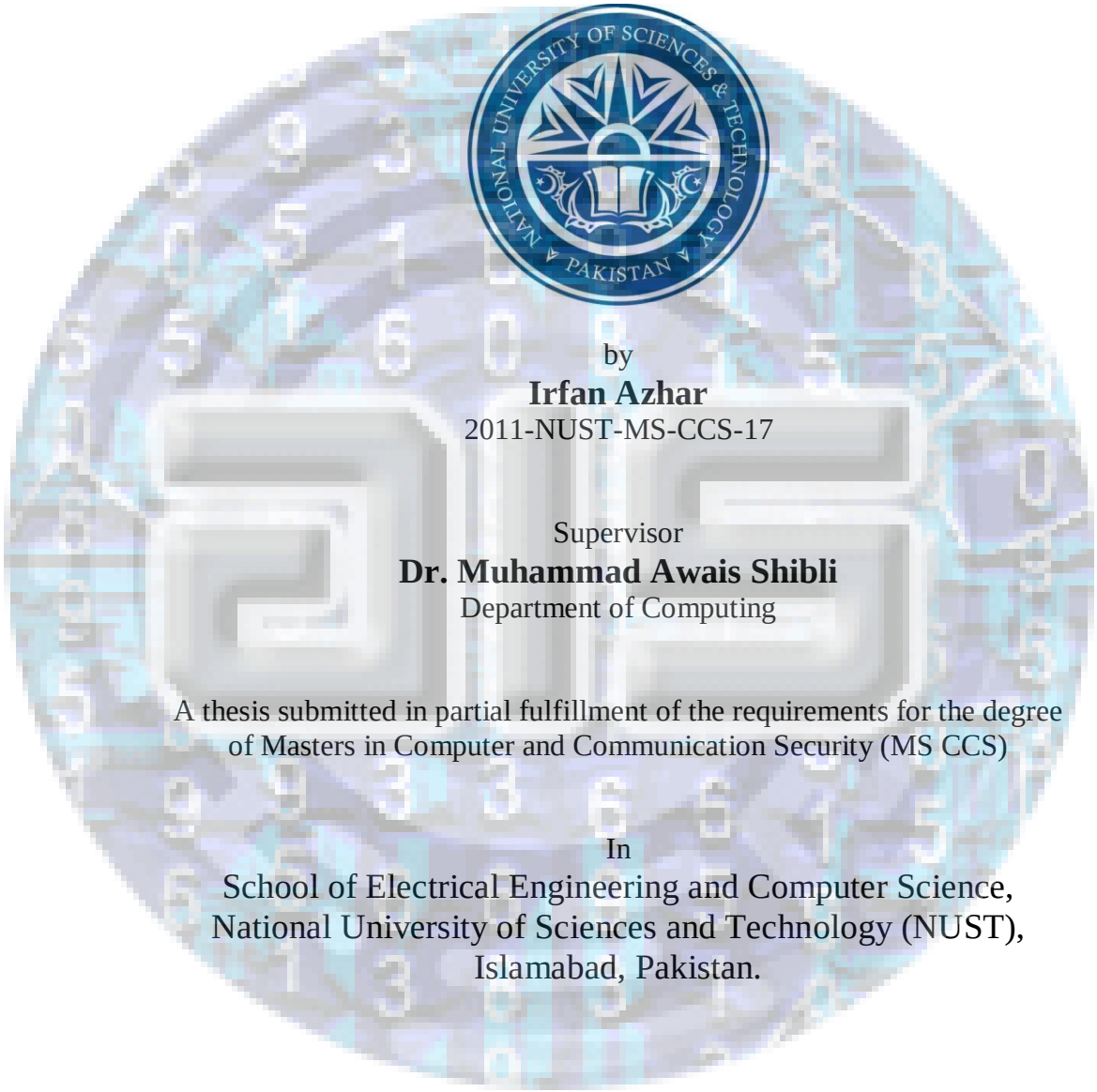
KEEPING KEYS SECRET IN PHYSICALLY ACCESSIBLE HOSTS



by

Irfan Azhar

2011-NUST-MS-CCS-17

Supervisor

Dr. Muhammad Awais Shibli

Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters in Computer and Communication Security (MS CCS)

In

School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(March, 2015)

Abstract

Security of secret keys stored on a user's machine is not assured and such an endeavour is indeed a daunting task. Careless handling of keys on physical y accessible hardware could easily mean loss of crypto material to unauthorized access. If an attacker can achieve access to a binary code, then well-known key-finding techniques and tools come handy to extract and compromise the key material. This thesis proposes and demonstrates a new technique for securing keys in storage and in software. In that, randomly generated bit-strings of a crypto key are 'transformed' into a set of randomized functions. This set is compiled and obfuscated to form part of a security critical application. Inverse transform is calculated dynamically to retrieve and use original bit-strings of the embedded key. It is demonstrated here that new methodology is effective against entropy based disc-surfing tools that scan host's memory devices/entities.