The Clean Thesis Style

Ricardo Langner

June 21, 2016
Version: My First Draft

Clean Thesis Style University

CleanThesis

Department of Clean Thesis Style
Institute for Clean Thesis Dev
Clean Thesis Group (CTG)

Documentation

The Clean Thesis Style

Ricardo Langner

1. Reviewer Jane Doe
Department of Clean Thesis Style
Clean Thesis Style University

2. Reviewer John Doe
Department of Clean Thesis Style
Clean Thesis Style University

Supervisors Jane Doe and John Smith

June 21, 2016

Ricardo Langner
The Clean Thesis Style
Documentation, June 21, 2016
Reviewers: Jane Doe and John Doe
Supervisors: Jane Doe and John Smith

Clean Thesis Style University
Clean Thesis Group (CTG)
Institute for Clean Thesis Dev
Department of Clean Thesis Style
Street address
Postal Code and City

Abstract

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

Abstract (different language)

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

Acknowledgement

Contents

1 Introduction **1**

2 Related Work **3**

3 Background **5**

3.1 UEFI 5

3.1.1 Boot Sequence 5

3.1.2 UEFI/PI Firmware Images 6

3.1.3 Executables 6

3.1.4 Programming 6

3.1.5 edk2 6

3.1.6 Security 6

3.2 Windows 6

3.2.1 User Access Control (UAC) 6

3.2.2 Signing 6

3.2.3 Bitlocker 6

4 Attacks **7**

4.1 No Secure Boot 7

4.2 Secure Boot 7

4.3 Bitlocker 8

5 Discussion **9**

5.1 Rootkit classification 9

5.2 Mitigations 9

5.2.1 User awareness 9

6 Conclusion **11**

A Example Appendix **19**

A.1 Appendix Section 1 19

A.2 Appendix Section 2 19

Declaration **21**

1 Introduction

definition of rootkit/bootkit

persistenz

2 Related Work

3 Background

general introduction to UEFI replace bios security

3.1 UEFI

3.1.1 Boot Sequence

1. Security (SEC)

establishment of root of trust

2. Pre-EFI (PEI)

3. Driver Execution Environment (DXE)

dxe core dxe dispatcher dxe drivers

4. Boot Device Selection (BDS)

5. Transient System Load (TSL)

boottime and runtime services/driver bootloader ExitBootServices()

6. Runtime (RT)

runtime services/driver

7. Afterlife (AL)

hibernation sleep

3.1.2 UEFI/PI Firmware Images

flash device flash volume flash file system

3.1.3 Executables

PE32 file format fixed and dynamic address loading relocatable application vs driver boot and runtime memory

3.1.4 Programming

boot and runtime services boot service table guids handles and protocols protocols

3.1.5 edk2

build system

3.1.6 Security

Secure Boot

Signed Capsule Update

3.2 Windows

3.2.1 User Access Control (UAC)

3.2.2 Signing

3.2.3 Bitlocker

how does it work explain TPM

4 Attacks

attacks with escalating security mechanisms assumptions: read/write access to firmware image through exploit or physical access (spi clamp override)

4.1 No Secure Boot

dump image open with UEFITool add in NTFS driver remove previous NTFS driver if present, for full control, might be read only etc try in EFI shell navigate to Windows folder create folder try in code SimpleFileSystem Protocol iteration write failed on hibernated file patch to allow write on hibernated drivers pack executable binary as uefi module iterate over firmware volume protocols search for payload guid check size match override notepad works

but no automatic execution nor elevated privileges dll proxying dll hijacking

Task Scheduler defined in xml cached in registry edit with start cmd.exe and trigger manually whoami

chntpw and reged port to uefi edit Task in machine under Control export target registry key modify so that registry key can differ and found via matching values import and override registry key on target machine payload whoami

4.2 Secure Boot

expect not to boot no difference secure boot default policy snippet instead relies on Signed Capsule Updates

4.3 Bitlocker

secure boot or not boot execution differs from normal tpm values different bitlocker encryption fails recovery key prompt prompt is still during transient system load phase therefor uses uefi services such as SimpleTextInputEx Protocol explain more in depth how protocols are returned to the end user explain basic hooking explain how we retain information of the hook in question keylog recovery key key input advancment is weird and makes tracking hard alternatively screen shot still hook to find when enter is pressed explain how screenshotting works some basic compression

network stack wasn't installed onto handles when boot over ip was disabled compared loaded dxe drivers between both configurations Realtek Family driver not loaded load manually reinstall all handle to controllers to enable network stack regardless

sending key out is only good for physical access attack vector dislocker linux utility mount encrypted drive with decryption mean read and write access dual boot in vm enter password and it works port to uefi bitlocker encrypts block-wise uefi protocol stack hook block io again hook data mapping wait for recovery key send recovery key on enter press

hook ExitBootServices enable hook write payload import registry key disable hook

persistence when part of root of trust fresh install / tpm update values hook Trusted Copmuting Group 2 (TCG2) Protocol TPM communication receive bitlocker vmk key and send to dislocker

5 Discussion

attack assumption reflected to real world aplicability

social engineering aspekt

driver vorhanden und was mitbringen, debloating

5.1 Rootkit classification

statisken zu bilocker und secureboot auf systemen

industrie standard zur system security in firmen

5.2 Mitigations

hardware validated boot

inaccessible spi flash

tpm + pin detectability

googeln wie legitime recovery key prompt reaktion aussieht

enterprise policy on reovery key loss

5.2.1 User awareness

vermitteln was das prompt bedeuten koennte

aber kann man einfach nicht anzeigen lassen

Security Flaw of entering a Recovery Password in an inheritly unsafe System

enterprise doesnt hand out recovery keys and instead receives hard drive

!!!!!!!!!!!!!!!!!!!!!!!! without hardware chain of trust a compromised system can patch/change any software and fixes are impossible

Conclusion

6

List of Figures

List of Tables

A.1 This is a caption text. 19
A.2 This is a caption text. 20

List of Listings

Example Appendix

A

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

A.1 Appendix Section 1

This is the second paragraph. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

Alpha	Beta	Gamma
0	1	2
3	4	5

Tab. A.1.: This is a caption text.

A.2 Appendix Section 2

And after the second paragraph follows the third paragraph. Hello, here is some text without a meaning. This text should show what a printed text will look like

at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

Alpha	Beta	Gamma
0	1	2
3	4	5

Tab. A.2.: This is a caption text.

After this fourth paragraph, we start a new paragraph sequence. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

Declaration

You can put your declaration here, to declare that you have completed your work solely and only with the help of the references you mentioned.

City, June 21, 2016

Ricardo Langner