where a SIP session is divided into two distinct segments: one between the endpoint and the SBC, and the other between the SBC and the phone system platform. This in effect hides the enterprise voice network from the larger internet.
- **DoS and DDoS Defense (Policers):** The Ribbon SBC uses specialized policing software to deal with high traffic volumes and protect the network from denial of service (DoS) and distributed denial of service (DDoS) attacks.
- **Encryption (Media and Signaling):** Real Time Communications (RTC) media traffic should be encrypted for privacy and regulatory compliance purposes. The Ribbon SBC uses Secure RTP (SRTP) to encrypt media packets, and all SRTP encrypted calls are routed through the SBC.
- **Malformed Packet Protection:** An attacker may attempt to send malformed packets to cause a voice/video application or service to crash, or otherwise exploit a vulnerability that provides unauthorized access. The Ribbon SBC maintains full session state and is therefore able to detect and respond to attempts to send malformed packets over the network.
- **Call Admission Control/Overload Controls:** The Ribbon SBC provides limits and system overload threshold parameters can be used to limit the number of concurrent sessions that can be simultaneously active to prevent network or system overload.
- **Full SIP Session State Awareness:** Enables the Ribbon SBC to initiate, re-initiate, maintain, or terminate real-time communication sessions, as necessary. Ribbon SBCs can dynamically process the deep real-time communications requirements associated with the SIP "state" and can parse and infer active and changing port numbers, UDP service types, stream activity/inactivity, and bandwidth requirements. In short, the Ribbon SBCs provide full SIP stack and session state knowledge to protect downstream UC elements (phones, PBX, UC stack itself, etc.) against security threats

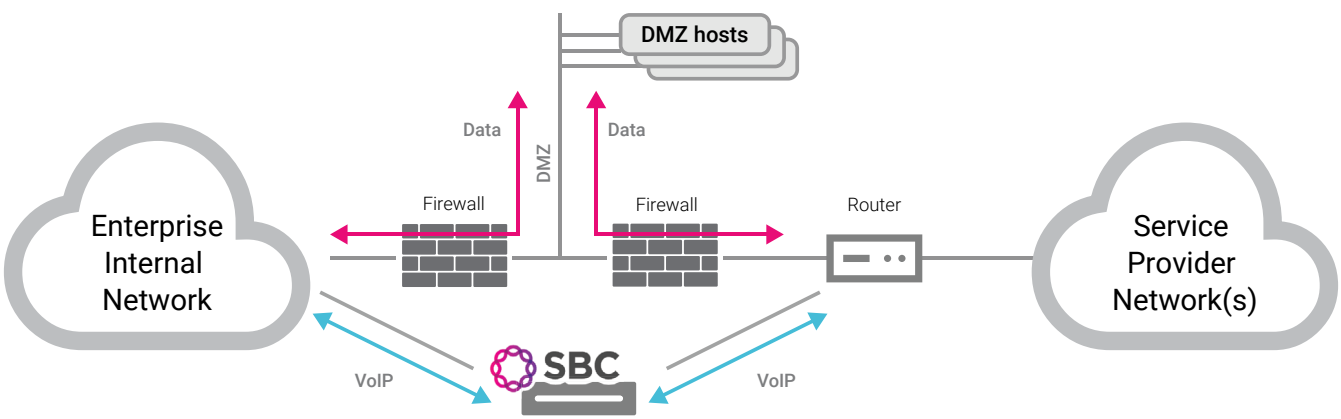

Figure 1. Common methodology for deploying an SBC in an enterprise network

By quickly identifying and mitigating threats, SBCs protect against a wide range of theft-of-service and fraud crimes. In addition, they help mitigate the bandwidth issues created by DoS and traffic flooding attacks by isolating the offending traffic and keeping it from hitting the VoIP network.

For addition reading, please check the resources on the Ribbon website, found here.

Advanced Capabilities

It should be abundantly clear that an SBC should be part of your network security infrastructure. However, given the many attack vectors that exist, an SBC should just be your starting point. Adding the power of analytics - machine learning and its pattern recognition capability - will greatly improve the ability to spot next-level threats.

Ribbon looks at a comprehensive security solution for the voice network across three realms:

- **Anomaly Detection:** Based on machine learning models, pattern recognition uses enterprise network call data to detect both unknown and repeat threats by learning normative call traffic behavior. These models use a feedback loop to continuously learn which refines the accuracy.
- **Reputation Scoring:** Utilizes multiple input data from pattern recognition and 3rd party databases to determine whether a call is likely malicious, outputting a reputation score in real-time. With real-time Reputation Scoring, enterprises are able to set up policies for how each call must be handled during call setup.
- **Policy Enforcement:** Takes instructions from defined policy rules to mitigate voice-based attacks before they disrupt legitimate voice calls or cause harm to an enterprise's business. A session border controller (SBC) will be the primary tool for enforcement.

Ribbon's Voice Threat Prevention service bundles the Anomaly Detection and Reputation Scoring functions into a single solution that greatly augments an enterprise's security implementation. This bundle works with Ribbon or 3rd party SBCs for policy enforcement and provides operational visibility to show the success a voice threat prevention deployment.

Figure 2: Voice Threat Prevention

Profiling an Attack

Real Life Example: US-based mid-sized business

Hackers targeted a small corporate office for an attack, sending various specially formed SIP packets to the public IP block on the WAN link. The messages were designed to go through the firewall on to the local private network, and further probe for security holes on any VoIP device on the LAN—a sophisticated first step as hackers see what generates a response and then try to steal credentials.

Monitoring this attack over a period of one-month, the customer's SBC recorded almost 200,000 SIP attacks resulting in nearly 15GB of data consumption. This contrasts what the phone system saw: only 5,600 sessions and 929Mb of data during the same period. Without a dedicated SBC in place, the company could have been easily compromised without even being aware that they were attacked.

Real Life Example: Fortune 500 Consulting Company

In this example, the enterprise was notified by their carrier that they were seeing a lot of international calls. An investigation revealed that a conference bridge was being hijacked externally, but to the enterprise it looked like a legitimate DID. The enterprise asked the carrier to block the number, however that was only a temporary solution as the hacker started using another number and fraud repeated itself.

All-in-all, the fraudsters ran up charges of over $100,000 – charges that the business was liable for. A voice analytics platform would have almost certainly saw this anomaly and appropriately reacted to the fraud attempt.

Conclusion

As attacks become more prevalent, enterprises must do everything in their power to secure all aspects of their business. For almost all organizations, their communications network will offer hackers a prime opportunity to exploit a weakness in the company's VoIP, SIP, or IT security infrastructure. With denial-of-service attacks, eavesdropping, registration hijacking, impersonating a server and other cyber-attack tactics available to hackers, organizations need tools of their own to protect themselves.

Ribbon provides a full suite of SBCs and analytics to mitigate voice threats to the Enterprise.

Ribbon offers:

- Security and connectivity ensured through an SBC providing a SIP-aware back-to-back user agent and protocol mediation.
- Machine learning modeling to spot fraudulent patterns and identify bad actors.
- Machine learning models for real-time scoring and policy decisions that are used to prevent malicious voice threats

Ribbon has the experience and the solutions to ensure enterprises can address voice network vulnerabilities before they can disrupt VoIP services or VoIP infrastructure.

About Ribbon Communications

Ribbon Communications (Nasdaq: RBBN) delivers communications software, IP and optical networking solutions to service providers, enterprises and critical infrastructure sectors globally. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge software-centric solutions, cloud-native offers, leading-edge security and analytics tools, along with IP and optical networking solutions for 5G. We maintain a keen focus on our commitments to Environmental, Social and Governance (ESG) matters, offering an annual Sustainability Report to our stakeholders. To learn more about Ribbon, please visit rbbn.com.