MITM and Proxy Vulnerabilities

News

- https://github.blog/2023-02-28-secret-scanning-alerts-are-now-available-and-free-for-all-public-repositories/
- Apple Post-quantum crypto
  - https://security.apple.com/blog/imessage-pq3/?is=6fa78154dbea9fd6a29caa59a8a9433f63d310cc0d643f0f38e7e9ff5be35bf6
  - Not much of a current need – at least 5 years off
  - PQC is tough – NIST has found issues with other submissions, so this might not get approved
  - Most attackers are more likely to use social engineering, not try to capture and decrypt instant messages

Topics

- Describe MITM attacks and how they can be used to attack mobile apps.
- Identify various mobile app communication flaws that are vulnerable to MITM attacks
- Describe the ARP spoofing and how it facilitates MITM attacks
- Implement a proxy and use it to test apps for basic MITM vulnerabilities

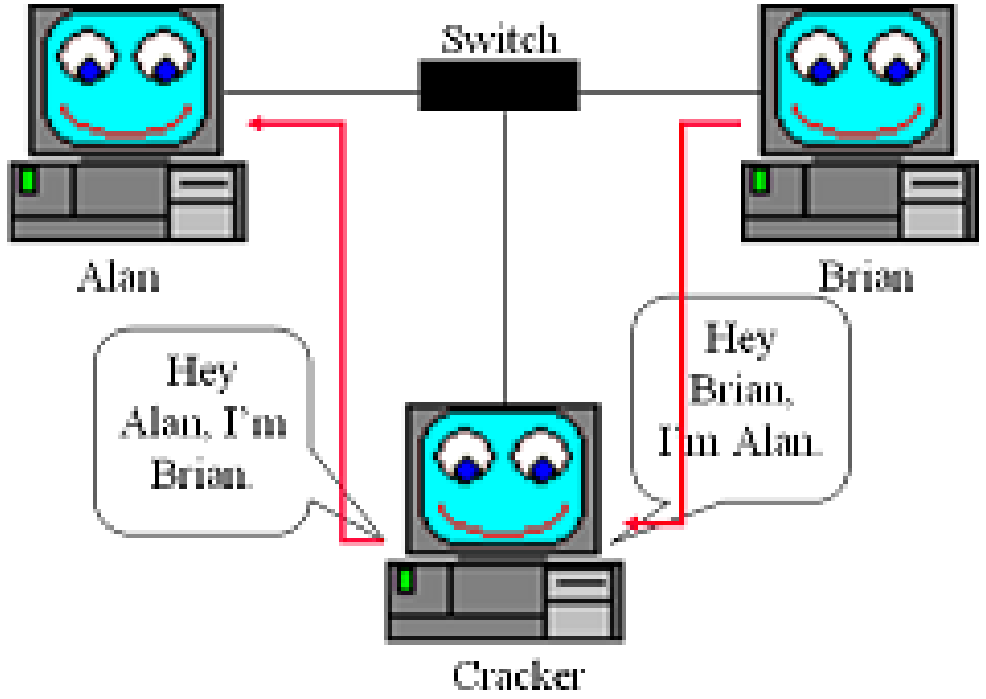
Man-in-the-Middle Attack (MITM)

- Attacker captures network traffic to and from the victim by sniffing the network medium
- Attacks include:
  - Tracking internet destinations
  - Stealing usernames, passwords, account numbers and any clear text traffic
  - Hijacking sessions to servers

Attacker MITM Tools – ARP Spoof

- Starts with wireless scanning to reveal MAC addresses, SSIDs, key material, etc.
- Wireshark in promiscuous mode can view unencrypted traffic on wireless
- After attacker identifies target device:
  - ARP response packets are flooded to device indicating attacker is the default gateway
  - ARP response packets are flooded to default gateway indicating attacker is target device
- All traffic is then routed through attacker device without the victim knowing
- This type of attack MAY result in noticeable performance degradation or denial of service to the victim if not managed correctly

Arpspoof Example



MITM and Spoofing Tools

- Linux – arpspoof and Wireshark, or Bettercap
- Mac – Dsniff download
- Windows – Bettercap
- Android – Kali NetHunter app
- Important Note – Exit these tools gracefully to restore ARP settings
  - ARP entries can remain in place even if MiTM device is not available to forward packets
  - ARP cache can hold entries up to 10 minutes

ARP Spoofing Demo

Clear Text Traffic Vulnerability

Capturing Clear Text Traffic

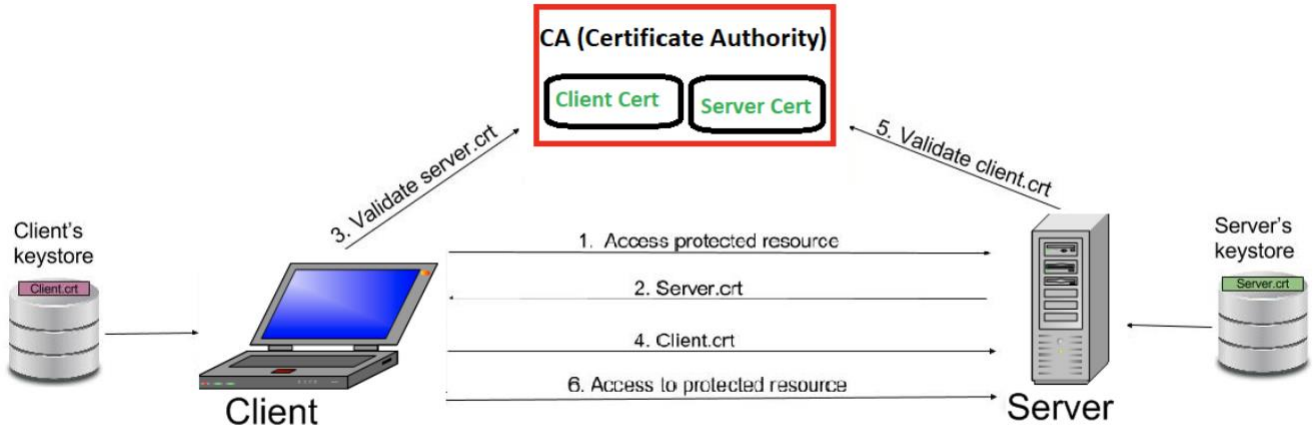
- Any packet capture tool can capture network traffic from the emulator
  - Wireshark
  - TCPDump – Linux
  - Pktmon – Windows
- Download traveler.apk and install on emulator
- Start packet capture and login with any credentials
- View HTTP traffic to see username and password

Broken TLS Vulnerability

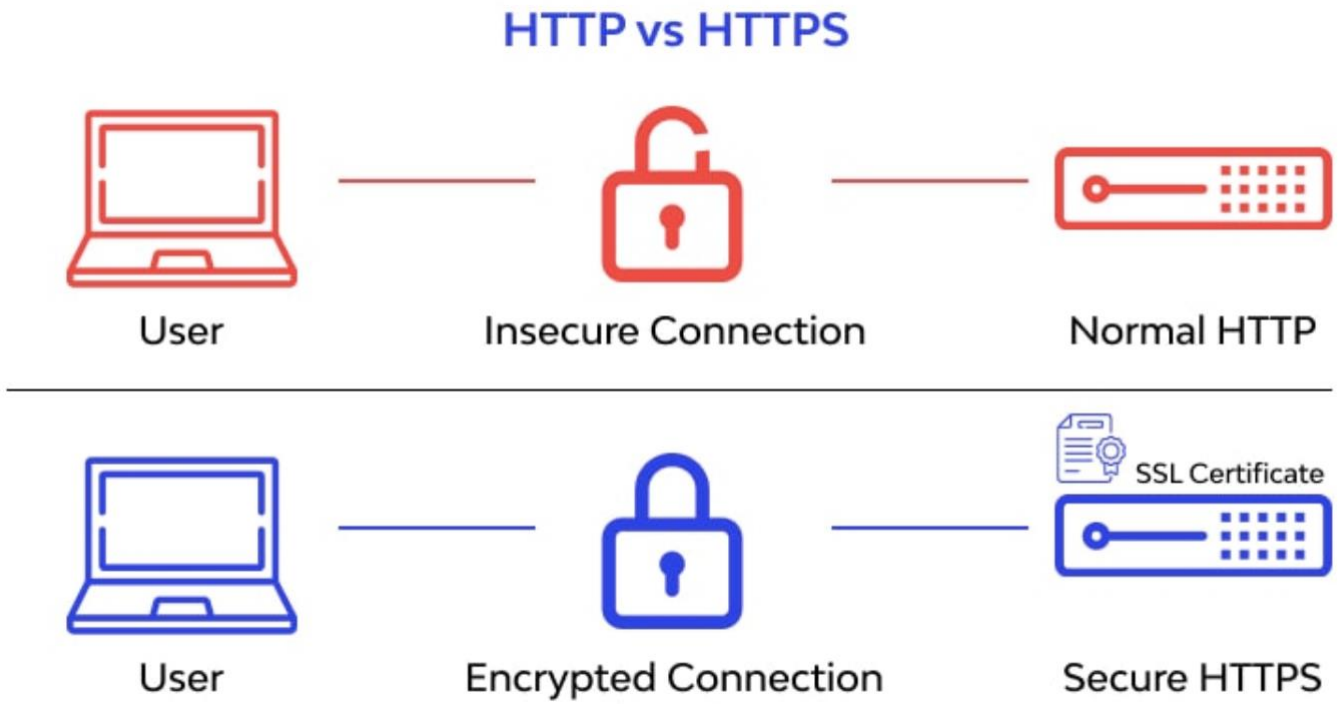
Failure to validate server certificate

TLS Overview

- TLS uses CA Certificates for public server keys
- The certificate must be registered with a valid Certificate Authority to be accepted
- Check certificate in browser and certmgr for examples



SSL Required for Secure HTTPS

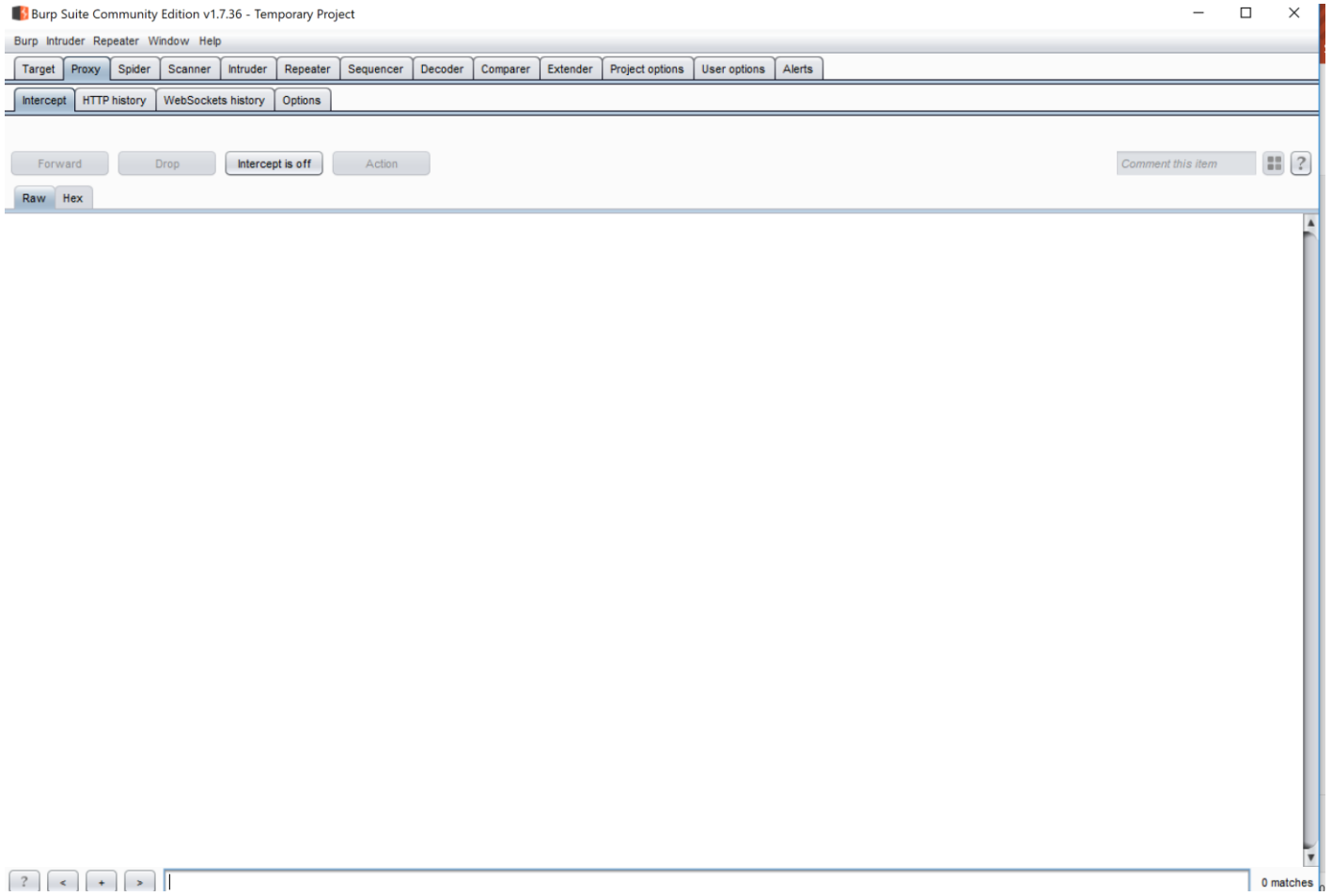


MITM Testing With a Proxy

- Encrypted traffic won't show clear text in Wireshark – requires proxy
- ARP spoofing can capture and forward traffic without knowledge from the client device
  - Can be unstable and cause performance issues
- Proxies like Burp Suite that we use for testing are ideal, BUT they require proxy configuration on the client device
  - Requires access to Encyconfiguration of target device

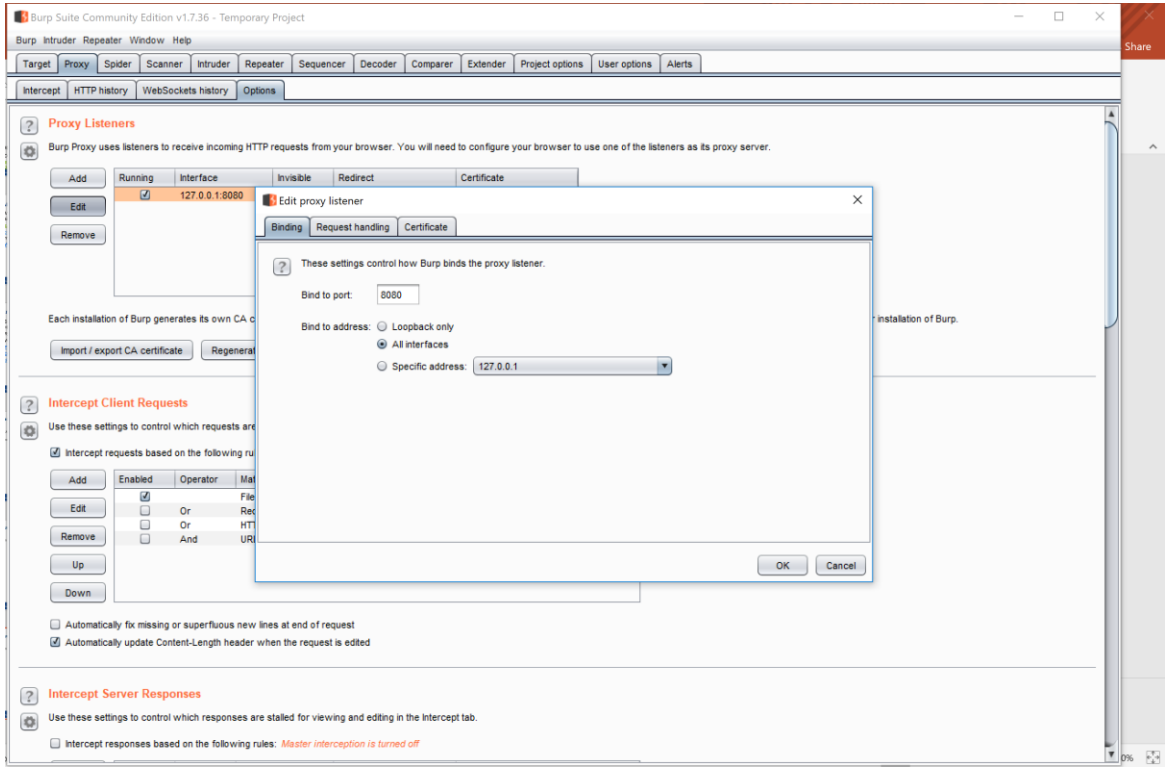
Start Burp Suite

- In Proxy-Intercept tab, ensure Intercept is off



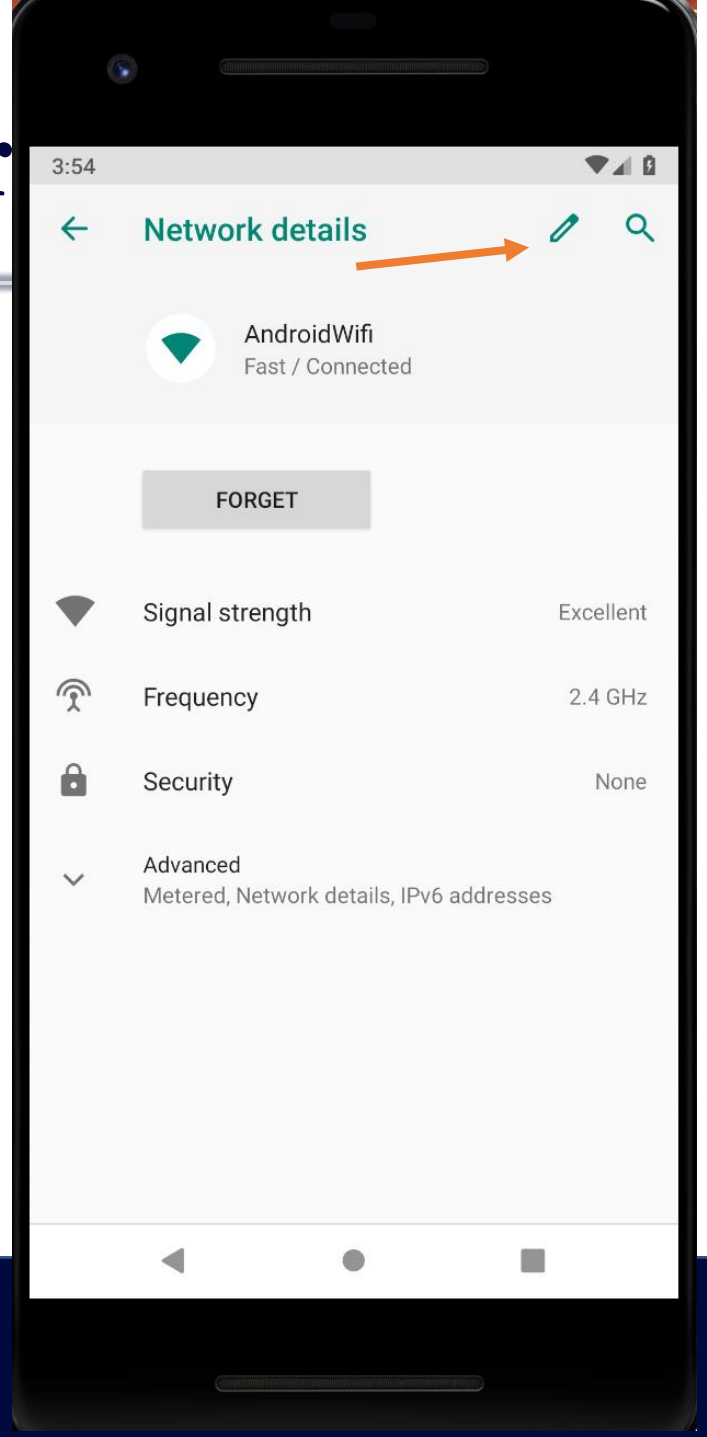
Burp Suite Proxy Config

- In Proxy – Options tab select loopback interface and select edit
  - Select all interfaces
  - On Certificates tab make sure selection is to generate certificates per host
  - In dashboard select Running



Set Proxy Server on Emulator

- Wifi click settings next to network name
- Click on pencil to edit network
- Advanced Options – Proxy – Manual
  - Enter your host's primary IP and Burp port number of 8080
  - Save
- Start Intercept on Proxy and open browser
- Ensure browser traffic works



Challenges

- Find the flags on the TravelZoo and Somnote apps
- Login with fake email and password

Summary

- App traffic is vulnerable to sniffing
- ARP Spoofing and proxies can be used to capture traffic
- Clear text traffic is easy
- Basic SSL functions and HTTPS vs HTTP
- Broken TLS does not validate certifcate