Project Description Form

M. Sc Information Security

One copy of this form (or a typed or computer-generated version) is to be completed by each project student and sent (by email) to the project supervisor **by the end of the second semester at the latest**. If the project supervisor is satisfied with the contents then they should sign the form for their own records and inform the student. The student should keep a copy of the final project description form. If the project starts to deviate significantly from the originally approved proposal then the student should discuss this with the project supervisor and, if necessary, complete a revised form.

TO BE COMPLETED BY THE PROJECT CANDIDATE

Name:

Contact email address(es):

Provisional Title of Project: Low Level Security Analysis of GlobalPlatform Card.

1. Statement of Objectives

a. What do you intend to achieve?

- Review relevant existing literature on security of smart cards.
- Review the security provisions of the components of GlobalPlatform (GP) card specification
- Compare GlobalPlatform card specification security with Multos
- Identify whether the operation of the mechanisms can be formalised and analysed by using formal methods or state analysis machine tools.
- Examine how GP specifications are adopted by the mobile phone industry in terms of secure element.

b. Why have you chosen the proposed project?

Technology is moving towards the convergence of card usage i.e. consumers using just one chip for making phone calls, identification, financial services and transportation, etc. There is therefore the need to improve/enhance the security of smart cards in order to encourage consumers to accept this emerging technology as not only being convenient, but safe and secure. GlobalPlatform card specification is widely adopted and supported by the smart card industry in view of its non-proprietary nature. The objective of this dissertation is therefore to investigate its existing smart card security provision, how it is being adopted in the financial and phone industry and recommend improvements where necessary in order to enhance the security required for the emerging smart card usage.

2. Methods to be used

a. How do you intend to achieve the objectives listed above?

The project is mostly theoretical in nature and GlobalPlatform security protocols are well documented in academic literature. Based on my findings, I would select some of the most widely used GP protocols and analyse them using formal methods or state machine analysis tools. The result derived from the formalisation process would be thoroughly analysed with a view to highlighting any security weaknesses in them and making recommendations for improvements.

b. What is your strategy for getting started?

The project requires extensive review and analysis of GlobalPlatform Card security provisions. I intend exploring available literature through written text books, on-line resources (internet search engine) and published academic research project works. For the practical part, I intend using available protocol analysis tools.

3. The work plan

Provide a rough schedule, showing any key milestones in the project.

PROJECT OUTLINE

Abstract
Acknowledgements
Table of Contents
List of Figures

Chapter 1: Introduction

- Introduction (3 pages)
- Motivation (1 Page)
- Structure of the Project (2 pages)

Chapter 2: Smart cards

- History and Evolution of Smart cards (2 pages)
- Types of Smart cards (2 pages)
- Current industrial Usage (2 pages)

Chapter 3: GlobalPlatform Card

- History of GlobalPlatform (2 pages
- Membership (1 page)
- Evolution of Card Specifications (2 pages)
- Importance of GP Standards (3 pages)

Chapter 4: Multos Operating System

- History of Multos (2 pages)
- Membership (1 page)
- Multos Security Provisions (3 pages)
- Multos Implementations (4 pages)

Chapter 5: GlobalPlatform Implementations

- GP implementations in the Financial industry (4 pages)
- GP implementation in the Mobile Phone Industry (4 pages)
- GP Implementations in other industries. (4 pages)
- Comparison of implementations between financial and mobile phone industries. (4 pages)
- Some known attacks on GlobalPlatform smart cards (5 pages)

Chapter 6: Secure Channel Protocols Analysis

- Formalisation of some GlobalPlatform card protocols (12 pages)
- Analyses of the result of the formalisation (3 – 4 pages)
- Recommendations (1 - 2 pages)

Chapter 7: Conclusion

- Conclusion (2 pages)
- Areas of Further research (1 page)

Appendix(es) (2 - 4 pages)

Bibliography (4 pages)

4. Additional comments

Use this section to make extra comments on the proposal on matters not covered above (use extra space if necessary). Include details of any involvement of external organisations.

S/No	Activity	Submission Date
1	**Submission of chapters 1 – 3 to Project Supervisor for review**	**30th April 2010**
	Collection of Project Supervisor's Review	26th May 2010
	Incorporation of Project supervisor's review	28th May 2010
2	**Submission of chapter 4 to Project Supervisor for review**	**4th June 2010**
	Collection of Project Supervisor's Review	15th June 2010
	Incorporation of Project supervisor's observations	17th June 2010
3	**Submission of chapter 5 to Project Supervisor for review**	**18th June 2010**
	Collection of Project Supervisor's Review	29th June 2010
	Incorporation of Project supervisor's observations	1st July 2010
4	**Submission of chapters 6 & 7 to Project Supervisor for review**	**16th July 2010**
	Collection of Project Supervisor's Review	27th July 2010
	Incorporation of Project supervisor's observations	29th July 2010
5	**Full Project submission for review**	**30th July 2010**
	Collection of Project Supervisor's Review	26th August 2010
	Incorporation of Project supervisor's observations	30th August 2010
6	**Project Submission to College**	**1st Sept. 2010**

TO BE COMPLETED BY THE PROJECT SUPERVISOR

I approve the attached project plan.

Signed:

Name:

Date: