Overview

- What is privacy vs security
- Challenges in wireless privacy
- Attacks
  - Probe requests
  - Device fingerprinting
  - Traffic Metadata analysis
  - Man-in-the-Middle

Privacy != Security

- **Security**
  - Protection of sensitive data from attacks from unauthorized third parties
  - Confidentiality, availability, integrity of data
  - Encryption, passwords, two-step authentication, etc.

- **Privacy**
  - Confidentiality of less sensitive personal information
  - Wireless security is often necessary to ensure wireless privacy, but is not sufficient
  - Privacy can be breached without breaching security. Information about a device can be gathered without accessing the device’s data
  - Location history, device purpose, personal habits
  - **Anonymity**

Challenges in Wireless Privacy

- **Open medium**
  - Impossible to control propagation of signals
  - Anyone can listen in to transmissions through the air

- **High mobility**
  - The node that wireless devices are associated to will change as they move around
  - Ensuring a constant and secure association is difficult
  - When a wireless device can be tracked, the location of the user can be monitored, both by authorized and unauthorized parties
Wi-Fi Tracking: Fingerprinting Attacks and Counter-Measures (2017)

- To discover and connect to APs, devices broadcast a lot of information
  - Probe request
- Passive attack listens for broadcasts, identifies devices/users
  - Hardware information
  - Chipsets
  - Supported encryption algorithms
- Enables tracking over time

Probe requests

- Allow devices to discover nearby access points
- Rich with information necessary for connection
- Rich with information not necessary for connection
- No hacking necessary, just sniffing

Tracking location history with probe requests

- Probe requests can broadcast to look for any AP or specific AP
  - Targeted vs broadcast
- Phones leak info about previously connected APs
  - Leaked AP history = Leaked location history
  - SSIDs have been mapped and can be looked up
- Probe requests are cleartext
  - Can’t use encryption because algos are part of handshake
Mitigation Techniques

- Not too many consumer-friendly protection options
- Use broadcast for probe request
  - No leakage, slow
- Geofence SSIDs
  - Some leakage, faster
- Turn off WiFi when not in use
  - Even when devices are connected they search for other APs
  - Not feasible option

Fingerprinting devices using probe requests

- Devices have different levels of privacy
  - Totally open: Self-identify manufacturer, device type, etc.
  - Kinda open: Don’t identify device type, not randomize MAC
  - In the middle: Don’t advertise previously connected access points
  - Kinda closed: Fully randomized MAC
  - Totally closed: No device-identifiable information in probe request
- Android 8 and iOS 11 leak least info
- Convenience vs. Privacy
Mitigation Techniques

- Randomize MAC until connect to trusted AP
  - Not necessary to broadcast globally unique identifier
- Don’t reveal vendor-specific information unless absolutely necessary
  - Less damning than broadcasting MAC, but still identifier

Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic (2017)

- Utilizes network traffic from a smart home and Internet of Things in order to violate the user’s privacy
  - Monitor user activity about the house
  - Collect information on usage of devices and determine behavior patterns
- No need to decrypt traffic in order to gather information
  - Gathered entirely through metadata that is available to the public

What is Metadata?

- Publicly available information that anyone in the vicinity of the wireless network can collect
  - MAC address
  - DNS queries
  - Network traffic rates
- Difficult or impossible to prevent an attacker from accessing such data
Traffic Rate Metadata Attack

- Fingerprint the device of interest
  - MAC Address, Probe requests
  - Fingerprinting using only traffic rates
- Information about type of device can be used to track user activities
  - Different types of devices serve different roles
  - A sleep monitor peaks in traffic usage during periods of use, and the activity of the sleep monitor can be used to determine when a person is asleep.
  - Even in the absence of a sleep monitor, the amount of wireless traffic in a house can be used to infer the current activities of the user.

Fingerprinting using Traffic Rates

- Internet traffic rates vary between devices

Fingerprinting using Traffic Rates

- Training Machine Learning algorithms to distinguish devices via traffic

Monitoring user activities

- Wireless Security Camera Traffic
  - High level of fluctuations when in livestreaming/constant monitoring mode
  - Less fluctuations with large peaks when in motion detection
- Can be turned against the user
  - A camera in motion detection mode can be used to determine level of user activity in the house
Monitoring user activities

- Wireless enabled appliances
  - Spikes in traffic often indicative of user interaction with device
  - Can be used to infer current user activity level
  - Long term monitoring can gather information on the user’s behavioural habits and patterns

Mitigation Techniques

- Countering Traffic Rate Metadata Attack: Tunneling traffic and Traffic shaping
  - Tunneling Traffic
    - VPN wraps all device traffic into a single flow
    - Makes devices indistinguishable from one another
  - Traffic shaping
    - Send fixed-size packets out of the local network at a constant rate
    - Masks actual traffic from wireless devices

Issues with disconnecting

<table>
<thead>
<tr>
<th>Device</th>
<th>Functionality</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Echo</td>
<td>limited</td>
<td>Can turn on Bluetooth speakers with previously paired smartphone</td>
</tr>
<tr>
<td>Echo Dot</td>
<td>limited</td>
<td>Can turn on Bluetooth speaker with previously paired smartphone</td>
</tr>
<tr>
<td>Echo Sub woofer</td>
<td>limited</td>
<td>Cannot use smartphone app to control device over voice telephone on local network</td>
</tr>
<tr>
<td>Echo Dot Smart Speaker</td>
<td>limited</td>
<td>Can turn on Bluetooth speaker with previously paired smartphone</td>
</tr>
<tr>
<td>TP-Link Smart Plug</td>
<td>limited</td>
<td>Can turn on Bluetooth speaker with previously paired smartphone</td>
</tr>
</tbody>
</table>

Automated Man-in-the-Middle Attack Against Wi-Fi Networks (2018)

- Active attack that alters the user’s normal connection with the Internet
  - Passive attacks only allow the attacker to listen in on traffic on the wireless network
  - Attack attacks also allow the attacker to edit traffic flowing between the user and the intended destination
- Automation makes the attack more viable as a means of collecting information on a large number of users
  - Considerably reduces the amount of effort an attacker needs to put into the attack

Fig. 6. All tested commercially available IoT devices had limited or non-functionality when disabled to prevent communication outside of the smart home LAN. This suggests that device manufacturers should be encouraged to improve their “smarter reliable product.”
Man in the Middle

- Inserting the attacker’s device in the middle of the connection
  - Inherently insecure - Allows a third party to intercept, analyze and alter all traffic between the user and their destination

Automated Attack Process

- Obtain access to network
  - Cracking the network
  - Phishing for user data
  - Impersonate the network to trick users into connecting to the attacker instead
- Monitor and tamper network traffic
  - Full access to all traffic to and fro the user

Cracking the Wireless Network

- Open Networks
  - Easy to impersonate
- WEP networks
  - WEP encryption is weak and can be attacked easily even if a random password is used
- WPA networks
  - Networks often suffer from issues such as weak or default passwords
  - Dictionary of common passwords can be used
  - Phishing for user data can be used if direct cracking does not work
Cracking the Wireless Network (WPA)

Mitigation Techniques

- Traffic Encapsulation (VPN)
  - Protects user security even if the connection is compromised
  - Will not protect user privacy, still gives attacker information on metadata

Cracking the Wireless Network (WEP)

Mitigation Techniques

- Detecting the attack
  - MitM is an active attack, as such it leaves traces of the attack behind
  - Once a MitM attack is detected, the user can simply disconnect from the compromised connection to deny the attacker access to their traffic
Sources

- Wi-Fi Tracking: Fingerprinting Attacks and Counter-Measures
- Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic
- Automated Man-in-the-Middle Attack Against Wifi Networks