OULUN YLIOPISTO
UNIVERSITY of OULU

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Ossi Herrala

FIXME FIRST FRONT PAGE TITLE LINE FIXME additional if needed

Bachelor's Thesis
Degree Programme in Electrical Engineering
FIXME: Month 2016

Herrala O. (2016) Secure Deployment Story for Challenging Environments. Department of Electrical Engineering, University of Oulu, Oulu, Finland. Bachelor's thesis, 13 p.

ABSTRACT

- **Background information (present tense)**
- **Principal activity (past tense/present perfect tense)**
- **Methodology (past tense)**
- **Results (past tense)**
- **Conclusions (present tense/tentative verbs/modal auxliaries)**

Keywords: sample, keywords

Herrala O. (2016) FIXME: Turvallinen käyttöönotto haastavissa ympäristöissä.
Oulun yliopisto, sähkötekniikan osasto. Kandidaatintyö, 13 s.

TIIVISTELMÄ

Esimerkkitiivistelmä

Avainsanat: esimerkki, sanoja

TABLE OF CONTENTS

FOREWORD

This LaTeX-template has been used by various people at department since the late 1990's, and has slowly improved over time. It is still somewhat rough at the edges, but hopefully will be helpful in reducing some of the pain involved in writing a diploma thesis.

Contributors to the template include Mika Korhonen (original author), Pekka Pietikäinen, Christian Wieser and Teemu Tokola. If you make any improvements to this template, please contact ouspg@ee.oulu.fi, and we will try to include them in further revisions.

The template was updated during the summer of 2013 by Juha Kylmänen.

ABBREVIATIONS

UDP	user datagram protocol
IP	Internet protocol
BOOTP	Bootstrap Protocol
TFTP	Trivial File Transfer Protocol
NFS	Network File System
RARP	A Reverse Address Resolution Protocol

1. INTRODUCTION

FIXME: TODO REMOVE THIS LIST

- INTRODUCTION: The Setting - bird eye's view - the challenge to be tackled / thing to be be improved in general
- INTRODUCTION: Past research done
- INTRODUCTION: Gap in knowledge/problem not yet solved
- INTRODUCTION: Purpose and method of this work
- INTRODUCTION: More detailed description what was done
- INTRODUCTION: Results acquired
- INTRODUCTION: Analysis and limitations of the result (Mostly relocate to Conclusions)
- INTRODUCTION: Value (Mostly relocate to Conclusions)

1.1. History

Loading operating system into computer remotely over network ("network booting", "diskless booting") has been used for decades already. Network booting could be used to bootstrap operating system installation or it could be used for diskless nodes to load the operating system and run it using disk provided by server.

Multiple procotols have been developed and used in combination to allow booting using UDP/IP network. Early published standards include RARP ("A Reverse Address Resolution Protocol", RFC903, published 1984[1]) or BOOTP ("Bootstrap Protocol", RFC951, published 1985[2]) could be used to allow "a diskless client machine to discover its own IP address"[2], TFTP ("Trivial File Transfer Protocol", RFC783, published 1981[3]) "may be used to move files between machines on different networks implementing UDP."[3].

Later developments include RARP and BOOTP to be superseded by DHCP ("Dynamic Host Configuration Protocol", RFC1531, published 1993[4]) and TFTP superseded by NFS ("Network File System", RFC1094, published 1989[5]) which "provides transparent remote access to shared files across networks."[5]

1.2. Current state

Alpine Linux's PXE Boot HOWTO[6] summarises the current situation:

> Alpine can be PXE booted starting with Alpine 2.6-rc2. In order to accomplish this you must complete the following steps:
>
> - Set up a DHCP server and configure it to support PXE boot.

- Set up a TFTP server to serve the PXE bootloader.
- Set up an HTTP server to serve the rest of the boot files.
- Set up an NFS server from which Alpine can load kernel modules.
- Configure mkinitfs to generate a PXE-bootable initrd.

As we can see, the whole process still relies on old protocols DHCP, TFTP, HTTP and NFS developed around 1980–1990. However, these protocols are not secure and should not be used over Internet.

1.3. Threats

Threats can be indentified in all components from hardware to operating system vulnerabilities. Table 1.3 lists some common known attacks.

Layer	Threat(s)
HTTP	malicious files
DNS	spoofing, hijack
NFS	MITM, malicious files
TFTP	MITM, malicious files
DHCP	spoofing, DNS hijack, TFTP hijack
Peripherals	backdoors
Hardware	backdoors

Table 1. Some threats to various components used in operating system installation over network

Hardware (e.g. physical server or laptop) and peripherals (e.g. displays, keyboards, mice, removable media) can have backdoored firmware. The backdoors could have been installed already on factory or firmware was infected with some malware previously ran on the machine.

DHCP and DNS protocols could be used to redirect future communications into malicious services. DHCP is commonly used to assign IP address to client and give various information (TFTP server's IP address, DNS servers' IP addresses). Malicious DHCP can take over future TFTP and DNS communications. DNS has many uses, but commonly it's used to translate host name into IP address and malicious DNS server could redirect future communications into malicious services.

TFTP, NFS and HTTP protocols could be used to deliver malicious files which when executed in target system could compromise the operating system installation and even firmwares of the hardware the operation was performed.

2. IMPLEMENTING SOMETHING

Your implementation.

3. TESTING SOMETHING

Your testing.

4. DISCUSSION

Your discussion.

5. CONCLUSION

- CONCLUSIONS: reference to purpose of study
- CONCLUSIONS: value of / reasons for the study
- CONCLUSIONS: review of important findings / conclusions
- CONCLUSIONS: comments, explanations or speculations about findings
- CONCLUSIONS: limitations of study
- CONCLUSIONS: implications of study or generalisations
- CONCLUSIONS: recommendations for future or practical applications - USUALLY SKIPPED

The best thesis evar.

6. REFERENCES

[1] Finlayson, Mann, Mogul & Theimer (accessed 26.5.2016.) RFC903: A reverse address resolution protocol. Tech. rep. URL: https://tools.ietf.org/html/rfc903.

[2] Croft B. & Gilmore J. (accessed 26.5.2016.) RFC951: Bootstrap protocol (BOOTP). Tech. rep. URL: https://tools.ietf.org/html/rfc951.

[3] Sollins K.R. (accessed 26.5.2016.) RFC783: The TFTP protocol (revision 2). Tech. rep. URL: https://tools.ietf.org/html/rfc783.

[4] Droms R. (accessed 26.5.2016.) RFC1531: Dynamic host configuration protocol. Tech. rep. URL: https://tools.ietf.org/html/rfc1531.

[5] Nowicki B. (accessed 26.5.2016.) RFC1094: NFS: Network file system protocol specification. Tech. rep. URL: https://tools.ietf.org/html/rfc1094.

[6] (accessed 26.5.2016.), PXE boot howto - Alpine Linux. URL: https://wiki.alpinelinux.org/wiki/PXE_boot.