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

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

3.1.2 UEFI/PI Firmware Images

flash device flash volume flash file system

3.1.3 Images

file format application vs driver boot and runtime services boot service table protocols protocol handles

3.1.4 Secure Boot

TPM spi write

3.2 Windows

3.2.1 Bitlocker

3.2.2 UAC

3.2.3 Signing

4 Attacks

common assumption read/write access to firmware image through exploit or physical access

4.1 No Secure Boot

4.2 Secure Boot

4.3 Secure Boot and Bitlocker

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

6 Conclusion

List of Figures

List of Tables

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