Lab Project,
Final report

Group 5
Magnus Krane, Erik Sørensen, Piyush Bajpayee

{eriksore, magnkr, piyushb }@stud.ntnu.no
TTM4135 Information Security
March 7, 2013

Abstract

Introduction

1 Specific questions from the lab

1.1 Q1

Comment on security related issues regarding the cryptographic algorithms used to generate and sign your groups web server certicate (key length, algorithm, etc.).

1.2 Q2

Explain what you have achieved through each of these verications. What is the name of the person signing the Apache release?

1.3 Q3

What are the access permissions to your web servers conguration les, server certicate and the corresponding private key? Comment on possible attacks to your web server due to inappropriate le permissions.

1.4 Q4

Web servers oering weak cryptography are subject to several attacks. What kind of attacks are feasible? How did you congure your server to prevent such attacks?

1.5 Q5

What kind of malicious attacks is your web application (PHP) vulnerable to? Describe them briey, and point out what countermeasures you have developed in your code to prevent such attacks.

Conclusion

References

[1] ITEM, *Part 3 - Design and implementation of a resource allocation service*. NTNU, 2013. http://www.item.ntnu.no/fag/ttm4120/current/lab/lab3spread.pdf

List of Figures