Trabalho 2
Surveilling the Masses with Wi-Fi-Based Positioning Systems

Matilde Simões
up202108782
Faculdade de Ciências
Universidade do Porto

***Resumo*—O estudo analisou problemas de privacidade nos sistemas de geolocalização da *Apple* baseados em Wi-Fi. Foi possível construir uma base de dados global de BSSIDs geolocalizados que permite monitorizar deslocações de indivíduos e populações inteiras. A recolha massiva de dados foi viabilizada pela ausência de autenticação e pela resposta da API da *Apple* com centenas de BSSIDs adicionais por pedido. O ataque, realizável com poucos recursos, levanta preocupações sérias de vigilância e levou a recomendações técnicas e éticas para mitigar o problema.**

I. Descrição e Entendimento do Problema

Este estudo [1] revelou uma vulnerabilidade de privacidade associada aos *Wi-Fi-based Positioning Systems* (WPSes). Uma vez que o GPS apresenta um elevado consumo de energia, os WPSes oferecem uma alternativa mais eficiente para a geolocalização frequente dos dispositivos móveis. Para tal, os dispositivos reportam os identificadores únicos dos pontos de acesso Wi-Fi (BSSIDs), juntamente com as respetivas coordenadas geográficas, contribuindo para o enriquecimento das bases de dados dos WPSes.

Contudo, o problema identificado reside no facto de o WPS da *Apple* permitir que qualquer dispositivo, sem autenticação ou comprovação de proximidade, submeta uma lista arbitrária de BSSIDs e receba, em resposta, a localização dos BSSIDs solicitados, bem como mais 400 BSSIDs geograficamente próximos, o que amplifica exponencialmente a capacidade de recolha de informação. Isto possibilita que, através da geração inteligente de endereços MAC baseados em *Organizationally Unique Identifiers* (OUIs) atribuídos pelo IEEE, se construa rapidamente uma base de dados global de pontos de acesso Wi-Fi. A ausência de restrições de consulta – chaves da API, limites na taxa de pedidos ou um dispositivo *Apple* – facilita a exploração em larga escala. O ataque descrito é exequível com poucos recursos, sem necessidade de dispositivos especializados ou acesso privilegiado. Adicionalmente, os autores validaram que o WPS da *Apple* responde de forma idêntica a partir de várias localizações globais, indicando que o ataque pode ser realizado em qualquer parte do mundo, com exceção das Regiões Administrativas Especiais (RAEs) de Hong Kong e Macau, onde a legislação restringe a recolha de localizações.

O problema agravou-se quando, ao consultar os mesmos BSSIDs de forma contínua ao longo do tempo, se tornou possível detetar com precisão movimentos reais dos dispositivos e, consequentemente, dos seus utilizadores. O estudo evidencia este risco através de vários casos práticos, como a movimentação de pontos de acesso Wi-Fi em zonas de guerra e, também, a monitorização dos dispositivos da *GL.iNet*, que são detetados em várias localizações geográficas ao longo do tempo, por serem portáteis, apresentando uma taxa de movimento 76 vezes maior que os outros dispositivos.

Por fim, o estudo foi validado pelo comité de ética institucional (IRB) e os autores ainda contactaram a *Apple*, a *Google*, a *SpaceX* e a *GL.iNet*. Em resposta, a *Apple* e a *SpaceX* adotaram medidas como concatenar *_nomap* ao SSID da rede Wi-Fi e a aleatorização de BSSIDs, respetivamente, para mitigar a vulnerabilidade.

II. Abordagem e Relevância dos Identificadores

Para explorar a vulnerabilidade, a abordagem [1] que foi adotada baseia-se na utilização de BSSIDs para monitorizar pontos de acesso Wi-Fi ao longo do tempo e do espaço. A estratégia consiste na construção de um vasto conjunto de dados longitudinais com geolocalizações de BSSIDs, recorrendo ao acesso não autenticado à API do WPS da *Apple*, e, de seguida, proceder à análise da movimentação desses identificadores em múltiplos períodos temporais.

O estudo incluiu dois conjuntos de dados longitudinais – um estudo mensal com 10 milhões de BSSIDs consultados diariamente, no qual cerca de 8% desapareceram da base da *Apple* e 0,06% deslocaram-se mais de 1 km – e um estudo anual com mais de 2 mil milhões de BSSIDs geolocalizados, utilizado para analisar eventos como a guerra na Ucrânia e na Gaza e os incêndios em Maui.

Em vez de gerar endereços MAC de forma aleatória, o ataque centra-se na utilização de OUIs atribuídos pelo IEEE, o que reduz drasticamente o espaço de procura e aumenta a taxa de sucesso. Adicionalmente, os autores exploraram variantes desses identificadores (com o `bit U/L` a 0 e a 1), abrangendo também BSSIDs utilizados por alguns dispositivos. Com este método, foi possível consultar aproximadamente 68.644 OUIs ao enviar uma média de 30 pedidos por segundo à API da *Apple*, sem qualquer limitação prática encontrada.

A importância dos identificadores utilizados reside no facto de os BSSIDs serem, na sua maioria, identificadores estáticos. Ao contrário dos dispositivos móveis recentes, que aplicam técnicas de aleatoriedade dos endereços MAC para mitigar/dificultar a monitorização/identificação, a maioria dos pontos de acesso Wi-Fi mantém o mesmo BSSID, a menos que sejam reconfigurados ou substituídos.

Esta ausência de variabilidade permite várias formas de exploração. Por um lado, ao observar alterações nas localizações dos mesmos BSSIDs, ao longo do tempo, é possível inferir movimentações físicas das pessoas e dos dispositivos associados. Por outro, a análise da distribuição geográfica de múltiplos BSSIDs permite identificar padrões de concentração, como zonas densamente povoadas. Adicionalmente, torna-se possível estabelecer relações com acontecimentos reais como a variação temporal na presença ou ausência de BSSIDs, podendo ser usada para acompanhar fenómenos como catástrofes ou operações militares.

Desta forma, o trabalho demonstra que, embora os BSSIDs sejam tecnicamente apenas identificadores de rede, a sua natureza estática nos pontos de acesso Wi-Fi e a forma como são obtidos e expostos pelos WPSes tornam-os em vetores de vigilância, com o potencial de comprometer a privacidade individual e coletiva numa escala global.

III. Formulação das Questões

A. Devemos tratar os routers Wi-Fi pessoais como elementos críticos da nossa privacidade pessoal e coletiva?

Considero que é assustador perceber que o meu *router* pode estar a servir como um identificador digital involuntário, monitorizado por qualquer serviço que use WPS. Nunca pensei que ter um *router* em casa fosse um risco à minha privacidade ou à dos meus vizinhos – mas é exatamente isso que este tipo de ataque revela.

Tal como o caso da NSA revelado por *Edward Snowden*, que mostrou que a vigilância em massa era mais real do que imaginávamos, o abuso de dados WPS demonstra que a tecnologia avançou mais rápido do que a nossa capacidade de proteger os nossos direitos.

Estas ameaças afetam a segurança pessoal, mas também a segurança coletiva, tendo como exemplo o facto de um dispositivo *Apple* conseguir fornecer as minhas geolocalizações, como também as das pessoas à minha volta [1]. Esta nova forma de vigilância é barata, invisível e democrática, no mau sentido, onde qualquer pessoa com conhecimentos mínimos pode fazê-la.

Penso que não podemos continuar a tratar a infraestrutura doméstica como um assunto privado, isolado e seguro. Se os dados que o meu *router* emite podem ser usados para realizar monitorização/identificação de outros dispositivos, então terá que ser tratado como um problema ético e de privacidade. Tal como exigimos segurança nos nossos sistemas elétricos ou hídricos, devemos exigir proteções na forma como os nossos dispositivos emitem dados. Isso inclui a aleatoriedade de identificadores, limitações legais no acesso aos dados de localização e transparência sobre o funcionamento de APIs que obtêm essas informações. Caso contrário, arriscamo-nos a viver num mundo onde, sem querer e sem saber, todos contribuímos para um gigantesco mapa de localizações e vigilância de indivíduos.

B. Tendo em conta que os dispositivos dos turistas obtêm dados em qualquer país, mesmo sob legislações restritivas, estaremos a entrar num período em que a soberania digital já não é exercida pelo Estado, mas sim pelas grandes empresas tecnológicas?

Hoje, são empresas como a *Apple*, a *Google* ou a *Meta* que, na prática, controlam a infraestrutura de obtenção e circulação de dados geoespaciais a nível global. O Estado, por muito poderoso que seja, está constantemente numa posição reativa, ao tentar legislar contra sistemas que não controla.

A situação na China, apresentada em [1], ilustra essa realidade com clareza. Apesar das políticas de proteção dos dados, um grande volume de dados de BSSIDs foram obtidos e mapeados por dispositivos de turistas, através de APIs como a da *Apple*. Na minha opinião, isso revela um paradoxo de que um país pode controlar os dados/informações dentro das suas fronteiras, mas não pode impedir um turista com *iPhone* de agir como um vigilante, ainda que de forma não intencional.

Isto leva a uma possível constatação. As grandes empresas tecnológicas tornaram-se potências geopolíticas, que conseguem ter acesso a informação sensível ao nível (ou acima) de muitos Estados. Isso já era evidente com o caso do *Snowden*, mas agora assume novas proporções – mais subtis, mais técnicas, mais difíceis de detetar.

Considero que o problema se configura numa nova forma de domínio global, porque as maiores empresas exercem controlo direto sobre os dados de cidadãos de qualquer país, ignorando fronteiras. Mesmo com leis de proteção de dados, como o RGPD, na prática continuamos sem conseguir ver ou controlar como as empresas realmente obtêm, processam e utilizam os nossos dados – os sistemas são tecnicamente complexos e opacos, tornando-se incompreensíveis para o utilizador comum.

Para alcançarmos soberania digital, é necessário exigir transparência técnica obrigatória nas APIs de geolocalização, implementar limites por defeito na quantidade de dados retornados (evitando, por exemplo, o envio de centenas de BSSIDs por cada pedido) e estabelecer um pacto internacional para a proteção de dados passivos – pois é precisamente nisso que estes dados se tornaram: elementos sensíveis exploráveis sem consentimento ou controlo.

Na minha opinião, enquanto continuarmos a aceitar que dispositivos comuns podem contribuir para mapear o mundo inteiro, nenhuma política nacional/europeia será suficiente para garantir o direito à privacidade ou à autodeterminação tecnológica.

Referências

[1] Erik Rye and Dave Levin. Surveilling the masses with wi-fi-based positioning systems. pages 2831–2846, 5 2024.