

フリーWiFi 接続サービス 監視方式 および 監視装置

背景

インバウンド観光など観光向けサービスや自治体の行政サービスとして、フリーWiFi接続サービスの提供が加速している。しかしその方式設計では利便性と安全性とのトレードオフが顕著で、安易な設計はセキュリティ上の重大な脅威をもたらす一方、安全サイドに振りすぎで観光客が事実上、利用困難なシステムも散見される。

問題点

フリーWiFi提供エリア内またはその近傍で悪意ある者がサービス提供者のWiFi識別子 (ESSID) と同一の ESSID を名乗る WiFiアクセスポイント (AP) を設置することがある。一般利用者は AP の真贋を見極められず、悪意ある者が設置した AP により中間者攻撃や盗聴の被害に遭う可能性がある。通信路を暗号化しても無防備な状態となる場合がある。

解決策

「ダミークライアント」と名付けた装置をフリーWiFi提供エリアとその周辺に配置。周辺APの識別情報 (BSSID) を定期的に取得し、クラウド上のサーバーに転送する。サービス提供者が設置した AP 以外の BSSID が観測されればすぐに悪意あるAPの存在が確認できる。ダミークライアントを継続的に動作させれば、BSSIDを偽装した悪意あるAPも検知できる。

副次的効果

施設管理者にとって管理がおろそかになりがちなフリーWiFi接続サービスの可用性の監視を併せて提供できる。災害発生時の避難場所などに設置する公共 WiFi 接続サービスなどに好適。

ダミークライアント

一般的なスマートフォンと同様なWiFi接続装置で、単三乾電池のみで1年間稼働。定期的に WiFiスキャン動作を行い、APにWiFi接続してクラウド上のサーバーにスキャン結果を転送。

本装置の稼働実績

大阪工大と連携協定を結ぶ奈良県川上村において、複数の公共施設で長期の運用評価を継続中。WiFi接続サービスの遠隔監視に絶大な効果をもたらしている。

研究のPRポイント

- 既設のWiFiアクセスポイントに後付け可能な構成
- サービス提供エリアを超える範囲も監視可能
- きわめて安価に製作可能なダミークライアント
- 乾電池2本で1年間以上稼働、AC電源を必要としない
- システム監視をマネージドサービスとして展開可能

フリーWiFi接続サービスの懸念事項



- 適切な暗号化をしなければ盗聴される
- 匿名性を悪用した違法・迷惑行為の可能性
- **中間者攻撃につながる偽アクセスポイント (Evil Twin)**
 - 対策1: WiFi接続用の専用アプリを事前インストール
 - 事業者が運営する大規模サービス以外では無理
 - 対策2: 接続後、VPNを使わせる
 - 初心者には難易度高すぎ
 - 危険性が騒がれている割には有効な手があまり打たれていないように見える

偽APは容易に判別できないのか?



利用者にとっては難しい → 接続先の検証に必要な重要情報が欠落している

サービス提供者にとってはある程度までは簡単では?

- 一般的な WiFiクライアント の動作
 - APが定期的に出すSSIDビーコンを受信、ビーコンにはBSSIDを含む
 - 同じ名前のSSIDビーコンを一つにまとめてリスト表示
 - 利用者が選んだSSIDの、最もRSSI (信号強度) が強いAPに接続
- BSSID: 個々のAPを区別する識別子 (MACアドレス)
 - 利用者はSSIDしか念頭にないが、WiFi接続時はBSSIDでAP指定
 - SSIDビーコンにはBSSIDの情報も含まれている
 - 設置した覚えがないBSSIDがビーコンに出現すれば偽AP
 - ダミークライアントでSSIDビーコンをひたすら収集する

