Man in the Middle Reborn

SecTor 2008

Jay Beale
Co-Founder, InGuardians
Author, Bastille UNIX

Beta Release this week at:
https://www.InGuardians.com/sector

Talk Agenda

This talk introduces The Middler, of which each of you will receive a beta release. It's an attack proxy tool to automate attacks on browsers and everything else that uses HTTP.

Here's the Talk Agenda:

- The Attack Vector: Shared Networks
- Automatically exploiting mixed HTTP/HTTPS sites, including Gmail, LinkedIn and LiveJournal
- Launching attacks on Online Banks
- Trojaning software installation and update
- Injecting browser-exploits and adding root certificates
- Protecting yourself on hostile WLANs and LANs

HTTP and Shared Networks Don’t Mix

Most users use a tremendous number of shared networks when they leave their homes and offices.

- Hotels
- Non-security Conferences
- Coffee Shops / Bookstores
- Airplanes

Whether those are wireless or wired networks, they open themselves up to application-level monitoring and attack constantly.

Proxy Attacks

If we share a LAN, I can view and modify all of your traffic:

I can replace the real DHCP server on the network, setting my laptop up as your DNS server, DHCP server, and router.

OR

I can ARP spoof the real router and any local DNS servers.

DNS

DNS is also a beautiful, beautiful thing to an attacker.

Dan told me so. And he’s right.

First, spoofing DNS on a local network means you can send connections anywhere you want.

Second, poisoning DNS for even an hour can get you an SSL certificate that will last much longer than your attack.

Mixed HTTPS/HTTP Sites are a Menace

Many companies misunderstand that encrypting only their application's password form leaves their users very vulnerable to man in the middle attacks.

Think about how LinkedIn.com works.

If you start up your browser with https://www.linkedin.com, click on "Sign In," you'll be taken to this URL:

```
https://www.linkedin.com/secure/login?trk=hb_signin
```

Following sign-in, you're taken to this one:

```
http://www.linkedin.com/home
```

What if I change the URL?

You can change the URL to:

https://www.linkedin.com/home

…but clicking on any link will just take you right back to an HTTP URL!

Unless you modify your browser or surf with a special defensive proxy, you'll constantly be pulling down cleartext links.

And all I have to do as an attacker is inject my own Javascript into a single one of those.

How Do I Attack This?

First, direct the client to my host with DNS, DHCP or ARP spoofing.

Second, pass the HTTPS traffic through unmodified, but:

1) Inject Javascript into the cleartext traffic.
2) Store session keys and send my own parallel requests.
3) Intercept logout requests.
4) Replace HTTPS links in any proxied pages with HTTP links.

Best of all, I'm releasing a tool right here to do this. It features a rich plug-in architecture to let other people add on handling for sites we're not including in this release.

The Middler

Interactively, we can:

- Clone session for the attacker by transparently using the same cookies and form parameters as the user.
- Inject Javascript into every HTML page
- Inject temporary or permanent redirects.
- Log the valid user’s session.

But there’s also real power in site-specific features, which The Middler knows how to use without human interaction.

- Gmail
- LiveJournal
- LinkedIn

Gmail and Other Webmail

Once the Gmail session moves back into cleartext, we can:

- Read the user’s e-mail
- Read past GoogleTalk conversations
- Harvest the address book
- Send our own e-mails
- Profile the user in other Google applications
- Prevent a real logout, presenting the user with an actual logout

Think about how much information Google has and will let you access.

How useful would it be to get access to someone else’s Google data.

LiveJournal

LiveJournal is a blogging site that's very much used for private friends-only blogging.

People have strong expectations that they can keep posts private, readable only by their friends or even small subsets of those friends.

As an attacker watching or middling a LiveJournal session after it moves back into cleartext, we can:

- Read the user's private and friends-only journal entries
- Make the user's private/friends-only entries public
- Harvest the friends list and those friends' private posts
- Add our own user to the victim's "friend" list

LinkedIn

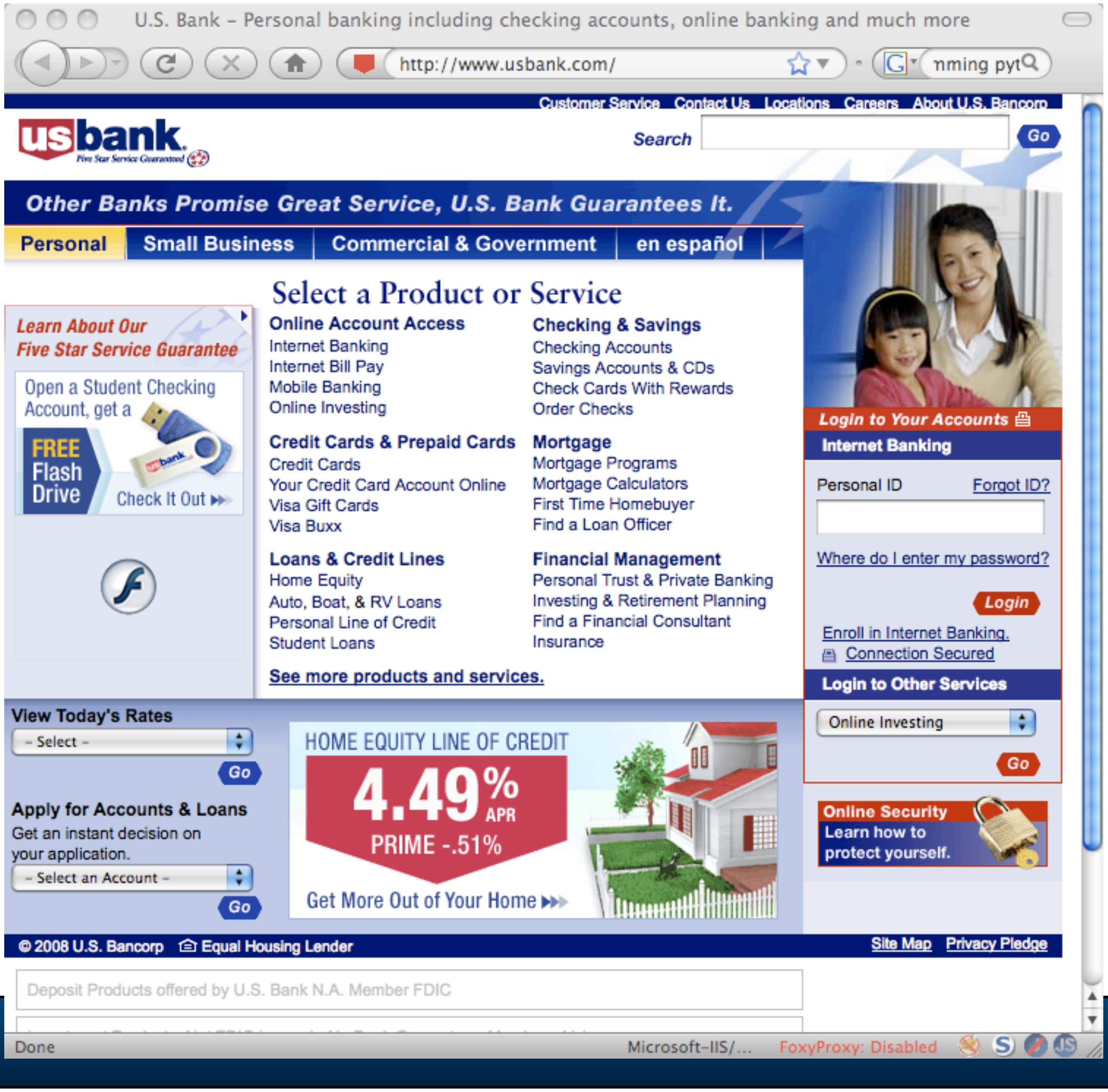
LinkedIn is a professional social networking site, trusted by many professionals. Outside of our ultra-paranoid security community, people trust this with their full contact information.

We all expect that we can’t be harrassed.

Once the LinkedIn session moves back into cleartext, we can:

- Read the user’s full contact information
- Gather full contact information for their entire Network
- Read the user’s Inbox
- Add ourselves to their Network
- Place the user in our Network

What’s Wrong With This Picture?



U.S. Bank - Personal banking including checking accounts, online banking and much more

http://www.usbank.com/

Customer Service | Contact Us | Locations | Careers | About U.S. Bancorp

usbank Five Star Service Guaranteed

Search | Go

Other Banks Promise Great Service, U.S. Bank Guarantees It.

Personal | Small Business | Commercial & Government | en español

Learn About Our Five Star Service Guarantee

Open a Student Checking Account, get a FREE Flash Drive Check It Out

Select a Product or Service

Online Account Access
Internet Banking
Internet Bill Pay
Mobile Banking
Online Investing

Checking & Savings
Checking Accounts
Savings Accounts & CDs
Check Cards With Rewards
Order Checks

Credit Cards & Prepaid Cards
Credit Cards
Your Credit Card Account Online
Visa Gift Cards
Visa Buxx

Mortgage
Mortgage Programs
Mortgage Calculators
First Time Homebuyer
Find a Loan Officer

Loans & Credit Lines
Home Equity
Auto, Boat, & RV Loans
Personal Line of Credit
Student Loans

Financial Management
Personal Trust & Private Banking
Investing & Retirement Planning
Find a Financial Consultant
Insurance

See more products and services.

Login to Your Accounts

Internet Banking

Personal ID | Forgot ID?

Where do I enter my password?

Login

Enroll in Internet Banking.

Connection Secured

Login to Other Services

Online Investing | Go

Online Security Learn how to protect yourself.

View Today's Rates

- Select - | Go

Apply for Accounts & Loans

Get an instant decision on your application.

- Select an Account - | Go

HOME EQUITY LINE OF CREDIT 4.49% APR PRIME -.51%

Get More Out of Your Home

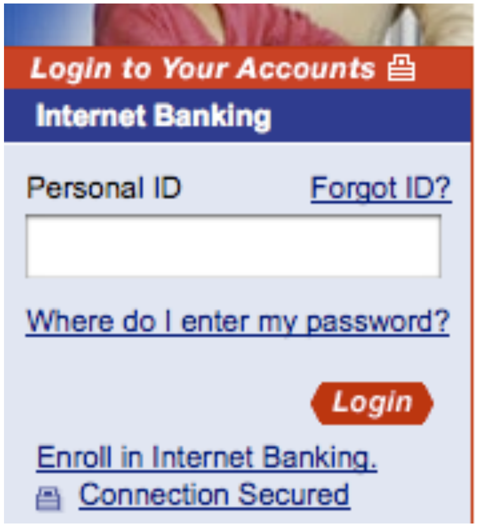
© 2008 U.S. Bancorp | Equal Housing Lender | Site Map | Privacy Pledge

Deposit Products offered by U.S. Bank N.A. Member FDIC

Done | Microsoft-IIS/... | FoxyProxy: Disabled

Cleartext Front Page

But it says our connection will be secured!



<form … action=https://www4.usbank.com/internetBanking/LoginRouter

What if I were to re-write all the URLs on this site to remove the SSL?

Rewriting HTTPS Links

TheMiddler can insert redirects with either HTTP codes or Javascript. It changes:

https://foo.com/bar

to:

http://foo.com/secure4/bar

Then it manages re-writes in both directions transparently.

CSRF's Attacks Made Easier?

Imagine a non-security friend on a hotel network…

He types the name of his online banking site into his browser:

http://www.bankofamerica.com

He's used to the bank protecting him from himself. The site reloads the page with an HTTPS version:

https://www.bankofamerica.com.

It's already too late. It's a race condition and he lost.

Race Condition

I have already served him my own index.html file for the HTTP site, which accomplishes the reload, but not before inserting its persistent window.

```
window.open(“http://www.bankofamerica.com
    /
    mitm”,”mitm”,’width=1,height=1,scrollbars=0,menubar=0,toolbar=0,location=0,s
    tatus=0’);
window.blur(“mitm”);
document.location.href=“https://www.bankofamerica.com”;
```

While his primary browser window is no longer under my control, I can continue to serve my own version of the bank’s website. From there, I’ll wait for the user to log in to the main site, then begin CSRF attacks.

How do I know when he logs in?

Knowing When the User Logs In

First, remember that I'm proxying the user's traffic.

Even if I wasn't, from my persistent HTTP-provided window, I can read the browser history to see what links the user has visited.

If the victim has pop-blocking in place, I can even just inject Javascript into any HTTP-carried pages the user has open.

Trojaning Software Installation

So far we’ve kept our eyes on web applications. But there’s more that happens over HTTP than that.

Several non-giant software vendors do software installation and update over HTTP, with no public key verification of the packages you’ll install.

Your system pulls down a page over HTTP that includes available update names, versions, locations, and sometimes MD5sums.

Software Installation

While the large operating system vendors generally get this right, packaging their own PGP public keys with the original operating system, not everyone does.

The Middler has plug-ins to automate:

- Installer.app for the iPhone
- MacPorts (formerly DarwinPorts)

I’ve worked to do a trojan horse insertion on both my iPhone and my MacbookPro.

Software Update

The race to patch and the proliferation of client-side exploitation has made self-update a standard feature.

Most of the software that updates itself does so over cleartext HTTP.

Some uses TLS/encryption to pull down the update, but they obtain the URL for that download by downloading an update catalogue via cleartext!

Exploiting Vulnerable Browsers

The Middler has one more attack feature.

As long as we're able to inject HTML into a users' browser windows, we can also serve up client-side attacks from Metasploit.

The Middler can insert Javascript to refresh the current page or a pop-under to an exploit that it serves. We could just take the exploit and serve it ourselves, but that's not as easy to maintain.

Exploiting a Browser

Think about what an attacker with Middling power can do.

The user surfs to a page, then gets redirected to the captive portal and pop-ups.

We can inject Javascript into the portal. That includes BEeF, the Browser Exploitation Framework.

We can also redirect the browser to a client-side exploit that we programmatically set up for it through Metasploit.

Go Further: DNS

Let’s talk about Dan for a moment.

OK, but it’s worse than that.

Go Even Further: Routing

Imagine I could attract of all of your inbound traffic to me and route it pretty transparently back to you.

I could modify anything in flight.

What info could I gather?

Who could I protect?

Stealing the Internet

It’s not just in your imagination.

Recently at DefCon, Pilosov and Kapela demonstrated how they could re-route traffic through their own AS on its way to its real destination. Check out the “Stealing the Internet” slides.

Protecting Yourself at a Conference

What can you do to protect yourself at a conference?

You could try bringing your own Internet connection. EVDO/CDMA and HSPDA/GSM modems make this very difficult or at least reduce the attacker pool to people with the equipment and know-how.

If this isn't an option, and even when it is, here's what I like to do.

Recipe for a Safer LAN Experience

Here’s what I do on a hostile conference network:

1. Set up a dynamic port forwarding SSH tunnel
2. Ask for the DHCP server’s and router’s MAC address and IP addresses
3. Set my DNS servers to localhost or tunnel over SSH
4. Configure my firewall to allow outbound IP traffic only to the SSH tunnel host and the DHCP server.
5. Configure static MAC address (ARP table) entries for the DHCP server and route.

Questions and Speaker Bio

Jay Beale created two well-known security tools, Bastille UNIX and the CIS Unix Scoring Tool, both of which are used throughout industry and government, and has served as an invited speaker at many industry and government conferences, a columnist for Information Security Magazine, SecurityPortal and SecurityFocus, and an author/editor on nine books, including those in his Open Source Security Series and the "Stealing the Network" series. Jay is a security consultant and managing partner at InGuardians, where he gets to work with brilliant people on topics ranging from application penetration to virtual machine escape.