UNIVERSITI TEKNOLOGI MARA

A FIRMWARE-BASED CHAINED CRYPTOGRAPHIC ATTESTATION PROTOCOL FOR SECURE EMBEDDED SYSTEM COMMUNICATION APPLIED IN U-BOOT BOOTLOADER

MOHD ANUAR BIN MAT ISA

Thesis submitted in fulfillment
of the requirements for the degree of
Doctor of Philosophy

Faculty of Electrical Engineering

November 2018

ABSTRACT

An increasing amount of attention is being given by researchers to the issues surrounding the security of embedded systems in recent years due to the emergence of IoT, and the proliferation of attacks on embedded systems. Recent research has suggested that embedded firmware in numerous embedded computing devices are not well protected compared to computing devices with comprehensive operating systems. This happens due to the lack of support for security enforcement stemming from the constrained environment of embedded systems. Due to this limitation, an adversary will compromise the lean and weak cryptographic protocols of the embedded devices by revealing its confidentiality, altering integrity and forging identities. Side-channel attacks such as timing attacks on a cryptographic computation, and relay attacks on Radio Frequency (RF) communication are mounted by the adversary to increase the probability to break weak cryptographic protocols in embedded systems. To address these matters, this work explores security issues particularly on the lack of secret key distributions for embedded firmware, and the lack of attestation between parties in embedded system communication. DenX Universal Boot Loader (U-Boot) firmware was chosen as the target of this study because it is widely used by embedded developers for booting embedded Operating Systems (OSs) that run on smartphones, tablets, Wi-Fi access points etc. The latest U-Boot source code distribution has shown that the preinstalled symmetric encryption scheme, namely AES128 is vulnerable to a session reveal attack because the preinstalled secret key is never renewed after U-Boot firmware is flashed due to the lack of a key distribution protocol in the U-Boot implementation. To address this issue, the thesis has proposed the Chained Cryptographic Attestation Protocol (CCAP), which allows U-Boot to establish a secure key exchange and provide an attestation between device-to-device connectivity. It also offers security against adversary attacks, namely session state reveal attacks, forward and backward secrecy, key independence, key derivation function attacks, replay attacks, timing attacks and relay attacks respectively. Two case studies were selected for an experimental study of the CCAP. The first is on a unique session identity attestation; and a secure secret key distribution for the U-Boot firmware. The second case study is on a technique to prevent a relay attack for an automotive smart key. The ARM RaspberryPi 2 (microprocessor) and ARM STM32F746G-DISCO (microcontroller) boards were used in the experiments. The first case study results had shown that 2048-bit CCAP executed within 6 seconds when CPU instruction and data caches were enabled. The extra 6 seconds for running the security protocol can be considered quite insignificant to U-Boot performance because it typically takes around 5 to 15 seconds to download 4 MB kernel image using a TFTP network boot. The second case study results have shown that 128-bit CCAP has been able to detect relay attacks whereby in such a circumstance the RF communication is delayed by at least twice compared to the non-relayed RF communication. Both case studies have shown that the CCAP is reliable to detect and prevent the aforementioned security attacks. The experiment has shown that CCAP cryptographic computation takes 2.6% until 9.5% more time to execute than the original unsecured Diffie-Hellman (DH), whereby another work by Fiore and Gennaro was shown to be 50% slower using their secure DH protocol.

ACKNOWLEDGMENT

I wish to convey my heartfelt gratitude to Professor Dr. Habibah Hashim and Dr. Jamalul-lail Ab Manan for their help on my journey for this research work as well as the thesis. Without them, I could not have ever imagined that this day would ever happen.

I would like to express my thanks to my family and friends for their support during the Ph.D. journey. I also want to acknowledge the Ministry of Education (MOE) Malaysia for providing various research grants (FRGS, ERGS and PRGS) and Universiti Teknologi MARA for supporting the research work. Thank you.

TABLE OF CONTENTS