Security Implications for Your Unified Communications

Leveraging Session Initiation Protocol (SIP) technology truly changes the way we think about communications these days. With SIP, unified communication (UC) applications become just another “data application” and without appropriate security measures in place, networks could be opened to bad actors exposing the business, technology, privacy and compliance to new attack threats.

Leveraging Session Initiation Protocol (SIP) technology truly changes the way we think about communications these days. With SIP, unified communication (UC) applications become just another “data application” and without appropriate security measures in place, networks could be opened to bad actors exposing the business, technology, privacy and compliance to new attack threats.

Unfortunately, bad actors are constantly looking for new ways to infiltrate corporate networks, and when they do their attacks will become more brazen and targeted. Just because you have not experienced a SIP/UC security breach does not mean the communications network has not been compromised. Bad actors 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 already penetrated and compromised your network - waiting for ‘the right time’ to attack and exfiltrate data or shut down communication access for your customers.

So, what are some of the more concerning threats against unified communications? Well, here are 4 to think about...

1. **Denial of Service on UC Ports**

Denial of Service (DoS) attacks are by no means unique to unified communications, however it is worth remembering that it is not just the source IP addresses that are relevant in UC, 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.

Bad actors will attack IP-PBXs directly by using SIP to crash the communication manager platform with an endless flood of valid but dishonest session requests.

The effect can range from legitimate users getting a busy tone when trying to dial any number or accessing an IVR to the bandwidth allocation for communication networks being filled by unwanted traffic. When UC is down, it is something that impacts people end-to-end.

2. **Telephony Denial of Service (TDoS)**

When compared to large bandwidth Distributed DoS (DDos) attacks, Telephony Denial of Service (TDoS) attacks don’t take as many computing resources or technical know-how. It is fairly easy to clog a phone line by simply calling it over and over again. Bad actors can employ SIP call generators to overwhelm the SIP trunks and make it impossible for other calls to come through. And because the attackers are able to use spoofed calling numbers, it is difficult for the organizations to differentiate between a TDoS call and a real call. TDoS attacks 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 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.

3. Theft of Service - Toll Fraud

Fraud on UC systems 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, bad actors gain access to corporate voice networks to make free international calls. In more sophisticated attacks, these same bad actors concoct complicated schemes to reap real financial rewards. 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.

So is the impact “real”...oh yes! 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.)

4. 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 compute servers running Linux. When this occurs, SIP platforms need to be considered as vulnerable as any other server in the network. Given 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.

Furthermore, due to the specialized nature of the UC protocols it is not uncommon for network administrators to assume the payload contents are safe (or at least benign). After all you need specialized CODEC algorithms to make sense of an RTP flow.

First of all, this has never really been true, it’s been well known for a while now that it’s 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.

Secondly, with the wide spread adoption of unified communications (UC) it is now possible for ingressing UC flows to include any sort of data including program code, malware or egressing UC flows to include corporate data or other trade secrets.

Therefore not only is UC now increasingly a threat vector where information can be leaked it is also a potential attack vector whereby incoming malicious payloads can be delivered or sensitive corporate data can be exfiltrated.

So how do you Secure Unified Communications?

It’s without question that the use of Session Border Controllers (SBCs) has grown exponentially in the past years. SBCs are built to create a secure unified communications environment, where multiple devices across numerous networks interwork to create a unified user experience.

As organizations move to SIP for their UC systems, the opportunity for "bank robbers" to access and steal services increases, unless an SBC is deployed. Sonus provides SBCs and UC security technology.

With Sonus SBCs, enterprises can focus on their core competencies while service providers can provide extraordinary communications features to their customers. Sonus can make sure both can do this without fear of theft on their networks.