You’re Under SIP Attack: Limiting SIP Vulnerabilities

White Paper

Contents

White Paper

Introduction

As the core enabler of VoIP communications, Session Initiation Protocol (SIP) is being used worldwide to support innovative solutions for voice, video conferencing, unified communications, presence and more. Despite its advantages, such solutions offerings come with some concerns in the IT community.

Companies worldwide are implementing solutions, and it is important to recognize—and address—the additional security issues that are exposed with currently deployed SIP-based solutions.

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

Today, firewalls alone are not enough to provide a secure network. Instead, both enterprise customers and service providers alike need a complete, seamless approach to network security—one that encompasses the unique vulnerabilities of VoIP communications systems—to preempt issues and protect the organization as a whole.

This whitepaper will discuss:

- **The Threat SIP Trunking Faces:** Hackers use many tactics to exploit the vulnerabilities of SIP-based communications. Understanding their tactics and motivations can help enterprise operators secure their networks from attack.
- **The Barriers to SIP Security:** Many SMBs and even enterprises fail to secure their SIP communications because of the lack of expertise, plan inconsistencies and other challenges.
- **Preparing a Defense:** With the right strategy and implementation, SIP-based communications can be safeguarded against cyber-attacks, allowing enterprise and SMBs to benefit from the support of VoIP for their communications.

Understanding the Threat

Cybercriminals look to exploit SIP vulnerabilities for many reasons. To fully secure SIP-based communications, IT professionals need to know what these motivations are. Depending on the hackers' goal, whether it is to gain free service or to steal sensitive information, their actual tactics may differ. Based on these tactics, it's essential for the organization to understand the effect a successful attack could have on its deployed VoIP solution, but also on its whole network.

In theft of service cases, hackers will break into an organization's communication systems (IP PBXs, voice mail systems, IP to PSTN gateways, IP phones, etc.) in order to make "free" long-distance calls using the compromised equipment often as a "proxy / relay" known and authorized to perform such calls by the Service Provider. The price of toll fraud can be quite high — estimated that it costs corporate customers $4 billion annually[1].

Bad actors focused on corporate espionage will try to eavesdrop on important conversations by tapping phone-based and video conferencing systems. This type of fraud can become quite costly when it remains undetected as hackers become privy to private communications with Board of Directors, suppliers, R&D groups, manufacturing partners and strategic customers.

Attackers will often send specially crafted SIP messages to a customers' network looking for any response. 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, many hackers have successfully breached and exploited corporate communications systems worldwide.

Denial of Service

Often, 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 Denial of Service (DoS) attacks can be severely disruptive for the company under attack. The added traffic strains bandwidth and limits the number of resources available to support legitimate corporate communication activities. This condition leads to degraded Quality of Service (QoS) across the board, a problem that can manifest itself in a variety of ways:

- Jitter, echo, and poor speech quality on individual phone calls and conference bridges
- Pixilation and freezing within video conferencing and video chat systems
- Dropped calls
- An inability to access voice mail and other resources
- Limitations on the number of simultaneous participants in a single bridge
- A complete inability to place voice or video calls

Maintaining QoS is becoming an increasingly important and difficult issue to address. As businesses use more data than ever before, it is becoming more challenging to keep the same speed and quality on the network. According to Kirk Parsons, senior director and practice leader of telecommunications at J.D. Power, "Given the increase in network connection problems, carriers providing faster and more reliable connections may have a competitive advantage."

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

Other Common SIP Attacks

Disrupted communications are one thing, but a full breach is another matter altogether. Often, hackers use DoS attacks to probe network vulnerabilities and find a way into the company's internal systems to steal customer data and proprietary information. This is not the only tactic they may use to gain access to critical systems either. Other common SIP attack techniques include:

- Registration Hijacking
- Session Hijacking
- Tampering with Message Bodies
- Tearing Down Sessions
- Impersonating a Server

To prevent the disruption of communications—which can lead to gradual loss of customers—or a full, highly damaging data breach—companies should prepare a proper defense for the variety of SIP trunking vulnerabilities that can impact their business.

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. This is especially true in SMBs whose organizations typically do not maintain a dedicated security staff. Hackers recognize this organizational vulnerability and often target SMBs for their limited ability to invest in IT support and security infrastructures.

Unfortunately, this often turns out to be a successful strategy. 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 routinely use monitoring software on their firewalls and on the network to determine where network traffic is going to/coming from to identify potential problems are still vulnerable.

If a server returns a locator message to find out where the attack is originating, the attacker will shut down that IP address and switch to a different one, in a different location and continue to attack.

Today attacks are more frequent and more companies are being targeted. Cyber espionage attacks will continue to increase in frequency, long-term players will become stealthier information gatherers, while newcomers will look for ways to steal money and disrupt their adversaries.

Worse, hackers have become even trickier as companies adapt their defenses against known attack types. Their automated "hit and run" policy is designed to test as many systems as possible—as quickly as possible—and assess their prospects from there.

Despite the need for better security measures, many enterprises, and VoIP service providers 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

Although securing a network comes with many difficulties and barriers that can seem outside the scope of a SMBs IT department, it is a vulnerability that can't be ignored. Most companies know there are steps they can take, but they allow barriers to prevent them from fully implementing these solutions.

Here are steps a company can take to protect itself and overcome the common hurdles to securing its SIP networks:

The first thing a company should do to protect itself against SIP-based attacks is to reset all default usernames/passwords for vendor supplied communication elements (PBXs, UC systems, voice mail, etc.). This simple change will help repel initial attacks from cybercriminals across the board.

However, best practice dictates the use of an enterprise-side session border controller E-SBC to terminate SIP trunks via a dedicated appliance and properly secure VoIP networks.

E-SBCs constantly monitor network traffic and use pattern analysis to spot a SIP-based attack quickly. For example, it may recognize that an overwhelming amount of traffic is originating from a specific address (127.138.50.XX) or is aimed at a particular phone extension or DID. Or, it may find that a set of similar machines are all trying to request the same server. Regardless of attack type, an E-SBC will automatically step in and initiate protection protocols—blocking traffic, notifying the CPE to ignore problems, etc.

E-SBCs are typically equipped with standards-based SIP and H.323 protocol support and SIP/H.460 for far end NAT traversal. They also secure mobile and remote use of any available network access points—enterprise, home, public, mobile—without compromising corporate security policies.

By quickly identifying and mitigating threats, E-SBCs protect against a wide range of Theft of Service, Toll Fraud and Wiretapping crimes. And, 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 at all, they ensure that valuable resources consumed by non-productive traffic.

An E-SBC ensures QoS rules are effectively applied to high-priority, realtime communications systems. In this way, the network performs as designed and no service degradations occur—even while under attack conditions.

In the end, an E-SBC that secures networks against SIP attacks also helps eliminate static, echo, pixilation and other quality related issues that can plague corporate communication solutions.

Profiling an Attack

A real-life example is seen at a small US business using VoIP.

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 E-SBC recorded almost 200,000 SIP attacks, resulting in nearly 15GB of data consumption. This represented a problem as the official phone system only used 5,600 sessions and 929Mb of data during the same period.

Without a dedicated enteprise SBC in place, the company could have been easily compromised without even being aware that they were attacked.

Conclusion

As attacks become more prevalent, companies must do everything in their power to secure all aspects of their business. For almost all organizations, their communications 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, wiretapping, registration hijacking, session hijacking, impersonating a server, tampering with message bodies, tearing down sessions, and other cyber-attack tactics all available to hackers to gain access to sensitive information, organizations need tools of their own to protect themselves.

SIP trunking offers an excellent opportunity for organizations to reduce costs and ensure business continuity—if they can use it securely. Enterprise session border controllers E-SBCs provide a way for companies to gain the benefits of supporting their VoIP with SIP trunking without the difficulty in securing it.

Ribbon provides a full suite of E-SBCs that simplify the entire process from installation to management to ensure companies can avoid the standard issues present when trying to implement and manage SIP-based communications manually. Ribbon's E-SBCs offer:

- Security and connectivity ensured through a SIP-aware firewall and protocol mediation.
- Traffic management, QoS, and call admission control help maintain high-quality voice on every call.
- By providing MOS scores, integrated VoIP test agents, and the backup and restoration of configurations in a single system, monitoring, management, & troubleshooting is easily achieved.
- Support for numerous PBX connection types including Ethernet (IP), PRI, and analog for simple installations.

About Ribbon

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.