Dissertation Project Proposal - Research on cryptographic backdoors

Name: Bancha Upanan
Student ID: 1604026

20th June 2016

1 Aim

This project aims to study malicious and surreptitious weakening cryptographic systems focusing on NIST's backdoored Dual EC pseudorandom number generator and discuss the security against mass surveillance. Finally I will implement attacks on TLS along with relevant countermeasures.

2 Plan

A tentative plan for the completion of this MSc project and the tasks involved are shown as a set of milestones, accompanied with an estimated date for finishing each milestone as follows.

Research on cryptographic backdoors - 8th July 2016, 3 weeks

- Susceptible cryptographic systems to sabotage
- Exploitability of Dual EC pseudorandom number generator
- Practical attacks on TLS

Application implementation - 5th August 2016, 4 weeks

- Systems design
- Development
- Integration and testing
- Deployment

Data collection and presentation preparation - 19th August 2016, 2 weeks
Presentation - 22nd August 2016, 1 week
Report writing - 9th September 2016, 3 weeks