A FRAMEWORK TO EVALUATE SECURITY OF SAME KEY USED IN CRYPTOGRAPHIC PRIMITIVES

Wijemanne Mohottige Dona Lakmali Wathsala Wijemanne

(118234T)

Degree of Master of Science

Dept. of Computer Science and Engineering

University of Moratuwa

Sri Lanka

June 2013

A FRAMEWORK TO EVALUATE SECURITY OF SAME KEY USED IN CRYPTOGRAPHIC PRIMITIVES

Wijemanne Mohottige Dona Lakmali Wathsala Wijemanne

(118234T)

Thesis submitted in partial fulfillment of the requirements for the Degree of MSc in Computer Science

Dept. of Computer Science and Engineering

University of Moratuwa

Sri Lanka

June 2013

"I declare that the work included in this report was done by me, and only by me, and this project report does not incorporate without acknowledgment any material previously submitted for a Degree or Diploma in any other University or institute of higher learning to the best of my knowledge. And to my belief it does not contain any material previously published or written by another person except where the acknowledgment is made in the text. Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my thesis, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books)".

Signature: Date:

"I certify that the declaration made above by the candidate is true to the best of my knowledge and she has carried out research for the Masters thesis under my supervision.".

Signature of the supervisor: Date:

Abstract

The convention in cryptography is to use separate key for separate activities and is known as the key separation principle. However, use of same key pair for different cryptographic primitives has become an interesting topic among the challenging ideas emerging to the area of cryptography. Because, such usage of same key has significant advantages as it reduces storage requirements for certified keys, cost of key certification and time taken to verify certificates, and reduces the footprint of cryptographic code. Research activities that had been carried on this regards, had concentrated on combining available cryptographic schemes, with same or related keys to construct new combined schemes without compromising the levels of security that the schemes preserved when operating distinctively. Others had concentrated on developing single schemes that achieves both encryption and signature functionalities under same key, with the help of techniques such as padding. Apart from combining different cryptographic primitives, in order to determine the concept of agility, ability of combining multiple instantiations of same cryptographic primitive with same key were also been tested. Considering those innovative attempts in combining schemes with same key, in 2011, Paterson *et al.* have raised an open research problem, 'under what general condition is it safe to use same key across multiple instantiations of same or different cryptographic primitives'. This research is carried out with the intension of providing a satisfactory answer to the above mentioned open research problem.

After identifying and classifying the cryptographic primitives and their instantiations that has been constructed over the time, three primitives and their instantiations were selected for the research. Under Public Key cryptosystems, Encryption, Signature and Pseudorandom sequence were selected along with their well-known multiple instantiations. These instantiations were studied to understand their functionalities and to determine algorithmic weaknesses and already existing operational vulnerabilities.

The research results a framework, which can be used to evaluate the security of multiple instantiations of different cryptographic primitives of user's choice. Through an analysis of the framework components one can estimate the

additional advantage caused by same key usage for adversary. Two test cases, for RSA and ElGamal encryption/signature combination, are presented in the thesis to validate the framework. As different real world applications may require different levels of security, one can decide that which schemes should be used with same key based on the analysis of the framework.

Keywords: Combined schemes, same key usage, encryption, signature, signcryption

Acknowledgment

First and foremost I offer my sincerest gratitude to my supervisor, Dr Chandana Gamage, who has supported me throughout my thesis with his supervision, encouragement and immense knowledge whilst allowing me the room to work in my own way.

Apart from my supervisor I would like to thank my MSc course coordinator Dr. Shehan Perera and research coordinator Dr. Malaka Walpola for their encouragement, insightful comments and guidance given throughout the research duration.

All the lecturers including Dr. Shantha Fernando, Dr. Vishaka Ratnayake, Dr. Gihan Dias, Dr. Chathura De Silva and Dr. Shahani Markus for immense knowledge, support and motivation given throughout the MSc program.

I wish to express my gratitude to all my MSc batch mates as well, for their constrictive comments and friendly encouragement given throughout the MSc program.

Last but not least, I would like to thank my family, especially to my husband whose constant encouragement and support was crucial for the completion of this thesis.

Contents

List of Tables

List of Figures