Man-in-the-Middle Attacks

Preventing network attacks on mobile devices

As sensitive data is increasingly accessed by mobile devices, mobile threats are growing in prevalence and sophistication. Man-in-the-middle attacks are an emerging example of these sophisticated threats, and according to a recent report, 24% of organizations report that mobile devices used in their company have connected to a malicious wifi network.[1]

How man-in-the-middle attacks happen

A man-in-the-middle attack on enterprise data typically requires two steps:

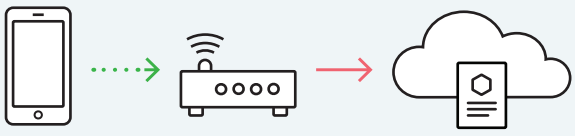
1. Getting access to network traffic
2. Decrypting the data

The second step is important because enterprise data is almost always encrypted, so simply getting in the middle of traffic is not likely to result in data theft.

1. Getting access to network traffic

There are a variety of ways for an attacker to get access to network traffic, including:

- **A.** Setting up a fake wifi access point or cell tower
- **B.** Invoking a VPN to tunnel traffic through their network
- **C.** Implementing proxy to redirect traffic in their network path
- **D.** Address Resolution Protocol (ARP) spoofing to advertise their own hardware address in place of a gateway



2. Decrypting the data

After getting into the network path, the attacker then has to manipulate the connection or user to view encrypted data. This typically involves one of the below methods:

Host Certificate Hijacking

An attacker introduces a malicious certificate authority under their control into the trusted root certificate authority store of the victim device, allowing the attacker to masquerade as a corporate resource that the victim intends to communicate with securely.

SSLStrip

An attacker subverts un-encrypted connections made by the victim, re-writing URLs that would normally be specified as HTTPS to use plaintext HTTP.

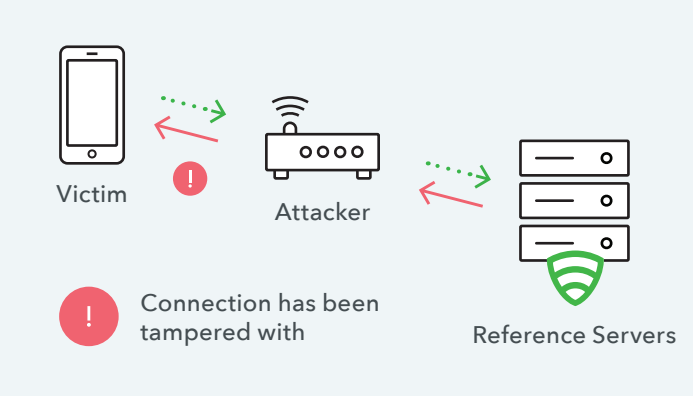
TLS Protocol Downgrade

An attacker manipulates the negotiated connection to downgrade the negotiated protocol or cipher suites and lower the security guarantees of the connection.

[1] CIO.com, "One-fifth of IT pros say their companies had mobile data breach", 2016

The Lookout Approach

Our on-device app probes reference servers with known certificate properties and known security protocol configurations. This allows us to compare *expected* network configuration properties with the *observed* network properties. By analyzing whether these observed connections meet expected properties, we can determine whether connections are being compromised by an attacker utilizing any of the methods described earlier.



Lookout's approach minimizes false positives

We DON'T alert solely on:

- Cafe or hotel captive portals
- Proxies
- VPNs

Prone to false positives

We DO alert on:

- Host certificate hijacking
- SSLStrip
- TLS protocol downgrade

Enterprise relevant threats

Lookout's approach focuses on the risks that are the most relevant to enterprises, namely, attempts to intercept encrypted data-in-transit.

Most progressive mobility programs do not restrict an employee's ability to connect to cafe, hotel, or airport wifi networks as that would hinder productivity, yet some other approaches to man-in-the-middle detection will surface admin alerts for this everyday activity. These other approaches lead to an abundance of false positives that are not actionable by the average IT organization.

Lookout's approach focuses on the types of connections that put encrypted data at risk. As a result, we minimize false positives for malicious network connections, while enabling users to stay connected and productive on the go.