# 18.3. Video & Telephony Conferencing and Internet Protocol Telephony

## Objective

18.3.1. Video & Telephony Conferencing (VTC), Internet Protocol Telephony (IPT) and Voice over Internet Protocol (VoIP) systems are implemented in a secure manner that does not compromise security, information or systems and that they operate securely.

## Context

### Scope

18.3.2. This section covers information on VTC and IPT including Voice over Internet Protocol (VoIP). Although IPT refers generally to the transport of telephone calls over IP networks, the scope of this section includes connectivity to the PSTN as well as remote sites.

18.3.3. Additional information relating to topics covered in this section can be found in

- Chapter 12 – Product Security;
- Chapter 11 – Communications Systems and Devices;
- Chapter 19 – Gateways Security; and
- any section in this manual relating to the protection of data networks.

### Exception for VTC and IPT gateways

18.3.4. Where a gateway connects between an analogue telephone network such as the PSTN and a computer network, Chapter 19 – Gateway Security **does not** apply.

18.3.5. Where a gateway connects between a VTC or IPT network and any other VTC or IPT network, Chapter 19 – Gateway Security applies.

### Hardening VTC and IPT systems

18.3.6. Data in a VTC or IPT network consists of IP packets and should not be treated any differently to other data. In accordance with the principles of least-privilege and security-in-depth, hardening can be applied to all handsets, control units, software, servers and gateways. For example a Session Initiation Protocol (SIP) server could:

- have a fully patched software and operating system;
- only required services running;
- use encrypted non-replayable authentication; and
- apply network restrictions that only allow secure Session Initiation Protocol (SIP) and secure Real Time Transport (RTP) traffic from IP phones on a VLAN to reach the server.

## References

18.3.7.

| Reference | Title | Publisher | Source |
|---|---|---|---|
| SP 800-58 | Security Considerations for Voice Over IP Systems | NIST | https://csrc.nist.gov/publications/sp |
| | Security Issues and Countermeasure for VoIP | SANS | https://www.sans.org/white-papers/1701/ |
| Report Number: I332-016R-2005 | Security Guidance for Deploying IP Telephony Systems Released: 14 February 2006 | Systems and Network Attack Center (SNAC) NSA | https://www.nsa.gov/ia/_files/voip/I332-016r-2005.pdf |
| Report Number: I332-009R-2006 | Recommended IP Telephony Architecture, Updated: 1 May 2006 Version 1.0 | Systems and Network Attack Center (SNAC) NSA | https://www.nsa.gov/ia/_files/voip/I332-009R-2006.pdf |
| | Mobility Capability Package March 26 2012 - Secure VoIP Version 1.2 | NSA | https://www.nsa.gov/ia/_files/Mobility_Capability_Pkg_Vers_1_2.pdf |
| | Protecting Telephone-based Payment Card Data PCI Data Security Standard (PCI DSS) Version: 2.0, March 2011 | The PCI Security Standards Council (PCI SSC) | https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf [PDF, 888 KB] |
| | PCI Mobile Payment Acceptance Security Guidelines Version: 1.0 Date: September 2012 | PCI SSC | https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Developers_v1.pdf [PDF, 579 KB] |
| | PCI Mobile Payment Acceptance Security Guidelines Version: 1.0 Date: February 2013 | PCI SSC | https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf [PDF, 630 KB] |
| | Understanding Voice over Internet Protocol (VoIP): 2006 | US-CERT | https://www.us-cert.gov/sites/default/files/publications/understanding_voip.pdf [PDF, 83 KB] |
| CNSS Instruction No. 5000 April 2007 | Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony | Committee on National Security Systems | https://www.cnss.gov/CNSS/issuances/Instructions.cfm |
| DHS 4300A | DHS 4300A Sensitive Systems Handbook Attachment QS To Handbook v. 11.0 Voice over Internet Protocol (VoIP) Version 11.0 December 22, 2014 | DHS | https://www.dhs.gov/sites/default/files/publications/4300A%20Handbook%20Attachment%20QS%20-%20Voice%20over%20IP.pdf [PDF, 586 KB] |

## Rationale & Controls

### Video and voice-aware firewalls

18.3.8.R.01. **Rationale**

The use of video, unified communications and voice-aware firewalls ensures that only video or voice traffic (e.g. signalling and data) is allowed for a given call and that the session state is maintained throughout the transaction.

18.3.8.R.02. **Rationale**

The requirement to use a video, unified communication or voice-aware firewall does not necessarily require separate firewalls to be deployed for video conferencing, IP telephony and data traffic. If possible, agencies are encouraged to implement one firewall that is either video and data-aware; voice and data-aware; or video, voice and data-aware depending on their needs.

18.3.8.R.03. **Rationale**

Refer to Section 19.5 - Session Border Controllers.

18.3.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3721]

Agencies SHOULD use a video, unified communication or voice-aware firewall that meets the same minimum level of assurance as specified for normal firewalls.

## Protecting IPT signalling and data

18.3.9.R.01. **Rationale**

IPT voice and signalling data is vulnerable to eavesdropping but can be protected with encryption. This control helps protect against DoS, adversary-in-the-middle, and call spoofing attacks made possible by inherent weaknesses in the VTC and IPT protocols.

18.3.9.R.02. **Rationale**

When protecting IPT signalling and data, voice control signalling can be protected using TLS and the 'sips://' identifier to force the encryption of all legs of the connection. Similar protections are available for RTP and the Real-Time Control Protocol.

18.3.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3728]

Agencies SHOULD protect VTC and IPT signalling and data by using encryption.

18.3.9.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3729]

An encrypted and non-replayable two-way authentication scheme SHOULD be used for call authentication and authorisation.

## Establishment of secure signalling and data protocols

18.3.10.R.01. **Rationale**

Use of secure signalling and data protects against eavesdropping, some types of DoS, adversary-in-the-middle, and call spoofing attacks.

18.3.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3732]

Agencies SHOULD ensure that VTC and IPT functions are established using only the secure signalling and data protocols.

## Local area network traffic separation

18.3.11.R.01. **Rationale**

Availability and quality of service are the main drivers for applying the principles of separation and segregation.

18.3.11.C.01. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:3735]

Agencies MUST either separate or segregate the VTC and IPT traffic from other data traffic.

18.3.11.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3736]

Agencies SHOULD either separate or segregate the IPT traffic from other data traffic.

## VTC and IPT Device setup

18.3.12.R.01. **Rationale**

VTC equipment and VoIP phones need to be hardened and separated or segregated from the data network to ensure they will not provide an easy entry point to the network for an attacker.

18.3.12.R.02. **Rationale**

USB ports on these devices can be used to circumvent USB workstation policy and upload malicious software for unauthorised call recording/spoofing and entry into the data network. Unauthorised or unauthenticated devices should be blocked by default to reduce the risk of a

compromise or denial of service.

18.3.12.C.01. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must** [CID:3740]

Agencies MUST:

- configure VTC and VoIP devices to authenticate themselves to the call controller upon registration;
- disable phone auto-registration and only allow an allow list of authorised devices to access the network;
- block unauthorised devices by default;
- disable all unused and prohibited functionality; and
- use individual logins for IP phones.

18.3.12.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3741]

Agencies SHOULD:

- configure VoIP phones to authenticate themselves to the call controller upon registration;
- disable phone auto-registration and use an allow list of authorised devices to access the network;
- block unauthorised devices by default;
- disable all unused and prohibited functionality; and
- use individual logins for IP phones.

## Call authentication and authorisation

18.3.13.R.01. **Rationale**

This control ensures server-client mutual authentication.

18.3.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3745]

Authentication and authorisation SHOULD be used for all actions on the IPT network, including:

- call setup;
- changing settings; and
- checking voice mail.

18.3.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3747]

An encrypted and non-replayable two-way authentication scheme SHOULD be used for call authentication and authorisation.

18.3.13.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3748]

Authentication SHOULD be enforced for:

- registering a new phone;
- changing phone users;
- changing settings; and
- accessing voice mail.

## VTC and IPT device connection to workstations

18.3.14.R.01. **Rationale**

Availability and quality of service are the main drivers for applying the principles of separation and segregation.

18.3.14.C.01. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must Not** [CID:3751]

Agencies MUST NOT connect workstations to VTC or IPT devices unless the workstation or the device, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between VTC, IPT and other data traffic.

18.3.14.C.02. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:3752]

Agencies SHOULD NOT connect workstations to VTC or IPT devices unless the workstation or the device, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between VTC, IPT and other data traffic.

## Lobby and shared area IPT devices

18.3.15.R.01. **Rationale**

IPT devices in public areas may give an attacker opportunity to access the internal data network by replacing the phone with another device, or installing a device in-line. There is also a risk to the voice network of social engineering (since the call may appear to be internal) and data leakage from poorly protected voice mail-boxes.

18.3.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3756]

Where an agency uses a VoIP phone in a lobby or shared area they SHOULD limit or disable the phone's:

- ability to access data networks;
- functionality for voice mail and directory services; and
- use a separate network segment.

18.3.15.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3758]

Agencies SHOULD, where available, use traditional analogue phones in a lobby and shared areas.

## Usage of softphones, webcams and similar sound and video devices

18.3.16.R.01. **Rationale**

Software and applications for softphones and webcams can introduce additional attack vectors into the network as they are exposed to threats from the data network via the workstation and can subsequently be used to gain access to the network.

18.3.16.R.02. **Rationale**

Softphones and webcams typically require workstation to workstation communication, normally using a number of randomly assigned ports to facilitate RTP data exchange. This presents a security risk as workstations generally should be separated using host-based firewalls that deny all connections between workstations to make malicious code propagation inside the network difficult.

18.3.16.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3766]

Agencies using softphones or webcams SHOULD have separate dedicated network interface cards on the host for VTC or IPT network access to facilitate VLAN separation.

18.3.16.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3768]

Agencies using softphones or webcams SHOULD install a host-based firewall on workstations utilising softphones or webcams that allows traffic only to and from a minimum number of ports.

18.3.16.C.03. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Should Not** [CID:3770]

Agencies SHOULD NOT use softphones or webcams.

## Workstations using USB softphones, webcams and similar sound and video devices

18.3.17.R.01. **Rationale**

Adding softphones and webcams to an allow list of allowed USB devices on a workstation will assist with restricting access to only authorised devices, and allowing the SOE to maintain defences against removable media storage and other unauthorised USB devices.

18.3.17.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3777]

Agencies SHOULD use access control software to control USB ports on workstations using softphones and webcams by utilising the specific vendor and product identifier of the authorised device.

## Developing a denial of service response plan

18.3.18.R.01. **Rationale**

Communications are considered critical for any business and are therefore especially vulnerable to Denial of Service (DoS). The guidance provided will assist in protecting against VTC or IPT DoS attacks, signalling floods, established call teardown and RTP data floods. These elements should be included in the agency's wider response plan (See Section 6.4 – Business Continuity and Disaster Recovery).

18.3.18.R.02. **Rationale**

Simple DoS attacks and incidents are often the result of bandwidth exhaustion. Agencies should also consider other forms of DoS including Distributed Denial of Service attacks (DdoS), DNS and latency incidents.

18.3.18.R.03. **Rationale**

System resilience can be improved by architecting a structured approach and providing layered defence such as network and application protection as separate layers.

18.3.18.C.01.

**Control System Classifications(s): All Classifications; Compliance: Should** [CID:3782]

Agencies SHOULD develop a Denial of Service response plan including:

- how to identify the precursors and other signs of DoS;
- how to diagnose the incident or attack type and attack method;
- how to diagnose the source of the DoS;
- what actions can be taken to clear the DoS;
- how communications can be maintained during a DoS; and
- report the incident.

## Content of a Denial of Service (DoS) response plan

18.3.19.R.01. **Rationale**

An VTC or IPT DoS response plan will need to address the following:

- how to identify the source of the DoS, either internal or external (location and content of logs);
- how to diagnose the incident or attack type and attack method;
- how to minimise the effect on VTC or IPT, of a DoS of the data network (e.g. Internet or internal DoS), including separate links to other office locations for VTC and IPT and/or quality of service prioritisation;
- strategies that can mitigate the DOS (banning certain devices/Ips at the call controller and firewalls, implementing quality of service, changing VoIP authentication, changing dial-in authentication; and
- alternative communication options (such as designated devices or personal mobile phones) that have been identified for use in case of an emergency.

18.3.19.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3785]

A Denial of Service response plan SHOULD include monitoring and use of:

- router and switch logging and flow data;
- packet captures;
- proxy and call manager logs and access control lists;
- VTC and IPT aware firewalls and voice gateways;
- network redundancy;
- load balancing;
- PSTN failover; and
- alternative communication paths.