TITLE OF THE PROJECT

Design and Formal Analysis of an Authentication Protocol, eWMDP on Wearable Devices

GROUP-4

- Akhil Sourav [S20180010007]
- Aman Shrivastava [S20180010010]

ABSTRACT

Since there is an increase in wearable devices, hackers are targeting these devices as they do contain some important info, or sometimes service providers data breach can cost huge damage. In particular, hackers can launch multiple attacks, such as DDoS attack, man-in-the-middle attack, and reflection attack, which may cause huge destruction to wearable devices. It is cleared that security analysis of protocol has a great importance to defend these attacks. Especially for authentication protocols whose security analysis have been developing rapidly in recent years. Formal semantics analysis of authentication protocol is a hot topic in current research. **This paper proposes an authentication protocol eWMDP for wearable devices** which surpasses another existing wearable authentication protocol (WMDP) due to its injective auth property. Also, Scyther and tamain-prover have confirmed that eWMDP is better than WMDP.

PLAN OF IMPLEMENTATION

Performance Analysis

eWMDP is found to be better than WMDP in several aspects, including Enc(number of encryption), SKR (secrecy property), Int (interaction wheel number), Ran(number of random), Dec (number of decryption), h (number of hash), non-A (non-injective authentication), and Injec (injective authentication) where WMDP failed to satisfy the last two security properties.

EXPERIMENTAL SETUP

System Configuration

The two communication roles, server and client in the protocol run on PC & Ti CC3200 LAUNCHPAD respectively. The server program runs in Ubuntu operating system (Intel i5 8th gen @2.4Ghz) which is implemented in C language and compiled by GCC in CCSv7 platform.

Libraries Used

We are planning to use OpenSSL Library for deploying the security algorithm on the server side to invoke different APIs .Based on our comprehensive search we found that **MIRACL** is better than JPBC Library because it is the gold standard for Elliptic Curve Cryptography and additionally supports over twenty protocols based on the new paradigm of Pairing-Based Cryptography. On the client side we are planning to use CC3200 SDK 1.3.0 Library .

SUMMARY OF THE RESULTS

It is expected that eWMDP protocol will show good performance as it holds in secrecy, non-injective authentication and injective-authentication properties. Under various configurations and in combination of different encryption algorithms and hashing algorithms eWMDP outperforms WMDP with higher transmission efficiency.