TechVision RESEARCH

Securing Unified Communications

Abstract

Unified Communications combines telephony, video, chat, email and presence together into one unified communications system. As the technology has become more complex and more accessible through the public Internet, the security threat has increased. In many ways it's easier than ever to attack business communications. Companies must be diligent in protecting their Unified Communication services as they are vital to business operations.

Unified Communications (UC) applications can be the hardest to secure within an enterprise. UC clients, APIs, and services need a full security suite to ensure an enterprise stays secure. Too many enterprises attempt to apply standard application security measures to UC applications, which limit what users can do and still leaves enterprises exposed to the complex UC security challenges. Security managers and architects understand standard web applications, but not all the nuances of UC, and UC managers and architects lack sophisticated security knowledge.

Conventional IP security products (such as firewalls and intrusion detection and prevention systems) were not designed with these kinds of real-time communications in mind—leaving organizations vulnerable to security threats.

In this report we'll describe the basics of UC security, the risks associated with poor UC security and how challenging UC security really is. We'll then describe how the NIST Cybersecurity Framework can be applied to UC security and how to apply a tiered approach and advanced techniques for securing UC communications. We'll highlight a few vendors that worth considering in this space and provide summary recommendations.

Authors:

Sorell Slaymaker

Principal Consulting Analyst
sorell@techvisionresearch.com

Table of Contents

Executive Summary

Unified Communications (UC) is critical to the vision most organizations have when they consider how they are embracing the Digital Enterprise. Unified Communications is a business and marketing concept describing the integration of enterprise communication services such as instant messaging (chat), presence information, voice (including IP telephony), mobility features (including extension mobility and single number reach), audio, web & video conferencing, fixed-mobile convergence (FMC), desktop sharing, data sharing (including web connected electronic interactive whiteboards), call control and speech recognition. UC also includes non-real-time communication services such as unified messaging which integrates voicemail, e-mail, SMS and fax.

Unified Communications is not necessarily a single product, but a set of products that provides a consistent unified user interface and user experience across multiple devices and media types. UC allows an individual to send a message on one medium and receive the same communication on another medium.

UC brings the customer and enterprise experience to life and provides multi-platform and multi-media capabilities to the Digital Enterprise. These multi-media features are particularly important to the customer experience and, increasingly, an expectation for customer digital offerings. That said, these added capabilities open up new threats and vulnerabilities that need to be addressed. Securing Unified Communications is the focus of this report and should be an important element of any enterprise UC program.

The reality is that conventional IP security products (such as firewalls and intrusion detection and prevention systems) were not designed with these kinds of real-time communications in mind—leaving organizations vulnerable to security threats. This requires security teams to craft new strategies and identify new security solutions to protect and control these diverse real-time communication flows.

Addressing these threats and securing UC can be addressed via a multi-tiered security approach. Of particular importance is the use of Session Border Controllers (SBCs) as they are designed to overcome the unique security challenges enterprises typically encounter when introducing VoIP/SIP. The role of an SBC is to be a voice application aware security solution that can control and log all voice sessions. We also recommend the use of the NIST Cybersecurity framework as a foundation, although it doesn't focus specifically on UC security.

In securing this challenging, but increasingly critical area, we describe several steps enterprises should take to improve their UC security posture. These are describe in greater detail in the report, but these are the key areas of recommended focus and should be part of an enterprise UC security strategy:

- Encrypt Everything
- Adopt a Zero Trust Strategy
- Build a Strong IAM foundation (MFA, least privileged access, etc.)

- Proxy All Services
- Secure UC Appliances
- Log and Event Monitoring for UC Services
- Conduct 3rd Party UC Security Audits
- Implement UC-Centric Security Training
- Deploy Phone Number Authentication
- Implement a Tiered Security Model

It is critical that most large enterprises explicitly assess their UC security posture while integrating these approaches into an overall security architecture and roadmap.

Introduction

Unified Communications (UC) is a business and marketing concept describing the integration of enterprise communication services such as instant messaging (chat), presence information, voice (including IP telephony), mobility features (including extension mobility and single number reach), audio, web & video conferencing, fixed-mobile convergence (FMC), desktop sharing, data sharing (including web connected electronic interactive whiteboards), call control and speech recognition. UC also includes non-real-time communication services such as unified messaging which integrates voicemail, e-mail, SMS and fax.

Unified Communications is not necessarily a single product, but a set of products that provides a consistent unified user interface and user experience across multiple devices and media types. UC allows an individual to send a message on one medium and receive the same communication on another medium. For example, one can receive a voicemail message and choose to access it through e-mail or a cell phone. If the sender is online according to the presence information and currently accepts calls, the response can be sent immediately through text chat or a video call. Otherwise, it may be sent as a non-real-time message that can be accessed through a variety of media. If properly integrated, UC can increase productivity and is part of what TechVision refers to as the "digital workplace".

UC is also moving (as are most applications and infrastructures) to the cloud, but current cloud platform offerings from Microsoft's Teams to Slack and most others are not secure enough for highly sensitive information. Enterprises and government agencies looking to further protect their organizations' intellectual property while meeting more stringent compliance and privacy regulations should add next- generation ultra-secure collaboration solutions to their portfolio. These platforms are based on a zero-trust architecture and multi-factor authentication.

Microsoft's Teams to Slack and most others are not secure enough for highly sensitive information.

Unified Communications applications can be the hardest to secure within an enterprise. UC clients,

APIs, and services need a full security suite to ensure an enterprise stays secure. Too many enterprises attempt to apply standard application security measures to UC applications, which limit what users can do and still leaves enterprises exposed to the complex UC security challenges. Security managers and architects generally understand standard web applications, but not all the nuances of UC, and UC managers and architects often lack sophisticated security knowledge.

Conventional IP security products (such as firewalls and intrusion detection and prevention systems) were not designed with these kinds of real-time communications in mind—leaving organizations vulnerable to security threats. When introducing UC platforms, IT teams must craft new strategies and identify new security solutions to protect and control real-time communications flows. Session Border Controllers (SBCs) were designed to overcome the unique security challenges enterprises typically encounter when introducing VoIP/SIP.

CISSP and standard IT security training focuses securing transactions, not interactions. This leaves UC security as a vulnerability within an enterprise's security strategy. In this research, we focus on the security vulnerabilities of real-time voice and video communication and phone number security. Someone's phone number can be used as part of their identity, but this attribute/identifier can be easily spoofed and should not be solely relied upon. Short Messaging Service (SMS) security is a focus in this research since many enterprises use SMS as part of their MFA strategy as TechVision described in detail in our recent report on MFA. This research does not cover email or voice-mail security.

CISSP and standard IT security training focuses securing transactions, not interactions. This leaves UC security as a vulnerability within an enterprise's security strategy.

Why Today's Collaboration Platforms Are Not Secure Enough

Gone are the days when are primary form of real-time communications was the phone and we could trust that the caller ID was accurate. These days we are inundated with robo-calls that have learned how to spoof caller ID. Robo-calling or spam has already infiltrated email and fax and is moving into SMS and conferencing.

Many enterprises and users assume that their mobile devices are secure and that using a corporate Mobile Device Management (MDM) solution is all the security that they need. As part of this assumption, many organizations are using Short Messaging Service (SMS) to a mobile device as part of a multi-factor authentication strategy. While this generally provides better security than just a standard username and password, using SMS for highly sensitive information is not good enough. But securing collaboration platforms have several major security shortcomings as described below:

1) **SMS Vulnerabilities**
    a. **No Encryption** – SMS messages are sent as clear text that is readable by anyone

on the sender's carrier network, anyone on the carrier-interchange network, and anyone on the recipient's carrier network. There is no integrity in SMS, it is vulnerable to many types of attacks, including the one suffered by German banking customers in 2017 as reported in The Register. Even the reliability of SMS is to be questioned – text messages can experience delays or even non-delivery as a result of cellular data network connectivity issues. To be sure, reliability and availability requirements are key security tenets and innately lacking in SMS.

b. **SMS Hijacking** – Organized crime constituents and sophisticated hackers may motivate international mobile network operator employees to mis-direct SMS messages from the legitimate user to an attacker's device for a period of time to capture the private keys associated with a user's account. SMS services are not a high-integrity system as the legitimate user would not be notified of the misdirection nor the keys being sent to the attacker until after they are finished with their attack.

The US Department of Homeland Security is recommending that government agencies and enterprise stop using SMS for sensitive communication. SMS can be exploited by criminals and nation-state actors.

Last year Twilio, the cloud communication as a platform service provider, became aware of an incident regarding Voxox, a wholesale SMS provider, in which an unsecured database was accessible to the Internet and exposed details of SMS messages and the companies that sent them. Media articles report that many of these SMS messages contained sensitive information such as authentication passcodes and delivery tracking numbers linking to unauthenticated details on the web.

The US Department of Homeland Security is recommending that government agencies and enterprise stop using SMS for sensitive communication. SMS can be exploited by criminals and nation-state actors.

2) **SIM Swapping Exposure** – The Subscriber Identity Module (SIM) inside a smartphone is used to uniquely identify its owner. Criminals who gather details about a victim such as their mobile phone number can get a wireless network company to transfer a phone number to a new phone for a short period of time. Attackers can then trick banks and other companies into granting a password reset sent to a new phone, enabling them to gain entry into a victim's most sensitive online accounts. This problem was recently reported in the Wall Street Journal

3) **iMessaging Weaknesses** - iPhone users often claim that iMessage is a superior technology, but it is also vulnerable to many of the same problems. For example, every iPhone inherently trusts over 150 organizations, some of which are affiliated with known-cyber-attackers and authoritarian regimes. Apple makes the list of these trusts available on their help website. A list of some of the countries which are allowed full eavesdropping on iMessage

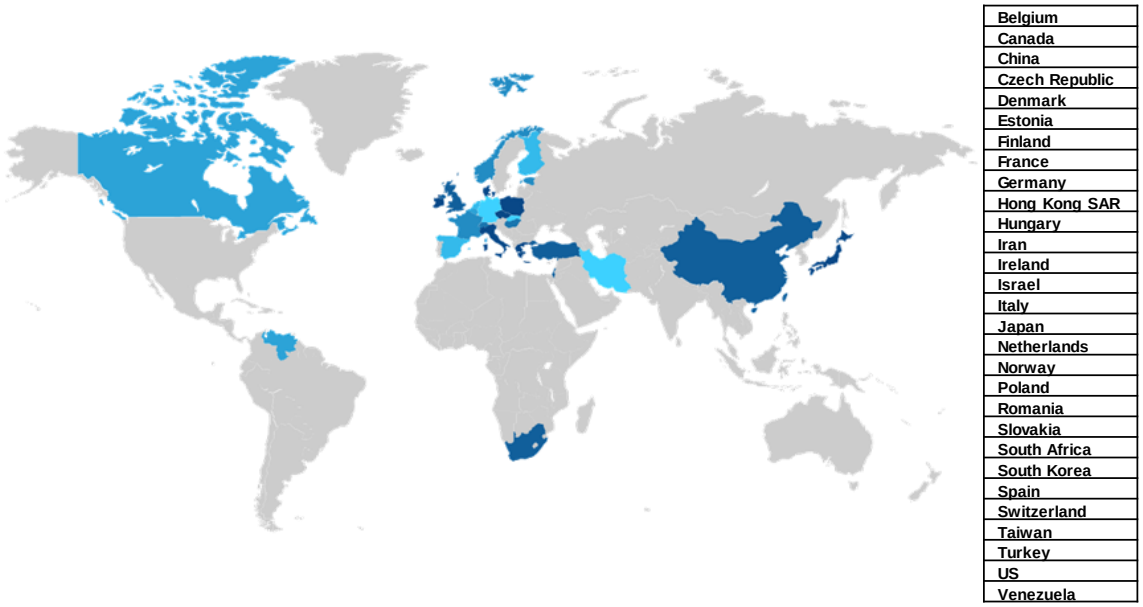

Figure 1. Countries That Have Access to Apple's iMessage

4) **Spying Application Risks** – If you're not using biometrics to protect your mobile devices, jealous lovers, frenemies, and other acquittances with physical access to your mobile device(s) (while you are sleeping, in the shower, at the gym, etc.) can load spyware on your mobile device. Once running they can monitor and record phone calls, track GPS location, read emails and instant message chats, check online activities, view photos, videos, and calendar entries, and remotely control the device. XNSPY is an example application that anyone can acquire for a monthly fee. This is reportedly how Jeff Bezos's wife caught him cheating and used this evidence for a multibillion-dollar divorce settlement.

5) **Enterprise Cloud Messaging Susceptibility** – Cloud-based messaging allows the back-end server operators access to all data that is sent through the system. While there are rules operators should adhere to that minimize the possibility of eavesdropping, it is still possible for their employees to violate those policies or for attackers to design exploits which bypass these policies. Permission models are also lacking, especially for guest accounts. This means that guests (those that are not employees of your organization) can access documents in channels, resources, chats, and applications. Thus, enterprises struggle to control what the organization is sharing. This is especially true when the service operator is presented with lawful intercept demands, in which a government law enforcement or espionage team orders the service operator to share all of the enterprise's information with them, many times without the enterprise's knowledge or consent. For companies that consider the US government to be actively hostile to their interests, the passage of the CLOUD Act gives US Law Enforcement full capability to intercept and store any data that they deem to be

within the bounds of any ongoing investigation.

6) **Shadow IT** – There is a principle of least resistance: people use what they know, is easiest to and most used by others. There is no difference with employees. If the tools the internal IT department provides are not known, easy to use, and/or cost too much, they will be ignored and replaced in the daily working process. Sensitive company data will then flow through Dropbox, Slack and WhatsApp without the owner's consent or even his knowledge. Team applications from companies like Slack make messages available for everyone in that group versus enforcing controlled, need-to-know, and least privileged messaging access. Many enterprise employees have leaked sensitive information this way.

Team applications from companies like Slack make messages available for everyone in that group versus enforcing controlled, need-to-know, and least privileged messaging access. Many enterprise employees have leaked sensitive information this way.

7) **'Secure' Messaging Apps** – WhatsApp, Signal and other consumer-grade secure messaging applications rely on users' mobile phone numbers as unique identifiers to deliver private key material. Due to the risks outlined above in the SMS and SIM Swapping sections, attackers can temporarily hijack the target user's SMS number (either virtually through an international carrier or physically through a SIM swap), send a request to the Signal or WhatsApp service and then receive the recovery keys for those applications, giving the attacker full access to messages sent through those systems. U.S. government agencies reportedly are using these methods to gather information on people inside and outside of the United States.

As if these vulnerabilities are not bad enough, there are also some very basic risks for international business travelers. Customs in many countries requires users to provide their devices and passwords prior to leaving the country. Intellectual property is worth a lot to the right buyer, and where money is involved there will be corrupt and malicious officials who will steal information. No institutions can be trusted.

So, we've defined several of the challenges and known vulnerabilities in securing current collaboration platforms. We'll now look at some of the explicit risks associated with "poor" UC security.

The Risks of Poor UC Security

TechVision broadly breaks Unified Communications Security threats into three categories as follows:

- **Theft of service –** such as toll fraud through the unauthorized use of UC resources

- **Denial of service –** implies a deliberate or accidental attack against services and applications that render them unusable for IT user;
- **Privacy and compliance –** focus on interception of communications and confidentiality challenges associated with the conformance of corporate compliance policies and legislation.

Now that we have identified some of areas where mobility, messaging and the cloud are highly vulnerable, we can look at some examples; such as when Cisco's WebEx team reported a critical security vulnerability that needed an immediate patch. The vulnerability allowed an authenticated, remote attacker to execute arbitrary code on a targeted system due to insufficient input validation by the Cisco WebEx clients.

Another example is when enterprises don't lock down their guest access accounts. In Microsoft Teams or Slack for example, if guest accounts are not appropriately managed, these accounts can view all communication and associated content occurring within an organization.

VoIP and UC networks are susceptible to a variety of security threats. Hackers and fraudsters may try to manipulate real-time communications signaling or media flows, or they may attempt to disrupt networking infrastructure to impair operations, eavesdrop on conversations, or commit service theft. This is a list of VoIP and UC security threats and their potential implication:

1. **Reconnaissance scan -** Address or port scan is used to footprint network topology - Targeted denial of service, fraud, theft
2. **Man in the middle -** Attacker intercepts session to impersonate (spoof) caller -Targeted denial of service, breach of privacy
3. **Eavesdropping -** Attacker "sniffs" session for the purpose of social engineering - Breach of privacy, fraud, theft
4. **Session hijacking -** Attacker compromises valuable information by rerouting call - Breach of privacy, fraud, theft
5. **Session overload -** Excessive signaling or media traffic (malicious, non-malicious) is experienced - Denial of service
6. **Protocol fuzzing -** Malformed packets, semantically or syntactically incorrect flows are encountered - Denial of service
7. **Media injection -** Attacker inserts unwanted or corrupted content into messages - Denial of service, fraud

Besides all these technical reasons for UC security threats, the most obvious threats are people. UC involves many people communicating and sharing ideas and content. People are the weak link ensuring that any communication is kept secure, private, and confidential. 80% of enterprise breeches have an internal component whether this is a person or malware, usually installed by an internal person. User security threats are categorized as follows:

1) **Laziness** – Users going with default or common passwords such as 123456 for voice mail access and not taking the few seconds to validate who is on a conference call. Executives are guilty of this too, with many leaving their calendars open for all to see along with the bridge numbers and passwords for their conference calls. By-passing corporate systems or guidelines with external solutions that are virtually free in the name of speed and convenience. While many enterprises have training programs to make users aware of industry best practices, they do not follow-up with any type of enforcement to ensure good behavior and inform managers of bad behavior
2) **Exploited** – Targeting one or a group of users to get information or do something to lead to a vulnerability such as clicking on a fraudulent email. Phishing attacks are growing more sophisticated and targeting specific users and systems. Many salespeople have built up relationships with internal enterprise employees through events and dinners and will use this information to help gather information on an organization. When million or even billion-dollar level sales are on the line, some folks cross the line. The line is usually crossed in telephony or in-person conversations that are not e-discoverable in case there is a lawsuit.
3) **Malicious** – An internal employee or contractor takes external money or favors to do something illegal. Organized crime and hackers are becoming more like spies and recruiting employees and officials to help them exploit enterprises. Exploiting enterprises and government agencies is big business and paying someone a million dollars or more to do something illegal is becoming more common. For instance, a man was charged for bribing an AT&T staff member to illegally unlock phones.

Organized crime and hackers are becoming more like spies and recruiting employees and officials to help them exploit enterprises.

Figure 2 illustrates some of the leading use cases for UC Security. Note, that UC security includes privacy and compliance along with security.

1. **Protecting Intellectual Property**: R&D team chats, files, and interactions are secured and controlled via strictly defined access rules including location such as R&D facility and manufacturing plant in foreign country

2. **Ensuring Privileged Company Communications**: CxO and Exec Management interactions regarding M&A deals, Investor relations, Sensitive HR comms, CxO status meetings

3. **Providing Ultra-Secure Communications**: In the event of a cyber-security breach or suspected attack, being able to communicate in a secure, out-of-band, trusted-circle or channel is critical so hackers cannot be part of your remediation actions

4. **Securing Sensitive Customer Service Interactions**: Some external customer and frontline communications need to be *kept from going rogue under any circumstances* due to potential brand and reputational damage implications

5. **Compliance:** Manage GDPR cross-border PII data transfers without hassles, Comply with labor laws such as "right to be forgotten," or "right to disconnect," be able to offer CCPA, HIPAA protection to customers along with the ability to provide compliance audits.

Figure 2 Common UC Security Use Cases

The risks to an organization that doesn't properly secure their UC system(s) include:

1) **Loss of Data** – UC is more than voice and video, there is a lot of data associated with Web conferencing and file sharing. Losing sensitive data can be exceedingly costly to an organization in terms of fines, intellectual property theft, brand damage and so forth.

2) **Back Doors** – Bad actors can bypass standard security controls to gain access to private networks, creating backdoors and leaving them open.

3) **User Tracking** – Using meta-data regarding communications to track who is talking to whom, when, and where, even if the media is encrypted.

4) **Blackmail** – Recording private conversations and threating to make the information public.

UC combines telephony, video, chat, email and presence together into one unified communications system. As the technology has become more complex and more accessible from the public Internet, the security threat has increased. In many ways it's easier than ever to attack business communications. Companies must be diligent in protecting their Unified Communication services as they are vital to business operations.

Companies have historically relied on the premise that their internal networks were secure as long as they required external users to use a VPN solution to gain access. This premise is no longer valid because:

1) **No network is secure** – It is been proven that the top vector for attacks come from inside the enterprise network. – *See the TechVision Research Zero Trust Networking Report*

2) **BYOD** – (Bring Your Own Device) UC from personally owned devices including employees, contractors, partners who do not have a VPN or MDM client software protections.
3) **Speed** – The delay or friction caused by setting up a VPN session incents users to bypass the "VPN step" in order to immediately start communicating.
4) **Public UCaaS** – Hosting UC externally at a 3rd party using Internet network connectivity is common, especially with the rise of freemium solutions.
5) **WebRTC** – Supporting standardized clientless UC anywhere and everywhere.

Each of these are avenues that can lead to breach, theft, and brand erosion.

Telephony Denial of Service (TDoS) is also a serious issue. Hackers have flooded enterprises and government entities with false calls that overwhelm their systems, which effectively block all legitimate calls. If the system under attack is an enterprise system, customer service callers cannot get through. More disturbingly, if the system under attack is a government system, citizens cannot reach their local 911 center. TDoS is similar to DDoS used on networks, except this one is specific to phone service.

Telephony Denial of Service (TDoS) is a serious issue. Hackers have flooded enterprises and government entities with false calls and overwhelm their systems, which effectively blocks all legitimate calls.

If securing UC was easy, we probably wouldn't be writing this report. Next we'll look at what UC is so difficult to secure and then describe some of the techniques for addressing these challenges.

Why UC is Difficult to Secure

Unified Communication applications have many unique attributes that make them more difficult to secure than standard client server applications. These attributes include:

1) **Users are Everywhere** – Unlike data centers where data can be kept physically in a well-guarded building, users are everywhere, can be anyone, using any device. The locations can include; home, mobile, in an office building, out of country on business travel – basically anyone on the planet. Users can also be anyone including employees, partners, contractors, customers, or guests. To make matters even more challenging, communication occurs across many different devices that have different operating systems. Bring Your Own Device (BYOD) was another challenge introduced about a decade ago where enterprises must support communication across personal devices that they do not own or manage.
2) **Compliance and Privacy** - Regulations create liabilities for those companies which do not implement the proper tools and controls. Recent regulations like GDPR, HIPAA,

California Privacy Law and local labor laws require enterprises to have data controls in place to protect sensitive data in all situations, regardless of which systems are used or what infrastructure is relied on. Enterprise compliance and security teams are looking for solutions which will support their objectives of ensuring the traditional ICA requirements for data protection. ICA stands for:

- **Integrity:** Ensure that the data being shared among team members is trustworthy, accurate and not manipulated by any outside party.
- **Confidentiality:** Prevent sensitive and regulated data from being accessed by any unauthorized individual, whether a nation/state attacker, service provider or malicious actor.
- **Availability:** Critical data is available to the right people at the right time in the right location.

3) **Remote Control** – One feature within web collaboration tools is to allow remote users to take control of the end device. This is great for IT support to fix problems and for teams collaborating on a drawing. However, remote control can be exploited by bad actors. For instance, a temporary employee can allow a nation-state to have access to their computer which can reside within an enterprise or government network. This makes it easier for the bad actors to gain access to private information and communication. Another example is a user is invited to a meeting but must download a UC client to participate. UC Client has malware embedded in it that can take over the PC once the user goes home.

4) **Unique Technology** – Communication technology focuses on interactions, while most of our security technology is focused on transactions. The unique technology to support interactions includes:

- **Peer-to-peer** – WebRTC and proprietary UC stacks allow one device to talk directly to another without going through a centralized service and security stack. Traditional applications are client/server based, where a security stack can reside at the server. This is a challenge to secure because it is reliant on end point security rather than more reliable server security.
- **Bi-Directional** – Sessions can be established in both directions due to the call/calling nature of UC versus a web application where a user establishes the session request. A home router for instance has a simple firewall rule that states all TCP & UDP sessions must be initiated from within the home network and why, in order to get a Skype call, the home user first must be logged into Skype. This is a challenge to secure because it is difficult to validate the credentials of the source of incoming traffic.
- **UDP Transport** – Unlike TCP which has connections, sequence numbers, and specific ports for different types of applications, UDP has none of these. Different vendors open up a range of UDP ports and UC sessions cycle through the range of ports. The range of ports must be bigger than the peak number of concurrent UC users. This is a challenge to secure because UDP does not keep state, have

handshakes, etc. This means an attacker could easily send a spoofed packet unless there are protections at other layers.

- **Multiple services** - Voice, video, chat, data – UC uses a range of services, each with their own TCP/UDP port. With conferencing, there can be hundreds of users interacting both internally and externally with the organization. This is a challenge to secure because it is porous, unlike a controlled user group using predictable protocols behind the firewall.
- **Jitter Sensitivity** – Jitter is the variation in latency, and jitter above 20ms will result in the effective loss of real-time voice/video traffic. With video conferencing, there can be instantaneous spikes in network traffic that are 100x the norm. Firewalls and other security appliances have trouble processing a lot of UC traffic without causing jitter. The primary reason why UC was the last major application to use virtualized infrastructure at scale is due to this.
- **Too Many Proprietary Appliances** – Legacy PBX, voice mail, conferencing systems use proprietary hardware with purpose-built operating systems. These appliances are subject to known security vulnerabilities.

5. **User Experience** – Users of communication technology are very particular about their experience. They want it to be easy to use with a simple menu of functions, quick to set-up, with quality voice and video and minimal latency so that when someone tells a joke you are not waiting half a second to hear people laugh. Many of the new Freemium platforms such as Slack and Zoom.us have gained popularity by offering a great user experience. Enterprise IT wants a single solution to support, but users by-pass the IT solution. These Freemium solutions are usually not tightly managed, yet proprietary and confidential information commonly flows through them.

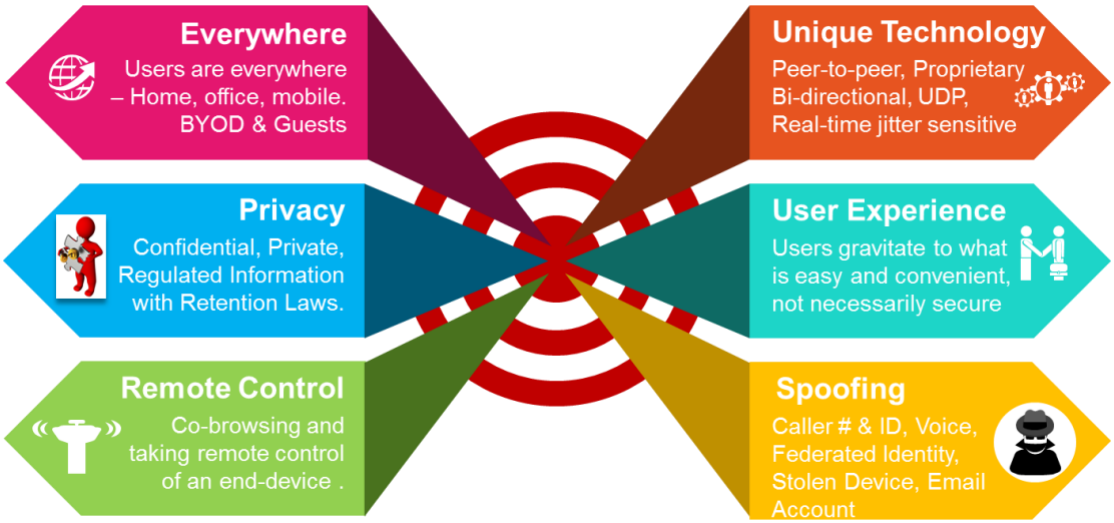

Figure 3 – Why UC is Difficult to Secure

6. **Phone Number Spoofing** - *We can no longer trust that someone's phone number and the sound of someone's voice as truly that person.* Phone number spoofing is a known problem, one that has been around for years. It is addressable via solutions from companies such as Pindrop that help determine the probability that the caller's number is legitimate. Through white and blacklists of phone numbers, testing network delay, and other audio heuristics, the confidence rates are in the high 90s. For instance, if a call comes in from a U.S. area code, but the network delay is over 100 milliseconds, then odds are high that the caller is really overseas.

We can no longer trust that someone's phone number and the sound of someone's voice as truly that person.

   This technology is beneficial in contact centers. Enterprise call centers deploy this technology to reduce the number of security questions they must ask, in turn reducing the average call handle time, saving money and providing a better caller experience.

   A newer problem, thanks to artificial intelligence (AI) in the speech world, is voice spoofing. We hear on the late-night talk shows people using these tools to mock our president and other officials.

   Voice verification technology has been around for at least 20 years, in use at many banks and stock trading companies as part of the multifactor authentication strategies they put in place to protect funds transfers. Voice verification systems require large base-line sample sizes for optimal performance, so work best when used regularly. Given that voice-spoofing capabilities are becoming more mainstream, enterprises that use voice verification technology should look at additional security controls for validating callers.

   Bad actors can easily use a site like spoofvoice.com to change their voices and phone numbers to remain anonymous. A more sophisticated bad actor can grab audio clips from YouTube and mimic someone else's voice. In many ways, this level of spoofing is mirroring the frightening onslaught of "deep fakes" of audio-video content.

So what do we do about these challenges? In the next section we'll introduce a specialized UC security device called the Session Border Controller (SBC). Given the magnitude and variety of threats we've discussed (and many we haven't touched on), TechVision recommends considering this "fit for purpose" approach to securing your Unified Communication portfolio.

About TechVision

World-class research requires world-class consulting analysts and our team is just that. Gaining value from research also means having access to research. All TechVision Research licenses are enterprise licenses; this means everyone that needs access to content can have access to content. We know major technology initiatives involve many different skillsets across an organization and limiting content to a few can compromise the effectiveness of the team and the success of the initiative. Our research leverages our team's in-depth knowledge as well as their real-world consulting experience. We combine great analyst skills with real world client experiences to provide a deep and balanced perspective.

TechVision Consulting builds off our research with specific projects to help organizations better understand, architect, select, build, and deploy infrastructure technologies. Our well-rounded experience and strong analytical skills help us separate the "hype" from the reality. This provides organizations with a deeper understanding of the full scope of vendor capabilities, product life cycles, and a basis for making more informed decisions. We also support vendors in areas such as product and strategy reviews and assessments, requirement analysis, target market assessment, technology trend analysis, go-to-market plan assessment, and gap analysis.

TechVision Updates will provide regular updates on the latest developments with respect to the issues addressed in this report.

About the Authors

Sorell Slaymaker has 30 years of experience designing, building, securing, and operating IP networks and the communication services that run across them. His mission is to help make communication easier, cheaper and more secure since he believes that the more we communicate, the better we are. Prior to joining TechVision Research, Sorell was an Evangelist for 128 Technology which is a routing and security software company. Prior to that, Sorell was a Gartner analyst covering enterprise networking, security, and communications.

Sorell is an IT Architect with a focus on network, security, and communications architecture. He specializes in IT Architecture – Network Architecture, SIP Trunking, Contact Centers, Unified Communications, and Security Architecture.