Real-Time Communications
Without Boundaries

Securing Real-Time Communications

White Paper

Contents

Introduction

SIP-based real-time communications (RTC) continues its rapid evolution, encompassing voice, video, UC&C, WebRTC, VoWiFi, and VoLTE. This evolution exposes new security threats to both service providers and the enterprise.

There are many examples of RTC security threats, but some notable attack vectors are denial of service attacks, telephony denial of service, toll fraud, and network penetration.

This paper will describe specific security exposures of SIP-based RTC as well as what are the implications for service providers and enterprises. It will also define Ribbon' approach to mitigating these security exposures.

Businesses Are Shifting

From TDM/Analog to SIP & Cloud-based Services

Legacy (TDM) telephony is largely being displaced, because it stopped evolving and could not match the business value, innovation, and flexibility provided by session initiation protocol (SIP) for cloud-based Unified Communications. From its modest roots as a hobby technology, SIP has matured considerably and is now becoming the standard in service provider and enterprise communication networks. Because of SIP's flexibility, enterprises are beginning to tap its potential as the workplace changes and demands new forms of real-time communica-tions (RTC).

Hybrid work is now common, employees are increasingly working off-site, such as from home, their cars, airplanes, hotels, client sites, etc. In addition, BYOD – bring your own device – is another trend with similar implications. Employees feel entitled to use their devices as they see fit. This often means they're not used with consideration for how the enterprise's security structure as a whole might be impacted.

Remote worker and BYOD scenarios provide one of the strongest use cases for Unified Communications, allowing businesses to adopt virtual user models, optimize office space, and be more responsive to customers. The challenge, however, is to enable all of this in a secure environment. As endpoints become more distant from the core network, it is harder to control access; plus, a great deal of the SIP communication traffic will be over the public Internet and often across unsecure WiFi connections such as at your local Starbucks. Hybrid worker productivity relies on this access, but the associated security risks must be understood and addressed to make it worthwhile.

SIP Security Implications for Your Real-time Communications

SIP telephony leverages the data network; it no longer has the "walled" protection offered by a dedicated voice network used to support legacy PBX infrastructures. With SIP, RTC apps such as voice, video, and chat become data applications, and without appropriate security measures in place, networks could be opened to hackers, exposing the business's technology, privacy, and compliance to attack threats.

In addition to conventional threats that have long existed with PBXs, such as toll fraud, message tampering, eavesdropping, etc., SIP exposes the network to new threats, several of which can be debilitating for your entire business, such as denial of service (DoS) attacks, data/identify theft, and network penetration exposure.

Movement to SIP for access into UC systems

- more than 50% of the world-wide market is now SIP trunking enabled
- SIP is easier/faster to make calls, easier to spoof
- SIP media payload is wide open to malware/exploit file transfer, which can lead to data breach
- Non-encrypted SIP calls open the door to eavesdropping and identity/content theft
- Left unprotected, SIP can be a weak link in the network for security vulnerabilities, making it an attractive point of entry for hackers.

Technology advances allow for easy access to scripting tools and botnets

- DoS, TDoS, malware attacks easier/low cost to put together
- "Hacking as a service" is the consumerization of cybercrime
- Books such as "Hacking VoIP" can easily be bought on Amazon.com

While security breaches attributable to SIP may not yet be widespread, that is changing as SIP adoption grows and hackers prey on vulnerabilities created by a lack of understanding of the risks and subsequent lack of best practices to address the threats and protect the network. Some attackers will target SIP specifically for toll fraud, but more likely this will be their point of entry for other forms of malicious activity such as disrupting operations, identity theft, financial theft, corporate espionage, or supporting political agendas. This makes SIP more of a means to an end, and it will be futile to build a security plan to only address specific motives or types of hackers.

Just because you have not experienced a SIP security breach does not mean the network has not been compromised. Hackers may well be monitoring the network without your knowledge and just waiting for a port to be left open, enabling them to go about their business with impunity, or have penetrated and compromised your network already and are waiting for 'the right time'.

SIP Security Threats

Hackers are constantly looking for other ways to monetize corporate data, and when they do their attacks will become more brazen and targeted. Since SIP currently poses limited financial risk, security measures may be limited as well. Service providers and enterprises will only have reactive after-the-fact options when more serious threats strike. Not only can hackers cause financial loss by accessing corporate data and accounts through a SIP breach, but some would not hesitate to use the same breach to launch DoS – denial of service – attacks. By constantly flooding the network with SIP messages through that breach, they can disrupt or even shut down operations, and much like kidnapping, will only stop once they have extracted blackmail payments from you. Even this is no guarantee, as once that breach is fixed, hackers may well keep pinging your network to find new points of entry, because they know SIP can be highly vulnerable if not properly secured.

High-Level Categorization of SIP Threats on Real-time Communications

- Denial of service on RTC ports
- Telephony denial of service
- Theft ofservice – toll fraud
- Network penetration

Denial of Service on RTC Ports

Denial of service attacks are increasing 100% YoY, and it is estimated that the average company is hit by 4 attacks each year. The impact of a DoS attack can on average cost victims $40,000 an hour, and with 20% of attacks lasting at least five days, these attacks can destroy businesses.[1]

Further findings from the Ponemon Institute study estimate that the average cost of one minute of downtime due to a DoS attack is $22,000. With an average downtime of 54 minutes per DoS attack, this amounts to a heavy toll. Attackers often plan the timing of their attack in order to maximize financial damage. For instance, online retailers would likely be targeted during the heavy traffic of holiday shopping seasons. Beyond lost revenue, financial losses may include other elements, such as the cost of investigating and responding to an attack, expenses related to customer support and public relations, and potentially even financial penalties or lawsuits.

While denial of service (DoS) is an attack method that has new and specific applications in the SIP world, it was virtually unknown with legacy circuit-switched telephony. However, today's attacker can aim to disrupt the communications infrastructure at the desktop level by swamping or crashing phones, or at the gateway level by taking out the network nodes that interface an enterprise SIP installation with the outside world.

Source: http://cloudtweaks.com/2015/10/bandwidth-average-cost-ddos-attack/

Denial of service (DoS) attacks are by no means unique to real-time communications; however, it is worth remembering that it is not just the source IP addresses that are relevant in RTC, but also the source telephone number or SIP URI identifying the user. More sophisticated attacks make use of multiple IP and SIP-level sources to further complicate the task of determining and filtering out unwanted traffic.

Hackers can also attack IP-PBX's directly by using SIP, or other IP protocols, to crash the session manager with an endless flood of valid but dishonest session requests.

The effect can range from legit users getting the busy tone when trying to dial any number, using voice mail or IVR to system bandwidth being filled by unwanted traffic. When Unified Communications is down, it is something that impacts people end-to-end.

Telephony Denial of Service (TDoS)

As compared to large-bandwidth DoS attacks, telephony denial of service (TDoS) attacks don't take many computing resources or technical know-how. It is fairly easy to clog a phone line by simply calling it over and over again. Attackers can employ call generators using SIP automation scripts to dial the victim's phone number, hang up, and then redial repeatedly, overwhelming the line and making it impossible for other calls to come through. And because the attackers are able to use spoofed calling numbers, it is difficult for the victim to differentiate between a TDoS call and a real call. TDoS attacks can appear as perfectly legitimate calls, because they are; they just come from a malicious source. Differentiating these calls from legitimate ones can be challenging, even with a hardened network and the right protections.

The effect from a TDoS attack can range from legit users getting the busy tone when trying to dial any number, using voice mail or IVR to system bandwidth being filled by unwanted traffic. The impact to an organization where attackers tie up every available voice session can be a catastrophic loss of the ability to conduct business at even the most basic level; the subsequent loss of service, business, and revenue can be devastating.

Theft of Service – Toll Fraud

IP telephony scams can come in many forms, can originate from inside or outside the company, and can impact any business regardless of size or industry. In simple cases, hackers gain access to corporate voice networks to make free international calls. In more sophisticated attacks, cybercriminals concoct complicated schemes to reap real financial rewards. Why does toll fraud happen? Because it is profitable. For example, scammers engage in hijacking schemes to generate illicit revenue as rogue service providers. They break into a corporate voice network and "resell" international minutes to other service providers or unsuspecting consumers. In a widely published Massachusetts case, cybercriminals hacked into a small-business phone system and made $900,000 in calls to Somalia. (The story made headlines when the service provider sued the business owner, who had refused payment.)

Malicious subscribers are defined as toll fraud, and the global impact has soared to more than $39.8 billion, or slightly more than 2% of all global telecom revenues, according to the CFCA's 2021 Global Fraud Loss Survey. To put that into perspective, credit card fraud was around $28.5 billion in 2020.

Toll Fraud examples:

- Malicious users gaining unauthorized access to an account and using it to make international or other expensive calls.
- Finding a way to subvert the permissions on an account (or the call routing related to an account) to allow communications that should not be permitted.
- More sophisticated examples include abusing special classes of numbers (such as toll free) to actually extract revenue from services by calling fraudulent numbers.
- Malicious users might tell the PBX/Application Server that a call will be voice-only, but then stream high-definition video instead, essentially defrauding the system owner of the higher revenues for the video traffic.

Network Penetration – Opening Other Entry Points

The attack vector of greatest concern is the one that is largely invisible: using SIP to open up other entry points into the enterprise domain.

Let's start with the SIP platforms that can be illegally accessed to help attack other parts of the network if they are not properly secured. Platform compromise is an increased security threat for SIP, because increasingly SIP services are now running on generic computer servers running Linux. When this occurs, SIP platforms need to be considered as vulnerable as any other server in the network. Given that most have common Linux shells and tools available, if compromised they can be prized targets for launching further attacks into other parts of the network.

And it is not just the SIP servers at risk, but also the desktops, IP phones, and mobile devices used by end users for SIP service.

A second concern is porous firewalls. Due to the way SIP, SDP, and RTP are designed, SIP flows frequently require multiple source/destination IP/Port combinations per session. If you then multiply that by the number of users in an enterprise or carrier environment, it is not uncommon to require thousands of firewall pinholes to support an RTC service. Less sophisticated systems may leave many thousands of holes open for sustained periods.

Not only does this give an attacker ample attack vectors to target the SIP servers, but it also gives them opportunity to flood common network segments with traffic that could hinder or knock out other services.

Finally, we have concerns about the Unified Communications flows. By subverting SIP applications, malicious hackers can launch all manner of attacks, including stealthy information-gathering campaigns and more brazen attempts at further compromises, denial of service, or vandalism. Two areas of great concern are:

- Exfiltration of data via media session. This is the sending of data out via the media session using RTP as a covert communication channel
- Malware embedded in signaling and media sessions. This is where SIP and RTP (or other signaling/media streams) are filled with malicious payloads.

It is possible to embed attacks such as SQL injections into SIP headers that can cause servers to crash, corrupt data, or deliver unintended access to an attacker. Similarly, it is possible for RTC flows to include any sort of data, including program code, malware, IPR, or trade secrets.

Ribbon SBCs – Required for Secure Real-time Communications

There is no question that the use of Session Border Controllers (SBCs) has grown exponentially in the past years. SBCs are built to create and leverage a secure real-time communications environment, where multiple devices across numerous networks interwork to create a unified user experience. Service providers are knowledgeable of the many purposes that an SBC has in implementing RTC, and one of the most important functions is maintaining security throughout the communication system. More specifically, a Ribbon SBC provides a holistic security strategy for RTC that includes:

B2BUA/Network Topology Hiding

The Ribbon SBC hides the core network topology by acting as a back-to-back user agent (B2BUA), where a session initiation protocol (SIP) session is divided into two distinct segments: one between the endpoint and the SBC, and the other between the SBC and the IP private branch exchange (PBX) or Unified Communications (UC) server.

DoS and DDoS Defense (Policers)

The Ribbon SBC uses specialized policing software to deal with high traffic volumes and protect the core network from denial of service (DoS) and distributed denial of service (DDoS) attacks. Different policers on the Ribbon SBC include the following:

- **Static blacklisting:** IP addresses and/or network prefixes that are discarded on ingress
- **Dynamic blacklisting:** Designed to detect and block misbehaving endpoints for a configured period of time rather than prevent malicious attacks, for which the system employs other defense mechanisms
- **Whitelisting:** Static list of IP addresses and/or network prefixes that are allowed to access the SBC
- **Micro-flow policer:** Allows registered endpoints through the SBC (primarily used in access scenarios)
- **Unknown peer:** Allows any unknown packet through the SBC up to the specified packet rate limit

Encryption (Media and Signaling)

RTC media traffic needs to 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. SRTP can be used inside or outside the network. SRTP on one call leg is independent of its use on other legs of the same call, and is negotiated for each leg.

SIP signaling messages are plain text and relatively easy to intercept. Ribbon SBCs can use transport layer security (TLS) and IPsec to encrypt signaling traffic. TLS supports peer authentication, confidentiality, and message integrity. IPSec supports cryptographic protection for non-media IP packets using the management or packet interfaces.

Toll Fraud Protection

The Ribbon SBC can be configured to disable secondary dial tone sources in order to prevent toll fraud. In addition, working with the Ribbon Policy server (PSX), RTC calls can be limited or blocked to international destinations that have a high susceptibility for toll fraud.

Malformed Packet Protection

An attacker may attempt to send malformed packets to cause an RTC application or service to crash, or otherwise exploit a vulnerability that provides unauthorized access. An SBC maintains full session state information, and is therefore able to detect and respond to attempts to send malformed packets over the network.

Call Admission Control/Overload Controls

Call admission control limits and system overload threshold parameters can be used to limit the number of RTC sessions that can be simultaneously active, in order to prevent network or system overload. An RTC overload can degrade the performance of other calls on the network, or crash an RTC environment — in effect, a self-inflicted denial of service.

Full SIP Session State Awareness

Full SIP session state awareness enables the Ribbon SBC to initiate, re-initiate, maintain, or terminate RTC sessions, as necessary. Ribbon SBCs can dynamically process the deep RTC 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. RTC is only getting more complicated, and it is becoming increasingly difficult to capture and act on this information. 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 DoS attacks.

Summary

Service providers and enterprises can leverage Ribbon SBCs to improve the security of their networks. As both entities move to using IP to provide real-time communications, the opportunity for ”bank robbers“ to access and steal services increases, unless an SBC is deployed. Ribbon provides SBCs and RTC security technology. With SBCs, enterprises can focus on their core competencies while service providers can provide extraordinary communications features to their customers. Ribbon can make sure both can do this without fear of theft on their networks.

About Ribbon Communications

Ribbon is a company with two decades of leadership in real-time communications. Built on world class technology and intellectual property, Ribbon delivers intelligent, secure, embedded real-time communications for today's world. The company transforms fixed, mobile and enterprise networks from legacy environments to secure IP and cloud-based architectures, enabling highly productive communications for consumers and businesses.

To learn more visit rbbn.com

Microsoft Partner
Gold Communications

Voice
Unified Communications
Business Productivity Solutions
Midmarket Solution Provider