Endpoint Security & Health Check Report

Background

The information contained within this report was generated by PhoneView from UnifiedFX (http://www.unifiedfx.com) by data gathering, testing and analysing Cisco Unified IP Phones.
The purpose of this report is to perform a security audit to ensure there are no issues pertinent to Security by Default (SBD) feature provided by Cisco Unified Communications Manager (CUCM) version 8.x and later and that Cisco Unified IP Phones are secured and running the correct levels of software to minimize the risk of any Cisco Unified IP Phone being compromised.
This report can be of value at any point, especially the first time it is used on CUCM Version 8 (or greater) for the first time. It is also recommended to generate this report before and after an upgrade to ensure that all endpoints are in a valid state.

Target System

Below is a summary of the system this report was generated from:

Cluster Name:	UCM91	Registered IP Phone Count:	33
Cluster Version:	9.1	Offline IP Phone Count:	10
Publisher:	10.10.100.91	IP Phone Total:	43

Report Highlight

Table 1 highlights the results of the Security Report for each section detailed within this report:

Table 1- Report Highlight Summary

Section	Description	Result
Firmware	All Phones using the same/default firmware	Pass
SSH Enabled	All Phones have SSH Disabled	Pass
ITL Status	No issues updating phones ITL Files	Fail
TVS Status	No issues with phones trusting TVS Service	N/A
Settings Access	No Phones with Settings Disabled/Restricted	Pass
Web Access	All Phones have Web Access Enabled or Disabled	Enabled
IP Phone Hardening	Phone settings consistent with hardening guidelines	Mixed
Security Mode	The Authentication and Encryption Level of the devices	Default
Remediation	Recommendations to fix any ITL Related issues	Remote

Report Purpose

The purpose of this report is to provide a concise view of the endpoint security profile of the target cluster as well as any issues related to Security by Default (SBD). The final section includes a breakdown of remediation options for any issues found for ITL Related problems.
Table 2 provides a short description of each section within this report:

Table 2 - Report Section Descriptions

Section	Description
Firmware	Provides an analysis of the different firmware versions used within the cluster and highlights any anomalies
SSH Enabled	Validates that no phones have SSH enabled
ITL Status	Validates there are no phones with an problem updating their ITL File
TVS Status	Validates there are no phones with an issue using Secure URL's
Settings Access	Validates the Settings Mode of each phone on the target system
Web Access	Validates all phones have the Web Access setting is enabled (or disabled) on the target system
IP Phone Hardening	Validates the device configuration in relation to the hardening of the device
Security Mode	Outlines the Security mode of each device, i.e. non-secure, authenticated or encrypted communication.
Remediation	Outline of any devices with an issue relating to Security by Default and how to Remediate the issue

The information in this report was created in collaboration with:
Akhil Behl,
Solutions Architect
Cisco Systems
Author of "Securing Cisco IP Telephony Networks"
http://www.ciscopress.com/title/1587142953
http://www.amazon.com/dp/1587142953

Firmware Summary

In order to ensure consistent functionality and minimize firmware related issues it is recommended to ensure all phone models are running the same version of software. Best practice includes ensuring that the 'Default' firmware versions used are assessed for any known exploits that pose a significant risk. Table 3 provides a summary of all firmware information by Phone Model of all default and non-default versions of firmware in use.

Table 3 - Cisco Unified IP Phone Firmware Summary

Model	Default		Non Default	
	Version	Quantity	Version	Quantity
Cisco 7961	SCCP41.9-3-1SR4-1S	5		
Cisco 7945	SCCP45.9-3-1SR3-1S	1		
Cisco 7941	SCCP41.9-3-1SR4-1S	26		
Cisco 7937	1.4	1		
Cisco 7841	sip78xx.10-1-1-9	1		
Cisco 6961	SCCP 9.3.3.2.SR1	1		
	Total	**35**	**Total**	**0**

Table 4 - Description of results in Table 3 - Firmware Summary

Column	Description
Model	This is a list of each unique model within the target cluster
Default Version	This is the 'most used' firmware for that phone model, it is assumed this is the 'Default' version that should be used for that model
Default Quantity	This is the count of devices for each model using the default firmware
Non-Default Version	This is a list of all non-default firmware versions used for the relevant phone model
Non-Default Quantity	This is a count of the number of occurrences the non-default firmware used for each phone model

Note: Firmware information is gathered from the web server of each Cisco Unified IP Phone, if the web server is disabled or unreachable then that device will not be included in this Summary (for example, if your security policy may not permit enabling the Cisco IP Phone web server)

Non-Default Firmware Sample

PhoneView's export spreadsheet includes all of the Devices running non-default firmware in the "Non-Default Firmware" Sheet. Table 5 is a sample of up to the first 5 Devices running Non-Default Firmware and should be upgraded:

Table 5 - Non-Default firmware exception sample

Location	Name	Description	Firmware
-	-	-	-

Conclusion

If there is no information listed in the 'Non-Default' columns in the Firmware Summary Table then all phones of that model are using the same firmware version. It is recommended to check each of the listed

‘default’ versions of Firmware for security vulnerabilities against the Cisco Product Security Incident Response Team (PSIRT) web site: http://tools.cisco.com/security/center/publicationListing.x
If there are any devices using ‘non-default’ firmware the relevant versions are listed and the quantity of devices using the ‘non-default’ version of firmware. It is always best-practice to run the same version of firmware for each phone model for consistent functionality unless there are known exceptional circumstances.

SSH Enabled Summary

Most models of Cisco Unified IP Phones provide the ability to connect using SSH for remote diagnostics. However, in some circumstances with affected IP Phone firmware it may be possible to compromise the device via SSH as highlighted in the following security notice:

Cisco Unified IP Phone Local Kernel System Call Input Validation Vulnerability:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130109-uipphone

For the reason mentioned earlier as well as Cisco best-practice recommendations SSH should be disabled on all IP Phones, and only temporarily enabled while in use for remote diagnostics.
The following summary highlights any devices with SSH enabled to ensure that this is intentional and if not can be remedied by updating the relevant device settings in CUCM

Total IP Phones with SSH Information Gathered:	43
Total IP Phones with SSH Disabled:	43

Table 6 - Summary of all Cisco Unified IP Phones with SSH enabled

Location	Models	Count
-	-	-
	Total	**0**

ITL Status Summary

As part of the Security by Default (SBD) feature introduced with CUCM 8.0 most Cisco Unified IP Phone models now include an Initial Trust List (ITL) file that contains a list of trusted entities within the cluster. As part of generating this report PhoneView gathers the "ITL Status" of each device in order to determine if any devices have an issue updating their ITL File.
For more information on SBD, ITL and CUCM security construct, refer to chapter 9 of 'Securing IP Telephone Networks'
http://www.ciscopress.com/title/1587142953
http://www.amazon.com/dp/1587142953

Table 7 - ITL status summary for all endpoints

ITL Status	Models	Count
ITL Installed	7941	1
Trust List Update Failed	7961	5
Trust List Updated	7945, 7941	26

Overview of ITL Status

When a Cisco Unified IP Phone configured on CUCM 8.0 or greater boots or restarts it will install or update its ITL file from the relevant (trusted) TFTP server. If the phone has an issue updating its ITL file this typically indicates that the contents of the phones ITL file are out of sync with the certificates used by the TFTP (and possibly TVS) service. In such case configuration updates to the phone will fail and typically all HTTPS communication to/from the phone will stop working.
Table 8 provides a description of the different ITL Status messages listed in Table 7 that a Cisco Unified IP Phone may report:

Table 8 - ITL status message description and recommended action

ITL Status	Description	Delete ITL
ITL Installed	The ITL File has been successfully installed	No
Trust List Updated	The ITL File has been successfully updated	No
No ITL Installed /No Trust List Installed	There is no ITL File Installed, typically because the 'Pre UCM 8 Rollback' setting is enabled	No[1]
Trust List Update Failed	There is an issue with the ITL file on the phone, deleting the ITL File will allow the ITL File to update correctly	Yes

[1] - This ITL status is typically seen because the 'Pre UCM 8 Rollback' enterprise parameter was enabled at some point, this status is normal if the 'Pre UCM 8 Rollback' parameter is still enabled, otherwise it's recommended to delete the ITL File on the phone.

Sample of Devices with Invalid ITL Status

PhoneView's export spreadsheet includes all of the Devices and their ITL Status in the "ITL Status" Sheet. Table 9 is a sample of up to the first 5 Devices with an ITL Status of "Trust List Update Failed" and should have their ITL File deleted:

Table 9 - ITL status exception sample

Name	Location	Description
SEP001D4543EE12	Hub_None	Auto 79155
SEP001E7AC33136	Hub_None	Auto 79120

SEP001D4543931F	Glasgow	SEP001D4543931F
SEP001D45439399	Glasgow	SEP001D45439399
SEP001DA290622B	Hub_None	SEP001DA290622B

For more insight of SBD and ITL features as well as leading practices associated with the same refer to book 'Securing Cisco IP Telephony Networks' chapter 9, chapter 15, and appendix A.
http://www.ciscopress.com/title/1587142953
http://www.amazon.com/dp/1587142953

TVS Status Summary

The Initial Trust List (ITL) file on the phone contains two main types of certificates namely TFTP and TVS. Table 7 in the ITL Status Summary section indicates if the TFTP certificate is out of sync in the phones ITL File when there is an issue updating the ITL file, however there are scenarios when the TFTP certificate is 'in-sync' but the TVS certificate is 'out of sync'. In that scenario the affected phone may have an issue with HTTPS connections to/from the phone, therefore the Directory and Services features of the affected phones will stop working if they are using a Secure URL.

Total Devices with TVS status information:	0
Total Devices with 'ok' TVS status:	0

Table 10 list all devices with a 'failure' TVS status and therefore require remediation:

Table 10 - Summary of phones with an invalid TVS status

Location	Models	Count
-	-	-
	Total	

Note: TVS status information is gathered within PhoneView by performing a test on each Cisco Unified IP Phone. If the option to perform a "TVS Status Test" was not chosen then there will be no TVS status information in this section of the report.

Overview of TVS Status

The TVS Status represents the phones ability to establish a HTTPS connection, an invalid TVS Status means the phone does not trust any TVS Service and therefore is unable to establish any HTTPS connections.
In some scenarios restarting the TVS service on each subscriber may resolve this issue from some or all phones, if that does not resolve the issue then it may be necessary to delete the ITL file on the phone so that an updated ITL file with the correct TVS Service certificates can be installed.

Sample of Devices with Invalid TVS Status

PhoneView's export spreadsheet includes all of the devices within the target cluster with an invalid TVS status in the "TVS Status" Sheet. Table 11 is a sample of up to the first 5 Devices with an invalid TVS status of "Trust List Update Failed" and should have their ITL File deleted:

Table 11 - TVS status exception sample

Name	Location	Description
-	-	-

For more insight to the Trust Verification Service (TVS) feature as well as leading practices associated with the same refer to book 'Securing Cisco IP Telephony Networks' chapter 9 and chapter 15.
http://www.ciscopress.com/title/1587142953
http://www.amazon.com/dp/1587142953

Settings Access Summary

The following is a summary of the Settings Access Modes configured on the target cluster, this helps to identify if any phones have their settings Restricted or Disabled.

Total Devices with Settings Mode information:	43
Total Devices with Settings Access Enabled:	43

Table 12 - Summary of Cisco Unified IP Phones with Restricted or Disabled Settings

Location	Device Pool	Restricted	Disabled
-	-	-	-
	Total	**0**	**0**

For further information on Cisco's leading practices for Cisco IP Phone Settings please refer to Chapter 15, "Wired IP Phone: Hardening" section of Securing Cisco IP Telephony Networks
http://www.ciscopress.com/title/1587142953
http://www.amazon.com/dp/1587142953

Overview of Settings Access Modes

Cisco IP Phones provide access to phone configuration information via the settings menu on the phone. The information available within the Settings Menu should be considered as confidential and therefore not accessible from public locations such as lobby phones. Cisco UCM provides three options for accessing the settings menu of an IP Phone:

Table 13 - Description of settings access modes

Mode	Description
Enabled (Default)	All local phone configuration information is readable, and using the phone unlock sequence can also be changed.
Restricted	This permits access to user preference settings such as the contrast of the display, but disabled access to the network configuration details
Disabled	This completely disables the settings menu so no settings can be changed.

Although Cisco best practice recommends restricting or disabling access to the settings menu for public devices there is a very important consideration relating to Security by Default (SBD).

Security by Default Consideration

With the introduction of Security by Default (SBD) a minimum level of Cisco Public Key Infrastructure (PKI) is enforced on most Cisco Unified IP Phone models, this takes the form of an Initial Trust List (ITL) file that the phone uses to validate interactions with the TFTP and Trust Verification Service (TVS) within the cluster.

However despite careful planning and performing a text-book upgrade (even for just a phone firmware upgrade) it is not uncommon for the ITL file to get 'out-of-sync' on a number of devices. This in itself is not a major problem as the phone still registers, however HTTPS connections to/from the phone typically fail. The most common way to resolve the issue is the deletion of the ITL file from the phone.

This can become a problem if the phone with the ITL problem has its Settings Menu Restricted or Disabled as it's no longer possible to delete the ITL file using the phones interface. In that scenario the only solution may be to perform a factory reset, something that can only be done by physically visiting the IP Phone.

Therefore UnifiedFX recommends ensuring the Settings Access Mode is set to 'Enabled' for all Phones before any upgrade is started. By doing that it will make it possible to remotely delete the ITL File from any phones that may encounter an issue.
Once the upgrade is complete and it's verified there are no phones with an ITL issue the relevant devices can be updated to Restricted/Disabled again.
For further information on Security by Default (SBD) and Cisco UC PKI refer to Chapter 9 and Appendix A respectively of Securing Cisco IP Telephony Networks
http://www.ciscopress.com/title/1587142953
http://www.amazon.com/dp/1587142953

Web Access Summary

Most IP Phone models include a built-in web server that provides access to configuration and diagnostic details as well as providing a method for applications to interact with the phone directly. Table 14 provides a summary of which Cisco Unified IP Phone models have their web server enabled or disabled:

Table 14 - Cisco Unified IP Phone Web Server Summary

Model	Enabled	Disabled
Cisco 6941	1	
Cisco 6961	1	
Cisco 7841	1	
Cisco 7906	1	
Cisco 7912	1	
Cisco 7937	1	
Cisco 7941	27	
Cisco 7945	1	
Cisco 7960	1	
Cisco 7961	6	
Cisco 8945	1	
Cisco 9971	1	
Totals	**43**	**0**

Security by Default Consideration

Cisco leading security practices recommend all Cisco Unified IP Phones should have their in-built web server disabled. Until CUCM Version 8.0 the default setting is enabled, however with a new installation of CUCM 8.0 the default setting has changed in line with this recommendation as part of Security by Default. However there are a number of situations that do require the web server to be enabled for example:

- Gathering inventory information (i.e. IP Phone Serial Number)
- Using PhoneView to gathering each IP Phones ITL Status
- Screenshots of the IP Phone, typically used for remote control
- Remote control is SRST Mode or when the IP Phone is 'Unregistered' using PhoneView
- Additional 3rd Party applications

Therefore it may be necessary to temporarily re-enable the built-in web server to perform some of the actions above. In particular it is recommended that the first step in any CUCM upgrade includes enabling the web server on all endpoints as the very first task, even before upgrading IP Phone firmware. This ensures that if any ITL related issues do occur (this has been witnessed even with a phone firmware upgrade) this provides the ability to detect and fix any issues remotely.

Once the upgrade is complete then the built-in web server can be disabled again as necessary.

For further information on Cisco's leading practices for Cisco IP Phone Settings please refer to Chapter 15, "Wired IP Phone: Hardening" section of Securing Cisco IP Telephony Networks

http://www.ciscopress.com/title/1587142953

http://www.amazon.com/dp/1587142953

IP Phone Hardening

Alike any network equipment or device, Cisco Unified IP Phones are also a target for attacks. Even more so as they are exposed directly to end users - which include employees, visitors, contractors, janitors, and so on. Some of the Cisco Unified IP Phone default settings can make them vulnerable to attacks. The good news is that, Cisco Unified IP Phones contain built-in features which can be enabled or disabled on a phone by phone basis to increase the resilience of endpoints against attacks from within and outside.

Following settings can be modified to harden Cisco Unified IP Phones:

- Disable Speakerphone or Disable Speakerphone and Headset
  Disable to prevent eavesdropping on conversations
- PC Port
  Disable to prevent a PC from connecting to the network via the IP phone's internal switch (recommended for phones in public area e.g. lobby, elevator, rest rooms and so on)
- Settings Access
  Disable access to the IP phone settings to mitigate information gathering via endpoints. Restrict if user is allowed to change contrast, brightness, ring tones etc. but the user won't have access to network settings
- Gratuitous ARP
  Disable to prevent Gratuitous ARP (Man-in-the-middle) attacks
- PC Voice VLAN Access
  Disable to stop the IP phone from forwarding voice VLAN traffic to the PC (unless required during troubleshooting session/phone communication debugging for example by Cisco TAC)
- Video Capabilities
  Disable if the phone is not going to host a camera
- Web Access
  Disable access to the IP phone from a web browser to mitigate risk of exposing details about the network infrastructure
- Span to PC Port
  Disable to ensure data cannot be sniffed by a connected to PC port on phone
- Cisco Discovery Protocol (CDP): PC Port
  Disable unless using Cisco VT Advantage camera with the phone
- Link Layer Discovery Protocol (LLDP): Media Endpoint Discover (LLDP-MED) Switch Port
  Disable unless using LLDP on Cisco or non Cisco switches
- Link Layer Discovery Protocol (LLDP): Media Endpoint Discover (LLDP-MED) PC Port
  Disable unless using LLDP on Cisco or non Cisco switches

For further information on hardening Cisco Unified IP Phones and leading endpoint security recommendations refer to Chapters 9 and 15 of ‘Securing Cisco IP Telephony Networks’
http://www.ciscopress.com/title/1587142953
http://www.amazon.com/dp/1587142953

Table 15 - Cisco Unified IP Phone hardening summary

Setting	Description	Enabled	Disabled
PCPortSpan	SPAN Traffic to PC Port	2	41
Video Capabilities	Enabled PC based video with IP Phone	0	34
Web Access	Enable the IP Phone web server	43	0

Security Mode Summary

Cisco Unified IP Phone can be set to three modes pertinent to signalling and RTP:

- Non Secure / Unencrypted (both signalling and media are unencrypted)
- Authenticated (signalling is authenticated and media is not authenticated)
- Secure / Encrypted (both signalling and media are encrypted)

For further details and insight on CUCM security and security settings for Cisco Unified IP Phones as well as leading security recommendations refer to 'Securing Cisco IP Telephony Networks'
http://www.ciscopress.com/title/1587142953
http://www.amazon.com/dp/1587142953

Table 16 provides a summary based on the security configuration of all scanned endpoints in the target cluster. This provides a high level view of each security mode, which models are configured for the relevant security level.

Table 16 - Summary of the security mode of all devices scanned

Security Mode	Models	Count
Non Secure	7961, 7945, 7941, 7841, 6961	34
Not Secure	7937	1

Security Mode Assessment

It is important to understand if there are inconsistencies with the security configuration of the systems endpoints. In order to do this the PhoneView has assessed the overall security mode:

Security mode assessment of cluster (UCM91) is:	Default

Table 17 describes the basis of the assessment in the relevant context of the endpoint configurations .

Table 17 - Description of the security mode assessment

Result	Description
Default	No authentication or encryption enabled on any device therefore default security
Mixed	A mixture of Authenticated and Encrypted devices
Partial Authenticated	A mixture of default/non-secure and Authenticated devices
Authenticated	All devices are set to Authenticated
Partial Encrypted	A mixture of default/non-secure and Encrypted devices
Encrypted	All devices are set to Encrypted
N/A	No Security Mode information available

Remediation

The following is based on a combined analysis of each device configuration and how to remediate any ITL related issues:

Table 18 - Remediation summary

Scenario	Registered		Unregistered	
	Remote Delete ITL	Quantity	Remote Delete ITL	Quantity
Settings Enabled & Web Server online	Yes	4	Yes	1
Settings Enabled & WebServer off-line	Yes	0	No	0
Settings Restricted/Disabled	No	0	No	0
Number of devices that can be fixed remotely using PhoneView:		5		
Number of devices that need to be fixed physically:		0		

PhoneView's export spreadsheet includes a list of all devices requiring physical remediation and an extend set of details to locate the device including the location, user id, user email address, switch and switch port. This information is detailed in the "Physical ITL Remediation" Sheet of PhoneView's export and can be used to simplify resolving ITL issues when it's not possible to use PhoneView to delete them remotely.

UnifiedFX Recommendation to ensure all ITL issues can be resolved remotely

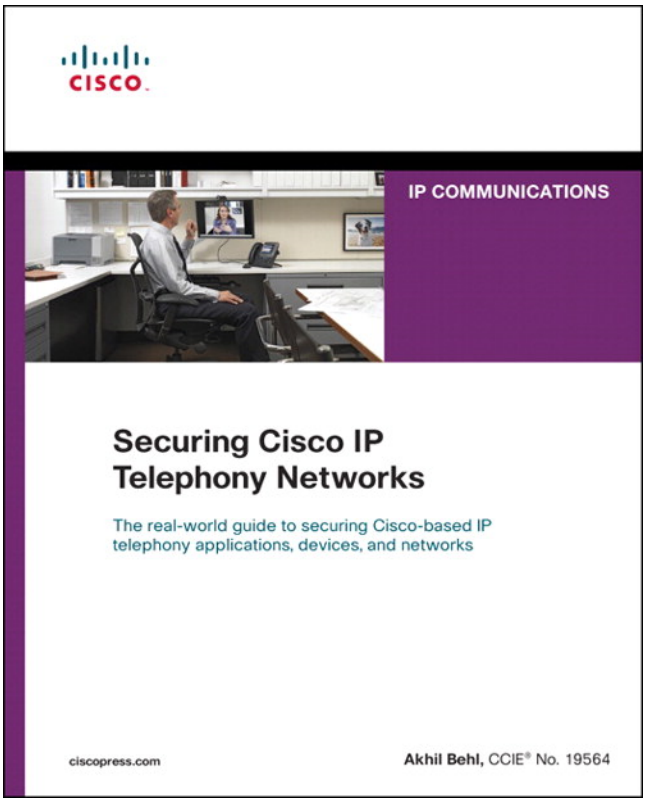
Based on assisting numerous clients with issues relating to Security by Default (SBD) there are a number of simple steps that can be performed prior to an upgrade to ensure that any issues with ITL files can be resolved remotely:

- Enable the Phones Web Server temporarily on all devices (Web server can be disabled one remediation is complete)
- Enable Settings Access on all devices temporarily
- Change the Authentication URL for all phones to be non-secure (i.e. HTTP) temporarily

By making these changes before an upgrade it's possible to resolve any ITL related issues remotely, both in terms of finding any issues as well as resolving them. Once the upgrade/migration is complete and this report confirms there are no issues, then the relevant settings can be changed back to their previous configuration as relevant.

Further Reading

In interest of safeguarding your Cisco UC environment from any unforeseen internal or external threats it is highly recommended to have the right set of security controls deployed where possible. For more information on the various Cisco UC security controls available, the right level of security for your UC solution, securing endpoints from malicious insiders or attacks from outside of your organization, building and maintaining a secure UC network; it is strongly recommended that you refer to 'Securing Cisco IP Telephony Networks' by Cisco Press.



http://www.ciscopress.com/title/1587142953
http://www.amazon.com/dp/1587142953