Smartphone based Authentication & Authorization Protocol for Smart Physical Access Control System (SPACS)

By
Faisal Karim Bhutta
2010-NUST-MSCCS-02

Supervisor
Dr. Abdul Ghafoor
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.

(January 2014)

Abstract

Nowadays smartphone is becoming multi-purpose device because it has more processing power at affordable cost. The trend of using smartphone for business, banking and everyday tasks has attracted research community to address security issues in smartphone applications and their communication with external systems. Due to their wide acceptability in community public, it is becoming trivial to use smartphone as an authenticating device for banking applications and access control management systems. Current legacy solutions used for Physical Access Control System (PACS) are combination of software and hardware to control the access of users to physical resources (rooms, offices, buildings etc). Most of them are using biometric or smart card as an identity token. The associated cost and limited freedom to customize these solutions to organizational needs open research areas for smartphone researchers to use them in PACS. In our research, architecture for PACS along with security protocol for smartphone is designed that is used for identity verification, authentication and authorization in PACS.

The designed authentication protocol is an extension of two-factor authentication protocol described in FIPS-196 standard. Furthermore, the usage of symmetric key cryptography provides an efficient solution to achieve confidentiality of messages exchanged between components of designed PACS. In order to ensure the presence of the legitimate user in the premises, the system uses a pass-code feature that is only valid for one time usage. Hence using designed protocol, user's smartphone can act as authenticator in the system. Since, the solution may be used by the non-technical persons so it is designed that it should be user friendly and require minimum efforts for configuration of security parameters. In order to validate the security of designed protocol, automated protocol verification tool Scyther is used. After validation, it is verified that our security protocol resists against Man-in-the-Middle, replay and attacks on confidentiality of user's credentials.