National Security Agency
Cybersecurity Technical Report

Deploying Secure Unified Communications/Voice and Video over IP Systems

June 2021

SN U/OO/153515-21
PP-21-0827
Version 1.0

Notices and history

Document change history

Date	Version	Description
15 June 2021	1.0	Initial release

Disclaimer of warranties and 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 necessarily 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.

Trademark recognition

Bluetooth is a registered trademark of Bluetooth Special Interest Group (SIG), Inc. NIST is a trademark and brand of National Institute of Standards and Technology.

Publication information

Contact information

Client Requirements / General Cybersecurity Inquiries:
Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov

Media Inquiries:
Media Relations, 443-634-0721, MediaRelations@nsa.gov

Purpose

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

Table of contents

Figures

Executive summary

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 to eavesdrop on conversations, impersonate users, commit toll fraud, or perpetrate a denial of service effects. Compromises can lead to high-definition room audio and/or video being covertly collected and delivered using the IP infrastructure as a transport mechanism.

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. *Deploying Secure Unified Communications/Voice and Video over IP Systems* 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

Using the mitigations and best practices explained here, organizations may embrace the benefits of UC/VVoIP while minimizing the risk of disclosing sensitive information or losing service.

Part I: Network security best practices and mitigations

To securely deploy Unified Communications / Voice and Video over Internet Protocol (UC/VVoIP) systems, the network is the first critical area to implement security protections. Part I of *Deploying Secure Unified Communications/Voice and Video over IP Systems* addresses how to secure the network of one of these systems.

UC/VVoIP call-processing security is dependent on a defense-in-depth approach. UC/VVoIP call-processing network elements are on the data network, requiring careful deployment and configuration of the network infrastructure to address possible threats related to UC/VVoIP systems. The data-only network infrastructure—including transport devices such as switches and routers—must mitigate known vulnerabilities of the Internet Protocol (IP) network to protect the call-processing devices.

Deploying across a data-only network infrastructure makes devices such as call servers, desktop video teleconferences (VTCs), and UC/VVoIP endpoints more accessible to malicious cyber actors. Compromises of the call-processing network are performed using the same tools used to compromise data-only networks and related peripherals (e.g., PCs, smartphones, printers, switches, routers). In addition, malicious actors can connect to the UC/VVoIP call-processing infrastructure using the data network infrastructure. Separating the UC/VVoIP call-processing and data-only infrastructures makes penetrating the UC/VVoIP systems harder. Virtual local area networks (VLANs) allow multiple networks to use the same physical layer 2/3 medium (e.g., switches, routers), but remain logically separated.

Because UC/VVoIP endpoint calls in UC/VVoIP systems are carried over more accessible data networks than the traditional public switched telephone network (PSTN), eavesdropping is more of a risk. While it cannot eliminate the risk altogether, network security can help make eavesdropping more difficult.

In addition, the data-only network infrastructure must now meet the same reliability and quality of service (QoS) requirements as the UC/VVoIP call-processing network. To ensure a secure deployment of UC/VVoIP systems and devices across the data network in a way that also ensures high availability requires the implementation of redundancy, data backups, power backups, and physical protection of the network.

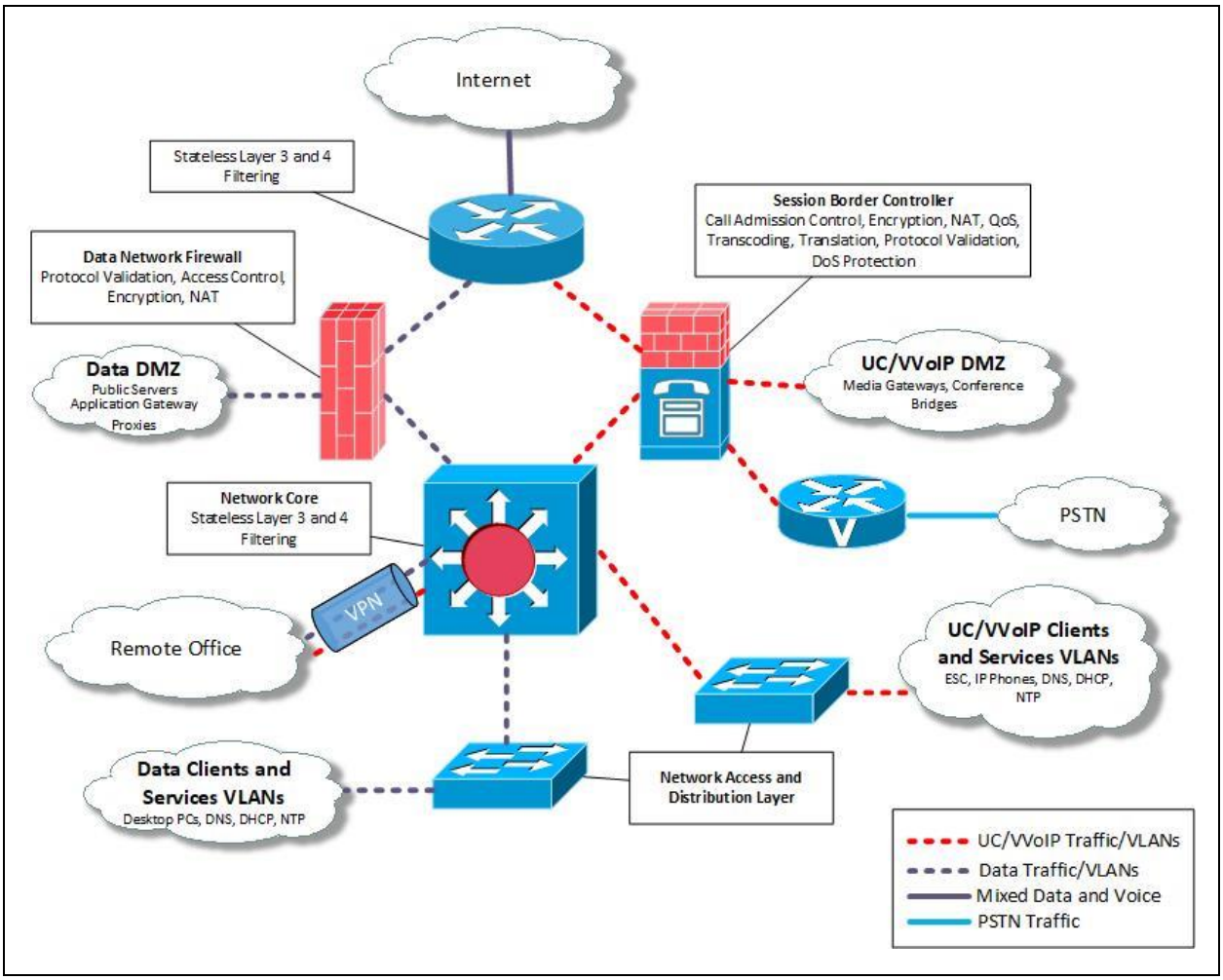

Figure 1: Logical view of a UC/VVoIP system following NSA guidelines

Accessibility and network separation

Physical convergence of voice/video technology across a data network is an advantage of UC/VVoIP call-processing systems. However, placing UC/VVoIP systems and data systems on the same network means both technologies are now susceptible to the same techniques and accessible by the same malicious actors. Once an actor has penetrated the network, both data services and UC/VVoIP call processing will be available for exploit. This violates the basic defense-in-depth principle, because vulnerabilities in one part of the network should not make another part of the network vulnerable. The border between the voice/video network and the data network should be treated as untrusted and secured accordingly. They should not be freely accessible to each other. Access from the data network to the UC/VVoIP network should be denied

unless explicitly allowed. The converse from the UC/VVoIP to the data network should also be enforced.

Mitigations

By using VLAN technology, lateral movement between the data network and the UC/VVoIP network can be limited, even though both networks share the same physical network. While VLANs were not designed as security mechanisms, they can be used to enable security features, such as placing access controls on the type of traffic that is allowed on specific VLANs. VLANs allow UC/VVoIP traffic to be isolated from data traffic and vice versa, while enabling any interactions between them to be tightly controlled. This limits the reconnaissance a malicious actor can perform from one network to the other and limits the protocols they can exploit.

Place all network devices not specifically used to support UC/VVoIP—such as PCs, file servers, and email servers—on data VLANs. UC/VVoIP devices should be placed on different VLANs according to their role in the network. Limiting each VLAN to groups of similar devices and protocols makes the development, implementation, and management of security features much easier. UC/VVoIP servers should be placed in different VLANs depending on the UC/VVoIP protocol they implement. As an example, all H.323 servers should be placed in an H.323-only VLAN, and all Session Initiation Protocol (SIP) servers should be placed in a SIP VLAN. If a single server implements multiple protocols, the network interface card (NIC) should support virtual VLANS so the server can participate in multiple VLANs. The UC/VVoIP network and the data network should have their own servers for standard network support services like the Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Network Time Protocol (NTP). This is necessary because traffic from these services should not have to cross the boundary between UC/VVoIP and data VLANs.

Dividing the network into multiple VLANs does not provide any benefit if the traffic between the VLANs is not restricted. As traffic enters the network through the border router, the border router only performs stateless packet filtering on the traffic due to routing load. Starting at the session border controller (SBC), control traffic between UC/VVoIP VLANs with stateful packet filtering devices. Configure the access control lists (ACLs) on the stateful packet filtering devices to allow UC/VVoIP endpoints to connect only to the UC/VVoIP servers the endpoints need to function and vice versa. Filter based on IP address, port number, and transport protocol instead of on port

number alone. Only allow protocols necessary for operation to be allowed by the filter. Everything else should be denied.

Use an application-layer firewall to separate the UC/VVoIP VLANs from the data VLANs. The application-layer firewall will function as a checkpoint for all traffic between the UC/VVoIP and data networks. No traffic should be allowed directly between the UC/VVoIP VLAN segmented network and the data VLAN segmented network without being examined at the application layer by either the firewall or a proxy device in the demilitarized zone (DMZ). Only necessary protocols should be allowed through the firewall.

Some devices, such as unified messaging servers, fulfill roles on both networks, and thus need access to both the data and UC/VVoIP VLANs. Place these devices in the DMZ managed by the application-layer firewall.

Call eavesdropping protections

Unencrypted voice and video communication is susceptible to eavesdropping when conversations travel over an IP network. Commercial tools exist that allow media streams to be reconstructed if packets can be captured, even when using proprietary coder-decoders (codecs). Network-layer security protections may not be able to prevent call eavesdropping completely, but they can make it much more difficult.

Mitigations

The best mitigation against eavesdropping is encrypting all voice and video traffic end-to-end. Additionally, limiting access to the traffic can be achieved by enabling port security on all switches. Port security restricts access to the network at the layer 2 level. If a rogue device physically tries to connect to a switch with port security enabled, the switch disables the port and does not grant the rogue device access to the network. Port security 802.1x device authentication should be enabled to force clients to authenticate before they are allowed onto the network.

Physical access protections

With physical access to equipment, a malicious actor can disable the network, eavesdrop, and otherwise compromise the UC/VVoIP call-processing system. Most digital safeguards on the network are meaningless if an intruder gains physical access to the equipment being protected. With physical access to equipment, malicious actors

can often use a simple USB device to install malware. Backdoors can be installed or entire databases containing sensitive information can be downloaded. For these reasons, it is imperative to put physical protections for the equipment in place.

Mitigations

Grant physical access to network hardware only to authorized personnel. Place network hardware in a locked, restricted, and controlled area. A log with timestamps of personnel accessing these areas should be kept, if possible. The hardware equipment should be kept in cabinets that can be locked. The cabinets should remained locked unless there is a need for authorized personnel to physically access the equipment. Video cameras should also be installed to provide video surveillance of the restricted areas if practicable.

Network availability protections

Denial of service (DoS) impacts take many forms and are difficult to prevent. DoS effects can be triggered by software vulnerabilities to disable UC/VVoIP devices, consume resources on a UC/VVoIP server, or consume excessive amounts of network bandwidth. The first two types are addressed by using trusted software and staying current on patching. However, over-consumption of network bandwidth can often be addressed at the network level.

There are also environmental factors that can disable or degrade availability of the network. Power outages are an example of such a factor. These events must also be taken into account.

Mitigations

DoS techniques using network bandwidth can directly target UC/VVoIP devices. Limiting the rate of traffic to UC/VVoIP VLANs can reduce the effects of such DoS attempts coming from outside the UC/VVoIP call-processing network. When designing the UC/VVoIP call-processing network, determine the number of simultaneous incoming external calls that can be handled without detrimentally affecting the ability to place internal calls. Use network perimeter devices such as firewalls, SBCs, and filtering routers to limit the bandwidth allocated to incoming external calls. These perimeter devices typically have built-in features that detect and limit DoS attempts. This reduces the amount of network traffic allowed into UC/VVoIP call-processing VLANs.

UC/VVoIP protocols are time sensitive protocols and vulnerable to jitter, latency, and packet loss. UC/VVoIP traffic should not be delayed due to lower priority traffic. There are mechanisms available to score and prioritize traffic traversing the network. One of these is QoS. Quality of service should be enabled on network hardware that route UC/VVoIP call-processing traffic and given a higher priority than less time-sensitive traffic.

To guard against power outages, a backup power source should be installed. UC/VVoIP endpoints receive power over the network cable using Power over Ethernet (PoE) technology. To ensure telephone service in the event of a power outage, any network hardware device that provides PoE to any UC/VVoIP client should be attached to a backup power source.

Network services and protocols protections

Many network-based services are required to maintain secure, enterprise-wide UC/VVoIP call-processing. This section covers three of them: DHCP, DNS, and NTP.

DHCP

DHCP is most often used to assign network settings such as IP addresses, DNS name servers, and gateway routers to UC/VVoIP clients. DHCP is a good option for assigning IP addresses to UC/VVoIP endpoints and other peripheral IP devices. The other option is to statically assign IP addresses, but that comes with a higher administrative burden as each IP address must be manually assigned to each device. Implementation of DHCP requires careful consideration because DHCP is inherently vulnerable. It does not possess security features such as authentication and encryption, which are prevalent in modern protocols. A rogue DHCP server can connect to the network and provide network settings to a UC/VVoIP endpoint, which could result in a DoS effect or man-in-the-middle interception. In addition, a malicious DHCP client can also cause a DoS effect by continuously requesting IP addresses until the DHCP pool is exhausted. Without an IP address, phone service is unavailable.

Mitigations

Since UC/VVoIP deployments may contain hundreds or thousands of endpoint needing IP addresses, DHCP may be the only reasonable solution in assigning IP addresses. Manually assigning IP addresses does not scale well in larger environments. To guard against rogue DHCP servers on the network, DHCP snooping should be employed on

local area network (LAN) switches. DHCP snooping is a layer 2 technology that drops DHCP messages from DHCP servers that are not authorized. DHCP snooping also keeps track of successful DHCP bindings and inspects DHCP traffic for malicious data.

To combat malicious DHCP clients connecting to the network, port security should be enabled on the LAN switches. If an unauthorized DHCP client is plugged into the switch, port security will disable the port and deny the unauthorized client access to the network. Port security 802.1x device authentication should also be enabled to force clients to authenticate before they are allowed onto the network.

The UC/VVoIP network should have a separate DHCP server from the data network. Only clients on the UC/VVoIP network should be allowed to request addresses from this DHCP server.

DNS

DNS is foundational to all data and UC/VVoIP networks for translating domain names into IP addresses where messages can be sent. In its inception, DNS was not designed with security in mind, so malicious issues such as DNS cache-poisoning, compromised DNS servers, and malicious DNS registrations have arisen. These have led to secure DNS-related proposals such as DNSSEC (DNS Security Extensions). Malicious DNS techniques could result in man-in-the-middle compromises or UC/VVoIP connections to malicious devices.

Mitigations

DNSSEC should be employed at your enterprise boundary, by enabling DNSSEC validation at the recursive resolvers. DNSSEC adds two important security features to DNS: authentication and integrity. DNSSEC assures that the data the DNS server receives from other DNS servers has not been modified and that the data was received from the authoritative zone the data originated from. If an error occurs in validating the DNS data, the data is dropped.

There are also techniques such as forward-confirmed-reverse-DNS that can make DNS more secure. This is a networking parameter configuration in which an IP address has both forward (name-to-address) and reverse (address-to-name) DNS entries that match each other.

In addition to DNSSEC and forward-confirmed-reverse-DNS, zone transfers should be disabled. With zone transfers enabled, a malicious actor could issue a DNS query that would initiate a zone transfer of the internal DNS database. A DNS zone transfer replicates DNS records across DNS servers, eliminating the need to manually update DNS servers. If a DNS server can be tricked into sending a DNS zone transfer to a malicious actor, the actor could use that information to easily map and target specific servers on the network. DNS zone transfers should only be allowed to servers that have a specific need for the information. All other zone transfer requests should be denied.

Lastly, use a dedicated DNS server to service UC/VVoIP clients. The DNS server should be separate from the DNS server that services the data network. The DNS server should be behind a firewall and access to the DNS server should be restricted by access control lists.

NTP

NTP is intended to synchronize all connecting IP devices on the UC/VVoIP call-processing network. Special attention should be paid to securing these timing servers. Abuse of NTP could desynchronize devices causing a denial of service.

Mitigations

The NTP server providing time to the UC/VVoIP clients should be a dedicated NTP server separate from the data network's NTP server. The UC/VVoIP server should use the latest available NTP version that supports authentication and integrity. Older versions of NTP have less robust security features.

To limit the attack surface of the UC/VVoIP NTP server, the server should be placed behind a firewall and access to the NTP server limited. Only clients on the UC/VVoIP VLAN should have the ability to request time from the UC/VVoIP NTP server. All other requests should be denied.

Trusted path and channel protections

When sensitive data is passed from client endpoint to a UC/VVoIP call-processing server, that data must be protected from modification and disclosure. Data must be protected when administering UC/VVoIP servers and endpoints as well. This can be achieved through using protocols that provide encryption. In addition to modification and disclosure protections, IP devices should also use protocols that provide two-way authentication that is cryptographically secure. In the absence of encryption, a malicious

actor could eavesdrop on a connection to steal credentials or sensitive information. In the absence of server authentication, a malicious actor could perform man-in-the-middle interception of a connection and masquerade as the server to compromise a client. In addition, in the absence of client authentication and encryption, a malicious actor could perform a man-in-the-middle on a client endpoint and masquerade as an authorized client endpoint.

Mitigations

Standard protocols can be used to provide encryption and two-way authentication to secure sensitive data: Internet Protocol Security (IPsec), Secure Shell (SSH), Transport Layer Security (TLS), Datagram TLS (DTLS), and Hypertext Transport Protocol Secure (HTTPS) are such protocols. The NSA-approved Commercial National Security Algorithm (CNSA) Suite provides cryptographic requirements for these protocols to be used securely and are listed in Committee on National Security Systems Policy No. 15 (https://cnss.gov/CNSS/issuances/Policies.cfm).

Summary of Part I

When securely deploying UC/VVoIP systems, the network is the first critical place to enact security. Leverage security features included in network equipment to enforce access control and data/voice separation and to implement traffic prioritization, encryption, and authentication services. By configuring the network to adhere to the recommendations in this guide, the network can provide essential security services to protect data traversing the network as well as the devices connecting to it.

Once an administrator has implemented these network security recommendations, the next step is to move on to security at the perimeter.

▲Back to Table of contents

Part II: Perimeter security best practices and mitigations

While the first part of this report addressed UC/VVoIP security on the network, Part II addresses security at the perimeter.

The perimeter is where all communications external to the organization's UC/VVoIP system enter or leave the call-processing network. Session border controllers are essential and enforce call signaling protocol standards for traffic entering and exiting the local UC/VVoIP network. By enforcing call signaling protocol standards, a layer of protection is provided to the servers residing on the internal network that process UC/VVoIP communication packets. In addition, SBCs support secure connectivity from local UC/VVoIP servers to remote service providers and other external UC/VVoIP systems. Implementation of perimeter security should be done after implementing best practices for the network, as described in Part I.

The perimeter, in this case, refers to the external method of communication for the UC/VVoIP call-processing system only. This includes PSTN gateways, SBCs, and virtual private networks (VPNs). All devices that form the perimeter should be securely managed from a dedicated management network.

PSTN gateway protections

PSTN gateways connect a UC/VVoIP call-processing system to the PSTN. The threat presented by gateway devices is that malicious users from outside of the network could connect directly to the gateway device and make unauthorized calls. Unauthorized calls could lead to toll fraud. Another problem with some PSTN gateways is that they can directly pass call-signaling messages to internal enterprise session controllers (ESCs). This could allow a direct compromise of the UC/VVoIP servers.

Mitigations

The best way to prevent unauthorized calls is to require authorized users or peer gateways to authenticate before the gateway will complete a call. Some gateways query a separate server to check if a call is authorized. In this case, a secure channel must be used between the gateway and the authorization server.

Place PSTN gateways on their own VLAN and in a DMZ off of a session border controller interface. Use packet filtering to allow signaling messages from authorized

servers only. Prevent UC/VVoIP endpoints from sending signaling messages directly to the gateway. Instead, use the UC/VVoIP server as an intermediary.

Gateways must validate and terminate all PSTN signaling at the gateway. The gateway should convert PSTN signaling messages to UC/VVoIP signaling messages. This reduces the likelihood of a successful compromise of the UC/VVoIP servers through the gateway. A malicious actor could still directly compromise the gateway and use it as a platform for lateral movement to other UC/VVoIP devices, but this requires additional steps.

Regularly apply security updates to the software on gateways located at the perimeter.

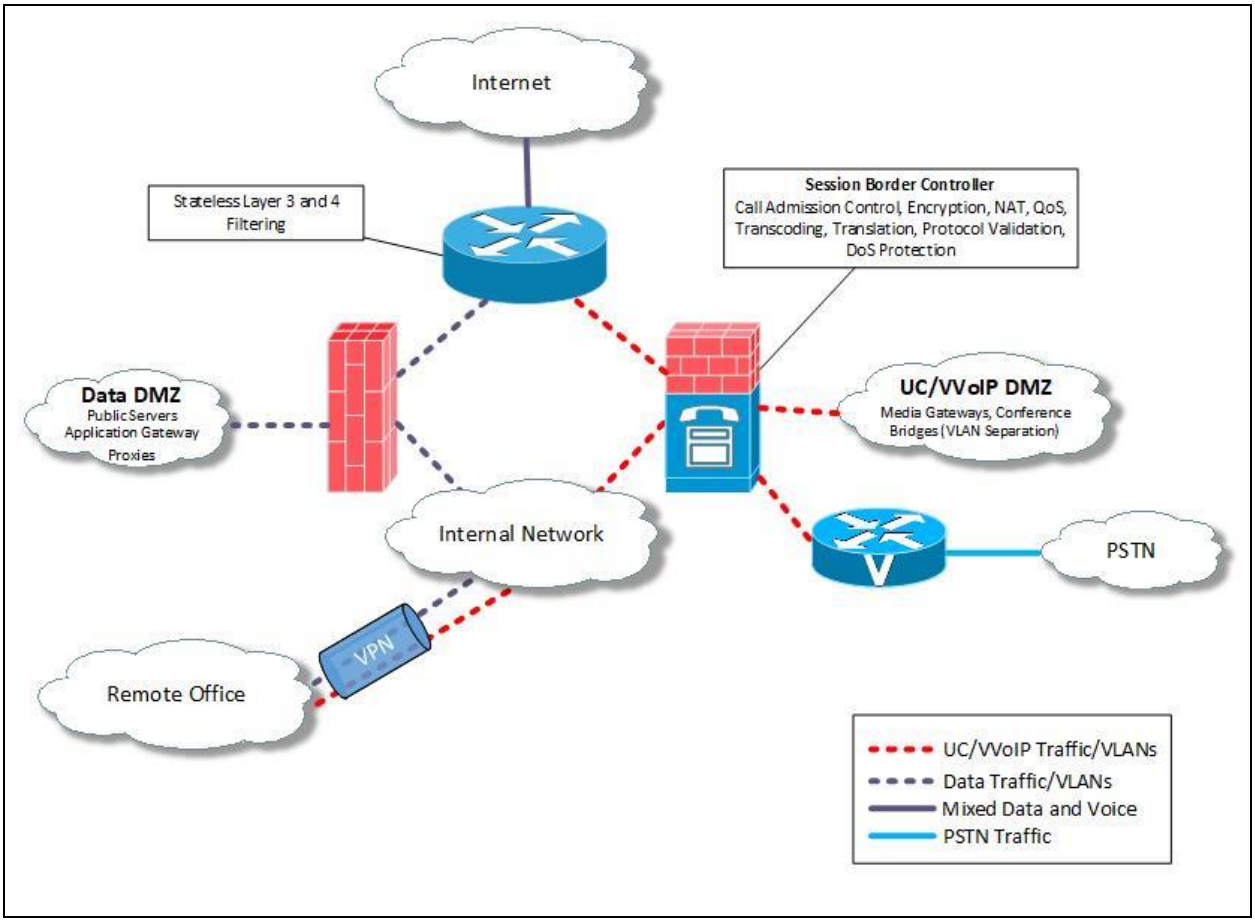

Figure 2: Perimeter security device placement following NSA guidelines

Protections for public IP networks functioning as voice carriers

A benefit of UC/VVoIP is the ability to use public IP networks to carry voice traffic between physically separate offices or between organizations. However, this use of

UC/VVoIP requires special security considerations because the organization has little control over its voice/video traffic once it enters other networks.

Once on the public network, an organization's UC/VVoIP call-processing traffic will traverse computers and networks owned by any number of third parties who could intercept and modify packets without the caller's or organization's knowledge. An organization's internal network policy may allow call-processing traffic to be sent in the clear; however, the accessibility of voice/video traffic on a public network necessitates the use of encryption and authentication to establish a secure channel between the calling and answering parties.

Mitigations

Using UC/VVoIP over a public network to establish calls between different organizations requires specific security steps. For confidentiality reasons, UC/VVoIP should use encrypted trunks when communicating over public IP networks. An organization should not trust the traffic originating from another organization. Decrypt and inspect any UC/VVoIP traffic before it is allowed into the internal network. Additionally, an organization should hide its internal network topology by using network address translation (NAT) and non-routable IP addresses on its internal UC/VVoIP network.

An SBC deployed at the network perimeter can provide inspection of the UC/VVoIP traffic as well as provide for NAT traversal. An SBC sits on the edge of the network and proxies the UC/VVoIP connection between the network and the service provider. The SBC rewrites signaling messages (control signals) and dynamically opens ports so media streams can traverse the SBC. SBCs are back-to-back user agents (B2BUAs). B2BUAs proxy connections between endpoints resulting in two separate connections for the communication channel. SBCs understand and inspect UC/VVoIP communication at a level that traditional network firewalls cannot. Because they are B2BUAs, SBCs maintain a separate connection between the internal network and the service provider. This property allows the SBC to inspect and manipulate (i.e., rewrite) portions of the UC/VVoIP packets traversing it. If the streams traversing the SBC are unencrypted, the SBC can rewrite the internal IP addresses buried within the UC/VVoIP packets with external IP addresses, allowing for NAT. The use of non-routable addresses prohibits a malicious actor from directly routing a packet across the Internet to a device on the internal network.

Inter-office communication can be established using encrypted VPNs. A VPN is likely already established between offices for data-only traffic. However, since it is recommended that UC/VVoIP call-processing and data networks should be kept on separate VLANs, a separate VPN must be established for call-processing traffic or the VPN must respect and maintain VLAN separation.

Signaling gateway protections

A signaling gateway is a translation device that is used to pass signaling (i.e., call control) information between two different network protocols or across a public IP network. In the case of UC/VVoIP, this is between an IP-based call-processing system and an external legacy telephony network (i.e., central office SS7, T1, etc.). A compromise of a signaling gateway can lead to a disruption of voice and video services, access to the topological information of the network, identifying the subscribers, or other effects. The gateway device can be stand-alone or integrated with another signaling gateway.

Mitigations

Signaling gateways are public facing servers. As with all public facing servers, the signaling gateway should be placed in a demilitarized zone (DMZ). The DMZ in this case should be an interface off of the SBC. In addition to being placed in a DMZ, the signaling gateway should be placed in its own VLAN. UC/VVoIP devices should not be able to send call control signaling messages directly to the gateway, and instead should use the UC/VVoIP server as an intermediary or protocol translation device. The gateway will send the signaling messages to the ESC server, which acts as an intermediary between the two UC/VVoIP endpoint devices. Signaling gateways must validate and terminate all PSTN signaling, then convert the terminated signaling messages to UC/VVoIP call control signaling messages for communications to UC/VVoIP-based devices. This type of protocol translation enacted by the signaling gateway helps reduce the likelihood of a successful compromise of the ESC server. For all signaling protocols that can be encrypted, encryption should be utilized.

The signaling gateway should be configured to log all calls. Because the signaling gateway is located at the perimeter, it is capable of keeping records of calls entering and exiting the network. Keeping call records that include call connection time, length of call, and other data often proves useful when trying to identify origin and identification of a malicious actor.

Media gateway protections

A media gateway is a translation device that converts media streams (voice, video) between different communications formats and protocols. For example, a media gateway device can convert voice media originating from a time-division multiplexing-based (TDM) system to voice media destined for a UC/VVoIP system. The media gateway device can be stand-alone or integrated with another device (i.e., signaling gateway). Also note that a signaling gateway can initiate and terminate communications on the media gateway. A successful compromise of the media gateway can lead to the eavesdropping or disruption of all voice and video calls traversing the gateway.

Mitigations

Place media gateways in their own media VLAN and in a DMZ off of an SBC interface. When calls are routed over public networks, encryption of media protocols is essential in the same way as with signaling protocols. Use a VPN for any inter-office communications across the public network.

Wide area network (WAN) link protections

Network connections to remote offices are considered part of the internal network and thus should follow the same data and UC/VVoIP call-processing separation guidelines. In this context, remote office WAN links refer to dedicated leased lines connecting the remote and primary networks where both ends of the link are managed by the same organization. Because the WAN link connects the internal network to the outside world, if it is not protected properly, it puts the internal network at risk.

Mitigations

WAN protection methods include VPN protocols such as IPsec and TLS. The VPN must support the separation of UC/VVoIP call-processing networks and data networks by either supporting VLANs or creating individual VPNs for each network.

Cloud connectivity protections

Some organizations are currently migrating the Internet Protocol private branch exchange (PBX) to the cloud to accrue benefits the cloud offers (increased efficiency, greater flexibility, reduced infrastructure costs, lower operational costs, and improved communications). Cloud-based communications systems can include IP PBXs, SIP servers, UC/VVoIP teleconferencing, and other applications.

With the rise of cloud computing, security remains a top concern. Just as security concerns expanded when PBXs migrated to IP PBXs and then evolved to UC/VVoIP systems, security is just as relevant now, as UC/VVoIP systems begin the migration to the cloud. Threats to the cloud include denial of service effects, access misconfigurations, and unsecured application programmable interfaces used by programmers. When migrating to a cloud-based solution, data security must be maintained. Confidentiality of the call signaling must be maintained, the media channel (voice, video, and data) must prevent eavesdropping, and all devices involved must be properly authenticated.

Mitigations

To help mitigate risks around migrations to the cloud, employ cryptographic protocols to encrypt communications between UC/VVoIP devices. Whether moving a call server entirely into the cloud, or just providing trunk connectivity from an external call server to the cloud, it is best to protect call server peripherals with encryption and authentication. The encryption should be configured on UC/VVoIP signaling and media devices. To protect call control signaling originating from local UC/VVoIP systems out to the cloud, use SIP over TLS or H.235 (H.323 over TLS). To protect voice/video media originating from local UC/VVoIP systems out to the cloud, use Secure Real-Time Protocol (SRTP). Secure connections to the cloud must be established by implementing trusted paths and channels that support encryption and two-way authentication such as IPsec, TLS, DTLS, HTTPS, and SSH.

DMZ-like separation between logical external gateways and logical internal capabilities should be maintained. Access control mechanisms should be employed to restrict access to the systems hosted in the cloud. Robust logging should be enabled and those logs routinely reviewed to detect and trace any potential compromises.

Summary of Part II

Perimeter security is paramount when deploying UC/VVoIP systems. Protection from external intrusions can be mitigated by employing the security features of devices located at the perimeter, as well as deploying special purpose UC/VVoIP security devices such as an SBC. Access control, data/voice separation, encryption, authentication, logging, and secure management are all considerations. By implementing these core security components in accordance with this document, the security at the perimeter will be greatly enhanced.

Once security at the network and perimeter is addressed, one can turn attention to ESCs.

▲Back to Table of contents

Part III: Enterprise session controller security best practices and mitigations

Parts I and II of *Deploying Secure Unified Communications/Voice and Video over IP Systems* lay out best practices for preparing the network infrastructure and perimeter in preparation for deployment of UC/VVoIP systems. Part III addresses the third step of securing UC/VVoIP systems by readying enterprise session controllers, also known as UC/VVoIP ESCs. A UC/VVoIP ESC is also commonly called an Advanced IP PBX, SIP server, SIP proxy, H.323 Gatekeeper, a call-processing server, or simply just an ESC.

These servers are analogous to the central switches in a legacy PBX system and are just as essential. They are necessary for establishing calls and using many features such as call forwarding, voice mail, and conference calling. Unlike a PBX, an ESC can securely manage all UC/VVoIP endpoint devices registered to it. They process calls between IP endpoints and/or trunk the calls to another ESC.

Several aspects of ESCs require security considerations to protect the UC/VVoIP call-processing system from compromise and misuse. The software installed on the ESCs—such as operating systems, databases, and call-processing applications—must be hardened by removing unnecessary applications, services, and default accounts. Most ESCs use remote management capabilities that make the server more vulnerable if not configured with appropriate security mechanisms. The ESCs must meet the stringent reliability and availability requirements of traditional (legacy) telephony systems.

ESCs also perform the critical function of authenticating and authorizing IP-phones and their users. In addition to discussing how to protect ESCs themselves, this section addresses what authentication and authorization features on the ESC should be used to control access to the UC/VVoIP call-processing network.

Software and application protections

ESCs usually execute on general-purpose server hardware. Administrators of call processing systems must pay special attention when managing user accounts, examining default configuration settings for security weaknesses, ensuring auditing and logging are enabled, and configuring any specialized services or features. This section will address these problems as they pertain to ESC software.

User accounts and passwords

User accounts grant access to the server with various rights and privileges. The more users with access to the server, the more opportunity for it to be intentionally or unintentionally compromised. Limiting access to the server helps prevent this. Many systems include a number of built-in default user accounts with default passwords, which are public knowledge or can be easily guessed. These accounts provide easy entry for malicious actors and are often overlooked during the installation process. The lack of a password or a bad password choice can allow easy access into the device and therefore into the network.

Mitigations

User accounts must only be created for those individuals who manage the server. These accounts should be granted the absolute minimum permissions necessary to complete the user's task. User accounts and passwords that are built-in or default should be deleted or changed. To prevent password guessing, enforce complexity rules for user account passwords and limit the number of consecutive failed login attempts. Follow National Institute of Standards and Technology (NIST®) Special Publication SP 800-63B Digital Identity Guidelines (https://pages.nist.gov/800-63-3/sp800-63b.html#sec5). NSA recommends using multi-factor authentication for managing critical IT components like ESCs, when possible. However, not all ESCs currently support multi-factor authentication.

Default UC/VVoIP server configuration settings

The software on call-processing servers is typically installed with default configuration settings. The server may be configured by default for maximum functionality instead of adequate security. Unknown to the administrator, features could be enabled that are not appropriate for the installation environment.

Mitigations

Servers should be configured in accordance with the Security Technical Implementation Guides (STIGs) maintained at the DoD CYBER EXCHANGE (https://public.cyber.mil/stigs). If no STIGs are available for the deployed server, the vendor hardening guides should be followed instead. Periodically check the configuration settings to verify unattended changes to the configuration have not occurred. Settings that enable extra features should be carefully considered and evaluated before enabling.

Audit and logging apparatus

Without auditing and logging, unauthorized access or modification of the ESC will not be recorded. System records should be kept for any and all accesses to the ESC, whether by a user or administrator. Even an authorized change to the ESC's configuration might result in a server malfunction. Detecting and recovering from server actions may require reconstructing the events from the audit log messages. UC/VVoIP systems perform call logging for calling records. This is done using call detail records (CDRs). CDRs can also be used for detecting toll fraud and other unauthorized usage of the UC/VVoIP call-processing system.

Mitigations

Enable auditing and logging (including CDRs) on the server and any critical devices such as conferencing systems, integrated voicemail systems, and gateway protocol translators. Review logs regularly for security and access violations. Store logs for a period of time in accordance with an organization's security policy. Securely transmit logs to a separate logging server that has been hardened and capable of encrypting the logs at rest. Configure the logging server to accept entries only from authenticated machines.

Software vulnerabilities

Software vulnerabilities will inevitably arise in the ESC operating system and server applications. Software vulnerabilities can leave an ESC open to denial of service and remote access techniques.

Mitigations

Applying software security patches to the ESC should be applied immediately once available. Software updates should be cryptographically signed by the software vendor to ensure authenticity. To reduce the chances of updates causing unforeseen problems on production servers, test the updates on a test network that approximates the production network.

Malicious software

Since many ESCs run general-purpose operating systems, they are susceptible to the same computer viruses. This includes Trojan horses, worms, and other malicious software that affect these operating systems.

Mitigations

For ESCs that run atop general-purpose operating systems, install anti-virus software and regularly update virus definitions. Do not use ESCs for general Internet activities, such as email and web applications. If available, use a host-based firewall to protect against malware and to limit the spread of any infection. Enforce signed software (see Enforce Signed Software Execution Polices, https://www.nsa.gov/What-We-Do/Cybersecurity/Advisories-Technical-Guidance) to verify that the software is valid and to keep malicious software off the device.

Network services

Network services running on production servers represent a threat because unknown vulnerabilities could be exploited by a malicious actor. Types of network service protocols include DHCP, DNS, File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP). Unnecessary network services running on an ESC provide additional attack surface and represent a drain on the resources needed to maintain calling services. If administrators are unaware of the services running on their ESCs, security updates could go unapplied, and compromises could go unnoticed.

Mitigations

Disable all network services on the ESC that are not in use and not needed for ESC functionality. Consult the server vendor to determine which services are required by the system. Carefully consider the security implications of maintaining a service against the features provided by the service.

Database security

UC/VVoIP call-processing systems may employ a separate database to store user, device, and call detail record information. Access to this database is typically managed via the remote management interface employed by the ESC, such as a web interface or vendor software. However, the database server may be directly accessible by other means that require protection. Compromising the database server compromises the call-processing network.

Mitigations

Secure the database by following all the guidelines for general software security outlined above.

Reference vendor documentation on securing the database. If the database is running on hardware (virtual or physical) separate from the ESC, VLANs should be used to create a dedicated communication channel between the database and the ESC. This channel should be encrypted. Authentication to the database server should be enabled. If possible, on the database server configure an allow list that only allows the ESC and management hosts to communicate with it.

Cryptographic key material

ESCs that support encrypted communications also store cryptographic key material for encryption and authentication purposes. A malicious actor with access to these servers may be able to extract the key material from the ESC. If successful, they may be able to impersonate the server and more easily eavesdrop on or capture calls, including some types of encrypted calls.

Mitigations

Different types of key material require different levels of protection. At a minimum, private keys used to digitally sign configuration and firmware files, downloadable applications, and certificates should be stored encrypted on the ESC. When backing up keys for recovery purposes, those keys should be stored on a computer or device that is not connected to the network. If supported by the ESC, use a cryptographic hardware token to store keys and to perform all cryptographic operations requiring access to the keys. Detailed information on key management, storage, and protection can be found in NIST Special Publication 800-57 (https://csrc.nist.gov/projects/key-management/key-management-guidelines).

Physical security protections

In most cases, a server that can be physically reached can be compromised. An unauthorized person could easily disable the server by shutting it down or physically damaging it.

An unauthorized person could also use one of many common techniques to try to gain administrative access to the servers. BIOS passwords can be reset using jumpers on the motherboard, boot disks can be used to load alternate operating systems, passwords can be changed on servers, and many other techniques can be used to break into a server once physical access has been obtained. Server hardware can be

physically damaged in a number of other ways, including intentional and unintentional fires, flooding from broken water pipes, and natural disasters.

Mitigations

Physical security precautions must be taken to deny unauthorized access to the ESC. Put the ESC in a locked cabinet in a locked and controlled room. Place alarms on the entry points to the server room. Use a control for access to the room that logs personnel entering and exiting. Use surveillance cameras and human monitoring in high-value installations.

Disable booting from removable media and enable BIOS passwords to prevent BIOS modification.

Install fire suppression systems to protect the ESC servers from fire damage. Use suppression systems safe for electronic equipment in high value installations. To prevent accidental flooding, do not run water or sewage mains through the room housing the ESC.

Ensure availability of services so, if a disaster destroys one data center, the whole organization does not lose UC/VVoIP call-processing services. For example, provide each geographic location with its own ESC and a backup connection to the PSTN service provider, or another remote ESC.

Service availability protections

Availability of UC/VVoIP call-processing services is one of the most important considerations, because UC/VVoIP device users are accustomed to the 99.999% telephone dial tone off-hook standard. To ensure ESCs meet this level of availability, potential power and hardware failures, data loss, and access to emergency services must be addressed.

Hardware and power failures

Disk drives, power supplies, motherboards, memory, and other equipment will eventually fail along with power outages.

Mitigations

At a minimum, server hardware must have RAID (redundant arrays of independent disks) support to protect against disk drive failure. To protect against total hardware

failure, configure ESCs in a high availability configuration that automatically takes over the duties of the primary server should it fail. Keep a spare duplicate server readily available to replace the failed server. Have redundant power supplies on separate circuits in case of a circuit failure. Provide short-term power backup using uninterruptible power supplies for all servers. When availability is critical, provide long-term backup power.

Data loss

High-availability hardware cannot protect against all hardware failures, software errors, or intrusions corrupting data on ESCs. Such failures should require quick recovery of ESCs to return to operational status.

Mitigations

To ensure a quick system recovery, regularly back up data from the UC/VVoIP systems. A backup and recovery policy that describes the recovery process must be in place. Test backup and recovery processes.

Store backups in an environmentally controlled secure location that will ensure they are not compromised. Encrypt any backups that leave the physical control of the organization (e.g., for shipping).

Emergency Services

One of the advantages of UC/VVoIP call-processing systems is being able to physically move a UC/VVoIP device from location to location and keep the same number. This physical move could be to a different room, a different building, or even a different city. The downside to having such flexibility is that it may be hard to pinpoint the exact physical location of a caller in cases of emergencies. The UC/VVoIP call processing system must maintain a reliable mechanism to connect to emergency services through the network that provides the location of the caller.

Mitigations

Subscribe to an enhanced 911 (E911) service through the UC/VVoIP service provider and only route 911 calls that originate within the network to the 911 service. The E911 service provides a callback number as well as the physical location of the caller to emergency personnel. The subscriber should keep location information updated with the service provider. In large enterprises where there are multiple buildings or geographic locations, phone numbers should be grouped into direct inward dialing

numbers (DIDs) denoting different physical locations. DIDs allow multiple phone numbers to be mapped to one virtual phone number. Users making emergency calls originating outside of the internal network should use other means (hotel phone, cell phone, etc.) to make emergency calls.

Client registration protections

Many UC/VVoIP call-processing systems allow clients to register automatically with the system. The automatic registration keeps the administrator from needing to individually provision each device. Ease of deployment can lead to a malicious actor masquerading as a legitimate device registering with the ESC and subverting the system.

Mitigations

Configure the call-processing systems to use two-way authentication. The ESC should authenticate the identity of the client, and the client should similarly authenticate the ESC. Disable automatic registration to control registration to the ESC and prevent unauthorized devices from registering.

Remote management protections

UC/VVoIP servers offer a variety of methods of remote management, such as web-based interfaces, proprietary vendor software, open source software such as Simple Network Management Protocols (SNMP) and—as part of a service agreement—remote management by service providers. Remote management poses a security threat because unauthorized access can seriously damage or compromise UC/VVoIP networks, capabilities, and security features. The flexibility and timesaving benefits of remote management can be safely used if appropriate security precautions are taken.

Web-based management interfaces

Many systems offer web-based remote management interfaces because of their familiarity and easy ability to remotely manage the UC/VVoIP system from anywhere on the network. However, web servers and web applications commonly are susceptible to a variety of vulnerabilities such as buffer overflows, cross-site scripting, authentication bypass, and injection. Additionally, some webservers allow communication over the HTTP protocol that is not encrypted. A malicious actor in the communication channel between the administrator and the web server could compromise important information such as the administrator’s password. Many browsers also allow users to cache login

information for authenticating to web sites. Unauthorized access to administrator workstations could potentially compromise the login for the ESC.

Mitigations

Remotely managing an ESC via a web interface should only be done over an encrypted channel. TLS on the web server should be enabled and all non-TLS web access disabled. This will ensure all management sessions protect sensitive information such as login information.

The web-based interfaces should be only accessible via a management network that is separate from the general-purpose network. Additionally, access to the web-based interface should be limited to IP addresses of administrative workstations. If remotely managing the ESC from a remote location outside of the network's perimeter, a trusted channel that connects the administrator into the management network before they can administer the ESC should be used.

Finally, all management hosts should have their web browsers configured to not cache login information.

Proprietary management software

Some vendors have written proprietary client and ESC software to manage their ESC. If the proprietary software and connection between the ESC and client are not encrypted and authenticated, then control over the ESC can be obtained by a malicious actor.

Mitigations

To protect the use of proprietary management software, take precautions similar to web-based interfaces. Network traffic should be encrypted. If the software does not support encryption, route traffic through an encrypted tunnel. Limit access of the management interface on the ESC to a separate administrative network and to specific IP addresses. Usernames and passwords must not be cached by the client software. Apply security updates to the ESC in accordance with the guidelines referenced in the Software Vulnerabilities, Malicious Software, and Network Services sections of this guide.

Summary of Part III

This part of the report covered UC/VVoIP ESC best practices and mitigations for a secure system. Software updates (operating system and applications) should be cryptographically signed to ensure authenticity. Only software needed by the server should reside on the server. Management accounts and access to the server should be minimized and protected by good password policy. All settings (including default) should be evaluated for their impact on ESC security and system security. Enable secure auditing and logging with regular review to identify security issues. All cryptographic keys should be securely stored. Physically secure the ESC machinery and limit physical access. Authenticate, encrypt, and limit remote access as much as possible. A secure ESC will produce a more secure UC/VVoIP system overall.

Once security of the ESC is addressed, one can turn attention to the UC/VVoIP endpoints.

▲Back to Table of contents

Part IV: UC/VVoIP endpoint best practices and mitigations

This fourth and final part to *Deploying Secure Unified Communications/Voice and Video over IP Systems* deals with securing UC/VVoIP endpoints. With voice/video/data and call-processing network infrastructures already securely in place, UC/VVoIP phones, desktop VTCs, and other UC/VVoIP endpoint devices can be added to the network and secured. Before adding UC/VVoIP endpoints to the call-processing network, administrators have key decisions to make so the endpoints and network are both secured against malicious actors:

- What elements of the hardware and software need to be locked down?
- Do administrators need to be able to remotely administer the UC/VVoIP endpoints?
- What convergence features are needed?
- Do the UC/VVoIP endpoints connect to the network over Ethernet or Wireless?
- Do UC/VVoIP endpoints running on general purpose operating systems need to be supported?

Software and hardware security

Traditional phones contain limited functionality in the actual phone hardware because telephony features are implemented in the central office switch (CO) or PBX. However, UC/VVoIP endpoints are more autonomous because many do not require a CO or PBX in order to take advantage of much of their functionality. This requires a more capable and complex endpoint. The additional functionality and complexity in UC/VVoIP endpoint software increases the chance of vulnerabilities. These vulnerabilities should be mitigated similarly to general-purpose computers on the network. In addition, like computers, some UC/VVoIP endpoints allow users to install third-party software. These applications could also add vulnerabilities if not properly controlled and managed.

Software vulnerabilities

UC/VVoIP endpoints run on embedded operating systems or as a software application (softphone) on a general-purpose machine. When running on a general-purpose machine, in addition to the UC/VVoIP software and OS potentially having vulnerabilities, other applications, such as web browsers, that are installed could contain vulnerabilities as well. These vulnerabilities could allow denial of service impacts against the endpoint,

modify remote management functionality, or allow a malicious actor to gain complete control of the endpoint and surreptitiously collect room audio.

Mitigations

Methods to mitigate the software vulnerabilities in UC/VVoIP endpoints are similar to methods used to protect other computer systems on the network. Disable unnecessary applications and services, particularly if they utilize remote connections or provide remote access. Any known vulnerabilities must be patched as soon as possible. This can be automated by having UC/VVoIP endpoints regularly and automatically download signed firmware files from a trusted central server. Finally, network access to the UC/VVoIP endpoints can be limited by placing them on separate UC/VVoIP-only VLANs. VLANs are covered in the first module of the *Deploying Secure Unified Communications/Voice and Video over IP Systems* document that covered securing the UC/VVoIP network. These steps make it more difficult for a malicious actor to exploit vulnerabilities on a UC/VVoIP endpoint or an application-laden video teleconferencing device.

Third-party software

Some UC/VVoIP endpoints have the capability to run third-party software downloaded from the network. For example, one Java-based endpoint allows the user to download Java applets from the vendor's Internet site. There are risks to allowing such behavior:

- Downloaded software that appears legitimate may contain malicious functionality.
- The software may contain unknown vulnerabilities, which could be exploited to compromise the endpoint.

Mitigations

Enforce a policy for downloading external software onto UC/VVoIP endpoints that is at least as strict as that for downloading software to desktop computers. In many cases, the need for higher reliability for the UC/VVoIP system will necessitate stricter policies. Where possible, disable the capability to download external software and only distribute necessary software with firmware upgrades via a controlled mechanism. If there is a need to allow users to load applications on the UC/VVoIP endpoint, then set up a separate server inside the organization to provide only cryptographically signed applications. Block access to vendor web sites offering application downloads for the UC/VVoIP endpoint. Block direct Internet access by the UC/VVoIP endpoints, if possible. If that is not possible, use a DMZ proxy server for Internet web access. If

users must connect back remotely with an UC/VVoIP endpoint, ensure the UC/VVoIP endpoint connects back to the enterprise using a cryptographic VPN (e.g., using IPsec).

Malicious software

Malicious software could exploit or introduce software vulnerabilities in the UC/VVoIP endpoint. Malicious software manifests in an organization's telephone network similarly to how it manifests on data-only networks. Malicious software can install backdoors into desktop VTC and UC/VVoIP endpoints, gather sensitive information, or use UC/VVoIP endpoints to compromise other call-processing systems. The spread of worms on UC/VVoIP call-processing networks could disrupt or disable voice/video capability.

Mitigations

Antivirus solutions exist for some embedded platforms, but not all because the UC/VVoIP industry is still catching up with technology to protect UC/VVoIP endpoint devices. Antivirus software does not completely mitigate malicious software because signature based virus scanners only detect known malware variants. Use cryptographically signed updates along with the antivirus software to minimize malware.

Embedded microphones

All UC/VVoIP endpoints contain at least a single microphone in the handset, and usually there is a speakerphone that contains an additional microphone. This includes desktop VTCs and softphones on laptops and PCs, as they too have microphones and speakerphones. The UC/VVoIP endpoints are software-controlled devices, with the microphones controlled by software. A software vulnerability could enable a malicious actor to control the UC/VVoIP endpoint and thus the microphones without the user's knowledge.

Mitigations

If a UC/VVoIP is placed in a sensitive area, its speakerphone microphone should be physically removed or at least disabled on the device. The original handsets should be replaced with push-to-talk handsets or headsets. This prevents the microphone from being activated except when a person is using the UC/VVoIP. Another possible mitigation is to use UC/VVoIP endpoints that have handsets and physically disconnect the microphone when the handset is on the hook.

Remote management of UC/VVoIP endpoints

The majority of UC/VVoIP endpoints can be classified as network-controlled devices. There are many UC/VVoIP endpoint types. The various UC/VVoIP endpoint types include handset voice-only VoIP phones, handset voice/video VVoIP phones, softphones with headsets for laptops and PCs, floor model telepresence (voice/video), room size telepresence (voice/video), desktop VTCs, and desktop USB phones. The sheer number of UC/VVoIP endpoints that an organization must deploy means that the UC/VVoIP endpoints are made to be easily configured and managed using remote tools over the network. This capability means that each UC/VVoIP endpoint represents another potential point of network infection and each must be secured. An exploit of this remote management functionality could have serious consequences including denial of unified communications and call-processing services to an organization, and leakage of information to unauthorized parties inside and outside the organization. The common methods for remotely managing UC/VVoIP endpoints are DHCP, firmware and configuration file downloads from a call server, web-based management consoles, network management such as SNMP, or administrative login tools. All of these methods must be addressed during the design of an UC/VVoIP network.

Downloading firmware and configuration files

Many UC/VVoIP endpoints are similar to network-booted desktop computers. They connect to the network, obtain an IP address using DHCP, and download operating system images and configuration files from a central server. This keeps the management of software and configuration versions centralized. It also allows for easy updates of the UC/VVoIP endpoint's firmware. However, for a malicious actor, it opens a pathway to completely control an organization’s UC/VVoIP endpoints and other voice/video endpoint devices. By modifying the firmware or configuration file, a malicious actor can insert malicious code into the UC/VVoIP endpoint’s operating system, use the endpoint device as a rogue agent, redirect calls to malicious servers, or disable the UC/VVoIP endpoint.

A UC/VVoIP endpoint’s firmware or configuration file could be modified in one of two ways. A malicious actor could perform a man-in-the-middle technique to intercept and replace the files as they are downloaded from the call server. This requires local network access or the ability to spoof DHCP messages. Or, a malicious actor could compromise the ESC storing the firmware and configuration files. This is a more serious

problem because control of an ESC enables a malicious actor to easily compromise all UC/VVoIP endpoints in an organization.

Mitigations
Choose UC/VVoIP endpoints that will process cryptographically signed firmware and configuration files. Each UC/VVoIP endpoint must have the signature verification key loaded on the UC/VVoIP endpoint in a secure manner such as on an isolated network or over a direct serial connection. Save the signing key in a secure place and do not store it on the download server. The UC/VVoIP endpoint must verify the signature on every file and reject any files with invalid signatures.

Web-based management interface
Most hardware UC/VVoIP endpoints have embedded web servers, which allow the modification of important settings on the endpoint device. Many times the same settings downloaded in configuration files are modifiable in this manner. Having web servers running on UC/VVoIP endpoints raise concerns as each UC/VVoIP endpoint now contains a web server that may be vulnerable.

Mitigations
The users should access necessary UC/VVoIP endpoint features through the phone's display, and administrators should configure UC/VVoIP endpoint settings using downloaded configuration files from a server. Deactivate the web interface. If there is a setting that needs to be set through the web server in the UC/VVoIP endpoint, the administrator should enable the web server through a secure signed download. Change the setting with web server, and disable the web server with another secure signed download.

Simple Network Management Protocol (SNMP)
SNMP is used to read and write settings on many network devices, allowing them to be integrated into comprehensive network management tools. Some UC/VVoIP endpoints may offer SNMP access to their settings. Compromising SNMP access to UC/VVoIP endpoints has consequences similar to compromising of configuration files or web interfaces.

Mitigations
Do not use SNMP to manage UC/VVoIP endpoints. Turn off all SNMP versions on the UC/VVoIP endpoint. If SNMP must be used to manage UC/VVoIP endpoints, then use

"SNMP version-3 over TLS or DTLS" (SNMPv3, RFC 5953) with its authentication features. Previous versions of SNMP do not offer the same protections. SNMPv3/TLSv1.3 (RFC 5953) allows per-user passwords and uses cryptographic functions to protect the password and message integrity. If SNMPv3/TLSv1.3 is not available, then use signed configuration files that can be downloaded from the call server rather than using SNMPv1 (or v2) to manage the UC/VVoIP endpoints.

Telnet

Telnet is another remote management solution available on many UC/VVoIP endpoints. And like DHCP, HTTP, NTP, SNMP, and many earlier protocols, Telnet was not designed with security in mind. Telnet is a command line interface to the UC/VVoIP endpoint configuration. It is an antiquated and unsecured protocol: sensitive information, such as passwords, is transmitted in the clear over the network. Without any analysis tools, a novice actor can view an administrator's Telnet login password and then use the information to create havoc on the system.

Mitigations

Disable Telnet. Use other methods of remote management like SSH. Relative to Telnet, SSHv2 is a better option that provides a secure channel for remote management because of its encrypted communications.

Network connectivity

UC/VVoIP endpoints include a variety of network connectivity solutions such as Ethernet, Infrared Data Association (IrDA), Bluetooth®, Console, and Wi-Fi access. Some UC/VVoIP endpoints offer all of these connectivity solutions, acting as a universal wireless access point. While some sort of network connectivity is required, too many connectivity options will make an UC/VVoIP endpoint more difficult to secure. Each connectivity solution adds configuration complexity and offers another potential path for a malicious actor to exploit.

Ethernet

Ethernet is a common means of connecting a wired UC/VVoIP endpoint to the UC/VVoIP network. To make deploying UC/VVoIP endpoints easier and to avoid adding additional Ethernet cabling, many UC/VVoIP endpoints feature an integrated Ethernet switch in the UC/VVoIP endpoint to provide another device connection. As an example, a PC can be plugged into the UC/VVoIP endpoint, and the UC/VVoIP endpoint can be

connected to the network. This effectively causes the UC/VVoIP endpoint to function like a bridge between the PC and Ethernet switch. The bridge on the UC/VVoIP endpoint will enable both the PC and UC/VVoIP endpoint to use the same network access switch port. Because the UC/VVoIP endpoint and computer will be privy to network traffic meant for each other, a malicious actor who compromises the PC may have direct access to the UC/VVoIP endpoint and vice versa.

Best practices require UC/VVoIP call-processing require voice/video call-processing and data-only networks be kept separate using VLANs. If the UC/VVoIP endpoint does not support VLANs on an integrated Ethernet switch, then a computer connected to the UC/VVoIP endpoint's PC port has access to the UC/VVoIP call-processing VLAN.

Mitigations

Do not use the PC port on the UC/VVoIP endpoint and disable it in the UC/VVoIP endpoint's configuration. This prevents a device from connecting to the UC/VVoIP endpoint and prevents a device from violating VLAN separation. If the environment mandates the PC port be used, then the UC/VVoIP endpoint's integrated Ethernet switch must support VLANs and be configured.

Infrared

Infrared data ports utilizing the IrDA protocol (an infrared protocol for wireless infrared line-of-sight communications for the last meter between devices) are used to transmit data between devices using invisible pulses of light. Example uses of infrared ports include synchronization of data between handheld devices and PCs and printing from handheld devices directly to a printer. Devices that communicate using infrared must be within sight of each other. While some UC/VVoIP endpoints presently have infrared ports, no UC/VVoIP endpoint is known to make use of this port, but its existence suggests that features using the infrared port will be available in the future. For example, a person could synchronize his mobile phone address book with the address book on the UC/VVoIP endpoint.

Infrared ports on UC/VVoIP endpoints raise several security concerns. First, there is no built-in security mechanism other than range of transmission and the line-of-sight requirement. Each application must implement its own confidentiality, authentication, and integrity mechanisms. Second, a malicious actor does not need to physically interact with the UC/VVoIP endpoint to access it. An actor with line-of-sight could

potentially compromise the UC/VVoIP endpoint. Third, a compromised UC/VVoIP endpoint could use the infrared port to capture other infrared communications in the same room as itself.

Mitigations

Cover the infrared port with metallic tape. This prevents any use of the port, including by a malicious actor who has compromised a UC/VVoIP endpoint. If use of the infrared port is necessary, then individually evaluate and configure each allowed application for security.

Wireless personal area network (WPAN)

Bluetooth is a short-range WPAN protocol that connects personal area network devices centered on an individual person's workspace. The primary differences between Bluetooth and infrared are that Bluetooth does not require line-of-sight for successful data transmission and Bluetooth features some security mechanisms that provide confidentiality and integrity. The designers of UC/VVoIP call-processing devices must be aware of the many security issues associated with WPAN technologies and implement mitigations for them.

Mitigations

The best solution is to use devices that do not support Bluetooth. If Bluetooth-enabled UC/VVoIP endpoints are used, then proper security measures must be taken. Disable Bluetooth functionality on UC/VVoIP endpoints and desktop VTCs. Addressing all the security issues related to Bluetooth is outside the scope of this document. NIST's Special Publication 800-121, Guide to Bluetooth Security (https://csrc.nist.gov/publications/detail/sp/800-121/rev-2/final) discusses the details of Bluetooth security.

Wireless local area network (WLAN)

WLANs are increasingly common in organizations. This category of connectivity includes technologies referred to as Wi-Fi or IEEE 802.11. Some UC/VVoIP endpoints can use WLANs as the primary source of connectivity instead of a wired (Ethernet) link.

UC/VVoIP endpoints that use WLANs to connect to the network must mitigate both WLAN and UC/VVoIP call-processing vulnerabilities. They must address problems such as confidentiality, integrity, and reliability of the wireless link in addition to the UC/VVoIP

call-processing vulnerabilities discussed elsewhere in this guide. This makes deploying WLAN UC/VVoIP endpoints more complex.

Mitigations

WLAN UC/VVoIP endpoints must meet the same security policy as other WLAN devices deployed by an organization. In addition, the WLAN UC/VVoIP endpoint and the WLAN network must meet the requirements placed on the overall wired UC/VVoIP call-processing infrastructure such as separation of data and voice/video call-processing traffic by using VLANs, different WLAN Service Set Identifiers (SSIDs) or entirely separate WLAN infrastructure.

Network connectivity mitigation summary

Of the various network connectivity solutions for UC/VVoIP endpoints, only connecting via Ethernet is recommended. If voice/video call-processing and data networks are separated onto different VLANs, the computer port on UC/VVoIP endpoints should not be used unless the UC/VVoIP endpoint supports VLANs.

The wireless network technologies discussed in this section could present significant vulnerabilities in the voice/video call-processing network. If the organization needs wireless access, it should be implemented using a separate and dedicated wireless infrastructure, and not integrated with the UC/VVoIP call-processing solution.

Convergence features

Convergence features allow the communication and synchronization of data between many different types of devices. UC/VVoIP endpoints and desktop VTCs may include features that allow them to interact with applications on other IP devices. For instance, an address book application on the PC instructs the UC/VVoIP endpoint to dial a number when the user clicks on an entry in the address book, or a mobile device synchronizes its address book with the address book on the UC/VVoIP endpoint. Each of these features requires another available service on the UC/VVoIP endpoint that could contain vulnerabilities. Each application requires an authentication and authorization mechanism to protect data stored on the UC/VVoIP endpoint and other convergence devices. The data must also be protected while it is in transit between IP devices. Since no standards exist, each application will likely have its own mechanisms for implementing integrity and confidentiality. This makes consistently managing and protecting the use of these applications difficult.

A more serious problem is that synchronization with mobile devices could result in the transfer of malicious code, such as viruses, from these devices to the UC/VVoIP call-processing network. Many UC/VVoIP endpoints are embedded systems that run software similar to that used on handheld devices and cell phones. If these devices are infected with malicious code, that code could be transferred to the UC/VVoIP endpoint.

Voicemail services are another area where the UC/VVoIP call-processing network interacts with the data network. Voicemail systems may make voice messages available to users in email messages. Similarly, users may be able to send email that can be accessed from the UC/VVoIP endpoint.

Mitigations

UC/VVoIP convergence opens the voice/video call-processing network to many of the same vulnerabilities that afflict the data-only network and also allow the UC/VVoIP network to afflict the data-only network as well. The safest mitigation is to block traffic between voice/video call-processing and data-only networks. However, the advantages of convergence may outweigh the risk. In that case, enforce strong authentication for any such service and put authorization controls in place to prevent malicious actors from abusing convergence solutions.

Authorized users can still inadvertently spread malicious code. In this case, the points where data moves between networks should be tightly controlled. Data transfer should not occur directly between the UC/VVoIP endpoint and other devices. Instead, a firewall or SBC should be set up to act as a gateway between the voice/video call-processing and data networks. At minimum, use a stateful layer 3 and 4 SBC. More appropriate is a stateful layer 3-7 SBC and an application-layer firewall that can check all data for malicious code. Place any services that must be used on both networks in a DMZ between the networks. For example, consider synchronizing a mobile device and UC/VVoIP endpoint with the same address book. The mobile device should not synchronize directly with the UC/VVoIP endpoint. Instead, employ a messaging server in the DMZ between the voice/video call-processing and data networks. The UC/VVoIP endpoint, mobile device, and desktop PC would all access the address book from the messaging server. The messaging server could then act as a gateway between devices, providing authentication and authorization services and scanning data for malicious code.

Softphones

A softphone is UC/VVoIP endpoint software that runs on a general-purpose device. The use of these phones poses several challenges when the voice/video call-processing and data networks are logically separated using VLANs. The softphones must operate on a computer that is connected to both the data and telephony networks. The PC violates the separation between the telephony and data networks because it must directly access both networks. Thus, compromise of the PC would allow access to both networks.

Replacing desktop UC/VVoIP endpoints with softphones also creates a single point of failure for communications. A widespread problem that affects many PCs or the network infrastructure will disable all communications. Users will not even have a means to report the failure. A fast spreading worm or power outage could create such a situation.

Softphones make management of the UC/VVoIP endpoint network more difficult because the UC/VVoIP call-processing server will not be able to reliably determine the type of device connecting to it. Untrusted softphones can be loaded on PCs by end users. Since the UC/VVoIP call-processing server does not know about these softphones, it will not be able to ensure they are configured securely.

Mitigations

If softphones are in use, create another VLAN and place all PCs with softphones on it. Configure traffic filtering rules to allow UC/VVoIP traffic between this VLAN and the UC/VVoIP call-processing VLANs, but do not allow UC/VVoIP traffic on the data VLAN. Similarly, do not allow general data traffic to flow to the UC/VVoIP call-processing server or on UC/VVoIP endpoint call-processing VLANs.

If softphones are densely deployed throughout the network, it is not practical to have separate data softphone VLANs. Instead, place all PCs—whether or not they have softphones installed—in data VLANs and filter traffic as described for the softphone VLAN in the previous paragraph.

When softphones are used as the primary voice communication mechanism, provide a backup communication method, which does not depend on the UC/VVoIP network, and make it available in every office to ensure some form of reliable communication.

Summary of Part IV

UC/VVoIP can be deployed securely in its environment following secure guidelines. An administrator can secure a UC/VVoIP endpoint by locking down the software and hardware. Update and patch the software as it becomes available using signed files from a trusted server. Limit network access of the UC/VVoIP endpoint. For UC/VVoIP endpoints that have handsets and used in areas where sensitive conversations occur, use an endpoint that physically disconnects the microphone when on hook, remove the speakerphone microphone, or replace the handset with a push–to-talk handset. Disable any unnecessary applications on the UC/VVoIP endpoint. Remote management should use secure paths, secure protocols, authentication between devices, and strong cryptographic functions. For network connectivity use wired Ethernet, and disable Wi-Fi, infrared, and other non-wired protocols. Place the UC/VVoIP endpoints in their own VLAN separating voice/video traffic from all other traffic. Computers and handheld devices may use softphones, but with the same precautions as in hardware UC/VVoIP endpoints. Using security guidelines with smart configurations and management controls increases the UC/VVoIP endpoint security.

▲Back to Table of contents

End of guidelines

This marks the end of the guidelines to deploy a secure UC/VVoIP solution. These guidelines address security concerns in four areas (network, perimeter, enterprise session controller, and UC/VVoIP endpoints) of a UC/VVoIP solution. Following these guidelines, deploying UC/VVoIP features and services can be achieved in a secure manner.▪