Lab Project,
Final report

Group 5
Magnus Krane, Erik Sørensen, Piyush Bajpayee

{eriksore, magnkr, piyushb }@stud.ntnu.no
TTM4135 Information Security
March 8, 2013

Abstract

Introduction

The web could be argued to be one of the most important infrastructures in the world.

1 Discussions from the lab

2 Specific questions from the lab

2.1 Q1

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

For the web server certificate, the signature algorithm were chosen as SHA1 with RSA encryption, with a public-key length of 2048 bits. At the current time, RSA laboratories (creators of the RSA algorithm) recommends a 2048 bits key size for extremely valuable keys, and 1024 bits key size for corporate use [2]. Even 768 bits key might be regarded as sufficient. The use of 2048 bits key size in this case could therefore be regarded as 'over-the-top'. Ultimately the choice of key length is a trade-off between de-/encryption speed and security.
SHA1 were chosen over Md5 as message digest due to known security problems with Md5

2.2 Q2

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

2.3 Q3

What are the access permissions to your web servers configuration files, server certificate and the corresponding private key? Comment on possible attacks to your web server due to inappropriate file permissions.

2.4 Q4

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

2.5 Q5

What kind of malicious attacks is your web application (PHP) vulnerable to? Describe them briefly, 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, downloaded Feb 27th 2013.

[2] RSA Laboratories, *How large a key should be used in the RSA cryptosystem?* http://www.rsa.com/rsalabs/node.asp?id=2218, downloaded Mar 8th 2013.

List of Figures