SecHack365

接触確認アプリのセキュリティ・プライバシーリスク評価

研究駆動コース　野本一輝

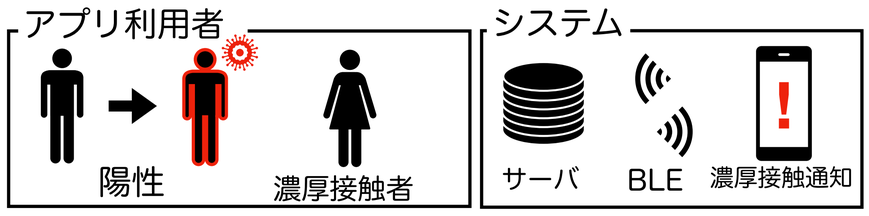
接触確認アプリのセキュリティ・プライバシーは？
攻撃者より先に問題を見つけて対処したい！！

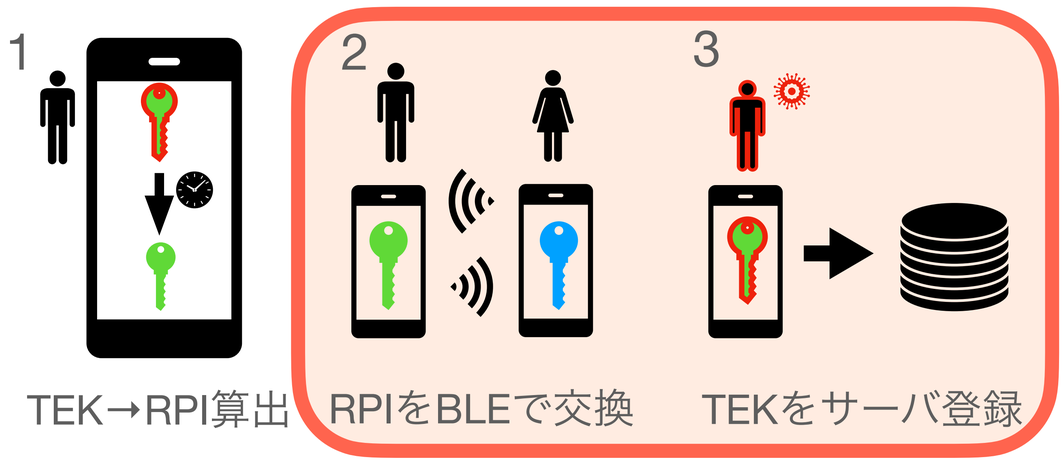
「陽性者特定攻撃」と「偽濃厚接触攻撃」を発見!
攻撃手法と対策について紹介するよ

接触確認アプリの仕組み

接触確認アプリの仕組みについて解説する。世界38ヶ国でGoogle/Appleが開発した
Exposure Notificationフレームワークが用いられている。(COCOA含む)

TEK (Temporary Exposure Key) : 24時間ごとに変動する識別子
RPI (Rolling Proximity Identifier) : TEKからおよそ20分おきに生成される識別子





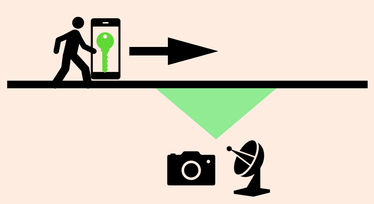
TEK→RPI算出　RPIをBLEで交換　TEKをサーバ登録 → 陽性者特定攻撃

陽性者TEKが配信　陽性者TEKとRPIを比較　濃厚接触判定 → 偽濃厚接触攻撃

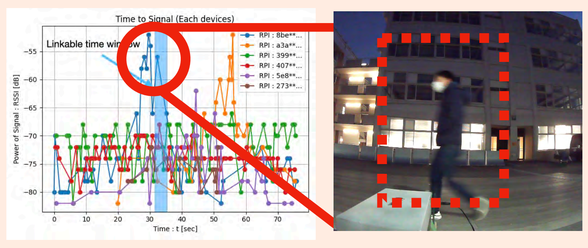
陽性者特定攻撃

攻撃者が陽性者の顔写真を特定する攻撃である「陽性者特定攻撃」の攻撃手法について解説する。

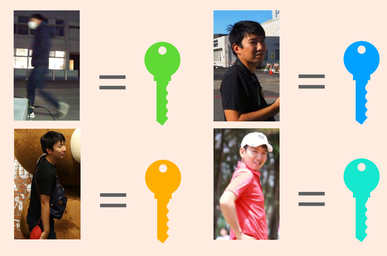
Bluetooth Low Energy受信機
Webカメラ・ログペリアンテナ



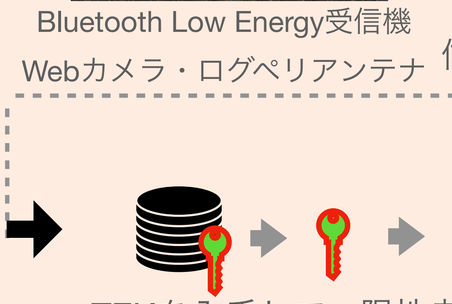
信号強度・RPI・カメラ画像を記録



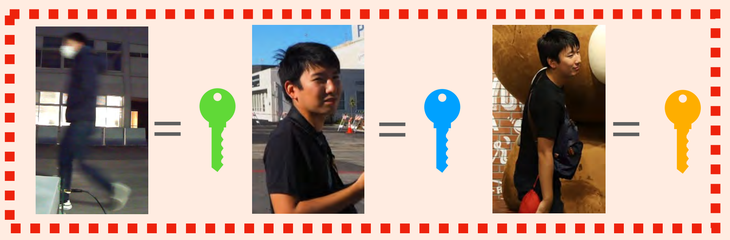
時間-信号強度グラフ　カメラ画像



アプリ利用者の画像とRPIを紐付ける



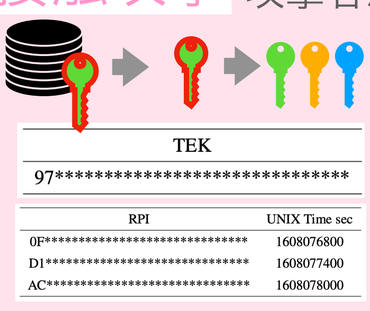
紐付けたアプリ利用者の画像とRPI
陽性者のRPIを比較



陽性者の写真が特定

偽濃厚接触攻撃

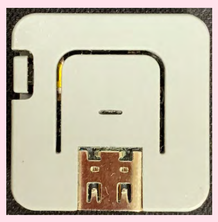
攻撃者が偽の濃厚接触者通知を引き起こす「偽濃厚接触攻撃」の攻撃手法について解説する。



TEK
97**********

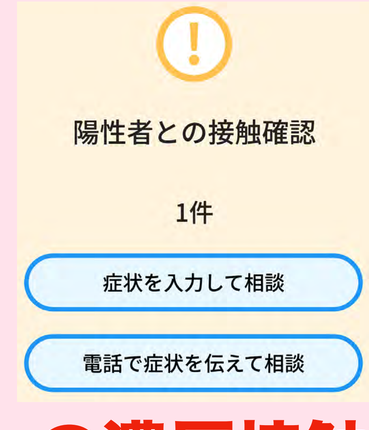
RPI	UNIX Time sec
0F**********	1608076800
D1**********	1608077400
AC**********	1608078000

TEKからRPIを算出



Bluetooth Low Energy 送信機
M5 Atom Lite

過去の時刻に設定した
スマートフォン



ニセの濃厚接触通知

対策

対策の検討と評価について解説する。また、本攻撃について関係機関への情報共有を行った。

陽性者特定攻撃の対策
- 信号発信強度の調整
- 信号発信周期の調整
- 複数RPIを用いた判定方式

偽濃厚接触攻撃の対策
- 判定対象とするRPIの適正化
- 時刻変更の記録と制限
- TEKダウンロード時の認証の追加

陽性者特定攻撃：Google・Appleに報告，ICSS・NDSSポスターセッションで発表
偽濃厚接触攻撃：JPCERT/CC・COCOA公式サポート・Googleに報告

国立研究開発法人 情報通信研究機構

著者
野本一輝
SecHack365 2020
研究駆動コース
nomoto@seclab.jp

外部発表

NDSS Poster: Can the Exposure Notification Framework Expose Personal Information?
Kazuki Nomoto, Mitsuaki Akiyama, Masashi Eto, Atsuo Inomata, and Tatsuya Mori

ICSS Exposure Notification Frameworkがもたらすプライバシーリスクの評価と対策
野本一輝・秋山満昭・衛藤将史・猪俣敦夫・森達哉