CT Console Hardening

Submitted By

Urvashi Chaturvedi

14mcei29

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

MAY 2016

CT Console Hardening

Major Project

Submitted in partial fulfillment of the requirements

for the degree of

Master of Technology in Information and Network Security

Submitted By

Urvashi Chaturvedi

(14MCEI29)

Guided By

Prof. Parita Oza

Nirma University, Ahmedabad.

Mr. Sagar Chandrashekar

Philips Innovation Campus,Bangalore

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

MAY 2016

Certificate

This is to certify that the major project entitled **"CT Console Hardening "** submitted by **Urvashi Chaturvedi (Roll No: 14MCEI29)**, towards the partial fulfillment of the requirements for the award of degree of Master of Technology in Information and Network Security of Institute of Technology, Nirma University, Ahmedabad, is the record of work carried out by her under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this project, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Prof. Parita Oza
Internal Guide & Assistant Professor,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Prof.(Dr.) Sharadha Valiveti
Associate Professor,
Coordinator M.Tech - INS
Institute of Technology,
Nirma University, Ahmedabad

Dr. Sanjay Garg
Professor and Head,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. P.N Tekwani
Director,
Institute of Technology,
Nirma University, Ahmedabad

Certificate

This to certify that **Ms.Urvashi Chaturvedi (Roll No: 14MCEI29)**, a student of M.Tech CSE(Information and Network Security), Institute of Technology, Nirma University, Ahmedabad was working in this organization since 2/07/2015 and carried out his thesis work titled **"CT Console Hardening "**. She was working in name of Security intern under supervision of Mr.Sagar Chandrashekar (Mentor), and Mr. Arun Satapathy (Manager). She has successfully completed the assigned work and is allowed to submit her dissertation report. The results embodied in this project, to the best of our knowledge, haven't been submitted to any other university or institution for award of any degree or diploma. We wish her all the success in future.

Mr. Sagar Chandrashekar
External Guide,
Philips Innovation Campus,
Bengaluru.

Mr. Arunkumar Satapathy
Manager,
Philips Innovation Campus
Bengaluru.

Statement of Originality

I, **Urvashi Chaturvedi**, Roll. No. **14MCEI29**, give undertaking that the Major Project entitled "**CT Console Hardening**" submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in **Computer Science & Engineering** of Institute of Technology, Nirma University, Ahmedabad, contains no material that has been awarded for any degree or diploma in any university or school in any territory to the best of my knowledge. It is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. It contains no material that is previously published or written, except where reference has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

_____

Signature of Student

Date:

Place:

Endorsed by

Prof. Parita Oza

(Signature of Guide)

Acknowledgements

First and foremost, sincere thanks to **Mr.Arun Satapathy**, Manager, Philips Innovation Campus, Bangalore. I enjoyed his vast knowledge and owe him lots of gratitude for having a profound impact on this report.

I would like to thank my Mentor, **Mr. Sagar Chandrashekar**(Sr.Technical Specialist), Philips Innovation Campus, Bangalore for his valuable guidance. Throughout the training, he has given me much valuable advice on project work. Without him, this project work would never have been completed.

It gives me immense pleasure in expressing thanks and profound gratitude to **Prof. Parita Oza** , Assistant Professor, Computer Science Department, Institute of Technology, Nirma University, Ahmedabad for her valuable guidance and continual encouragement throughout this work. The appreciation and continual support she has imparted has been a great motivation to me in reaching a higher goal. Her guidance has triggered and nourished my intellectual maturity that I will benefit from, for a long time to come.

It gives me an immense pleasure to thank **Dr. Sanjay Garg**, Hon'ble Head of Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad for his kind support and providing basic infrastructure and healthy research environment.

A special thank you is expressed wholeheartedly to **Dr P.N Tekwani**, Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad for the unmentionable motivation he has extended throughout course of this work.

I would like to thank the Institution, all faculty members of Computer Engineering Department, Nirma University, Ahmedabad for their special attention and suggestions towards the project work.

I also owe my colleagues in the Philips, special thanks for helping me on this path and for making project at Philips more enjoyable.

- Urvashi Chaturvedi

14MCEI29

Abstract

As the clinical usage, security of the CT Scanner is of very much of concern.Our goal is to make CT console more secure in order to protect Information System.Following are some projects carried out in order to harden CT Console.

- We are making the CT Scanner compliant with the DOD (department of defense, US) and DISA compliant to ship the CT Scan machine to US. The concern is to to harden the operating system (windows 7) to meet the compliance. And at the end, providing solution as a deliverable to the manufacture team to meet such compliance.

- SignTool facilitate the user to sign the binaries using digital certificates and before signing scan for malware using Antivirus.

- Hardening the operating system in order to reduce the attack area by disabling functionality that is not required and keeping the minimum functionality that is required and make the system safe.

Abbreviations

DOD	Department of Defense
DIACAP	DoD Information Assurance Certification and Accreditation Process
STIG	Security Technical Implementation Guides
CT	Computed Tomography
DB	Database
OS	Operating System
HDD	Hard disk drive

Contents

Certificate **iii**

Certificate **iv**

Statement of Originality **v**

Acknowledgements **vi**

Abstract **viii**

Abbreviations **ix**

List of Figures **xii**

List of Tables **1**

1 Introduction **2**
1.1 Background 2

2 Literature Survey **3**
2.1 Motivation 3
2.2 Problem Statement 3
2.3 Significance 4
2.4 Challenges 4
2.5 Constraints and Trade-off 4
2.5.1 Constraints 4
2.5.2 Trade-off 5
2.5.3 Test Cases Generation 5

3 About CT **6**
3.1 Gantry 6
3.2 Console 7

4 Technical Requirements **8**
4.1 Hardware Requirement 8
4.2 Software Requirement 8

5 Implementation **9**
5.1 Phase 1 9
5.2 Unit Testing 11

5.2.1 Setting lock screen after wake up: . . . 11
5.2.2 Interactive logon: . . . 12
5.2.3 Access Control: . . . 12
5.3 Integration Testing . . . 13
5.4 Results . . . 14

6 Result **17**
6.1 Output . . . 17
6.2 Result Analysis . . . 17

7 Tool Development **18**
7.1 Sign Tool . . . 18
7.1.1 Purpose of Tool . . . 18
7.1.2 How it Works . . . 18
7.1.3 Limitation . . . 18
7.1.4 Technology . . . 18
7.1.5 Further Addition . . . 18
7.1.6 Layout . . . 20
7.2 FileUpdater Tool . . . 21
7.2.1 Purpose of Tool . . . 21
7.2.2 Limitation . . . 21
7.2.3 Technology . . . 21
7.2.4 Layout . . . 22

8 Lync Access from Console **23**
8.0.1 Project Objective . . . 23
8.0.2 Project Description . . . 23
8.0.3 Limitation . . . 23
8.0.4 Outcome . . . 24

9 Windows 10 Hardening **26**
9.1 Objective . . . 26
9.2 Project Description . . . 26
9.3 Technology . . . 26
9.4 Implementation . . . 26

10 Conclusion and Future Work **29**
10.1 Conclusion . . . 29
10.2 Future Work . . . 29

References **32**

List of Figures

3.1 Gantry 6
3.2 CT Console Dual Monitor 7

5.1 Security Technical Implementation Guide 9
5.2 Lock Screen Registry 10
5.3 Interactive Logon inf File 10
5.4 Interactive Logon Configure 11
5.5 Access Control ICACLs 11
5.6 Integration Testing 13
5.7 Lock Screen Registry setup 15
5.8 Interactive Logon Setting 16
5.9 Access Control Result 16

7.1 Layout of Sign Tool 20
7.2 Layout of Sign Tool 20
7.3 Layout of FileUpdater Tool 22

8.1 Lync 25

9.1 Registry Update 27
9.2 Registry Update 27
9.3 Registry Update 28

List of Tables

Document has no Tables

Chapter 1

Introduction

1.1 Background

X-ray computed tomography (X-ray CT) is a technology that uses computer-processed X-rays to produce tomographic images (virtual 'slices') of specific areas of a scanned object, allowing the user to see inside the object without cutting. Digital geometry processing is used to generate a three-dimensional image of the inside of the object from a large series of two-dimensional Radiographic images taken around a single axis of rotation. Medical imaging is the most common application of X-ray CT. Its cross-sectional images are used for diagnostic and therapeutic purposes in various medical disciplines. The software driving the CT Scan machine is called the SYSTEM. The System is connected to two different networks at the same time. One to the hospital network and the other to the PHILIPS Remote System (PRS). The SYSTEM has two major parts: CIRS and Gantry. Gantry is used to take raw x-ray images and the gantry is used to convert those images to the computer readable form.

The DoD Information Assurance Certification and Accreditation Process (DIACAP) is a United States Department of Defense (DoD) process that means to ensure that companies and organizations apply risk management to information systems (IS). DIACAP defines a DoD-wide formal and standard set of activities, general tasks and a management structure process for the Certification and Accreditation of a DoD IS that maintains the information assurance (IA) posture throughout the system's life cycle.

Chapter 2

Literature Survey

2.1 Motivation

Information security and privacy in the Healthcare sector is an issue of growing importance. The adoption of digital patient records, increased regulation, provider consolidation, and the increasing need for information between patients, providers, and payers, all point towards the need for better information security. We critically survey the research literature on information security and privacy in Healthcare, published in both information systems, non-information systems disciplines including health Informatics, public health, law, medicine, and popular trade publications and reports. In this paper, we provide a holistic view of the recent research and suggest new areas of interest to the information systems community.

2.2 Problem Statement

As the clinical usage, security of the CT Scanner is of very much of concern.Our goal is to make CT console more secure in order to protect Information System.Following are some projects carried out in order to harden CT Console.

- We are making the CT Scanner compliant with the DOD (department of defense, US) and DISA compliant to ship the CT Scan machine to US. The concern is to to harden the operating system (windows 7) to meet the compliance. And at the end, providing solution as a deliverable to the manufacture team to meet such compliance.

- To sign a binary required to run on trusted environment, user need to sign through

command execution with Certificate installed. This manual process take time and it doesnot support audit logs. SignTool facilitate the user to sign the binaries using digital certificates and before signing scan for malware using Antivirus.The signing activity will be logged in a XML database.

- Hardening the operating system in order to reduce the attack area by disabling functionality that is not required and keeping the minimum functionality that is required and make the system safe..

2.3 Significance

- The project is for a very important and sensitive industry i.e., HealthCare. The product supplied or provided to HealthCare should be reliable, sustainable and most importantly secure from inner/outer networks, viruses and other malicious processes and methods. The security perspective of the project is always the point of concern since any discrepancy in the patient information or any of the confidential information may lead to a very specific disaster.

- The binaries signed by Sign tool indicate that the files are from trusted path and malware free.

- Windows hardening improves system performance and minimize network based attacks and prevent system access when some unauthorized user is interfacing with the system, either physically, or over a network at the machine.

2.4 Challenges

- Meeting 100 % security compliance for DIACAP.

- Maintaining Inter-operability of the SYSTEM and the compliance.

2.5 Constraints and Trade-off

2.5.1 Constraints

- User must have knowledge of the hardware components and Implementation and architecture.

- To work with the sub-system functionalities, the architecture and implementation of the sub-systems should be known. But in this short time, I cannot get the complete implementation of a very big project. So working with a black-box (no insight to the implemented code) is a very big constraint.
- User must have knowledge of programming languages.
- Minimum system requirements must be met to use the product.

2.5.2 Trade-off

- Cost Vs Feature Trade Off: Selenium does not support Internet Explorer on par with other testing tools but we are using it as it is open source.
- Effort Vs Time Trade Off: Ids for many UI elements were not provided for testing.

2.5.3 Test Cases Generation

The DIACAP component is tested with various manual testing methods including log viewers, event viewer and manual verification. For each finding solution, the corresponding log or group policy is checked to verify whether the setting is implemented. After implementation, the system is checked for any deviation from core functionality or any misbehaviour.

Chapter 3

About CT

3.1 Gantry

Figure 3.1: Gantry

3.2 Console

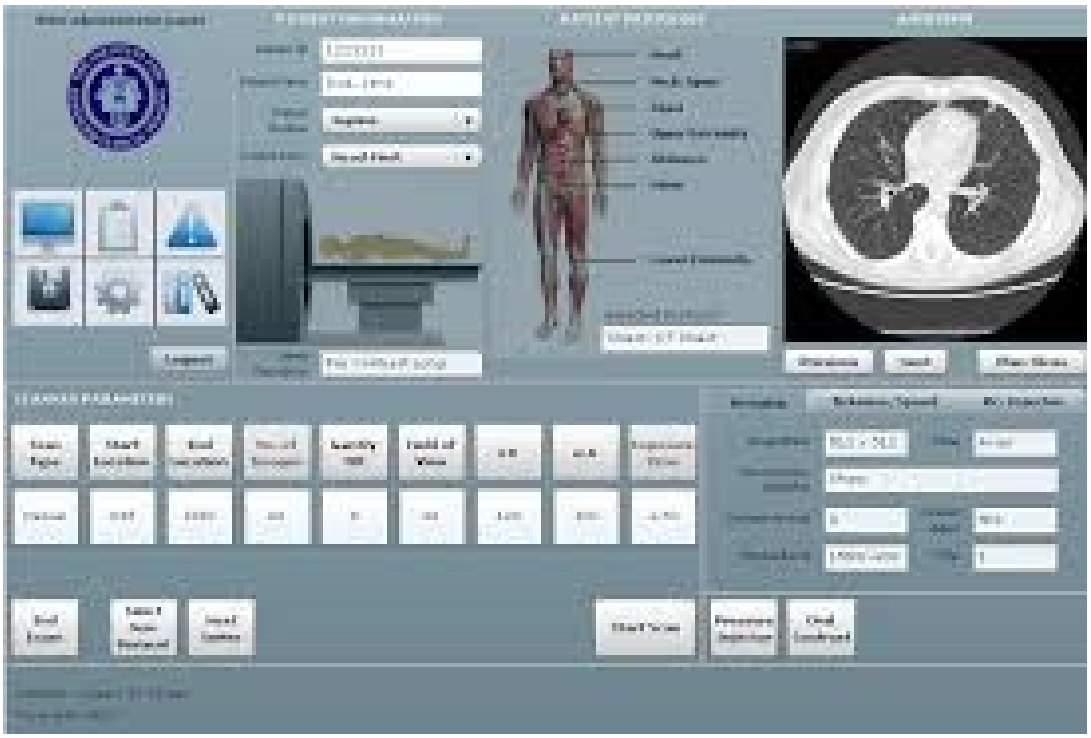


Figure 3.2: CT Console Dual Monitor

Chapter 4

Technical Requirements

4.1 Hardware Requirement

- RAM : 12 GB.
- HDD processing Speed :7200 rpm or 9000 rpm

4.2 Software Requirement

- VBScript
- C #
- Nessus Tool
- Nmap
- Oracle Virtual Box

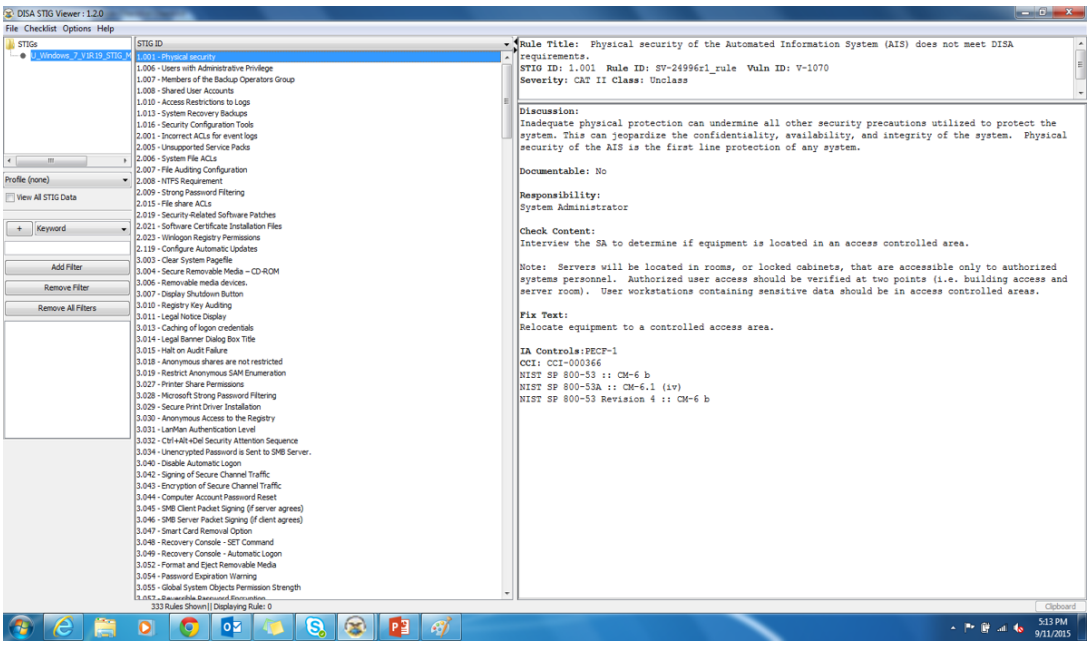
Chapter 5

Implementation

5.1 Phase 1

The component is coded in C# using .NET and ICACLS tool from Microsoft. Security Editor Auditor Policy from Microsoft are also used for various configuration settings.

Figure 5.1: Security Technical Implementation Guide



These are the stigs which is given by DIACAP for assessment which is to be fixed Below mentioned are few Scenarios of the above STIGs:

- **Scenarios 1**– Setting lock screen after wake up: Using Registry class from .NET framework and SetValue function, the value for the value is set to integer 1. It will

enforce every user to be prompted to enter the credentials on resume from sleep when plugged-in.

Figure 5.2: Lock Screen Registry

```
Registry.SetValue(
"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Pow
er\\PowerSettings\\0e796bdb-100d-47d6-a2d5-f7d2daa51f51
\\" ,"ACSettingIndex", 1,RegistryValueKind.DWord);
```

- **Scenarios 2**– Interactive login: This will make sure the only the administrators and Users are able to logon to the system locally. Since the many other groups or users may exist on the system, that will not be provided with the local access to the system. This will restrict all other groups and users from logging in locally. Fig 7.2 is the inf(configuration template) file snippet with SeInteractiveLogonRight privilege right set to Administrators and Users groups only.

Figure 5.3: Interactive Logon inf File

```
[Unicode]
Unicode=yes
[Privilege Rights]
SeInteractiveLogonRight = Administrators, Users
[Version]
signature="$CHICAGO$"
Revision=1
[Profile Description]
Description=%V_26472%
```

Fig 7.3 shows how the template is implemented to the system with the help of security editor(secedit) which will include following steps:

  - Importing a cfg(inf) file into a database(sdb) file.
  - Configuring the SDB file to the system using /configure switch.

- **Scenarios 3**– Access control:Fig 7.4 shows the creation and configuration of a cmd.exe thread and running a Icacls command

Figure 5.4: Interactive Logon Configure

```
Process p= new Process();
p.StartInfo.UseShellExecute=false;
p.StartInfo.CreateNoWindow= false;
p.StartInfo.FileName="cmd.exe";

p.StartInfo.Arguments = "/C secedit /import /cfg
\"C:\\Users\\ceh\\Desktop\\deployment\\inf\\privilege
rights\\interactivelogon.inf \" /db
C:\\Windows\\security\\database\\fake.sdb";
```

Figure 5.5: Access Control ICACLs

```
Process p= new Process();
p.StartInfo.UseShellExecute=false;
p.StartInfo.CreateNoWindow= false;
p.StartInfo.FileName="cmd.exe";
p.StartInfo.Arguments = "/C icacls
C:\\Windows\\System32\\Drivers\\etc\\hosts /grant:r
Users:(F) Administrators:(R,W) \"NT
Service\\eventlog\":(F) SYSTEM:(F)";
p.Start();
```

5.2 Unit Testing

Unit testing of the individual finding is done manually with the help of various tools such as log viewer, event viewer, firewall, group policy editor, Audit policy viewer and registry editor.

This Examples describe the procedure carried out for Unit Testing for above **Scenarios**

Scenarios 1 (5.2.1)

5.2.1 Setting lock screen after wake up:

For this finding, following steps are followed to make sure fixing it will not impact the system functionalities

- Merge the ACSettingIndex registry with the current registry state.

- Lock out from the system and check for the logon screen.
- After waking from screensaver, check for the logon screen.
- After waking from sleep, check for the logon screen.
- Check for any background process at the time of sleep or Screensaver.

Scenarios 2 (5.2.2)

5.2.2 Interactive logon:

For the second finding, above steps are followed to make sure it will not impact the system functionalities.

- After configuring the created database, check if any user, other than Administrators or Users group, is able to logon.
- Check if this setting affects the remote logon for the same users.
- Check if any user is added to the ACL and also added to some other group, will its logon is prevented,
- Check the system event logs for any logon events for Users and Administrators group.

Scenarios 3 (5.2.3)

5.2.3 Access Control:

For the third finding, above steps are followed to make sure it will not impact the system functionalities.

- After running the specific command, check for the ACL of the file C:\Windows\Drivers\etc\hosts.
- Check the file system object audits for any access to the particular file. If there is any access, then the fix may affect the system.
- Check the ACL of the specified file for any special permissions to any user or process for some specific operations.

5.3 Integration Testing

Figure 5.6: Integration Testing

```
Registry.SetValue("HKEY_LOCAL_MACHINE\\Software\\
Policies\\Microsoft\\Power\\PowerSettings\\0e796b
db-100d-47d6-a2d5-f7d2daa51f51\\"
,"ACSettingIndex", 1,RegistryValueKind.DWord);

Process p= new Process();
p.StartInfo.UseShellExecute=false;
p.StartInfo.CreateNoWindow= false;
p.StartInfo.FileName="cmd.exe";

p.StartInfo.Arguments = "/C icacls
C:\\Windows\\System32\\Drivers\\etc\\hosts
/grant:r Users:(F) Administrators:(R,W) \"NT
Service\\eventlog\":(F) SYSTEM:(F)";
p.Start();

p.StartInfo.Arguments = "/C secedit /import
/cfg
\"C:\\Users\\ceh\\Desktop\\deployment\\inf\\privi
lege rights\\locallylogon.inf \" /db
C:\\Windows\\security\\database\\low.sdb";
p.Start();

p.WaitforExit();
```

After implementing above code, all of the settings and configurations are checked manually for being implemented. The logs are checked for any error message or any warning.

5.4 Results

The fix to the first ACSettingIndex registry does not fix the problem. The impacts are following:

- No logon screen appears after waking up from sleep.
- No logon screen appears after waking up from screensaver.

Now checking Manually all the fix :

Figure 5.7: Lock Screen Registry setup

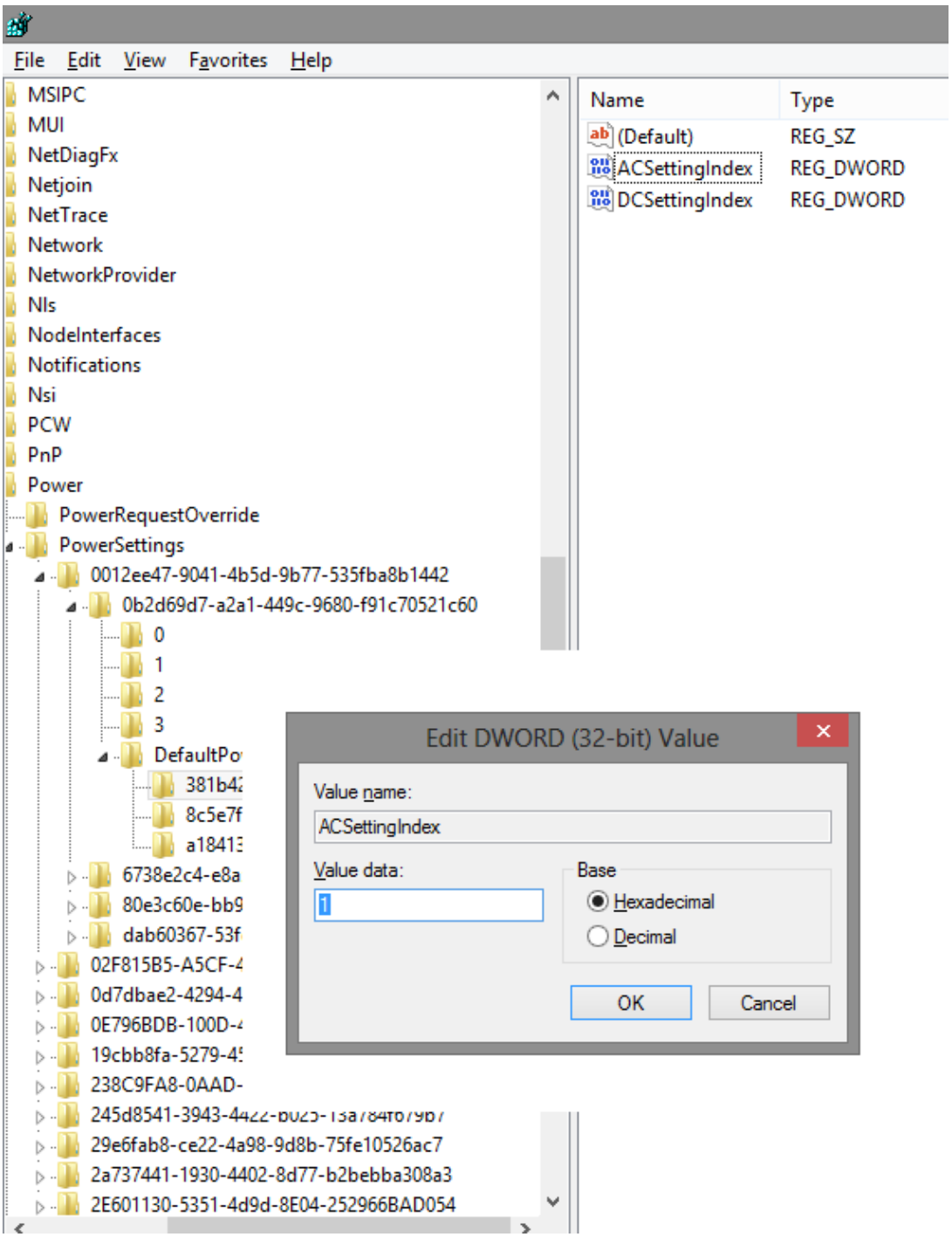


Figure 5.8: Interactive Logon Setting

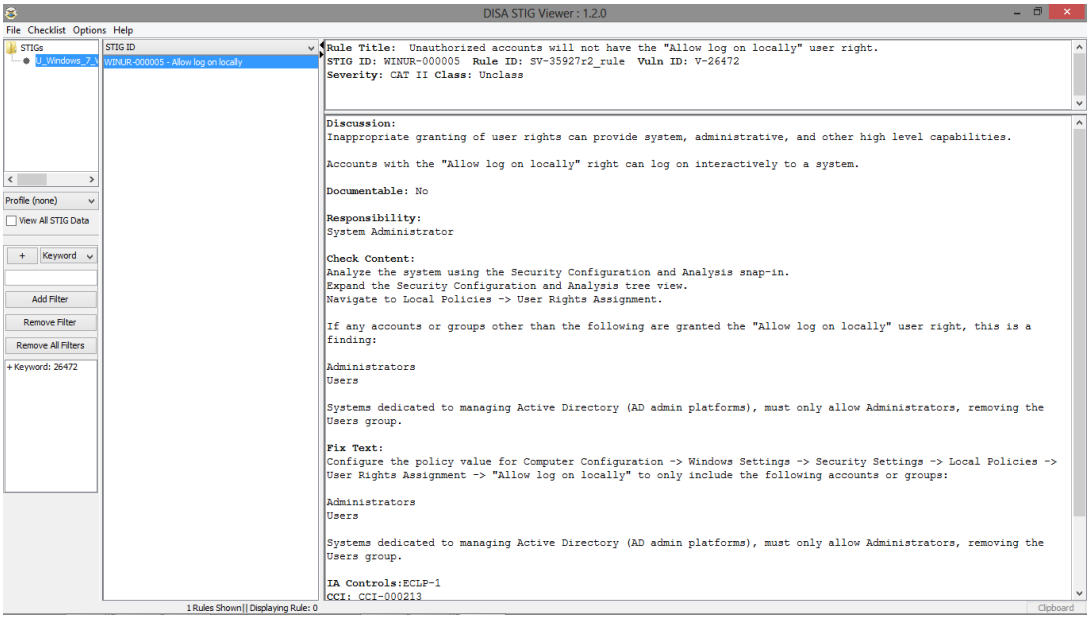
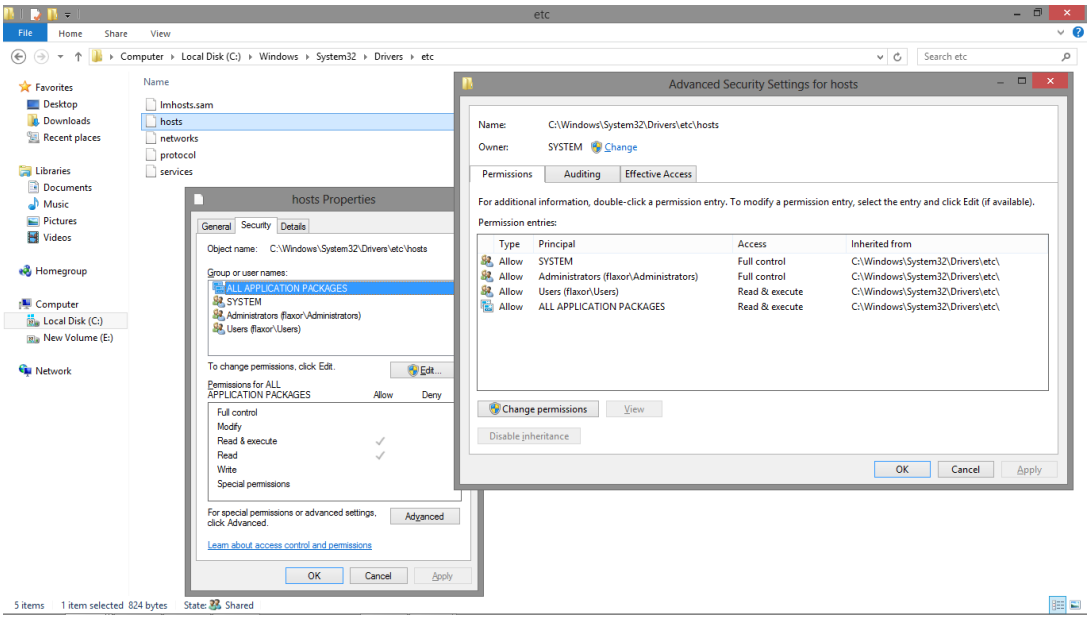


Figure 5.9: Access Control Result



Chapter 6

Result

6.1 Output

Under results the number of passed, failed and executed test cases are shown and also the test cases which fail will have the information of the why they failed. They also have the information of the test start time, test end time, type of browser and testing type.

6.2 Result Analysis

The result from the log files, event logs and configuration templates are analyzed for the final documentation. Comments and process is documented for future reference.

Chapter 7

Tool Development

7.1 Sign Tool

7.1.1 Purpose of Tool

To sign a binary required to run on trusted environment, user need to sign through command execution with a certificate installed. This manual process takes time and it doesnt support audit logs.

7.1.2 How it Works

The Sign Tool facilitates the user to sign the binaries using digital signing certificates. User authentication for signing is done using certificate and all binaries to be signed are scanned for Malware using Antivirus. The signing activity will be logged in a database for the audit purpose

7.1.3 Limitation

Tool should be digitally signed to make it work.

7.1.4 Technology

C#

7.1.5 Further Addition

- XML database for storing the logs of signed document.
- Included Sign report which display user all the details of signed files according to

selected range of date.

- Included more digital certificates as it can be used by all programs in general.
- Removed the dependency of tool on IST validation dongle and SQL database.
- Unit testing of each and every module.
- Documentation.

7.1.6 Layout

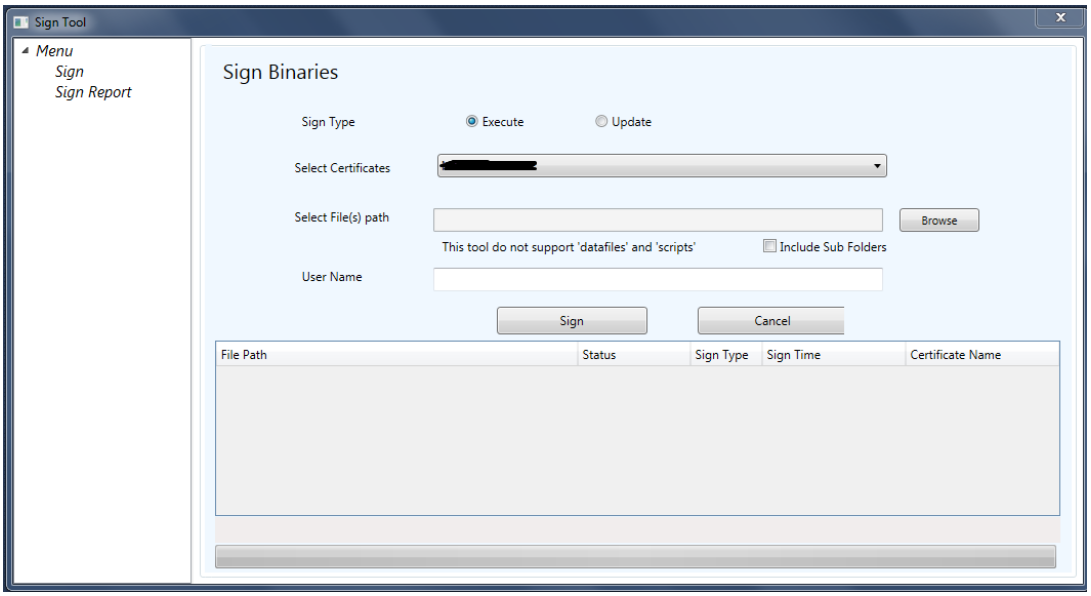


Figure 7.1: Layout of Sign Tool

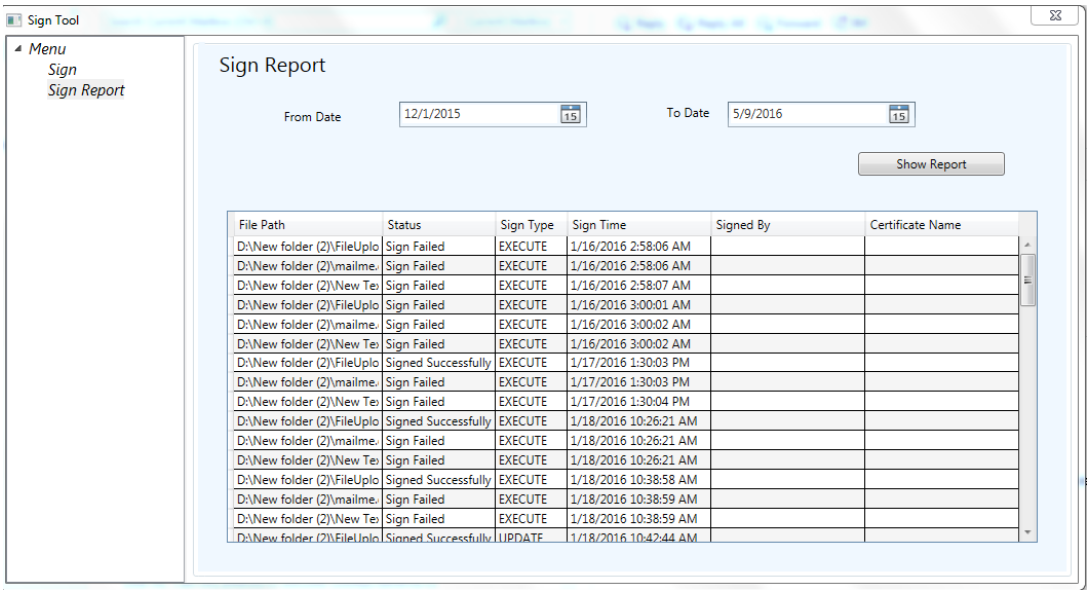


Figure 7.2: Layout of Sign Tool

7.2 FileUpdater Tool

7.2.1 Purpose of Tool

To copy/update multiple binaries manually is time consuming and it doesnot verify the status that whether file has been copied or not . This tool allows the user to update the system and facilitates to copy multiple files collectively and provide following notifications to the user :

1. file has been copied successfully
2. check whether destination have enough memory to store files
3. to check whether destination directory exist
4. audit logs for future reference

7.2.2 Limitation

This tool is designed for signing only .msi , .dll , .exe files only.

7.2.3 Technology

C#

7.2.4 Layout

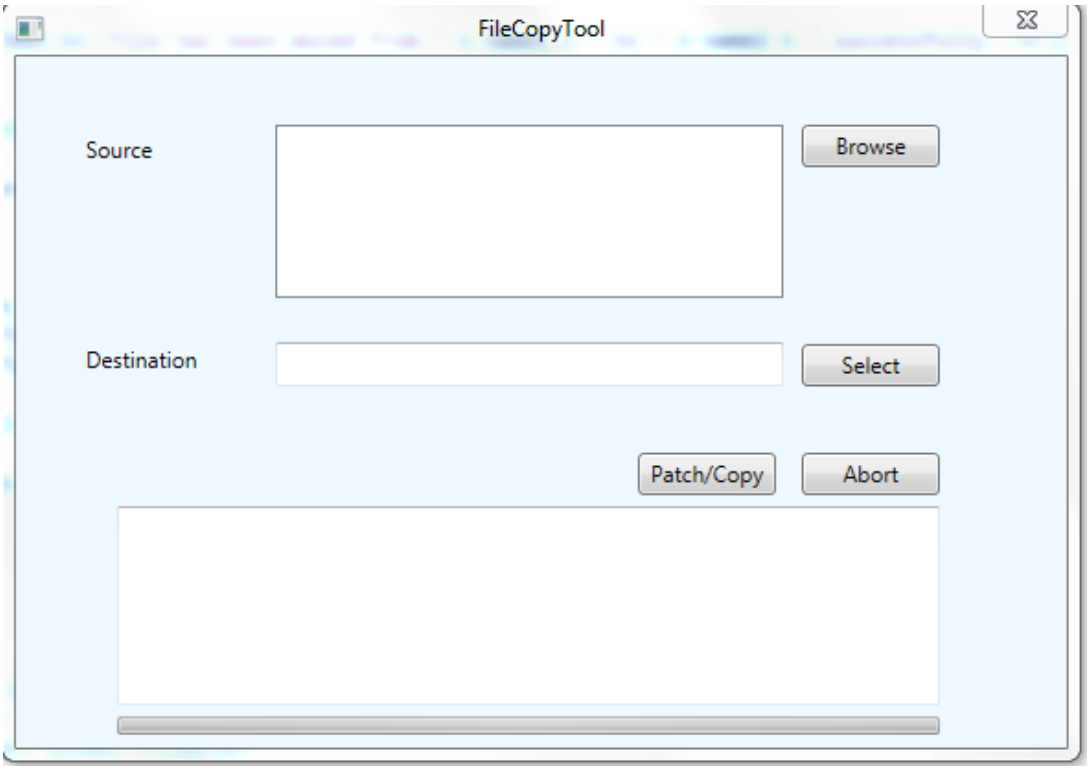


Figure 7.3: Layout of FileUpdater Tool

Chapter 8

Lync Access from Console

8.0.1 Project Objective

Unified communication is a tool which allows users to communicate from anywhere with an Internet Connectivity.

8.0.2 Project Description

- Most of the Hospitals have more than one scanner and more than one radiologists and technicians who operates scanner and performs the studies. In most cases, Technicians are the ones who setup and performs the studies / scans and sends the final resulted images to radiologist for review and diagnostics. There are cases where technicians need to consults the radiologists to review and approve the study details and other information related to studies. There is a need to have a communication mechanism established in the hospital network where technicians and radiologists discuss the clinical parameters related to study and have Instant Messaging, share, audio and video connectivity. Unified communication is a tool which allows users to communicate from anywhere with an Internet Connectivity.
- This project is to integrate the Unified Communication with in the CT (Computed Tomography) systems, This is complex as the OS (Operating System) in the CT Host machine is hardened and all the firewall configuration is closed.

8.0.3 Limitation

This POC is only for establishing the communication within the Hospital Network.

8.0.4 Outcome

- Integrate the Unified Communication in the CT (Computed Tomography) systems.
- Analyze the existing OS hardening and firewall settings deployed on the CT Host machine , Come up with the strategy to deploy Unified Communication on the CT host system and document the detailed changes to OS, Firewall configuration and any other settings on the system.

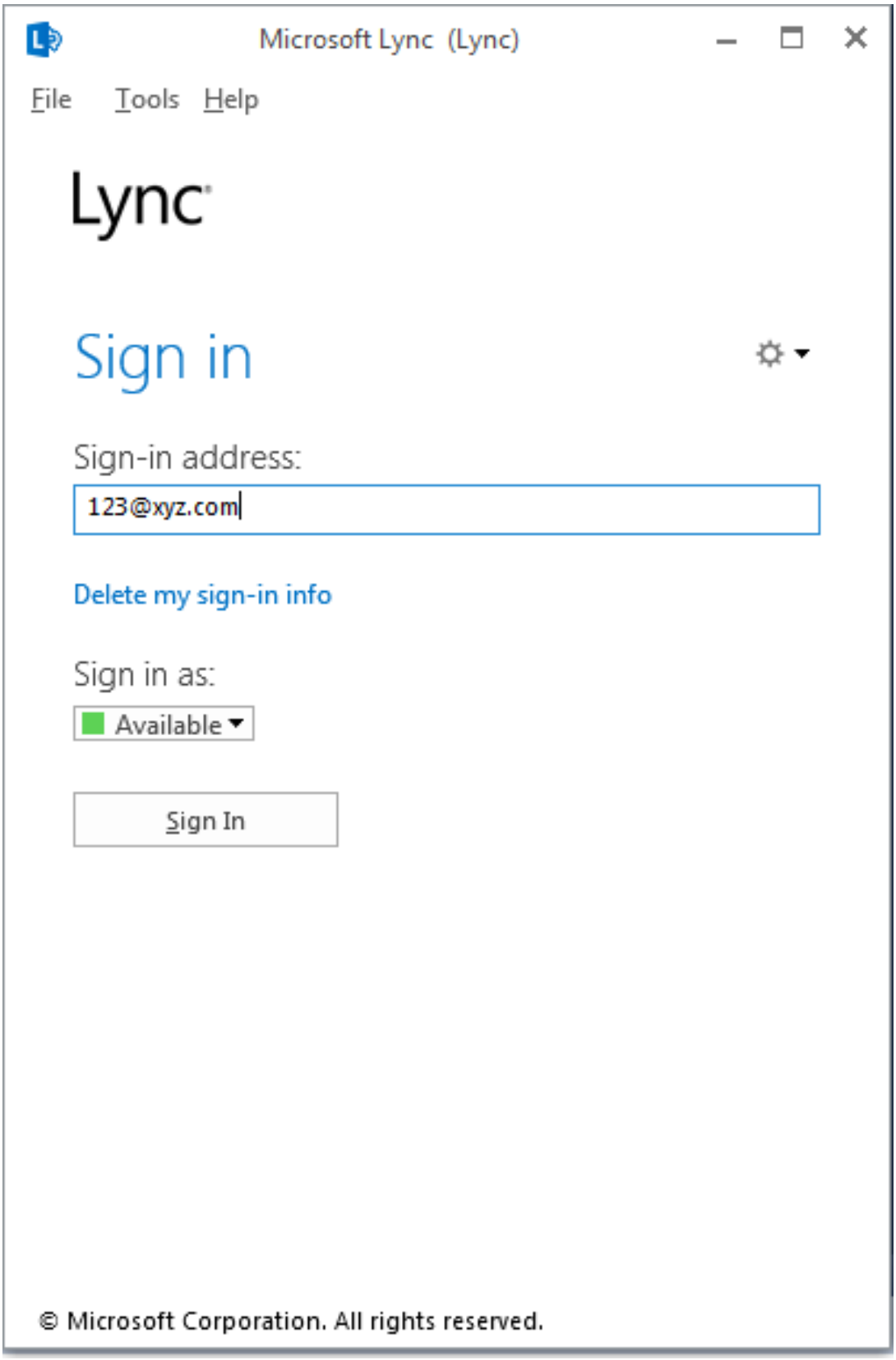


Figure 8.1: Lync

Chapter 9

Windows 10 Hardening

9.1 Objective

Hardening the operating system in order to reduce the attack area by disabling functionality that is not required and keeping the minimum functionality that is required and make the system safe.

9.2 Project Description

Worked on securing the system from external as well as internal vulnerabilities and to improve the performance of the system.

- Compared all the existing hardened windows 7 group policy and registries with the windows 10.
- Prepared brief document which tells about all changes between Windows 7 and Windows 10 registry entry.
- Implemented configuration file for enabling all the changes for all type of user separately like Field Service engineer, Technician.

9.3 Technology

C#, VBScript, Batch Script

9.4 Implementation

- Following are the dummy snapshot of implementation

```
3993
3994 [HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Preferences\ProxySettings]
3995
3996 [HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Preferences\ProxySettings\HTTP]
3997 "ProxyStyle"=dword:00000001
3998 "ProxyName"=""
3999 "ProxyPort"=dword:00000050
4000 "ProxyBypass"=dword:00000000
4001 "ProxyExclude"=""
4002
4003 [HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Preferences\ProxySettings\MMS]
4004 "ProxyStyle"=dword:00000000
4005 "ProxyName"=""
4006 "ProxyPort"=dword:000006db
4007 "ProxyBypass"=dword:00000000
4008 "ProxyExclude"=""
4009
4010 [HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Preferences\ProxySettings\RTSP]
4011 "ProxyStyle"=dword:00000000
4012 "ProxyName"=""
4013 "ProxyPort"=dword:0000022a
4014 "ProxyBypass"=dword:00000000
4015 "ProxyExclude"=""
4016
4017 [HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Preferences\VideoSettings]
4018
4019
4020 [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
4021 "DisableLockWorkstation"=dword:00000001
4022
4023 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
4024 "IgnoreShiftOverride"="1"
```

Figure 9.1: Registry Update

```
; Added per Jared Blouse to allow active X on the local machine without warnings
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN]
"iexplore.exe"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0]
"1201"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1]
"Flags"=dword:000000db

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoDriveTypeAutoRun"=dword:000000ff
"CDRAutoRun"=dword:00000000
"NoSimpleStartMenu"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableChangePassword"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\LocalMachine\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services]
"fDenyTSConnections"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StuckRects2]
"Settings"=hex:28,00,00,00,ff,ff,ff,ff,01,00,00,00,03,00,00,00,3c,00,00,00,1e,\
  00,00,00,fe,ff,ff,ff,e4,03,00,00,02,05,00,00,02,04,00,00

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Desktop\General]
"TileWallpaper"="1"
"WallpaperStyle"="0"

[HKEY_CURRENT_USER\AppEvents\EventLabels\ActivatingDocument]
```

Figure 9.2: Registry Update

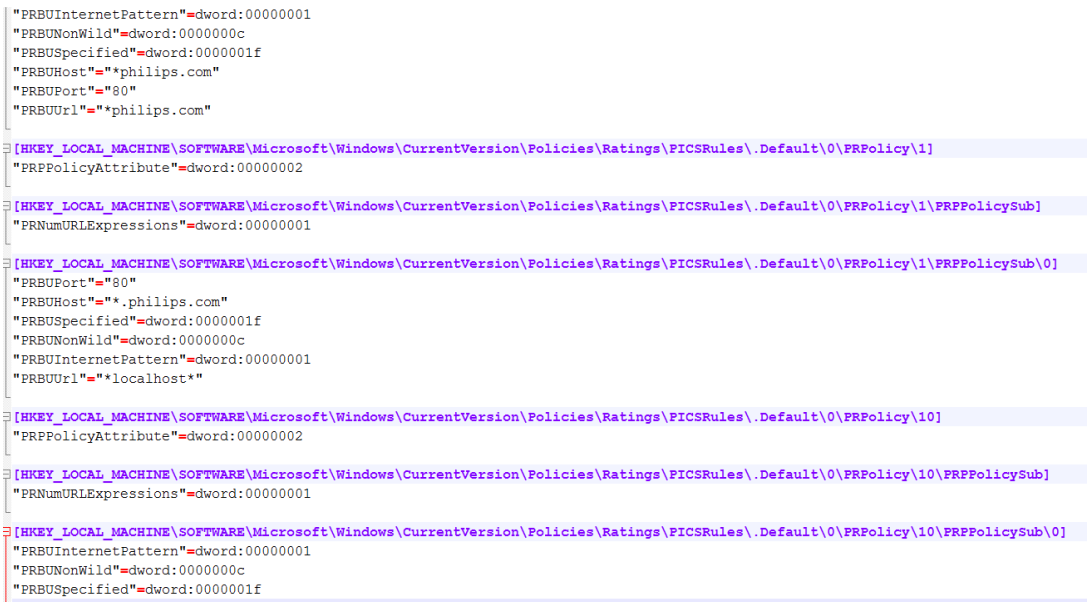


Figure 9.3: Registry Update

Chapter 10

Conclusion and Future Work

10.1 Conclusion

- DOD compliance increased to 90%, it enables sales for Philips CT to DoD.
- SignTool helped in signing multiple files at once while previously individual file has to be selected and signed.
- FileUpdater helped in updating a frozen system with new set of files collectively.
- Lync Access from console will allow user to communicate through internet.
- Windows 10 hardening reduce the attack area by disabling functionality that is not required and keeping the minimum functionality that is required and make the system safe.

10.2 Future Work

- The same component can be used for other versions of the CT Scan machine.
- Modulating the code further in order to incorporate further changes very easily.
- Validating the tool before deploying it.
- Additional Functionality will be added in the tools.
- The component, will be modified to be used as a security benchmark for all systems which do not require often maintenance.

- Also this component can also be modified to be used for other products which use .NET framework and supports vast number of platforms.

References

[1] [Agrawal, 2007] Agrawal. R, and Johnson
Title of the publication
International Journal of Medical Informatics vol. 76, no. 5-6, pp 471 479

[2] Philips Confidential Documents

[3] https://msdn.microsoft.com/en-us/library/windows/privileges

[4] https://msdn.microsoft.com/en-us/library/windows/desktop/ee663293(v=vs.85).aspx

References