NFCとセキュリティ

Fourteenforty Research Institute, Inc.
株式会社 フォティーンフォティ技術研究所
http://www.fourteenforty.jp

シニア・リサーチ・エンジニア
鈴木 秀一郎

背景

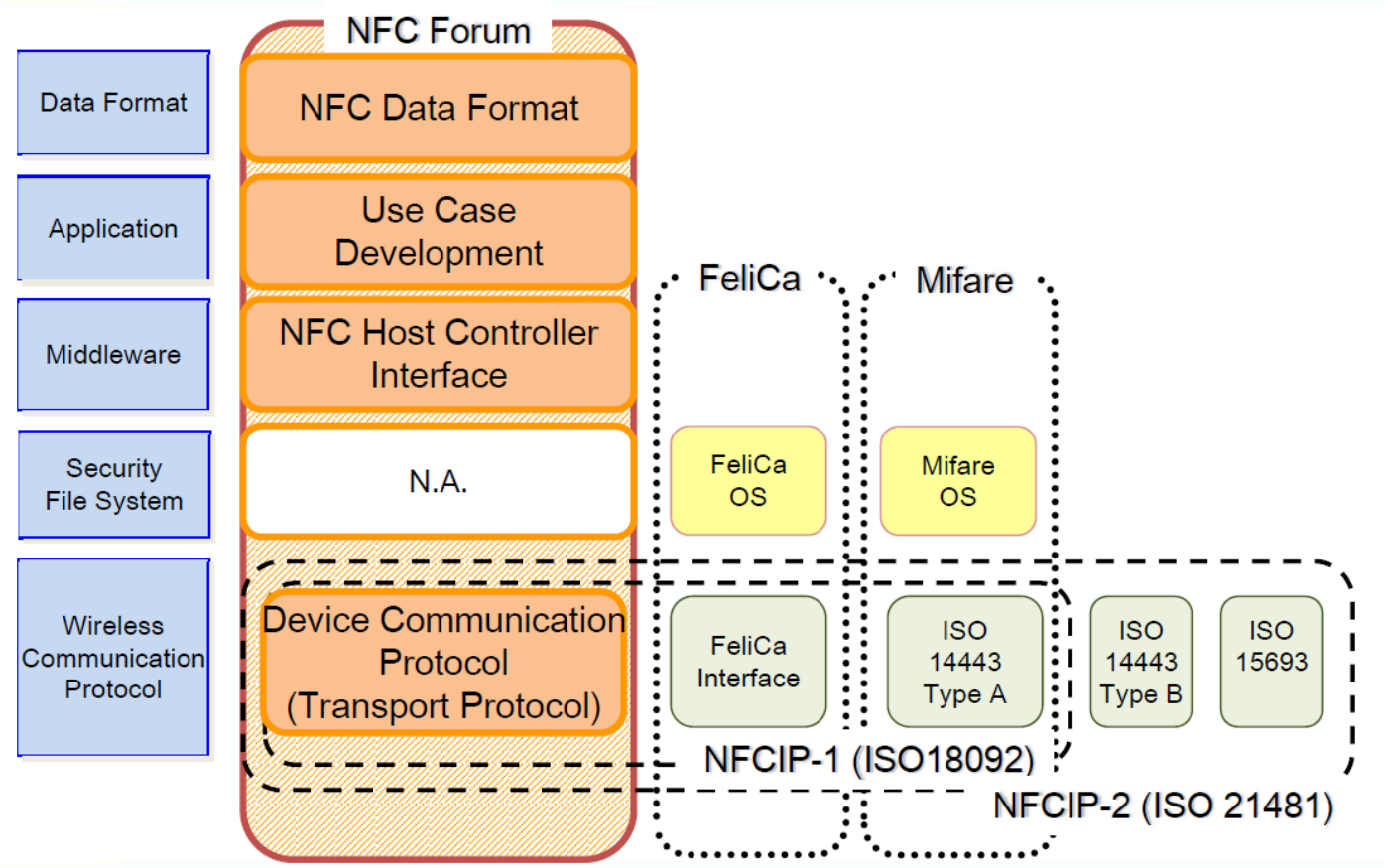
- 国内のスマートフォンでNFC機能の搭載、利用が進んできている
- さまざまな利用方法やサービスが考えられており、今後普及するものと思われる
- 一般開発者もAPIを通じて機能を利用することができ、NFC利用アプリも増えるものと思われる
- 新たな技術が利用される場合にセキュリティ上の問題が現れることが多い

NFC技術の利用においてセキュリティ上どのような問題が考えられるのか、現状を調査する必要がある

NFCとは

- Near Field Communicationの略。「近距離無線通信」という意味。
- 一般的には、近距離無線通信を利用した技術全般を指す。
- ただし、スマートフォン等でNFC対応などという場合、通信規格TypeA, TypeB（後述)を用いたデバイス、機能を指すことが多い。
- これは、これまで国内で利用されてきた主要なNFCの応用であるFelicaと区別する意味で使用されている
- NFCデバイスに関して、NFC Forum(www.nfc-forum.org/)にて標準化が進められている。

NFC関連技術の関係



NFCのコンセプトとNFC Forumの主要な活動（http://www.sony.co.jp/Products/felica/events/data/201110_B-1.pdf)より引用

世界的な流れ

- 世界的にNFCデバイスが普及しつつある
- NFCデバイスは日本では昔から存在しFelicaが最も普及しているが、世界的には、別の規格(TypeA, TypeB)が普及しつつある
- AndroidはNFCにすでに対応しており、iPhoneについても対応するのではないかと言われている。

国内の流れ

- NFCデバイスは日本では以前よりFelicaが最も普及している
- ただしFelicaはSonyの独自規格
  - 世界的には普及していない
- Felicaは鉄道での利用や、携帯（モバイルFelica）の利用が前提であるため、NFCでできることの一部しか実装されていない

  → Androidデバイス等のNFCでは、P2P（デバイス間通信）、タグリーダー機能などが使える
- AndroidのNFCへの対応などにより、NFCに対応する端末が増えてきており、国内でも決済サービスが提供され始めている
- FelicaからNFCへの移行が進むのではないかと考えられている

NFC関連のセキュリティ状況

- NFCの規格自体はセキュリティ(データの暗号化、通信相手の認証等)に関して規定しない
  - 通信方法やデータフォーマットのみを規定
- 盗聴に対してそのままでは脆弱
  - Security in Near Field Communication
- ただし、「近距離」であることが、一つのセキュリティ対策となっており、攻撃シナリオとして現実的なものは少ない
  - 盗聴を行うには、攻撃者が対象に物理的に近づく必要がある
- NFCで実現されるサービスのデータセキュリティは別のレイヤで実装される
  - Felica OS
  - Mifare OS

Secure Element

- NFCに関するセキュリティで大きな役割を担うのがSecure Element
- 電子決済などデータ、処理の改ざん等が問題になるサービスに利用される。
- モバイルNFCでは以下の3つのエリアのいずれかにデータは保存される
    - On Chip（スマートフォン本体）
    - SIMカード
    - SDカード

NFCの主な3つの利用形態とセキュリティ

電子決済系
- 重要な情報をSecure Element内に持ち、その情報を読み書きする。
- カード、モバイル両方で利用可能
- モバイルNFCの場合、Card Emulationモードとして動作

Secure Elementによる安全性の確保

情報読み取り系
- 簡単な情報をポスターなどに張り付けておき、それを読み取る
- モバイルでのみ利用可能
- モバイルNFCの場合、リーダ/ライタモードとして動作

情報交換系
- 携帯端末同士で情報をやり取りする
- モバイルでのみ利用可能
- モバイルNFCの場合P2Pモードとして動作

国内利用実績が少ない利用方法を誤ることでセキュリティ問題となることがあるか？

NFCのセキュリティ対策

- NFCの規格そのものには暗号化などの対策はない
- Secure Elementを用いることで決済サービスなどは安全性を保っている
- NFCが近距離でしか通信できないことがある面では盗聴防止のセキュリティ対策になっている

地下鉄システムの実装問題

- UltraReset – Bypassing NFC access control with your smartphone
- サンフランシスコの地下鉄で利用されているNFCによる改札システムの問題
- チケットに利用されていたのはMifare Ultralightチップ
- このチップは一度Onにするとoffにできないビット(On way counter)を持つ
- このビットで利用できる回数を制限できる
- 問題の地下鉄システムでは、この仕組みを利用せずに、乗車回数を記録

乗車記録を改ざん
リセットして何度でも乗り降り可能

他に報告されている問題や研究

- Security in Near Field Communication
- Exploring the NFC Attack Surface
- Practical Attack Scenarios on Secure Element-enabled Mobile Device
- A Practical Relay Attack on ISO 14443 Proximity Cards
- Applying recent secure element relay attack scenarios to the real world: Google Wallet Relay Attack

- **盗聴に対する脆弱性**
  - 基本的にNFCによる通信の盗聴は可能である
  - ただし、近距離でないとできない
  - Secure Channel（暗号化通信）により解決可能
- **リレー攻撃**
- **利用の仕方、設定の問題**
  - AndroidでNFC経由で任意のウェブページを表示させられる問題

NFCの実装方法、設定の仕方に気を付ける必要がある

まとめ

- NFC技術そのもののセキュリティリスクは少ない
- モバイルNFCは新たな攻撃経路を提供するという意味で、他のデバイス、ソフトウェアへの攻撃経路となる可能性がある
- 利用、応用方法を誤ると新たな問題が出る可能性はある
- 今までに起きているNFC関連の現実的問題は利用方法（実装方法）を適切にすることで回避できる
- NFCの適切な利用方法のガイド、セキュリティチェックリストなどの整備が望まれる