Privacy-Preserving Protocol Based On Bluetooth Encrypted Data Sharing

Wangzhihui Mei 2019124044 Hongyi Huang 2019180029
Zijia He 2019124057 Chang Xu 2019180034
Tianyu Jin 2019180030 Zhanping Zhou 2019124060
Senmiao Liu 2019180036 Caiming Qian 2019124036

CCNU-UOW JI

maywzh@gmail.com

May 10, 2020

Overview

Introduction

- Background
- Requirement

Protocol

- Analysis
- Proposed Protocol
- Bluetooth Data Transmission

Security and Functionalities

- Security
- Functionalities

Background

The pandemic of COVID-19 is devastating, which has caused global impact.
The ”health code”, as a pass for returning personnel, records the individual’s health and takes the form of ”green code”, ”red code”, and ”yellow code” to dynamically detect data.

Requirement

- The personal information is hidden to server
- Location and time window of infected ones is possible
- Statistical data is available
- Information transferred between parties should be protected

Analysis

- Privacy should be kept on local device except for being infected
- All data transmission process should be encrypted
- The client is anonymous to other clients and servers

Protocol I

- Periodic Rolling Exposure Key(PREK)
- Interval Proximity Identifier Key(IPIK)
- Encrypted User Metadata Key(EUMK)

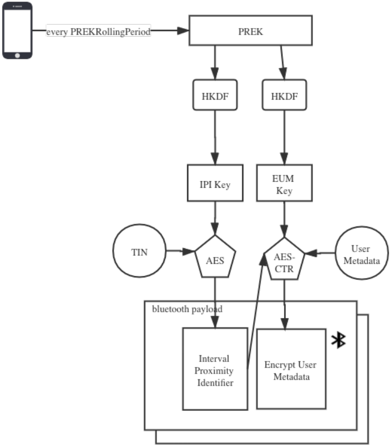

Figure: Key generation and Encryption

Protocol II

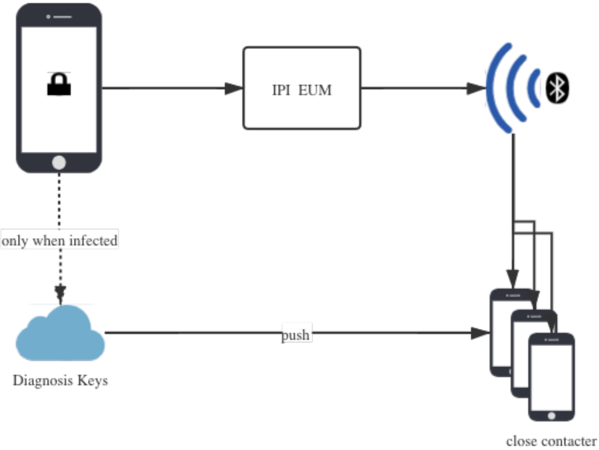

Figure: Data transmission

Mathematic Details

$$\mathit{TIN}(\mathit{timestamp}) \leftarrow \mathit{timestamp}/(60\times 15)$$

$$i \leftarrow \lfloor \mathit{TIN}(\mathit{timestamp})/\mathit{PREKP} \rfloor \times \mathit{PREKP}$$

$$\mathit{PREK}_i \leftarrow \mathit{CRNG}(16)$$

$$\mathit{IPIK}_i \leftarrow \mathit{HKDF}(\mathit{PREKP}_i, \mathit{NULL}, \mathit{UTF}8(\text{"}\mathit{IPIkey}\text{"}), 16)$$

$$\mathit{IPI}_{i,j} \leftarrow \mathit{AES}_{128}(\mathit{RPIK}_i, 0 || \mathit{TIN}_j)$$

$$\mathit{EUMK}_i \leftarrow \mathit{HKDF}(\mathit{PREK}_i, \mathit{NULL}, \mathit{UTF}8(\text{"}\mathit{EUMKey}\text{"}), 16)$$

$$\mathit{EUM}_{i,j} \leftarrow \mathit{AES}_{128} - \mathit{CTR}(\mathit{EUMK}_i, \mathit{IPI}_{i,j}, \mathit{BLEMetadata})$$

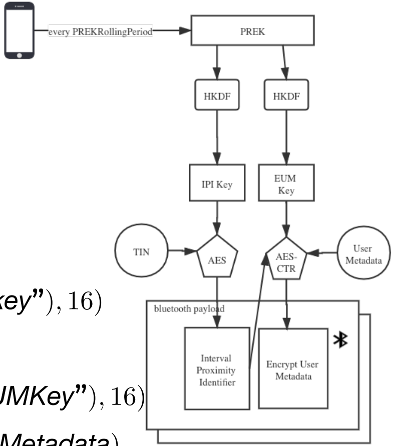

Figure: Key generation and Encryption

Bluetooth Data Transmission

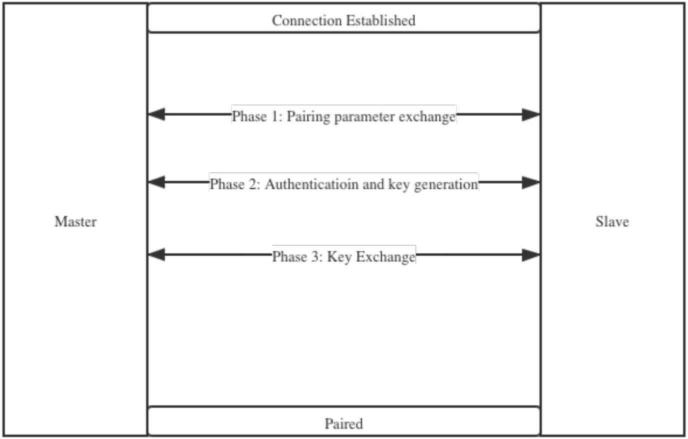
Connection Established
Phase 1: Pairing parameter exchange
Phase 2: Authenticatioin and key generation
Master
Slave
Phase 3: Key Exchange
Paired

Figure: Bluetooth Data transmission

Security

- Only infector's Periodic Rolling Exposure Key will upload to the cloud server
- The encrypted metadata cannot be decrypted without PREK
- Client-to-client communication is based on authenticated Bluetooth data transmission

Functionalities

- Data statistics is possible as the register data can be collected.
- Location and time windows of infected can be tracing.

The End