7Y-07

Bluetooth 検出機能を利用した位置偽装対策

川口裕己† 小林信博†
長崎県立大学情報システム学部情報セキュリティ学科†

1. はじめに

近年、位置情報を利用する様々なサービスが展開されている。例えば、小売店の提供するスマートフォン向けアプリ（スマホアプリ）では、GPS から取得したユーザの現在位置情報を利用し、来店時にチェックインを行うことで来店ポイントをためることができる。そのようなスマホアプリに対して、偽装した位置情報を利用することで不正にチェックインを行い、来店ポイントを不正取得する事件があった[1]。また、事件後の対策として以下の 3 つの制限が設けられた[2]。

- 同一店舗でのチェックインは 1 日 1 回
- チェックインは 1 日 3 回
- 別の店舗でチェックインをする前に 30 分の経過時間が必要

しかし、この制限では位置情報の正しさが判断できず、位置偽装の対策として不十分である。

一方、店舗には顧客の購買行動や在庫等の分析などの目的で、Wi-Fi や Bluetooth Low Energy（BLE）などの通信機能を備えた IoT 機器が導入されつつある。

本論文では、位置情報を利用する際にその場にいることの証明として、Bluetooth 検出機能を時刻と同期させて認証に用いる位置偽装対策を提案する。

2. 提案手法

本論文では、ワンタイムパスワード時刻同期方式を応用し、Bluetooth 検出機能を利用した位置偽装対策を提案する。

サービス提供者から認証に利用する情報（位置認証情報）を生成し、店舗に設置された IoT 機器に送信する。そして、IoT 機器の BLE を利用して位置認証情報を発信する。ユーザのスマホアプリが受信した位置認証情報をサービス提供者に送信し、サービス提供者が認証することで位置偽装対策を実現する。

2.1. APS 方式のワンタイムパスワード時刻同期方式

ワンタイムパスワード時刻同期方式（OTP）は、トークンとサーバで共有する鍵、時刻の２つをハッシュ関数などのアルゴリズムによって認証値を出力し比較する認証方法である。提案手法では、事前に登録したスマホなどにワンタイムパスワードを発行し認証を行う「帯域外トークン」を応用する。認証値を含む位置認証情報をサーバで生成・送付し、ユーザがこれをサーバに送信する。この位置認証情報により認証を行う方式を APS(Anti Positioning Spoofing)方式とした。APS 方式の OTP の概要を図 1に示す。

なお、提案手法では、BLE の位置認証情報がユーザ側でも設定できてしまうため、位置偽装の対策が無効化される恐れがある。そのため、時刻を同期させるとともに、位置認証情報の有効期間を設けることとする。有効期間には、UNIX 時間を加工した同期値を利用して確認を行う。

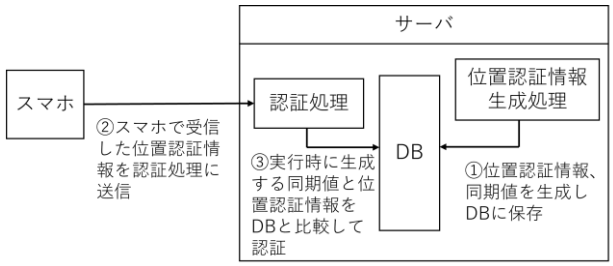

図 1 APS 方式の OTP

2.2. BLE における Advertise 機能

BLE の仕様では、接続待ちのペリフェラル機器をセントラル機器が発見した後に通信する。ペリフェラル機器が BLE の被検出機能を ON にすると Advertising と呼ばれる状態になる。この状態では、周囲のセントラル機器に向けて自身の情報を Advertising パケットでブロードキャストする。そこで、この Advertising 機能を利用して IoT 機器からスマホに位置認証情報を発信する。スマホが位置認証情報を取得するには、IoT 機器の Advertising パケットを受信する必要があるため、店舗に設置された IoT 機器の付近にスマホを持ったユーザがいると判断できる。

2.3. BLE における Alias 機能

BLE では、Advertising パケットに BLE デバイスの名前が含まれる[3]。更に、Alias の機能を利用することによって、任意の名前に変更する

Anti Location spoofing using Bluetooth detection
†Kawaguchi Yuki・University of Nagasaki
†Kobayashi Nobuhiro・University of Nagasaki

ことができる。そこで、Alias の機能で位置認証情報をもとにデバイスの名前を変更し、Advertising パケットでブロードキャストする。

2.4. 位置認証情報

位置認証情報は、4 つのパラメータを組み合わせて生成する。1 つ目のパラメータは APS である。位置認証情報受信時に他の BLE 通信と区別するための独自の識別子である。2 つ目のパラメータはバージョン番号である。3 つ目のパラメータは店舗番号である。店舗番号には、店舗ごとに固有の番号を入れる。国内のコンビニ店舗数(約 56,000 店、2022 年 11 月現在)を参考に、7 桁としている。4 つ目のパラメータは乱数である。乱数は、位置認証情報生成処理で生成されるが、位置認証情報は 1 分間隔で更新するため、4 桁の英大文字(26 文字種)から生成することとした。

一例として、バージョン番号が「1」、店舗番号が「1000000」、乱数が「AAAA」の場合、位置認証情報は、「APS_1_1000000_AAAA」となる。

3. 提案システムの試作

本論文で提案する位置偽装対策システムは、位置認証情報の生成と認証を行うサーバ、位置認証情報を発信する BLE 機能を搭載した IoT 機器、位置認証情報を受信する位置偽装対策を組み込んだスマホアプリから構成される。提案システムの構成を図 2 に示す。

更に今回は、提案システムを試作した。サーバに XAMPP を導入したノート PC (Windows11)、位置認証情報を発信する IoT 機器にラズパイ (Raspberry Pi 3B)、スマホは Android 端末 (Android バージョン 12) を使用した。

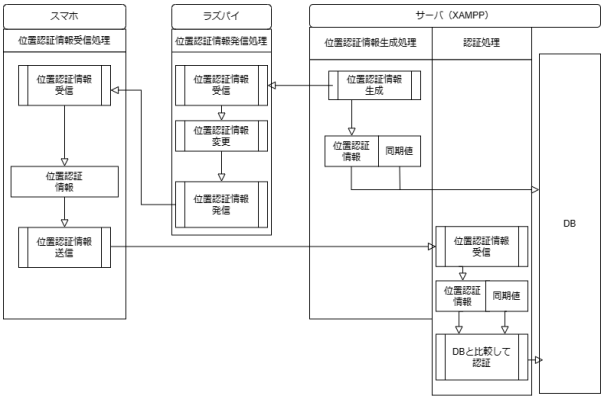

図 2 位置偽装対策システムの構成概略図

4. 評価

提案システムの評価として、攻撃者が不正な IoT 機器を手元に置き、偽の位置認証情報をサーバに送信する状況を想定した実験を行った。送信した位置認証情報と、認証結果を以下に示す。

4.1. 実際に店舗で入手した過去の認証情報の再利用

実際に店舗で入手した過去の認証情報の再利用では、攻撃者によって偽装された位置認証情報がサーバの DB に存在することを想定する。模擬攻撃の認証情報と認証結果を図 4 に示す。

結果として、同期値の不一致が検出され、不正な認証情報であると判定された。

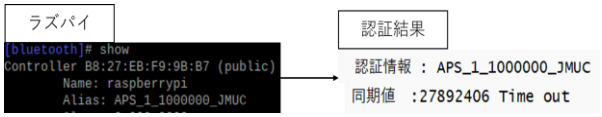

図 4 過去の認証情報の再利用の実験結果

4.2. 別店舗で利用できる値の利用

別の店舗で利用できる値の利用では、店舗番号を変えることによって短時間で認証を行う攻撃を想定する。模擬攻撃の認証情報と認証結果を図 5 に示す。

結果として、店舗番号の不一致が検出され、不正な認証情報であると判定された。

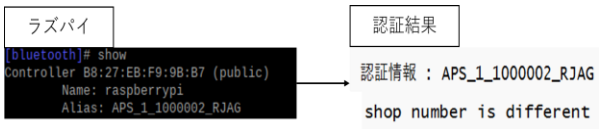

図 5 別店舗で利用できる値の実験結果

5. まとめ

前章の評価結果より、位置情報の正しさが判断できない課題に対して、ワンタイムパスワード時刻同期方式を応用し、Bluetooth 検出機能を利用する APS 方式で解決した。このことから、位置偽装対策として有効に働くと考える。

参考文献

[1] 朝日新聞 DIGITAL “イオンから来店ポイント詐取容疑” 2018 年 11 月 12 日

[2] イオン九州株式会社 “イオン九州公式アプリ来店ポイント不正取得と取得未遂に関してのお知らせ”, https://www.aeon-kyushu.info/files/management_news/1656/pdf.pdf, (参照 2022-9-7)

[3]Supplement to the Bluetooth Core Specification https://www.bluetooth.com/specifications/specs/core-specification-supplement-10/