# Deploying Secure Unified Communications/Voice and Video over IP Systems (Abridged)

Unified Communications (UC) and Voice and Video over IP (VVoIP) call-processing systems provide rich collaboration tools and offer flexible ways to communicate by combining voice, video conferencing, and instant messaging in the modern workplace. Today these systems are integrated into an enterprise's existing Internet Protocol (IP) infrastructure, use commodity software, and are likely to use open-source and standard protocols.

However, the same IP infrastructure that enables UC/VVoIP systems also extends the attack surface into an enterprise's network, introducing vulnerabilities and the potential for unauthorized access to communications. These vulnerabilities were harder to reach in earlier telephony systems, but now voice services and infrastructure are accessible to malicious actors who penetrate the IP network.

If properly secured, a UC/VVoIP system limits the risk to data confidentiality and communication system availability. This security requires careful consideration, detailed planning and deployment, and continuous testing and maintenance.

NSA has released a comprehensive Cybersecurity Technical Report, *Deploying Secure Unified Communications/Voice and Video over IP Systems,* which outlines best practices for the secure deployment of UC/VVoIP systems and presents mitigations for vulnerabilities due to inadequate network design, configurations, and connectivity. This report is separated into four parts. Each part speaks to the system administrators who will lead mitigation efforts in each area of the system. It describes the mitigations and best practices to use when:

- Preparing networks
- Establishing perimeters
- Using enterprise session controllers (ESCs)
- Adding UC/VVoIP endpoints for deployment of a UC/VVoIP system

This abridged report captures some of the key takeaways. System administrators are encouraged to access the full report for a complete list of best practices and mitigations.

## What are the vulnerabilities?

Legacy telephony systems were more isolated from other networks due to the use of dedicated infrastructure. Additionally, they were based on proprietary software and protocols that could not communicate with other devices. On the other hand, UC/VVoIP systems are integrated into the enterprise's existing IP infrastructure, use commodity software, and are likely to use open source and standard protocols. These systems and protocols are very familiar to malicious actors, making UC/VVoIP systems potentially susceptible to the same malicious activity constantly targeting existing IP systems, including through spyware, viruses, software vulnerabilities, or other malicious means. These avenues of attack can be used to eavesdrop on conversations, impersonate users, or perpetrate denial of service effects if robust mitigations are not put in place. Compromises can lead to high-definition room audio and/or video being covertly collected and delivered to a malicious actor using the IP infrastructure as a transport mechanism.

Sharing the IP infrastructure also creates a single point of failure in an organization's communication capabilities. If the IP network fails or there is a widespread denial of service, all UC/VVoIP services could be severely degraded or lost.

UC/VVoIP endpoint devices offer a richer set of capabilities than legacy telephony endpoints, but also come with an increased attack surface. When using a UC/VVoIP system, many of these devices on the enterprise network could be offering services such as Hypertext Transfer Protocol (HTTP), Simple Network Management Protocol (SNMP), telnet, and Wi-Fi and Bluetooth® connectivity. These UC/VVoIP devices must be examined and configured to protect against vulnerabilities in these services, just like computers and other network endpoints. In addition to UC/VVoIP endpoints, UC/VVoIP servers can be vulnerable to exploitation like other servers on the enterprise network, including from remote access capabilities.

Even though fraud existed in legacy telephony systems, the scope of impact was limited based on the number of phone lines compromised. In UC/VVoIP systems, once a phone line is compromised, multiple calls can be made with that phone line simultaneously, greatly increasing the severity of the fraud. Fraud, in both legacy and UC/VVoIP systems, can target either subscribers (service customers) or service providers. The aim of fraud at either the subscriber-level or service-provider level is to make free calls and/or financial gain.

Critical emergency services based on physical location, such as 911, can also present challenges. Users of UC/VVoIP systems can move their endpoint devices between

physical locations, but function as if they were in the office. Examples include taking an office endpoint device to a remote site to work for the day or taking it home to telework. If proper procedures are not in place to account for these moves, a call from the endpoint device reporting an emergency may result in first responders arriving at the wrong location.

## What can be done?

UC/VVoIP systems introduce a new class of attacks that did not pertain to legacy telephony systems. To minimize the risk of having your telephony system on the data network, follow the guidelines below. For more details, reference the full-length *Deploying Secure Unified Communications/Voice and Video over IP Systems* Cybersecurity Technical Report for a comprehensive set of mitigations related to network security, perimeter security, enterprise session controller security, and UC/VVoIP endpoints.

### *Segment the network*

Virtual Local Area Networks (VLANs) can be used to segment voice and video traffic from data traffic and separate IP address ranges to limit access to a common set of devices. Create VLANs for:

- IP phones
- UC/VVoIP servers
- Public Switched Telephone Network (PSTN) gateways
- Administrative access to infrastructure
- Existing data devices

In addition to using VLANs, use access control lists and routing rules to limit access to devices across VLANs. This makes it more difficult for a malicious actor to access open services on phones and servers from outside of the VLAN.

Converged services, such as unified messaging, should be placed in a demilitarized zone (DMZ) similar to the DMZ between trusted and untrusted networks. Tightly control traffic with stateful filtering, application layer proxies, and malware scanning.

Lastly, exclusive reliance on softphones (software applications installed on a personal computing device to make telephone calls) can be risky because the security and

availability of them depend on the underlying general-purpose device. In addition, it violates the principle of UC/VVoIP and data network separation. When softphones are used, either use them only as a secondary voice device and establish a separate VLAN for PCs with softphones, or require that they connect through an IP gateway.

## *Implement layer 2 protections*

Add layer 2 protections, such as port security, assigning static media access control (MAC) addresses to switch ports, and other Address Resolution Protocol (ARP) and IP spoofing defenses. Only use switches that offer these protections. Using a packet sniffer, ensure switches embedded in IP phones (to enable PC port connectivity) properly handle VLANs and limit access to the phone from the connected computer. Prevent Dynamic Host Configuration Protocol (DHCP) abuse by designating trusted switch ports for DHCP server responses.

## *Protect the PSTN and Internet perimeters*

PSTN gateways should authenticate all UC/VVoIP connections and not allow calls directly from IP phones without permission of the UC/VVoIP server. When using UC/VVoIP trunks over public IP networks, session border controllers (SBCs) should control access to internal UC/VVoIP resources, deal with network address translation (NAT) traversal issues, and encrypt traffic. In addition, SBCs inspect UC/VVoIP traffic at the application layer to check for Request for Comment (RFC) compliance and malicious data embedded into the UC/VVoIP packets. NSA recommends deploying SBCs evaluated under the National Information Assurance Partnership's (NIAP) Extended Package for Session Border Controller Protection Profile. When using VVoIP trunks over VPNs, be sure to maintain VLAN security across the VPN.

## *Stay up to date with patching*

Patches should be signed by the vendor and only downloaded from trusted sources. Before applying patches to a production network, they should first be vetted on a test network to ensure no unexpected or adverse conditions are caused by the software

update. Once vetted, they should be applied to the system immediately. Timely patching helps to mitigate software vulnerabilities that exist in UC/VVoIP systems and devices.


## *Authenticate and encrypt signaling and media traffic*

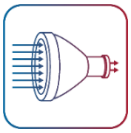
Authentication and encryption of all signaling and media traffic prevents impersonation and eavesdropping by malicious actors. Mutual authentication of signaling traffic is critical to prevent intruders from easily impersonating legitimate users. When authenticating to UC/VVoIP servers, it is strongly recommended to use multi-factor authentication. UC/VVoIP traffic should be protected using a trusted channel employing strong encryption protocols, such as Transport Layer Security (TLS) or Internet Protocol Security (IPsec). Unencrypted UC/VVoIP traffic can lead to a malicious actor gaining valuable information about the UC/VVoIP endpoints and details of the calls.

## *Prevent fraud*

Deploy an SBC to monitor UC/VVoIP traffic at the perimeter and between service provider networks. Audit call data records (CDRs) using fraud detection solutions that monitor CDRs and detect fraud in near real-time. Block calls to destination countries known to have high incident rates of fraud.

## *Ensure availability*

Maintain backups of software configurations and installations, acquire high availability hardware, build redundant network paths, and have standby hardware. Provide backup power to servers, phones, and network infrastructure in case of power outages. For phones this may mean supplying power over Ethernet and expanding backup power capacity in network closets. Use monitoring software that alerts administrators to any hardware failures and temperature spikes on critical servers.



### *Manage denial of service attacks*

Utilize rate limiting settings, quality of service controls, and secondary connections to outside networks. Limit the number of incoming calls to prevent overloading of the UC/VVoIP servers. Implement quality of service controls to ensure UC/VVoIP traffic has priority even on a saturated network. Have secondary Internet connections to UC/VVoIP service providers or backup circuit-switched PSTN connections.

### *Control physical access*

Secure areas with network and UC/VVoIP infrastructure (e.g. routers, switches, and servers). Locks requiring identification cards, biometrics, or other electronic means can also provide useful auditing information about access to equipment. Two-person access control is recommended. These areas should also include measures to reduce the risk of other potential physical threats, such as from fire or flooding.

### *Verify features and configurations in a test bed*

Test before adding devices to operational networks. Do not allow rogue devices to auto configure themselves with the UC/VVoIP servers. Choose a single, secure remote management protocol. Disable all others and block them on the network.

## Final word

Taking advantage of the benefits of a UC/VVoIP system, such as cost savings in operations or advanced call processing, comes with the potential for additional risk. A UC/VVoIP system introduces new potential security vulnerabilities. Understand the types of vulnerabilities and mitigations to better secure your UC/VVoIP deployment. NSA recommends deploying the technology using the guidance presented in this paper. For more detailed guidance, please consult the *Deploying Secure Unified Communications/Voice and Video over IP Systems* Cybersecurity Technical Report on NSA.gov.▪

## Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

## Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

## Trademarks

Bluetooth is a registered trademark of Bluetooth Special Interest Group (SIG), Inc.

## Contact

- Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
- Media Inquiries / Press Desk: Media Relations, 443-634-0721, MediaRelations@nsa.gov