UNIVERSITEIT VAN AMSTERDAM

MSc. System and Network Engineering

SSN Project

”SSL session key extraction from memory on Android mobile devices”

Stamatios Maritsas - Stamatios.Maritsas@os3.nl
Yadvir Singh - Yadvir.Singh@os3.nl
Kenneth van Rijsbergen - Kenneth.vanRijsbergen@os3.nl

December, 2015

Abstract

asjhdjahfslkdffsd

Contents

Chapter 1

Introduction

1.1 Your Section title Here

Chapter 2

Related Work

The article by Gursev Singh Kalra, titled Extracting RSAPrivate- CrtKey and Certificates from an Android Process, describes how to dump X.509 certificates and construct a RSA private key (RSAPrivate- CrtKey) from the Android application memory using Eclipse Memory Analyzer Tool (MAT) and Java code. This paper gave us the indication that there are possibilities to extract the keys from a running process.[1]

Chapter 3

Approach

3.1 Heap dumping

3.2 Dynamic code instrumentation (Frida)

Chapter 4

Experiments

4.1 Setup

4.1.1 Traffic capture

Proxy server

Wireshark

4.1.2 Desktop/Smartphone Setup

Chapter 5

Results

Chapter 6

Conclusion

Chapter 7

Attack Limitations

Chapter 8

Contribution

Bibliography

[1] Gursev Singh Kalra. Extracting rsaprivatecrtkey and certificates from an android process. http://blog.opensecurityresearch.com/2013/10/extracting-rsaprivatecrtkey-and.html, 2013.