

# New Tricks For Defeating SSL In Practice



Moxie Marlinspike  
[moxie@thoughtcrime.org](mailto:moxie@thoughtcrime.org)

# The Back Story

# SSL And Certificate Chaining

General | Details

This certificate has been verified for the following uses:

SSL Server Certificate

**Issued To**

Common Name (CN) www.paypal.com  
Organization (O) PayPal, Inc.  
Organizational Unit (OU) Information Systems  
Serial Number 63:4D:CE:1C:61:9F:FB:6B:26:1E:05:AD:5B:A9:85:86

**Issued By**

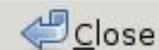
Common Name (CN) VeriSign Class 3 Extended Validation SSL SGC CA  
Organization (O) VeriSign, Inc.  
Organizational Unit (OU) VeriSign Trust Network

**Validity**

Issued On 05/01/2008  
Expires On 05/02/2009

**Fingerprints**

SHA1 Fingerprint A4:25:F6:7E:D2:C9:AC:D6:DE:F6:53:DA:79:5E:01:C5:17:B3:75:2D  
MD5 Fingerprint 22:B7:78:93:7D:BA:56:8B:84:BD:F9:A9:74:70:07:00

Close

You probably know what they do...

More specifically...

# CA Certificate

Embedded in browser.

All powerful.

Certifies that a site certificate is authentic.

# Site Certificate

Identifies a particular URL.  
Is known to be authentic based on CA Certificate's signature.

# CA Certificate

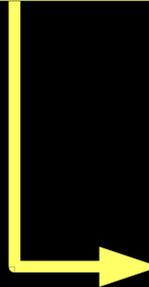
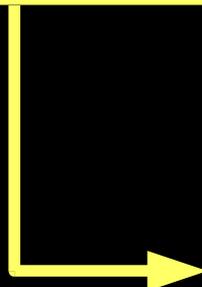
Embedded in browser.  
All powerful.  
Certifies that an intermediate  
CA is authentic.

# Intermediate

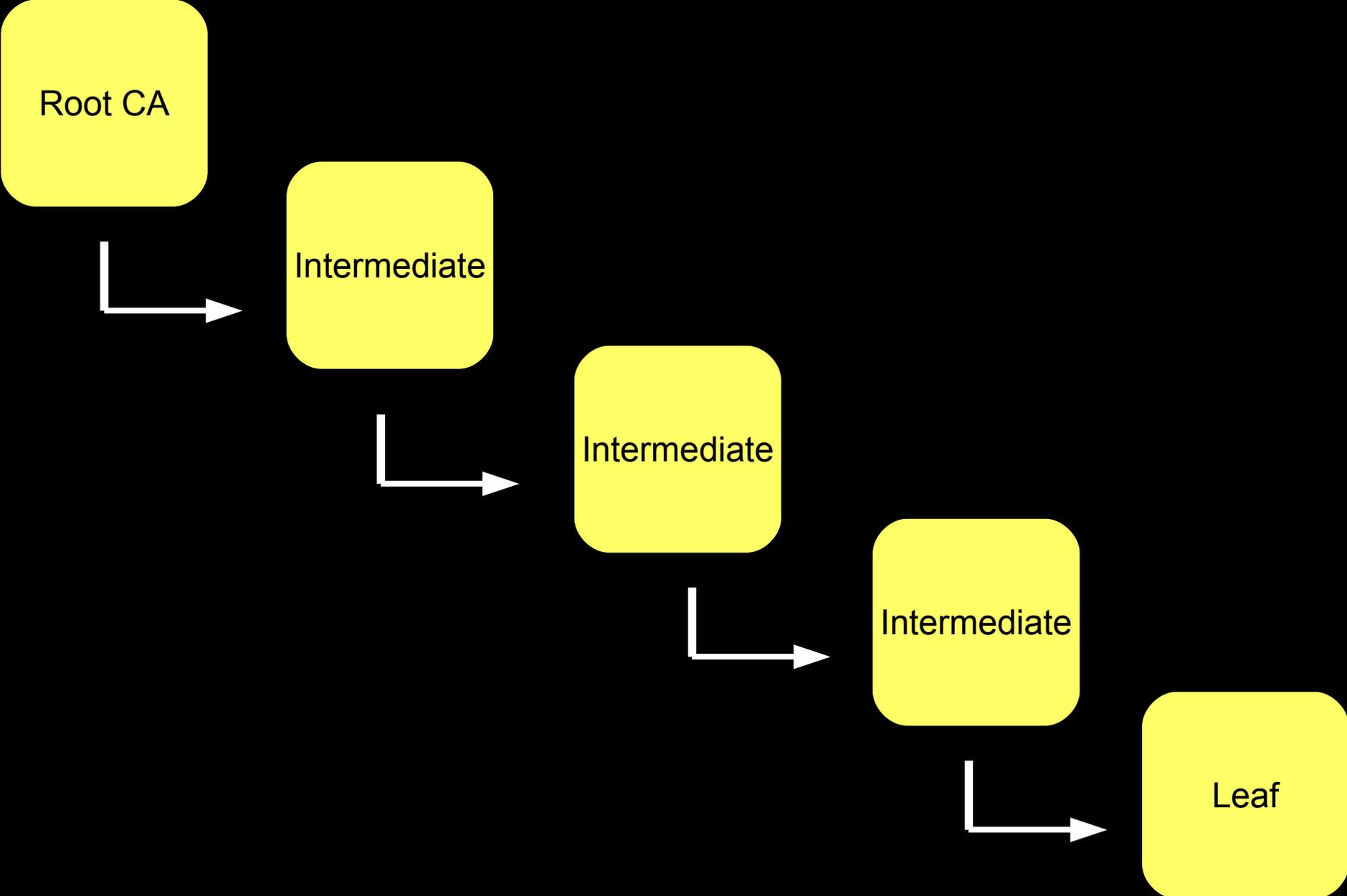
Not embedded in browser.  
Still sort of all-powerful.  
Certifies that a site certificate is  
authentic.

# Site

Identifies a particular URL.  
Is known to be authentic based  
on CA Certificate's signature.



# Certificate Chains Can Be $> 3$



How do we validate these things?

Almost everyone tells you the  
same story.

# What they say:

Verify that the leaf node has the name of the site you're connecting to.

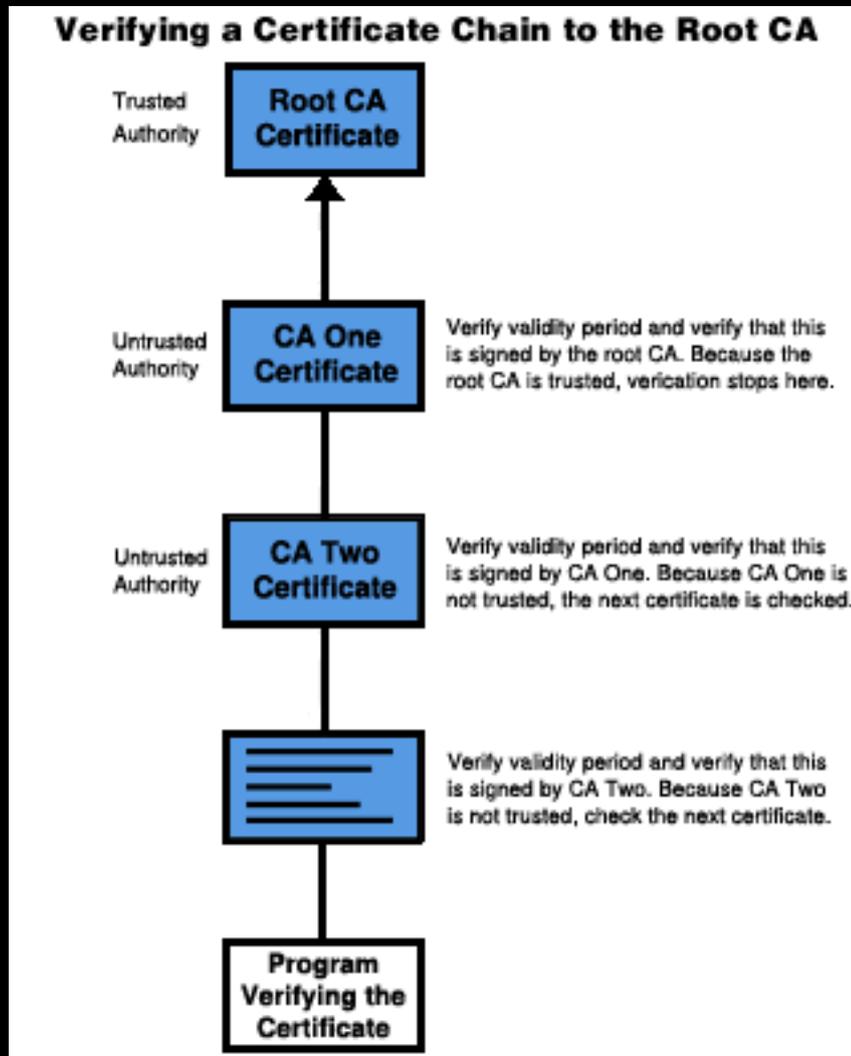
Verify that the leaf node hasn't expired.

Check the signature.

If the signing certificate is in our list of root CA's, stop.

Otherwise, move one up the chain and repeat.

# Here Be Dragons

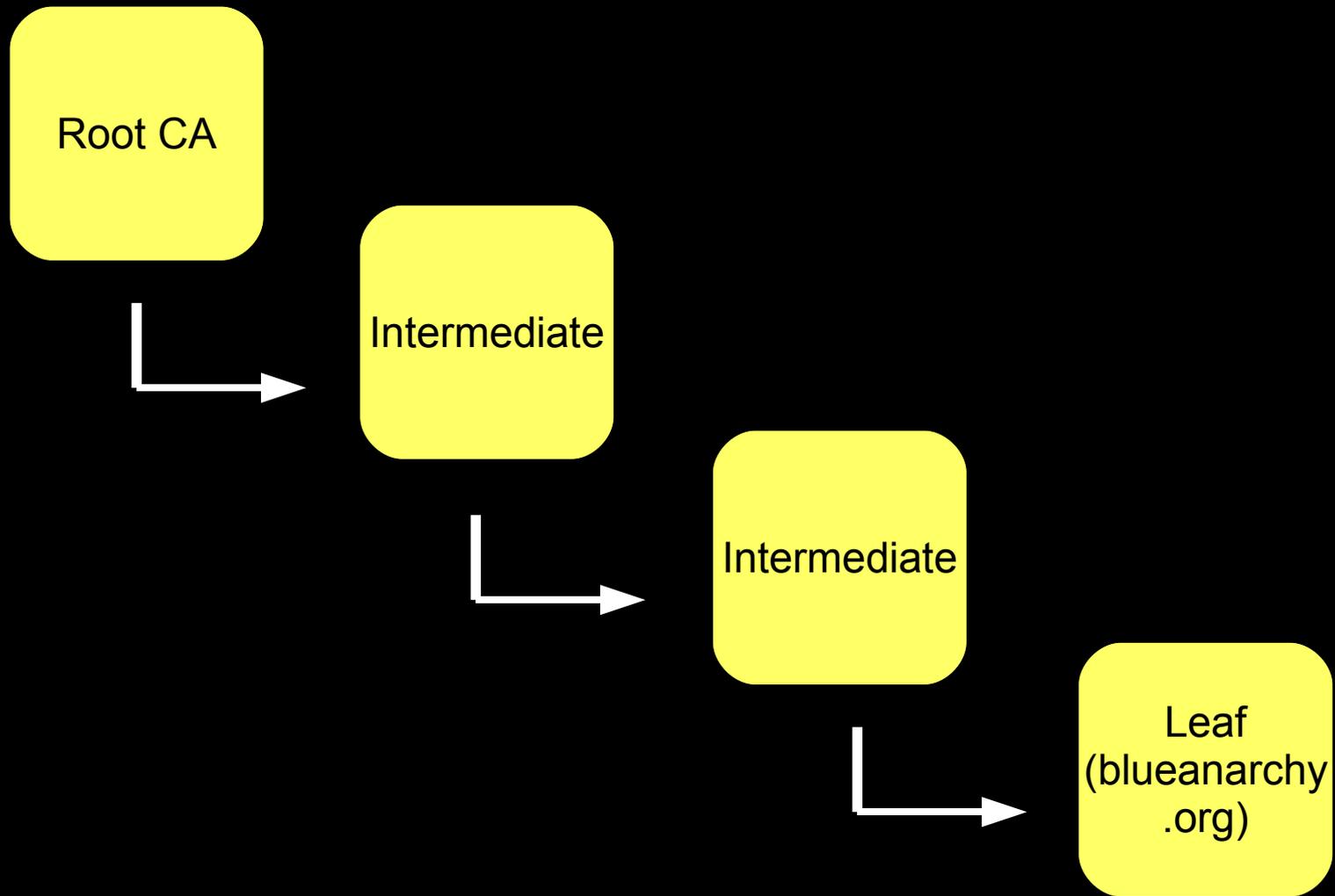


Very tempting to use a simple recursive function.

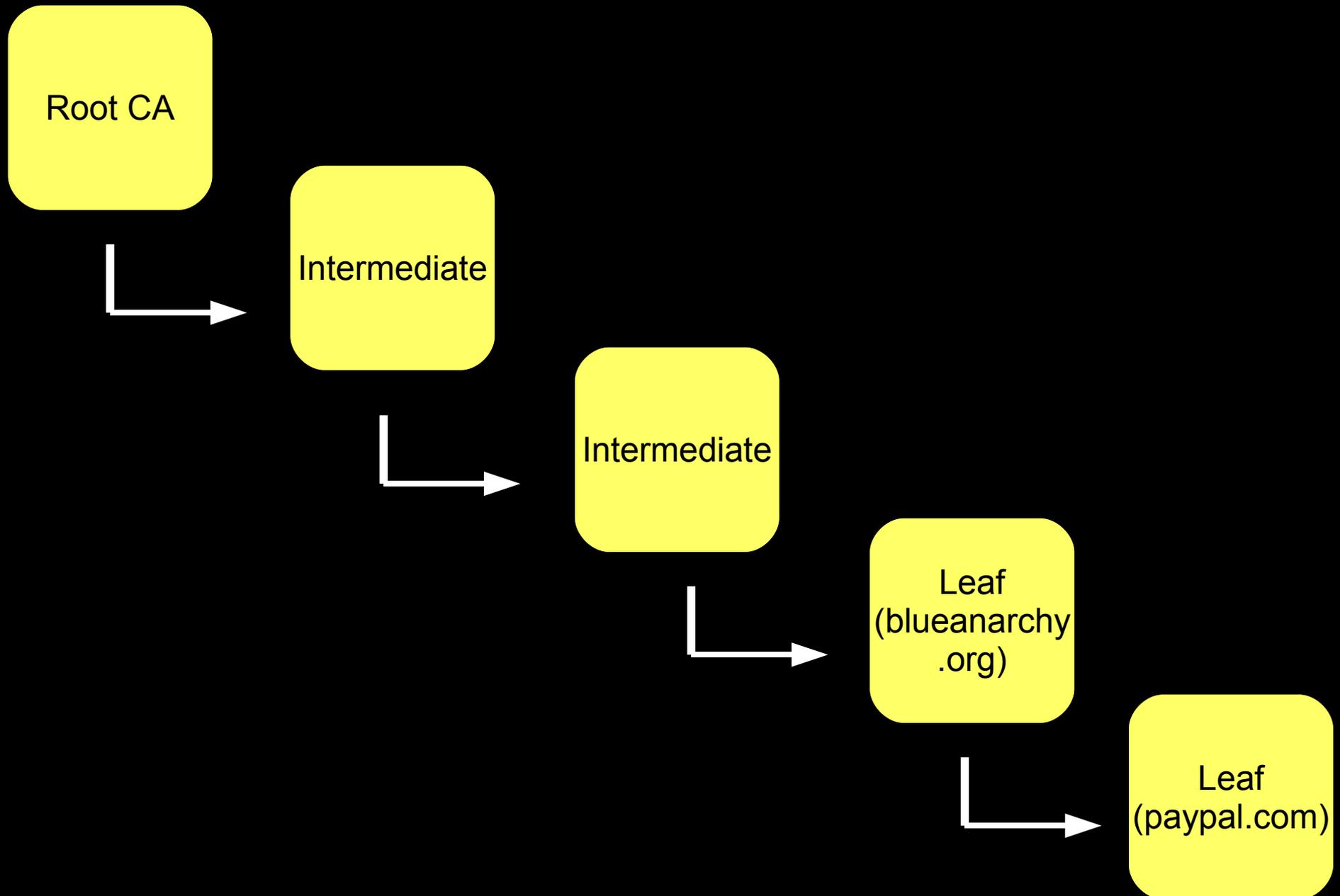
Everyone focuses on the signature validation.

The result of a naïve attempt at validation is a chain that is complete, but nothing more.

# What if...



# What if...



# What they say:

Verify that the leaf node has the name of the site you're connecting to.

Verify that the leaf node hasn't expired.

Check the signature.

If the signing certificate is in our list of root CA's, stop.

Otherwise, move one up the chain and repeat.

# Something must be wrong, but...

All the signatures are valid.

Nothing has expired.

The chain is in tact.

The root CA is embedded in the browser and trusted.

But we just created a valid  
certificate for PayPal, and we're not  
PayPal?

The missing piece...

...is a somewhat obscure field.

```
File Edit View Terminal Tabs Help
moxie@searching: ~/Desktop/b... X moxie@searching: ~/Desktop/b... X moxie@searching: ~/Desktop/b... X
      f8:c9:0f:24:d2:c7:c2:92:0c:13:54:93:d5:9b:c7:
      0e:fa:19:a8:d5:d3:f7:ab:5d
      Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Key Usage: critical
    Digital Signature, Non Repudiation, Key Encipherment, Data Encip
herment
  X509v3 Subject Key Identifier:
    DF:48:EF:25:BF:D2:23:B0:F0:C2:AC:FA:5A:85:50:74:FF:F9:34:EF
  X509v3 CRL Distribution Points:
    URI:http://crl.geotrust.com/crls/globalca1.crl

  X509v3 Authority Key Identifier:
    keyid:BE:A8:A0:74:72:50:6B:44:B7:C9:23:D8:FB:A8:FF:B3:57:6B:68:6
C

  X509v3 Extended Key Usage:
    TLS Web Server Authentication, TLS Web Client Authentication
  X509v3 Basic Constraints: critical
    CA:FALSE
Signature Algorithm: sha1WithRSAEncryption
7a:58:f9:88:14:cb:77:32:aa:83:12:de:d9:15:74:8e:34:e3:
66:ca:bc:24:2c:28:96:54:cd:be:51:56:60:87:e3:be:c6:2e:
86:7e:74:c1:68:01:b6:8c:07:c6:a2:0c:a4:36:ca:e1:a8:e9:
```



# Back In The Day

Most CA's didn't explicitly set basicConstraints:  
CA=FALSE

A lot of web browsers and other SSL implementations didn't bother to check it, whether the field was there or not.

*Anyone* with a valid leaf node certificate could create and sign a leaf node certificate for *any other* domain.

When presented with the complete chain, IE, Konqueror, OpenSSL, and others considered it valid.

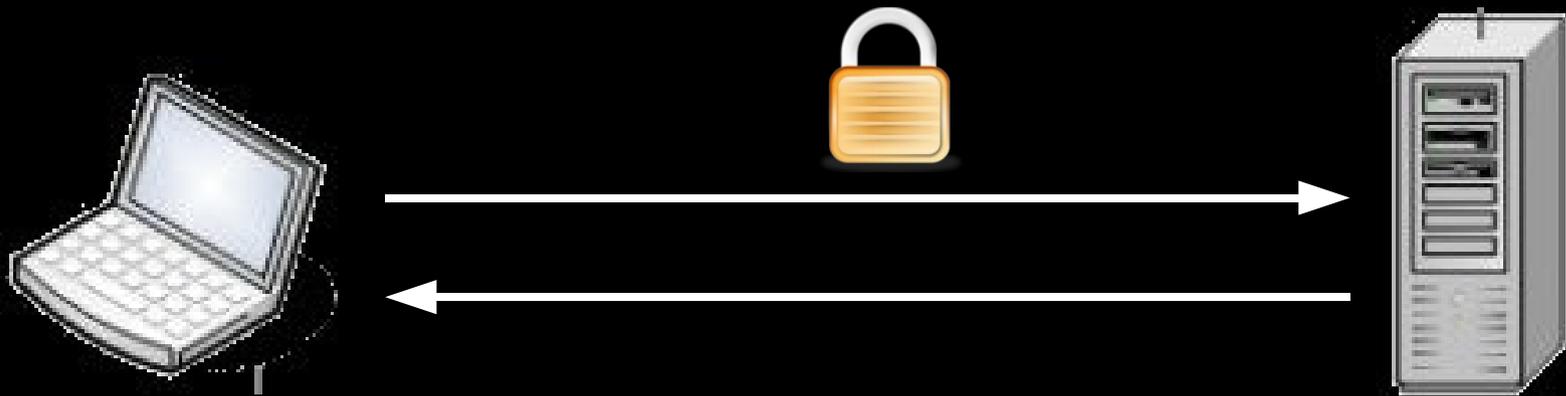
# And then in 2002...

Microsoft did something particularly annoying, and I blew this up by publishing it.

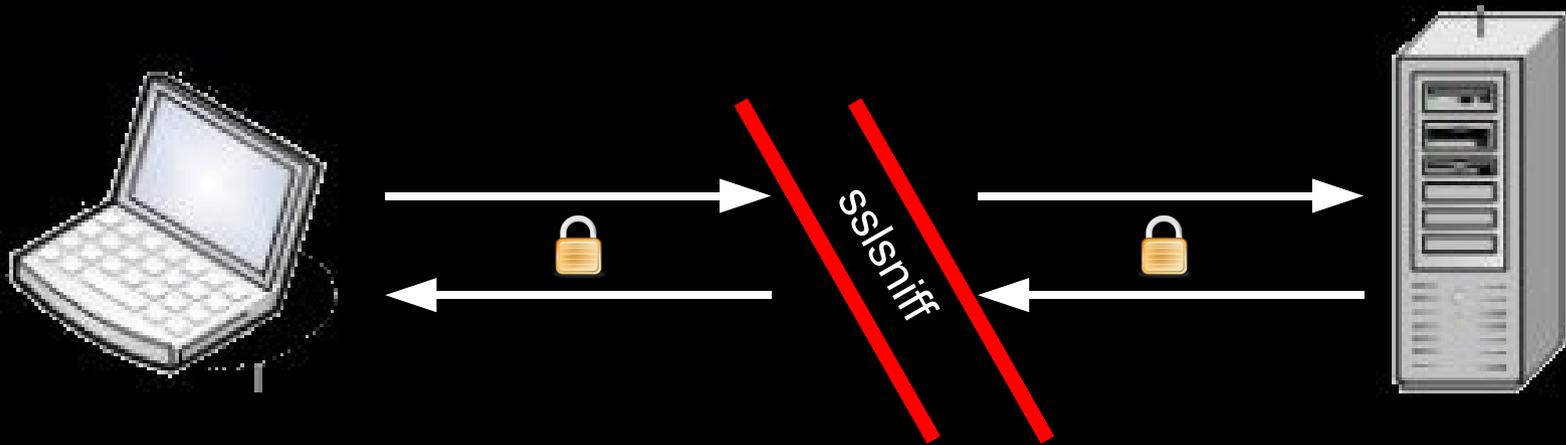
Microsoft claimed that it was impossible to exploit.

So I also published a tool that exploits it.

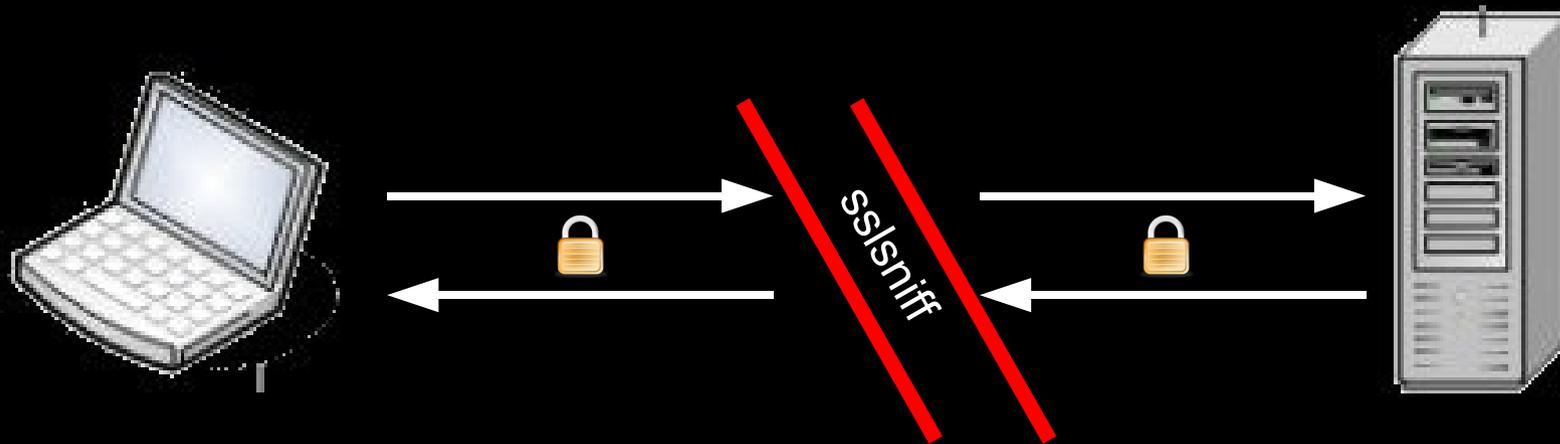
# sslsniff



# sslsniff



# sslsniff



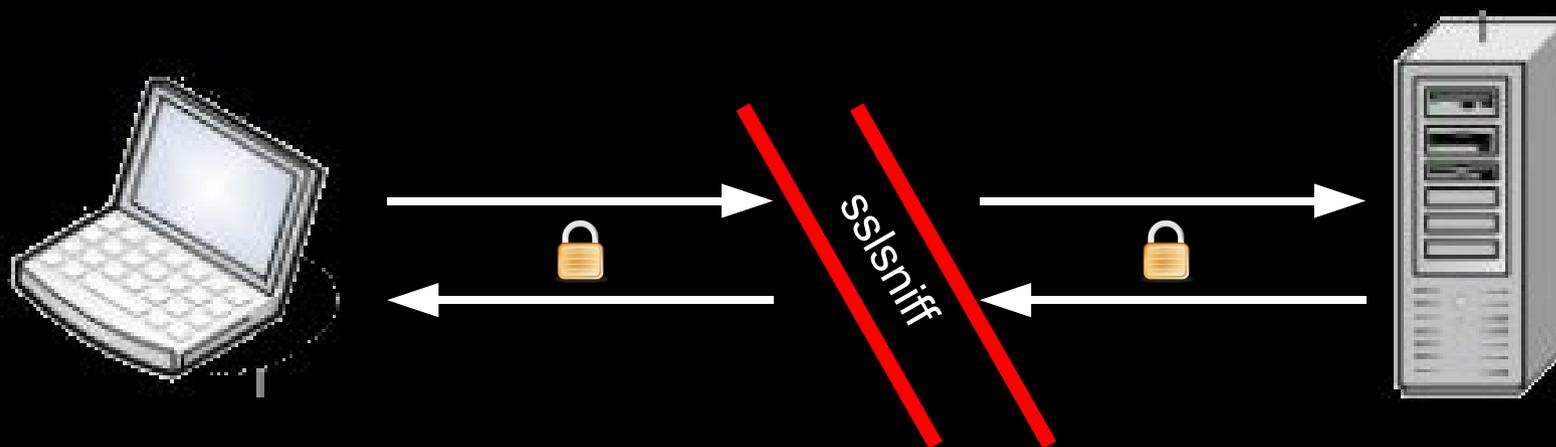
## Client Side:

Intercepts HTTPS traffic.  
Generates a certificate for the site the client is connecting to.  
Signs that with whatever certificate you specify.  
Proxies data through.

## Server Side:

Makes normal HTTPS connection to the server.  
Sends and receives data as if it's a normal client.

# sslsniff



Back before people started checking BasicConstraints:  
All you had to do was pass sslsniff a valid leaf node certificate for any domain.  
It would automatically generate a certificate for the domain the client was connecting to on the fly.  
It would sign that certificate with the leaf node.  
IE, Konqueror, etc... wouldn't notice the difference.

# sslsniff post-disclosure

You'd be surprised who still doesn't check basic constraints.

Even when people got warning dialogs in browsers that had been fixed, most of the time they'd just click through them.

Still useful as a general MITM tool for SSL.

The folks who did the MD5 hash collision stuff used sslsniff to hijack connections once they'd gotten a CA cert.

There are other uses yet, to be disclosed another day.

Surely we can do better.

# The things you learn in TV studios.

The image shows a screenshot of the Bank of America website as it appeared in a Mozilla Firefox browser window. The browser's address bar shows the URL `http://www.bankofamerica.com/index.jsp`. The website features the Bank of America logo and navigation links for "Locations", "Contact Us", "Help", "Sign In", and "En Español". A search bar is also present. The main navigation menu includes "PERSONAL", "SMALL BUSINESS", "CORPORATE & INSTITUTIONAL", and "ABOUT BANK OF AMERICA".

The "Online Banking" section on the left includes the text "Easy. Secure. Free." and an "Enroll" button. Below this, there are input fields for "Enter Online ID:" and "Password:", along with a "Sign In" button and a link for "Forgot or need help with your ID?".

The central banner features the headline "You've served our country. Now it's our privilege to serve you." and promotes "Military Banking accounts from Bank of America." with a "Get started today" button. The banner includes an image of a soldier's photo album and dog tags.

The "Products & Services" section is divided into three columns:

- Products & Services:** Checking, Savings & CDs, Credit cards, Mortgage, Refinance, Home equity, Auto loans, IRAs, Investment Services.
- Manage Your Accounts:** Fees and processes, Order Check Card, Online Investing, **Online Banking >** Viewing your accounts, Accessing credit cards, Bill Pay, Tracking your expenses.
- Achieve Your Goals:** Keep the Change®, Buying a home, Searching for a home, Retirement Center, Planning for college, Student loans, Purchasing a car, Consolidating debt, Small Business Online.

At the bottom, there is a search bar with the text "Find:" and options for "Previous", "Next", "Highlight all", and "Match case".

# The things you learn in TV studios.

Bank of America | Home | Personal - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.bankofamerica.com/index.jsp

Most Visited

Locations • Contact Us • Help • Sign In • En Español

**Bank of America**

PERSONAL > SMALL BUSINESS > CORPORATE & INSTITUTIONAL > ABOUT BANK OF AMERICA >

**Online Banking**

Easy. Secure. Free.  
**Enroll** View demo | Learn more

Enter Online ID:

Save this Online ID

Password:

Where do I enter my Passcode?  
**Sign In**

Forgot or need help with your ID?  
Reset Passcode

Your Privacy & Security  
Report suspicious email  
Norton 360 - Free Trial

**You've served our country. Now it's our privilege to serve you.**  
Military Banking accounts from Bank of America.  
Convenient, secure banking wherever you are.  
Military Banking from Bank of America.  
**Get started today**

**Products & Services**  
Checking  
Savings & CDs  
Credit cards  
Mortgage  
Refinance  
Home equity  
Auto loans  
IRAs  
Investment Services

**Manage Your Accounts**  
Fees and processes  
Order Check Card  
Online Investing  
**Online Banking >**  
Viewing your accounts  
Accessing credit cards  
Bill Pay  
Tracking your expenses

**Achieve Your Goals**  
Keep the Change®  
Buying a home  
Searching for a home  
Retirement Center  
Planning for college  
Student loans  
Purchasing a car  
Consolidating debt  
Small Business Online

Find:  Previous Next Highlight all Match case

Done

# The things you learn in TV studios.

The image shows a screenshot of the Bank of America website as viewed in a Mozilla Firefox browser. The browser's address bar shows the URL `http://www.bankofamerica.com/index.jsp`. The website header includes the Bank of America logo, navigation links for "Locations", "Contact Us", "Help", "Sign In", and "En Español", and a search bar. A red navigation bar contains links for "PERSONAL", "SMALL BUSINESS", "CORPORATE & INSTITUTIONAL", and "ABOUT BANK OF AMERICA".

The main content area features a "Sign In" section on the left with the text "Easy. Secure. Free." and an "Enroll" button. Below this are input fields for "Enter Online ID:" and "Password:", a "Save this Online ID" checkbox, and a "Sign In" button highlighted by a red arrow. A link "Forgot or need help with your ID? Reset Passcode" is also present. To the right is a promotional banner for "Military Banking" with the headline "You've served our country. Now it's our privilege to serve you." and a "Get started today" button.

Below the banner are three columns of "Products & Services":

- Products & Services:** Checking, Savings & CDs, Credit cards, Mortgage, Refinance, Home equity, Auto loans, IRAs, Investment Services.
- Manage Your Accounts:** Fees and processes, Order Check Card, Online Investing, **Online Banking >** Viewing your accounts, Accessing credit cards, Bill Pay, Tracking your expenses.
- Achieve Your Goals:** Keep the Change®, Buying a home, Searching for a home, Retirement Center, Planning for college, Student loans, Purchasing a car, Consolidating debt, Small Business Online.

The browser's status bar at the bottom shows "Done" and a search bar with options for "Previous", "Next", "Highlight all", and "Match case".

# The things you learn in TV studios.



Online Banking 

Easy. Secure. Free.

**Enroll** [View demo](#) | [Learn more](#)

Enter Online ID:

Save this Online ID

**Password:**

[Where do I enter my Passcode?](#)

**Sign In**

[Forgot or need help with your ID?](#)  
[Reset Passcode](#)

This button posts to an HTTPS link, but there's no way to know that.

It's a button, so if you mouse-over it, the link isn't displayed in the browser bar at the bottom.

The best you could do would be to view the page source, but that's problematic in browsers like Firefox that issue a second request to the server for the source.

# Still prevalent today...

Wachovia - Personal Finance and Business Financial Services - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.wachovia.com/

Most Visited Getting Started Latest Headlines

Customer Service | Contact Us | Locations



**The time is now.**  
Mortgage rates are at an all-time low.  
Refinance today and save.

[Learn How >](#)

**LOGIN**

User ID:  
  
 Remember my User ID

Password:  
  
(case sensitive)

Service:  
Choose a service...

Forgot [User ID](#) or [Password](#)?

Retirement Plan Participants: [Login](#)  
Education Loan Customers: [Login](#)

**PERSONAL FINANCE**

**Online Services**  
Online Banking with BillPay  
Mobile Banking  
Online Brokerage  
More...

**Banking**  
Checking  
Savings & CDs  
Credit Cards  
Check Cards  
More...

**Retirement Planning**  
Tools & information for  
Lifetime Retirement Planning

**Lending**  
Mortgage  
Home Equity **New!**  
Education Loans  
Vehicle Loans

**Investing**  
Accounts & Services  
IRAs  
More...

**Rates**  
Mortgage Rates  
Home Equity Rates  
Credit Card Rates

**Insurance**  
Life, Auto, Home,  
Health

**Payment Challenges?**  
Explore your loan options

**STRENGTH AND STABILITY**  
Wachovia is now  
part of Wells Fargo.  
[Learn More >>](#)

**WACHOVIA SECURITIES**  
An industry leader in investment and  
advisory services for individuals,  
corporations and institutions.

**SMALL BUSINESS**  
The tools, services, and research to  
manage your company.  
[Small Business Login](#)

**ONLINE BANKING.**  
Securely manage your business  
finances online.  
[Wachovia Business Online.](#)

**Refer a Friend**  
It adds up to \$25 for both  
of you.  
[See How >>](#)

**Ready to get organized?**  
It's easier than you think.  
[Go Paperless >>](#)

**Online Security**  
[Wachovia Security Plus<sup>SM</sup>](#)  
[Online Services Guarantee](#)

**Sign Up for Online Banking**  
[Sign Up](#) | [Learn More](#) | [Demo](#)

**LOCATIONS**  
ZIP:    
[More Search Options](#)

Done

# Still prevalent today...

The image shows a screenshot of a Mozilla Firefox browser window. The title bar reads "Sign In - Mozilla Firefox". The address bar contains the URL "http://login.live.com/login.srf?wa=wsignin1.0&r...". The page content features the Windows Live logo and a sign-in form. The form includes fields for "Windows Live ID" (with an example email address) and "Password", along with checkboxes for "Remember me on this computer" and "Remember my password", and a "Sign in" button. A "Sign up" button is also visible for users without an ID.

Sign In - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://login.live.com/login.srf?wa=wsignin1.0&r... Google

Most Visited Getting Started Latest Headlines

## Windows Live

One Windows Live ID gets you into **Hotmail, Messenger, Xbox LIVE** — and other places you see

### Hotmail

- Powerful Microsoft technology helps fight spam and improve security.
- Get more done thanks to greater ease and speed.
- Lots of storage (5 GB) - more cool stuff on the way.

[Learn more](#)

Don't have a Windows Live ID?

[Sign up](#)

### Sign in

Windows Live ID:   
(example555@hotmail.com)

Password:   
[Forgot your password?](#)

Remember me on this computer (?)

Remember my password (?)

[Sign in](#)

Use enhanced security

Done

There are some generalizable attacks  
here.

# Browsers Then And Now...

# Then: A Positive Feedback System

A number of indicators deployed to designate that a page *is* secure.

A proliferation of little lock icons.

URL bars that turn gold.

# Then: An example from Firefox 2

Yahoo! Mail: The best web-based email! - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://login.yahoo.com/config/mail?.intl=us& Google

**YAHOO! MAIL** Yahoo! - Blog - Help



**Chat right from your Inbox.**  
» [See how](#)

**Your Inbox understands you've got news to share.**

-  See which of your contacts are online at a glance.
-  Easily switch from email to chat and back again.
-  Start right away, no download or setup needed.

[See how](#) to instantly reach friends and family from the New Yahoo! Mail.

**Sign in to Yahoo!**

 **Are you protected?**  
Create your sign-in seal.  
(Why?)

Yahoo! ID:  
  
(e.g. free2rhyme@yahoo.com)

Password:

**Keep me signed in**  
for 2 weeks unless I sign out. [Info](#)  
[Uncheck if on a shared computer]

[Forget your ID or password?](#) | [Help](#)

**Don't have a Yahoo! ID?**  
Signing up is easy.  
[Sign Up](#)

Done | login.yahoo.com | Tor Disabled | FoxyProxy: Disabled

# Then: An example from Firefox 2

Yahoo! Mail: The best web-based email! - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://login.yahoo.com/config/mail?.intl=us&

Google

**YAHOO! MAIL** Yahoo! - Blog - Help

**Chat right from your Inbox.**  
» [See how](#)

**Your Inbox understands you've got news to share.**

- See which of your contacts are online at a glance.
- Easily switch from email to chat and back again.
- Start right away, no download or setup needed.

[See how](#) to instantly reach friends and family from the New Yahoo! Mail.

**Sign in to Yahoo!**

**Are you protected?**  
Create your sign-in seal. (Why?)

Yahoo! ID:  
  
(e.g. free2rhyme@yahoo.com)

Password:

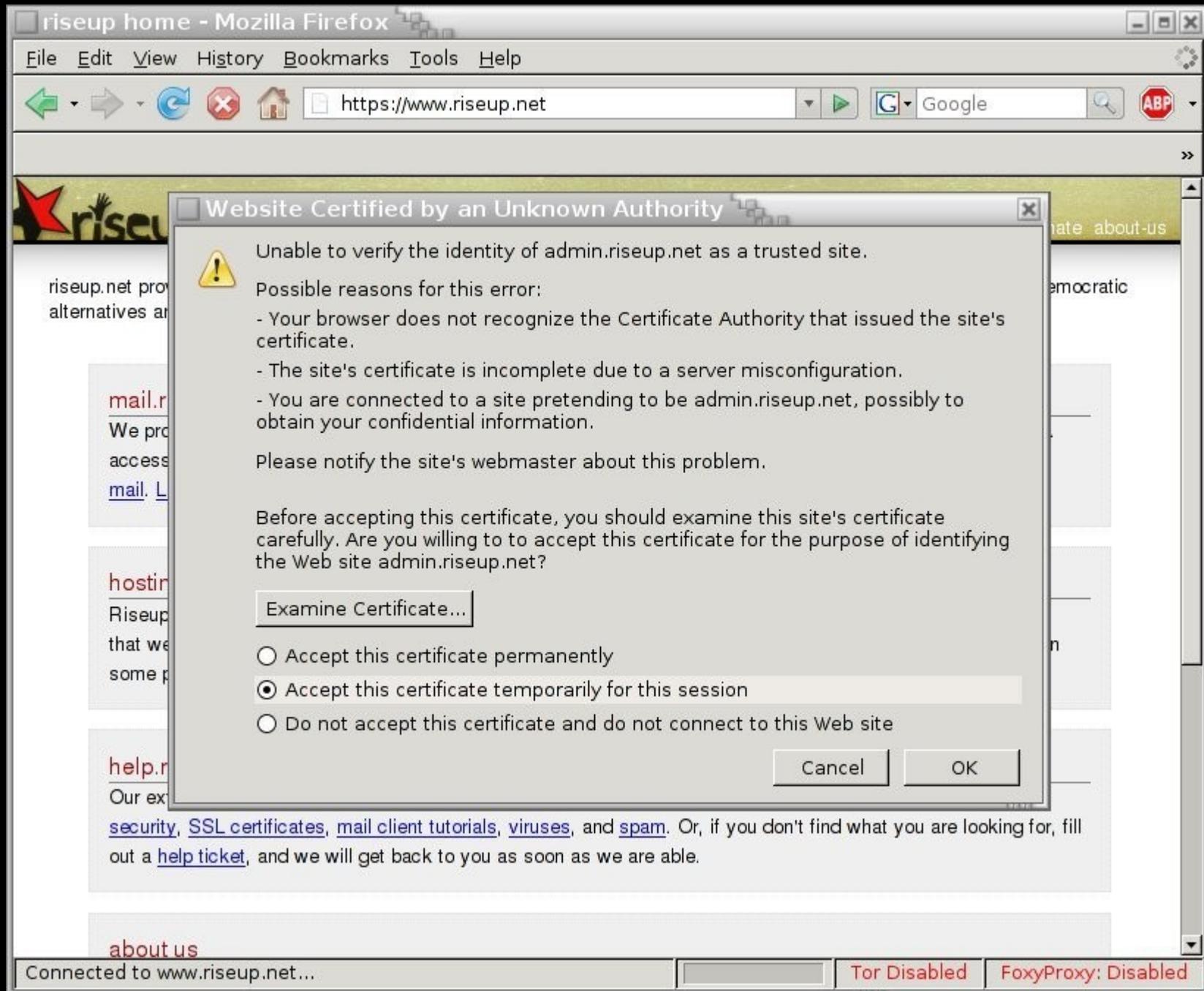
**Keep me signed in**  
for 2 weeks unless I sign out. [Info](#)  
[Uncheck if on a shared computer]

[Forget your ID or password?](#) | [Help](#)

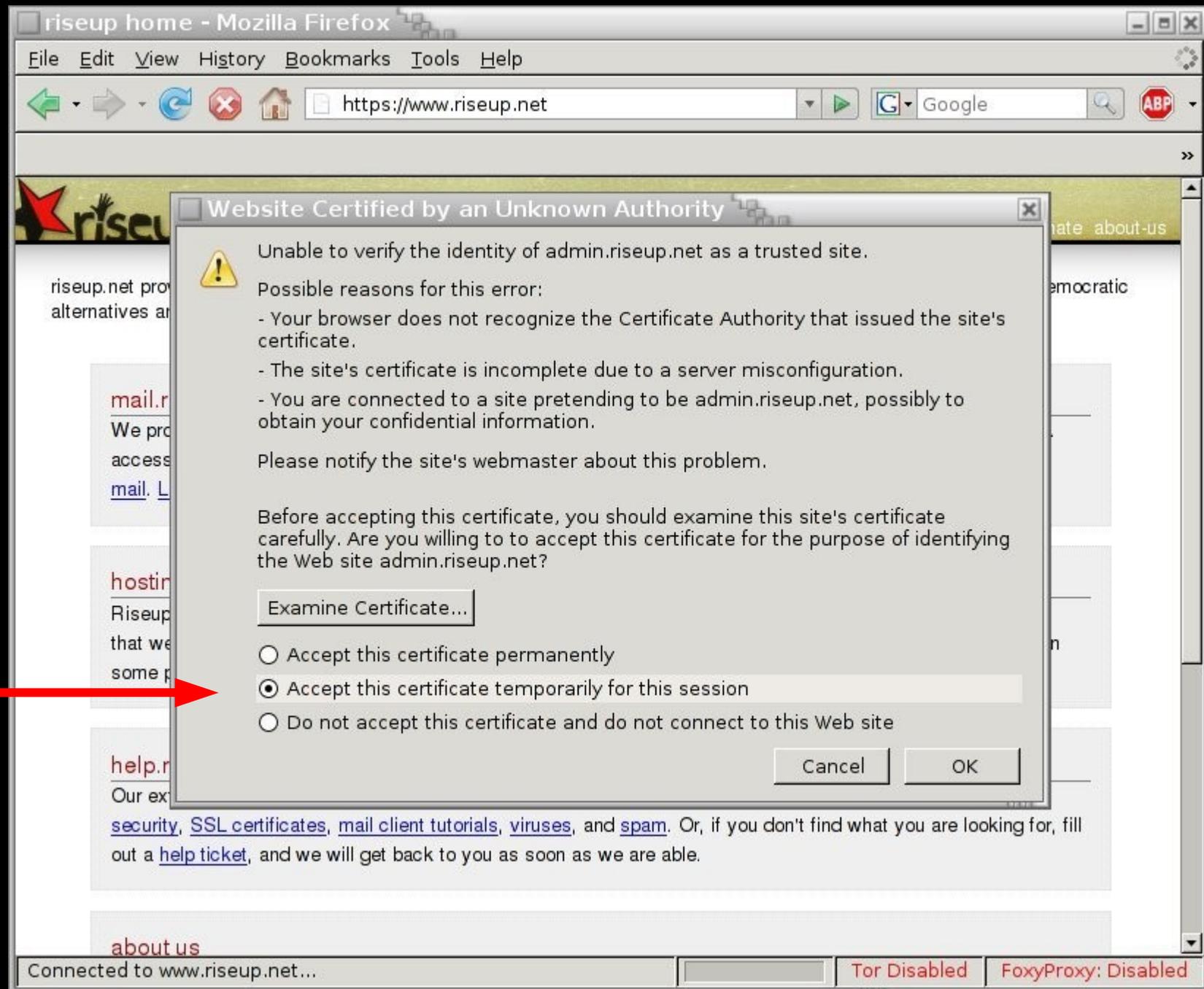
**Don't have a Yahoo! ID?**  
Signing up is easy.  
[Sign Up](#)

Done | login.yahoo.com | Tor Disabled | FoxyProxy: Disabled

# Then: An example from Firefox 2



# Then: An example from Firefox 2



# Now: A Negative Feedback System

Less emphasis on sites being secure.

The proliferation of little locks has been toned down.

Firefox's gold bar is gone.

More emphasis on alerting users to problems.

A maze of hoops that users have to jump through in order to access sites with certificates that aren't signed by a CA.

# Now: An example from Firefox 3

Yahoo! Mail: The best web-based email! - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://login.yahoo.com/config/login\_verify2?&.src=ym

Most Visited Getting Started Latest Headlines

**YAHOO! MAIL** Yahoo! - Help



**Chat right from your Inbox.**

» [See how](#)

**Your Inbox understands you've got news to share.**

-  See which of your contacts are online at a glance.
-  Easily switch from email to chat and back again.
-  Start right away, no download or setup needed.

[See how](#) to instantly reach friends and family from the New Yahoo! Mail.

**Don't have a Yahoo! ID?**  
Signing up is easy.

[Sign up for Yahoo!](#)

---

**Already have a Yahoo! ID?**  
Sign in.

 **Are you protected?**  
Create your sign-in seal. (Why?)

Yahoo! ID:  
  
(e.g. free2rhyme@yahoo.com)

Password:

**Keep me signed in**  
for 2 weeks unless I sign out. [Info](#)  
[Uncheck if on a shared computer]

[Sign In](#)

Done | login.yahoo.com

# Now: An example from Firefox 3

Yahoo! Mail: The best web-based email! - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://login.yahoo.com/config/login\_verify2?&.src=ym

Most Visited Getting Started Latest Headlines

**YAHOO! MAIL** Yahoo! - Help

**Chat right from your Inbox.**  
» [See how](#)

**Your Inbox understands you've got news to share.**

- See which of your contacts are online at a glance.
- Easily switch from email to chat and back again.
- Start right away, no download or setup needed.

[See how](#) to instantly reach friends and family from the New Yahoo! Mail.

**Don't have a Yahoo! ID?**  
Signing up is easy.  
[Sign up for Yahoo!](#)

**Already have a Yahoo! ID?**  
Sign in.

**Are you protected?**  
Create your sign-in seal. (Why?)

Yahoo! ID:  
  
(e.g. free2rhyme@yahoo.com)

Password:

**Keep me signed in**  
for 2 weeks unless I sign out. [Info](#)  
[Uncheck if on a shared computer]

[Sign In](#)

Done login.yahoo.com

# Now: An example from Firefox 3

Yahoo! Mail: The best web-based email! - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://login.yahoo.com/config/login\_verify2?&.src=ym

Most Visited Getting Started Latest Headlines

## YAHOO! MAIL

Yahoo! - Help



**Chat right from your Inbox.**

» [See how](#)

**Your Inbox understands you've got news to share.**

-  See which of your contacts are online at a glance.
-  Easily switch from email to chat and back again.
-  Start right away, no download or setup needed.

[See how](#) to instantly reach friends and family from the New Yahoo! Mail.

**Don't have a Yahoo! ID?**  
Signing up is easy.

[Sign up for Yahoo!](#)

---

**Already have a Yahoo! ID?**  
Sign in.

 **Are you protected?**  
Create your sign-in seal. (Why?)

Yahoo! ID:  
  
(e.g. free2rhyme@yahoo.com)

Password:

**Keep me signed in**  
for 2 weeks unless I sign out. [Info](#)  
[Uncheck if on a shared computer]

[Sign In](#)

Done login.yahoo.com

# Now: An example from Firefox 3

Yahoo! Mail: The best web-based email! - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://login.yahoo.com/config/login\_verify2?&.src=ym

Most Visited Getting Started Latest Headlines

## YAHOO! MAIL

Yahoo! - Help



**Chat right from your Inbox.**

» [See how](#)

**Your Inbox understands you've got news to share.**

-  See which of your contacts are online at a glance.
-  Easily switch from email to chat and back again.
-  Start right away, no download or setup needed.

[See how](#) to instantly reach friends and family from the New Yahoo! Mail.

**Don't have a Yahoo! ID?**  
Signing up is easy.

[Sign up for Yahoo!](#)

---

**Already have a Yahoo! ID?**  
Sign in.



**Are you protected?**  
Create your sign-in seal.  
(Why?)

Yahoo! ID:  
  
(e.g. free2rhyme@yahoo.com)

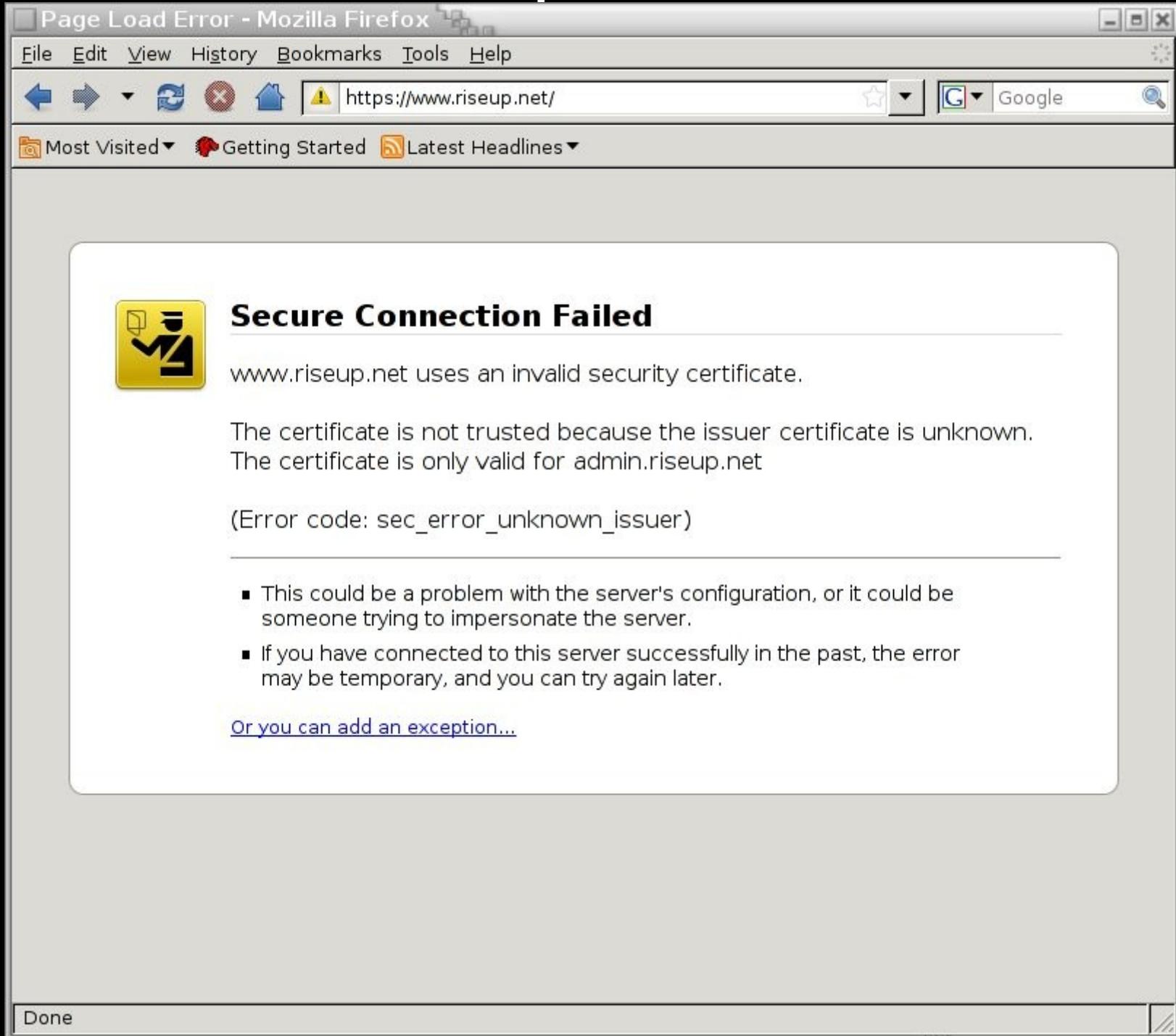
Password:

**Keep me signed in**  
for 2 weeks unless I sign out. [Info](#)  
[Uncheck if on a shared computer]

[Sign In](#)

Done login.yahoo.com

# Now: An example from Firefox 3



The screenshot shows a Mozilla Firefox browser window with the title "Page Load Error - Mozilla Firefox". The address bar displays "https://www.riseup.net/" with a warning icon. The error message is displayed in a white box with a yellow border. It features a yellow icon of a person with a question mark, followed by the heading "Secure Connection Failed". The text explains that the certificate is invalid because the issuer is unknown and only valid for "admin.riseup.net". It includes the error code "sec\_error\_unknown\_issuer" and a list of two possible causes: a server configuration problem or a temporary connection issue. A link "Or you can add an exception..." is provided at the bottom of the error box. The status bar at the bottom left shows "Done".

Page Load Error - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.riseup.net/ Google

Most Visited Getting Started Latest Headlines

 **Secure Connection Failed**

www.riseup.net uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.  
The certificate is only valid for admin.riseup.net

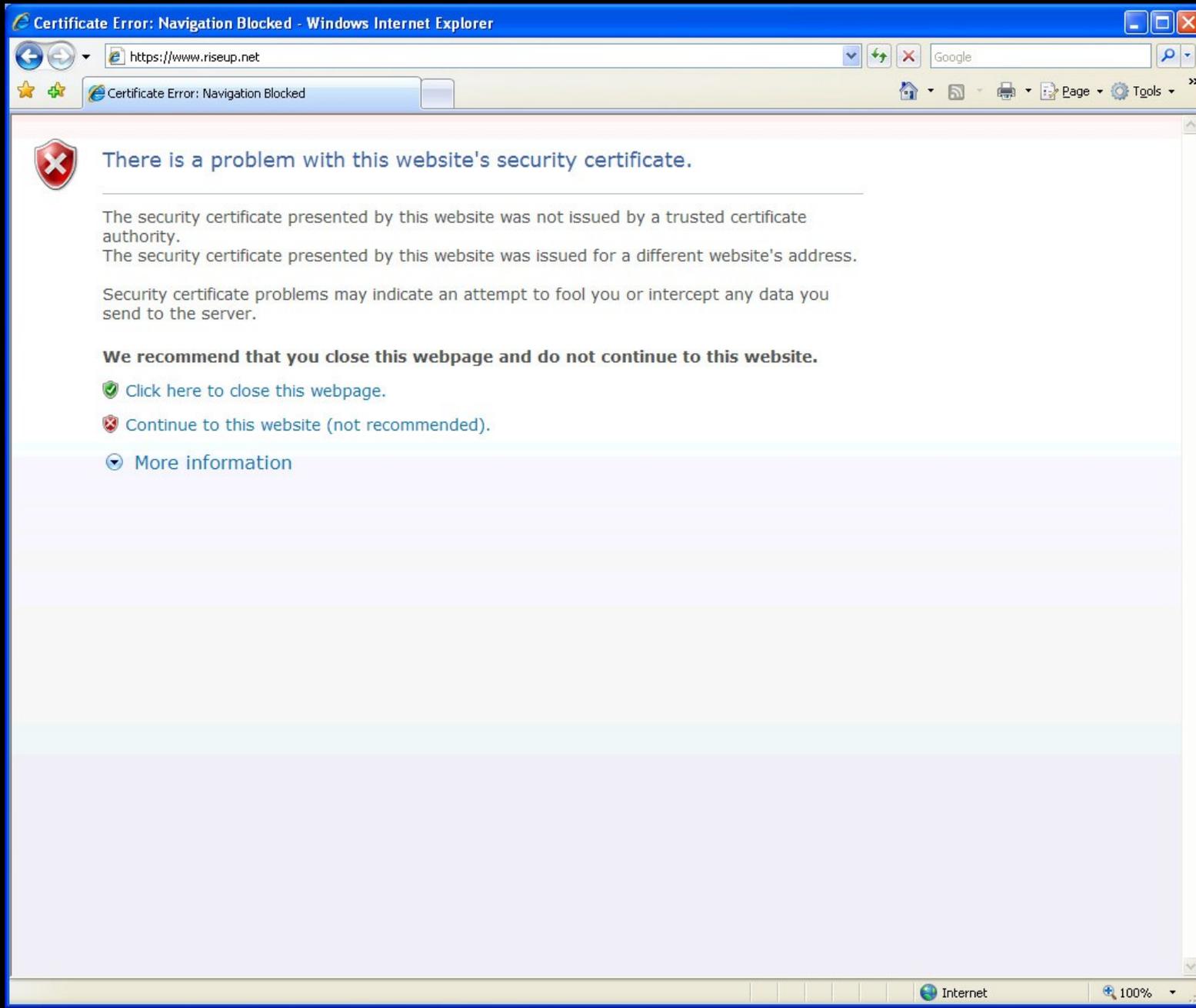
(Error code: sec\_error\_unknown\_issuer)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

[Or you can add an exception...](#)

Done

# Now: An example from IE



# Conclusions

If we trigger the negative feedback, we're screwed.

If we fail to trigger the positive feedback, it's not so bad.

How is SSL used?

Nobody types https://  
(or http:// for that matter)

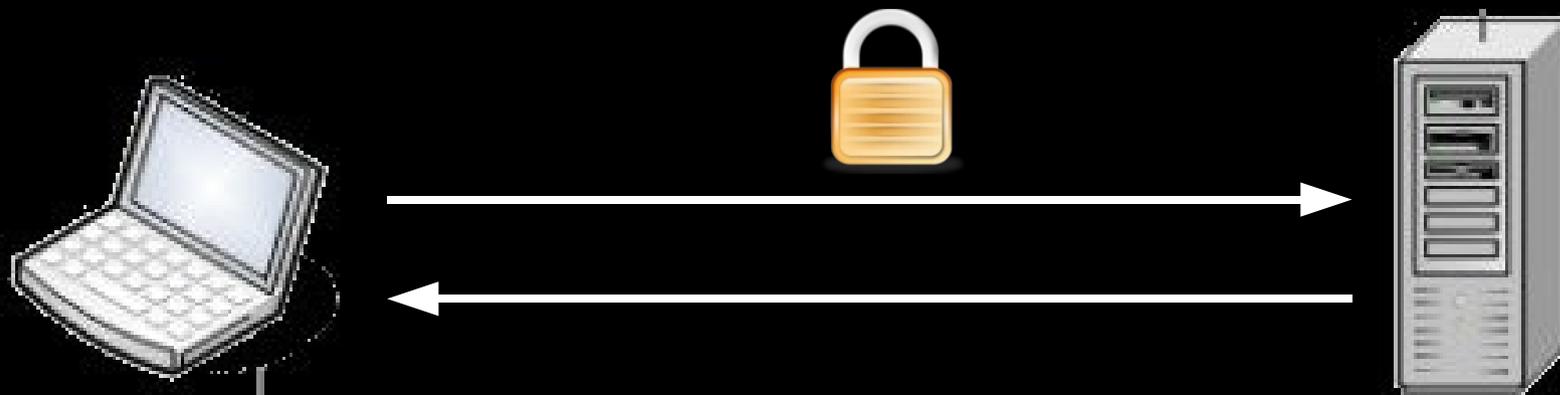
People generally encounter SSL  
in only two ways:

Clicking on links.

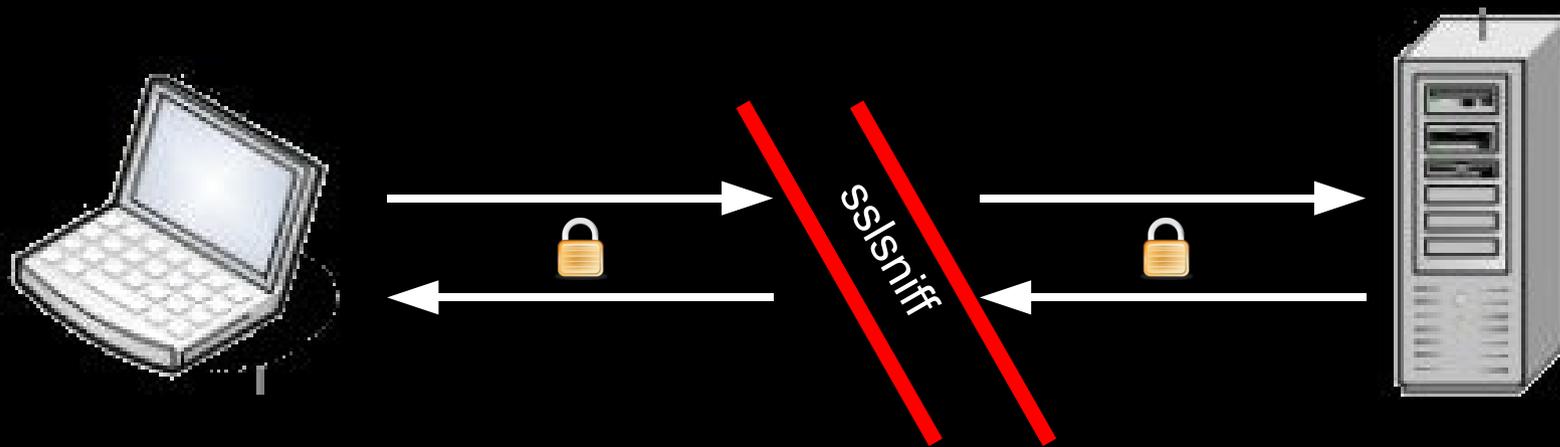
Through 302's.

Which means that people only encounter SSL through HTTP...

# First cut: A different kind of MITM



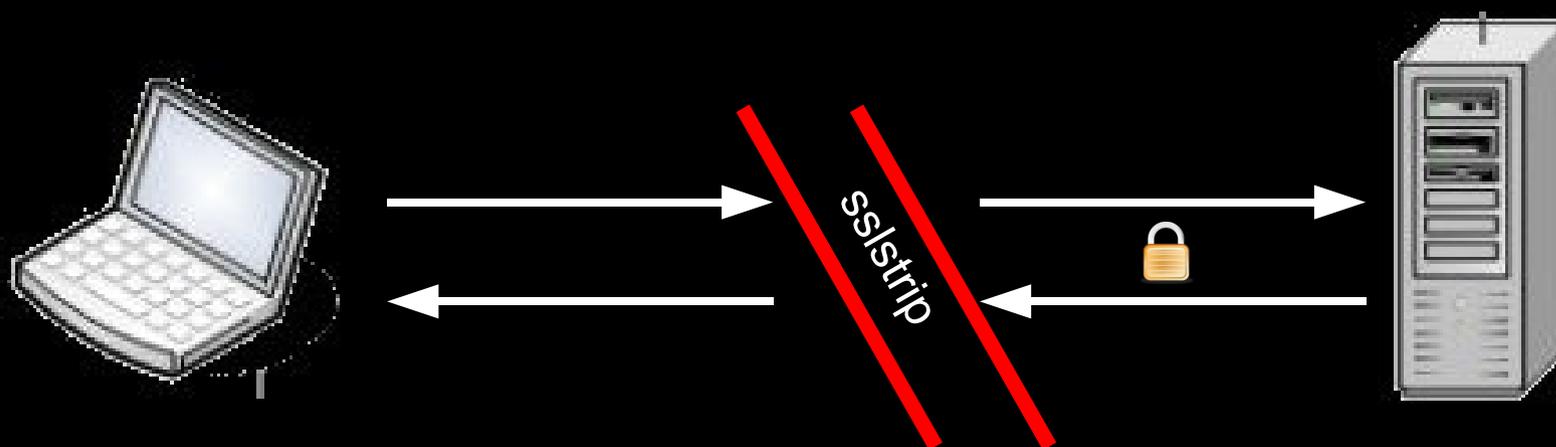
Normally we attack the SSL connection...



# First cut: A different kind of MITM



What if we attacked the HTTP connection instead...



## Remember:

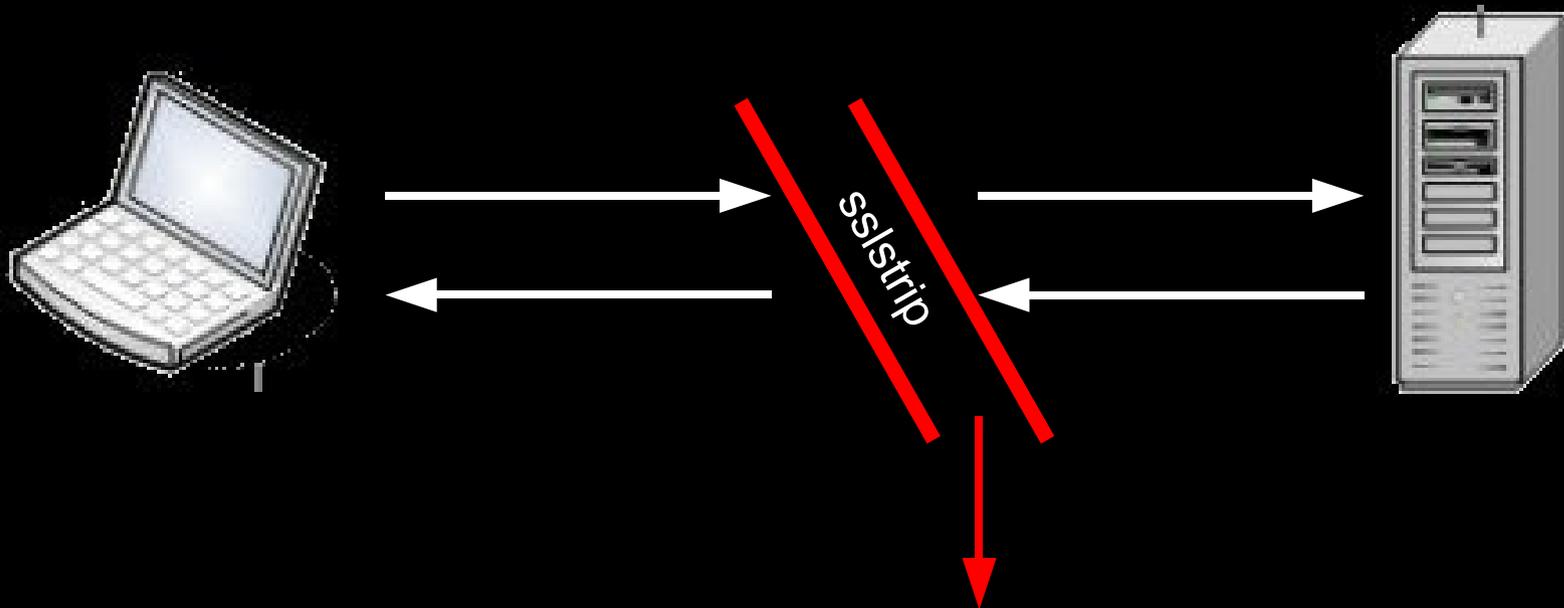
SSL is normally encountered in one of two ways.

By clicking on links.

Through 302 redirects.

We can attack both of those points through a HTTP MITM.

# A First Cut Recipe: sslstrip

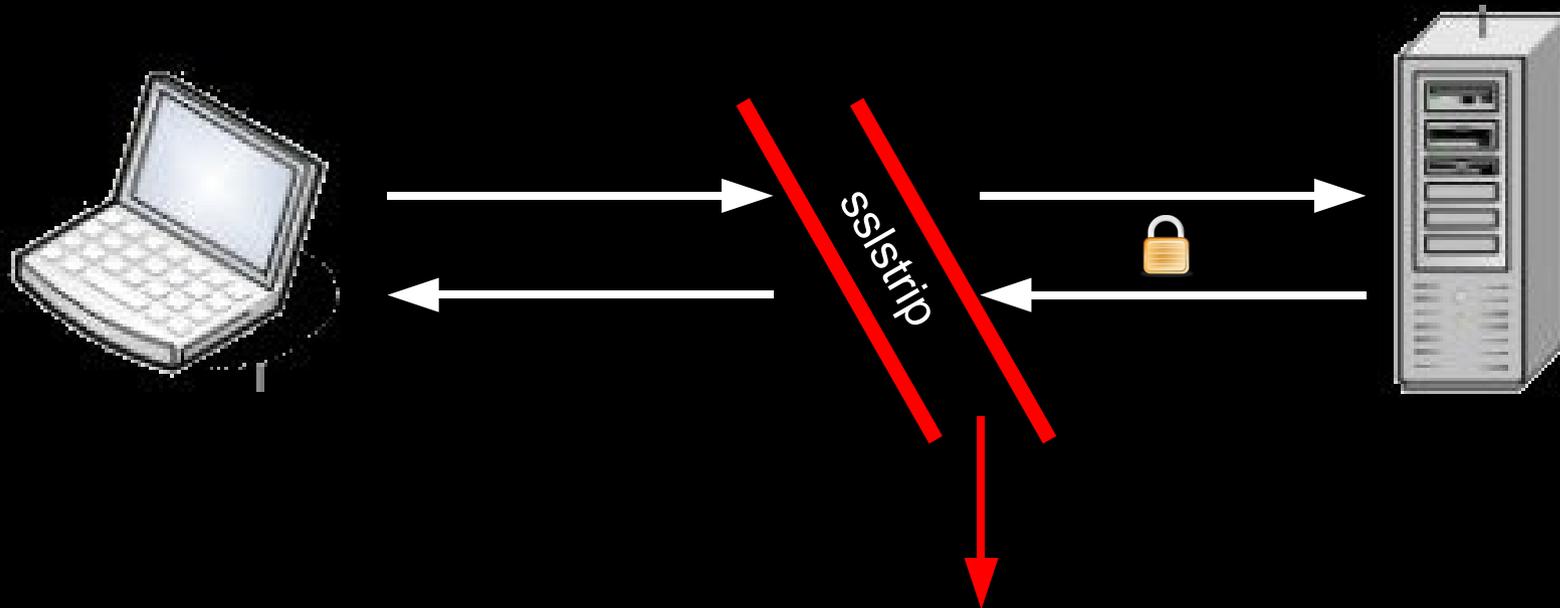


Watch HTTP traffic go by.

Switch `<a href="https://...">` to `<a href="http://...">` and keep a map of what's changed.

Switch Location: `https://...` to Location: `http://...` and keep a map of what's changed.

# A First Cut Recipe: sslstrip

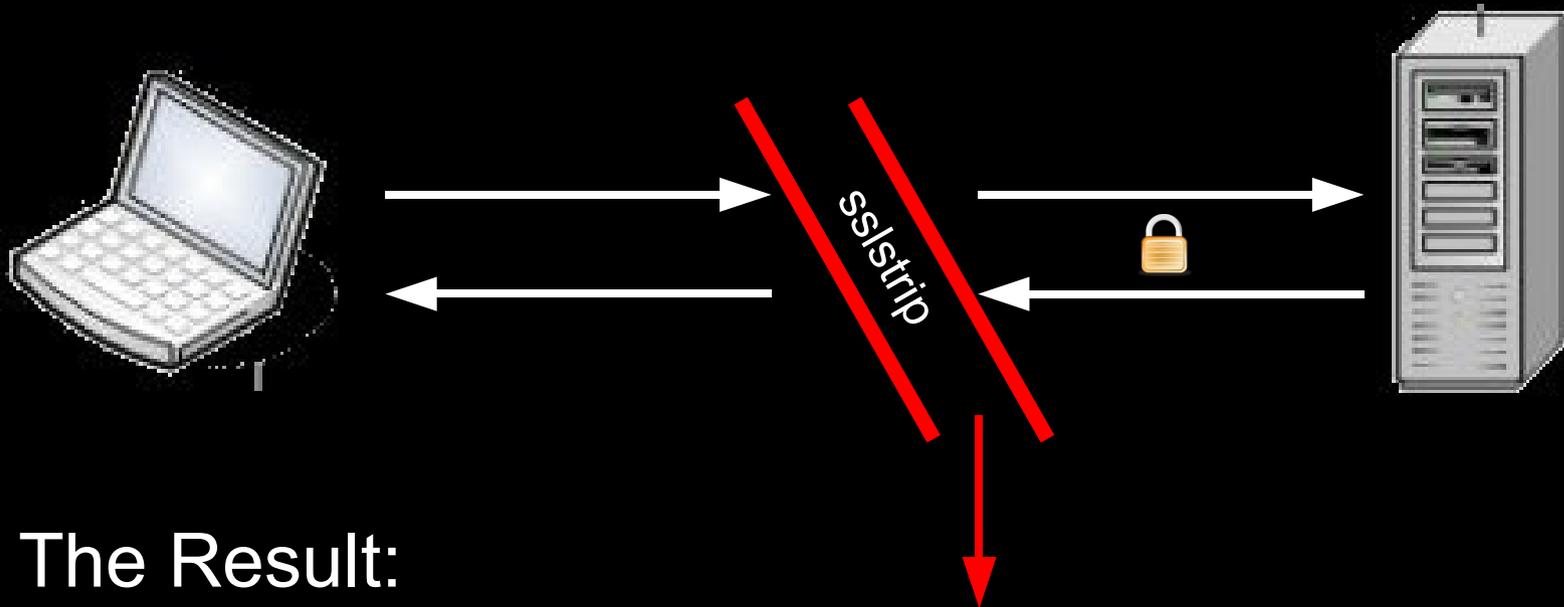


Watch HTTP traffic go by.

When we see an HTTP request for a URL that we've stripped, proxy that out as HTTPS to the server.

Watch the HTTPS traffic go by, log everything if we want, and keep a map of the relative links, CSS links, and JavaScript links that go by.

# A First Cut Recipe: sslstrip



## The Result:

The server never knows the difference. Everything looks secure on their end.

The client doesn't display any of the disastrous warnings that we want to avoid.

We see all the traffic.

How does it look?

# Secure Site

Gmail: Email from Google - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.google.com/accounts/ServiceLogin?service Google

Most Visited Getting Started Latest Headlines



## Welcome to Gmail

**A Google approach to email.**

Gmail is a new kind of webmail, 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/app>. [Learn more](#)
-  **Lots of space**  
Over 7290.461681 megabytes (and counting) of free storage so you'll never need to delete another message.

Sign in to Gmail with your **Google Account**

Username:

Password:

Remember me on this computer.

[I cannot access my account](#)

[Sign up for Gmail](#)

[About Gmail](#) [New features!](#)

©2009 Google - [Gmail for Organizations](#) - [Gmail Blog](#) - [Terms](#) - [Help](#)

Done www.google.com

# Secure Site

Gmail: Email from Google - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.google.com/accounts/ServiceLogin?service=

Most Visited Getting Started Latest Headlines



## Welcome to Gmail

### A Google approach to email.

Gmail is a new kind of webmail, 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/app>. [Learn more](#)
-  **Lots of space**  
Over 7290.462157 megabytes (and counting) of free storage so you'll never need to delete another message.

Sign in to Gmail with your  
**Google Account**

Username:

Password:

Remember me on this computer.

[I cannot access my account](#)

[Sign up for Gmail](#)

[About Gmail](#) [New features!](#)

©2009 Google - [Gmail for Organizations](#) - [Gmail Blog](#) - [Terms](#) - [Help](#)

Done

# Secure Site

Gmail: Email from Google

https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&co Google

Apple Yahoo! Google Maps YouTube Wikipedia News (26) Popular



**Welcome to Gmail**

**A Google approach to email.**

Gmail is a new kind of webmail, 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/app>.  
[Learn more](#)
-  **Lots of space**  
Over 7295.652889 megabytes (and counting) of free storage so you'll never need to delete another message.

Sign in to Gmail with your  
**Google Account**

Username:

Password:

Remember me on this computer.

[I cannot access my account](#)

[Sign up for Gmail](#)

[About Gmail](#) [New features!](#)

©2009 Google - [Gmail for Organizations](#) - [Gmail Blog](#) - [Terms](#) - [Help](#)

# Secure Site

Gmail: Email from Google

http://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&con - Google

Apple Yahoo! Google Maps YouTube Wikipedia News (26) Popular



**Welcome to Gmail**

**A Google approach to email.**

Gmail is a new kind of webmail, 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/app>.  
[Learn more](#)
-  **Lots of space**  
Over 7295.653389 megabytes (and counting) of free storage so you'll never need to delete another message.

Sign in to Gmail with your  
**Google Account**

Username:

Password:

Remember me on this computer.

[I cannot access my account](#)

[Sign up for Gmail](#)

[About Gmail](#) [New features!](#)

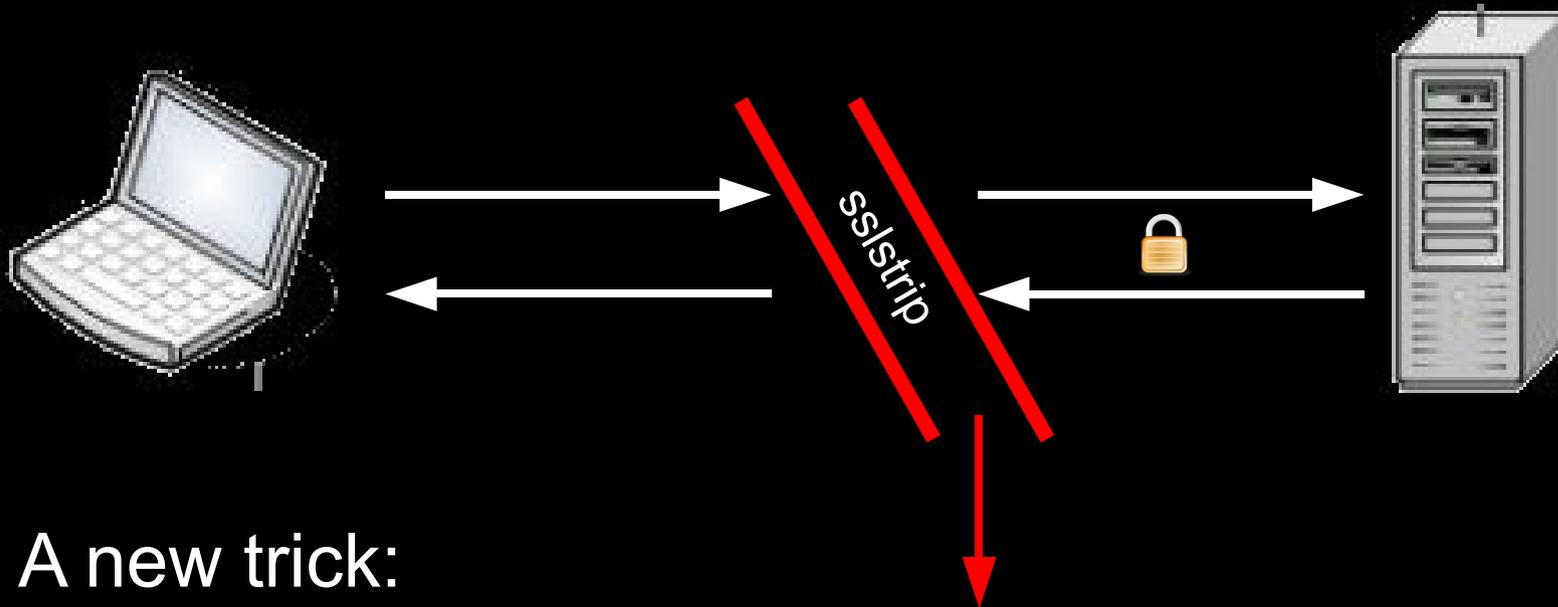
©2009 Google - [Gmail for Organizations](#) - [Gmail Blog](#) - [Terms](#) - [Help](#)

# What else can we do?

We've managed to avoid the negative feedback, but some positive feedback would be good too.

People seem to like the little lock icon thing, so it'd be nice if we could get that in there too.

# A 1.5 Cut: sslstrip



## A new trick:

Let's do everything the same, but now watch out for favicon requests as well.

If we see a favicon request for a URL that we've stripped, we'll send back a favicon of our choosing instead.

What should our favicon be?  
You guessed it:



# Once again, a secure site:

Gmail: Email from Google - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.google.com/accounts/ServiceLogin?service Google

Most Visited Getting Started Latest Headlines



## Welcome to Gmail

### A Google approach to email.

Gmail is a new kind of webmail, 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/app>. [Learn more](#)
-  **Lots of space**  
Over 7290.461681 megabytes (and counting) of free storage so you'll never need to delete another message.

Sign in to Gmail with your  
**Google Account**

Username:

Password:

Remember me on this computer.

[I cannot access my account](#)

[Sign up for Gmail](#)

[About Gmail](#) [New features!](#)

©2009 Google - [Gmail for Organizations](#) - [Gmail Blog](#) - [Terms](#) - [Help](#)

Done www.google.com

# Once again, a secure site:

Gmail: Email from Google - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.google.com/accounts/ServiceLogin?service=

Most Visited Getting Started Latest Headlines



**Welcome to Gmail**

**A Google approach to email.**

Gmail is a new kind of webmail, 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/app>. [Learn more](#)
-  **Lots of space**  
Over 7290.462157 megabytes (and counting) of free storage so you'll never need to delete another message.

Sign in to Gmail with your **Google Account**

Username:

Password:

Remember me on this computer.

[I cannot access my account](#)

[Sign up for Gmail](#)

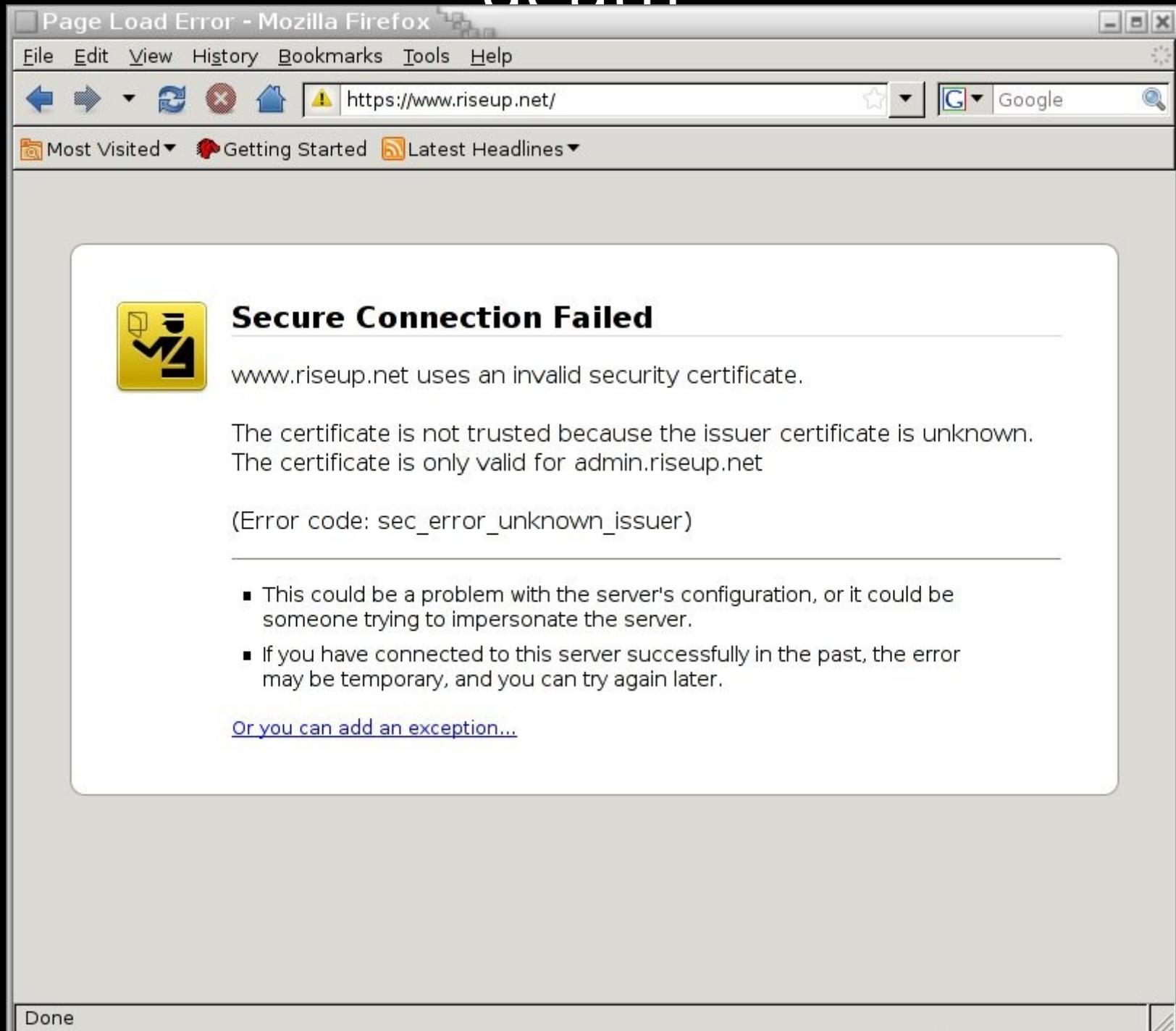
[About Gmail](#) [New features!](#)

©2009 Google - [Gmail for Organizations](#) - [Gmail Blog](#) - [Terms](#) - [Help](#)

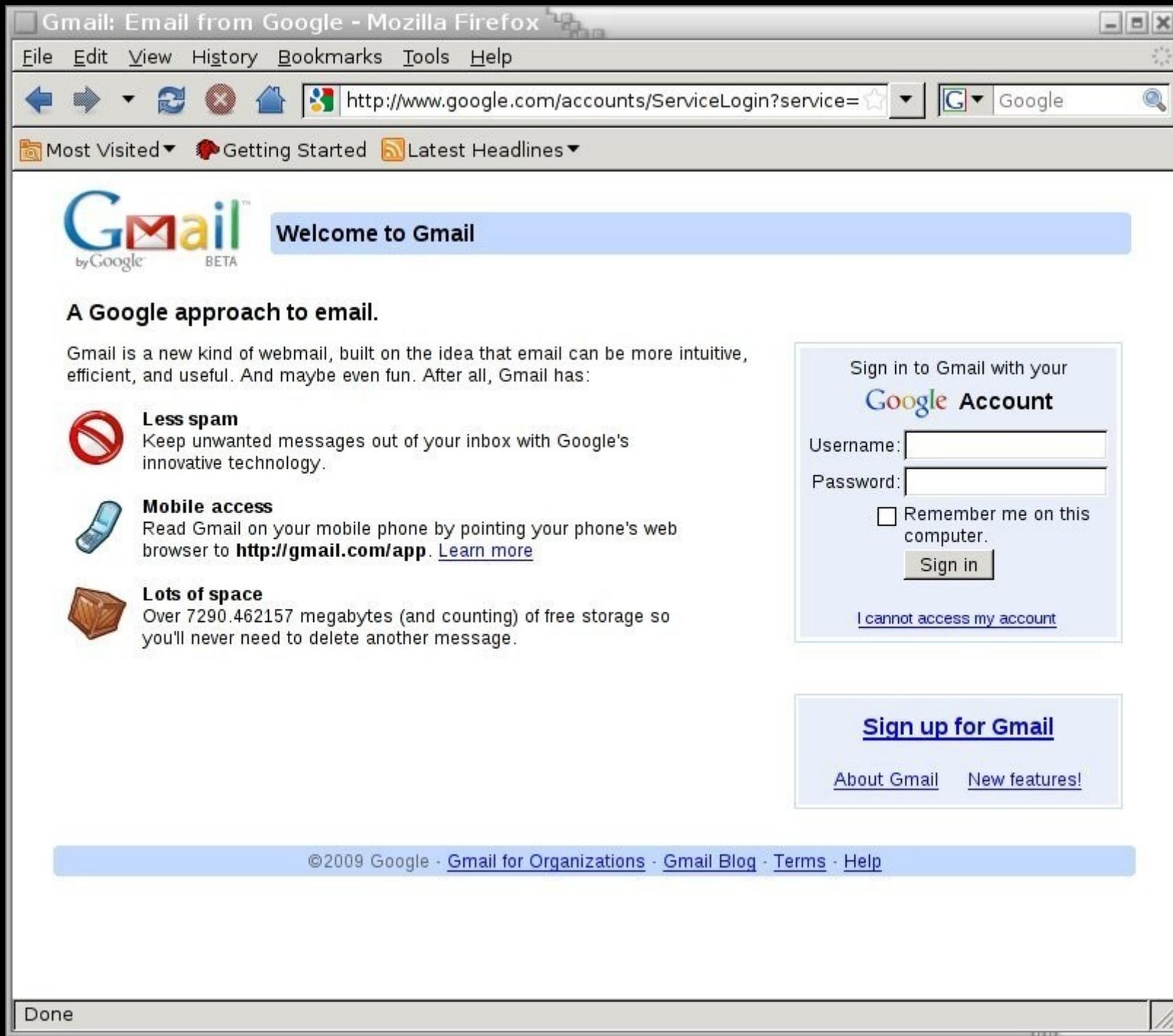
Done

We're doing pretty good.

# We've avoided the negative feedback of death



# We can do a subtle MITM via HTTP.



# And if we want we can throw in a little lock icon

Gmail: Email from Google - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.google.com/accounts/ServiceLogin?service=

Most Visited Getting Started Latest Headlines

## Gmail by Google BETA

### Welcome to Gmail

#### A Google approach to email.

Gmail is a new kind of webmail, 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/app>. [Learn more](#)
-  **Lots of space**  
Over 7290.462157 megabytes (and counting) of free storage so you'll never need to delete another message.

Sign in to Gmail with your **Google Account**

Username:

Password:

Remember me on this computer.

[I cannot access my account](#)

[Sign up for Gmail](#)

[About Gmail](#) [New features!](#)

©2009 Google - [Gmail for Organizations](#) - [Gmail Blog](#) - [Terms](#) - [Help](#)

Done

# Some sites provide no visible difference

Wachovia - Personal Finance and Business Financial Services - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.wachovia.com/

Most Visited Getting Started Latest Headlines

Customer Service | Contact Us | Locations



## The time is now.

Mortgage rates are at an all-time low.  
Refinance today and save.

[Learn How >](#)

**LOGIN**

User ID:

Remember my User ID

Password:

(case sensitive)

Service:  
Choose a service... ▾

[Login](#)

Forgot [User ID](#) or [Password](#)?

Retirement Plan Participants: [Login](#)  
Education Loan Customers: [Login](#)

**PERSONAL FINANCE**

**Online Services**  
Online Banking with BillPay  
Mobile Banking  
Online Brokerage  
More...

**Banking**  
Checking  
Savings & CDs  
Credit Cards  
Check Cards  
More...

**Retirement Planning**  
Tools & information for  
Lifetime Retirement Planning

**Banking**  
Mortgage  
Home Equity **New!**  
Education Loans  
Vehicle Loans

**Investing**  
Accounts & Services  
IRAs  
More...

**Lending**  
Mortgage  
Home Equity **New!**  
Education Loans  
Vehicle Loans

**Rates**  
Mortgage Rates  
Home Equity Rates  
Credit Card Rates

**Insurance**  
Life, Auto, Home,  
Health

**Payment Challenges?**  
Explore your loan options

**STRENGTH AND STABILITY**

Wachovia is now  
part of Wells Fargo.  
[Learn More >>](#)

**WACHOVIA SECURITIES**

An industry leader in investment and advisory services for individuals, corporations and institutions.

**SMALL BUSINESS**

The tools, services, and research to manage your company.  
[Small Business Login](#)

**ONLINE BANKING.**  
Securely manage your business finances online.  
[Wachovia Business Online.](#)

**Refer a Friend**  
It adds up to \$25 for both of you.  
[See How >>](#)

**Ready to get organized?**  
It's easier than you think.  
[Go Paperless >>](#)

**Online Security**  
[Wachovia Security Plus<sup>SM</sup>](#)  
[Online Services Guarantee](#)

**Sign Up for Online Banking**  
[Sign Up](#) | [Learn More](#) | [Demo](#)

**LOCATIONS**  
ZIP:  [Find](#)  
[More Search Options](#)

Done

# Some sites provide no visible difference

Wachovia - Personal Finance and Business Financial Services - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.wachovia.com/ Google

Most Visited Getting Started Latest Headlines

Customer Service | Contact Us | Locations



## WACHOVIA



The time is now.  
Mortgage rates are at an all-time low.  
Refinance today and save.

[Learn How >](#)

**LOGIN**

User ID:

Remember my User ID

Password:  
  
(case sensitive)

Service:  
Choose a service... ▾

[Login](#)

Forgot [User ID](#) or [Password](#)?

Retirement Plan Participants: [Login](#)  
Education Loan Customers: [Login](#)

**PERSONAL FINANCE**

**Online Services**  
Online Banking with BillPay  
Mobile Banking  
Online Brokerage  
More...

**Banking**  
Checking  
Savings & CDs  
Credit Cards  
Check Cards  
More...

**Retirement Planning**  
Tools & information for  
Lifetime Retirement Planning

**Banking**  
Mortgage  
Home Equity **New!**  
Education Loans  
Vehicle Loans

**Lending**  
Mortgage  
Home Equity **New!**  
Education Loans  
Vehicle Loans

**Rates**  
Mortgage Rates  
Home Equity Rates  
Credit Card Rates

**Investing**  
Accounts & Services  
IRAs  
More...

**Payment Challenges?**  
Explore your loan options

**Insurance**  
Life, Auto, Home,  
Health

**STRENGTH AND STABILITY**

Wachovia is now  
part of Wells Fargo.  
[Learn More >>](#)

**WACHOVIA SECURITIES**

An industry leader in investment and advisory services for individuals, corporations and institutions.

**SMALL BUSINESS**

The tools, services, and research to manage your company.  
[Small Business Login](#)

**ONLINE BANKING.**  
Securely manage your business finances online.  
[Wachovia Business Online.](#)

**Refer a Friend**  
It adds up to \$25 for both of you.  
[See How >>](#)

**Ready to get organized?**  
It's easier than you think.  
[Go Paperless >>](#)

**Online Security**  
[Wachovia Security Plus<sup>SM</sup>](#)  
[Online Services Guarantee](#)

**Sign Up for Online Banking**  
[Sign Up](#) | [Learn More](#) | [Demo](#)

**LOCATIONS**  
ZIP:  [Find](#)  
[More Search Options](#)

Done

# The sites themselves confuse us.

Online Payment, Merchant Account - PayPal - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.paypal.com/

Most Visited Getting Started Latest Headlines

Sign Up | Log In | Help | Security Center

Search

U.S. English

**PayPal**

Home Personal Business Products & Services Developers

Get Started Send Money Request Money Sell on eBay Developers

**Account login**

Email address

PayPal password

Log In

Forgot your [email address](#) or [password](#)?

New to PayPal? [Sign up](#).

**Top questions**

- [Why use PayPal when I have credit cards?](#)
- [What can I do with PayPal?](#)
- [Is PayPal free to use?](#)

Limitless love?  
Limited budget?  
We've got you covered.

**Shop Now** | Save 15% at [1-800-flowers.com](#)™ [Terms](#)  
plus new customers get a \$20 Savings Pass

Pay With:

**Pay online**

- [Learn how PayPal works.](#)
- [Shop without exposing](#) your financial information.
- [Send money](#) to friends and family around

**Get paid online**

- [Accept payments](#) for your eBay listings.
- [Start accepting credit cards](#) on your website.
- [See all the ways](#) to get paid online.

Done

# The sites themselves confuse us.

Online Payment, Merchant Account - PayPal - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.paypal.com/

Most Visited Getting Started Latest Headlines

Sign Up | Log In | Help | Security Center

Search

U.S. English

PayPal

Home Personal Business Products & Services Developers

Get Started Send Money Request Money Sell on eBay Developers

**Account login**

Email address

PayPal password

Log In

Forgot your [email address](#) or [password](#)?

New to PayPal? [Sign up](#).

**Top questions**

- [Why use PayPal when I have credit cards?](#)
- [What can I do with PayPal?](#)
- [Is PayPal free to use?](#)

Limitless love?  
Limited budget?  
We've got you covered.

Shop Now

Save 15% at [1-800-flowers.com](#) [Terms](#)  
plus new customers get a \$20 Savings Pass

Pay With: VISA MasterCard DISCOVER BANK

**Pay online**

- [Learn how PayPal works.](#)
- [Shop without exposing](#) your financial information.
- [Send money](#) to friends and family around

**Get paid online**

- [Accept payments](#) for your eBay listings.
- [Start accepting credit cards](#) on your website.
- [See all the ways](#) to get paid online.

Done

# A Few Gotchas

Content encodings that are difficult to parse  
(compress, gzip, etc...)

Secure cookies won't get sent over HTTP that's  
been stripped of SSL.

Cached pages that don't give us a chance to swap  
out their links.

# A Few Gotchas

Content encodings that are difficult to parse  
(compress, gzip, etc...)

Secure cookies won't get sent over HTTP that's  
been stripped of SSL.

Cached pages that don't give us a chance to swap  
out their links.

## A Simple Solution

Strip all that stuff too.

Kill the secure bit on Set-Cookie statements, strip  
the content encodings we don't like from client  
requests, and strip if-modified-since headers too.

# Another problem: sessions

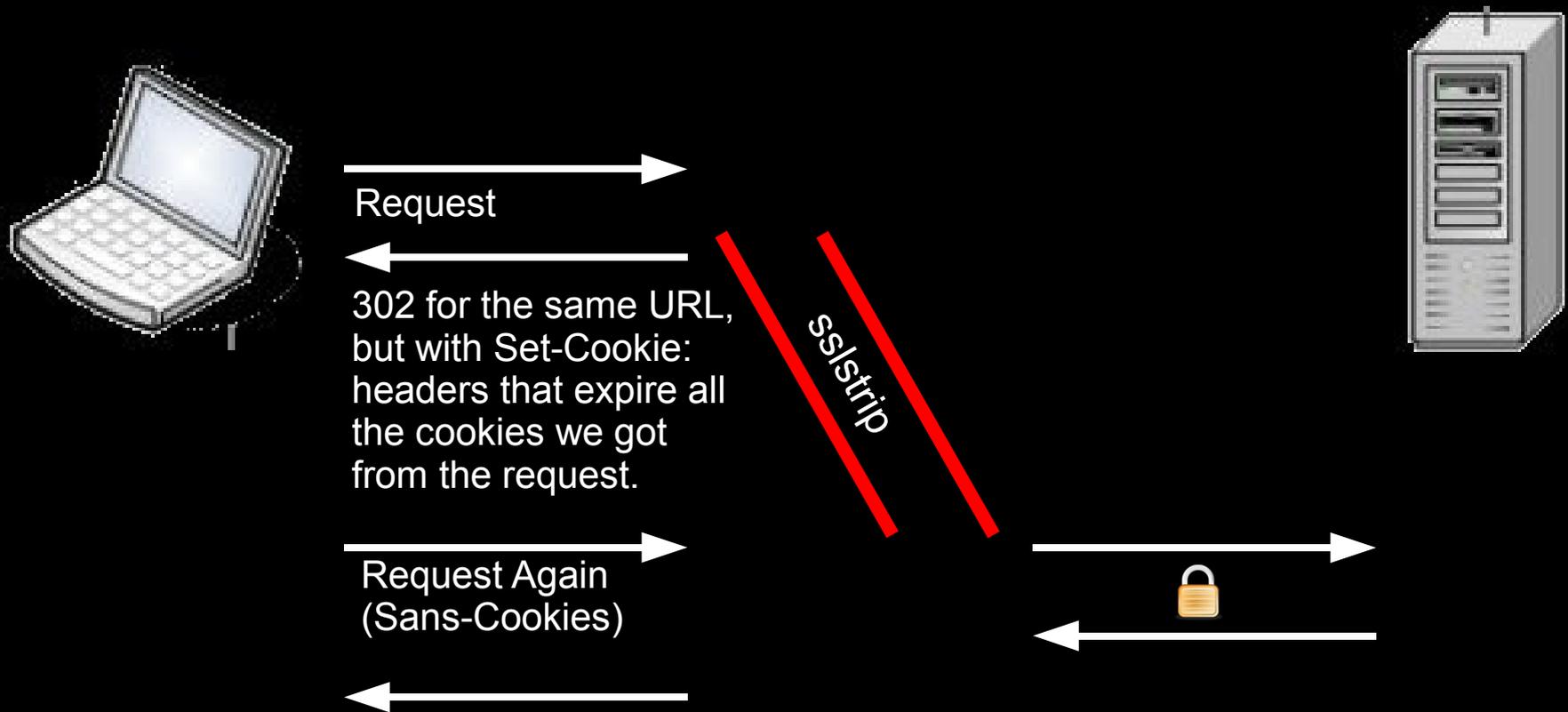
The most interesting stuff to log are POSTs that would have been sent via SSL.

Particularly, usernames/passwords.

Sessions often cause us to miss the login step, which is unfortunate.

Sure, we can get the session cookie, but that's small change.

# So let's strip sessions too.



## And a little less sketchy...

Sessions expire, and it's not always clear when or why, but they don't usually expire right in the middle of an active session. So what we do now:

When we start a MITM against a network, strip all the traffic immediately, but don't touch the cookies for 5 min (or some specified length of time).

As the cookies go by, make note of the active sessions.

After the time is up, start killing sessions, but only new sessions that we haven't seen before. These should be the “long running” sessions that won't be seen as suspicious should they disappear.

# Some Results Of This Trick?

login.yahoo.com	114
Gmail	50
ticketmaster.com	42
rapidshare.com	14
Hotmail	13
paypal.com	9
linkedin.com	9
facebook.com	3

# In 24 Hours

117 email accounts.

16 credit card numbers.

7 paypal logins.

Over 300 other miscellaneous secure logins.

Number of people that balked.

0

Where can we go from here?

# Combining this technique with homograph attacks.

Standard homograph attack:

Sometimes the glyphs of different characters look alike. PayPal.com looks like paypal.com but is really paypai.com

Made more interesting by IDN. It became possible to register a domain with characters that appear identical to the glyphs of characters in the Latin character set.

In 2005, Eric Johanson registered p#1072;ypal.com, which uses the Cyrillic 'a' look-alike character and displays as paypal.com

# Combining this technique with homoglyph attacks.

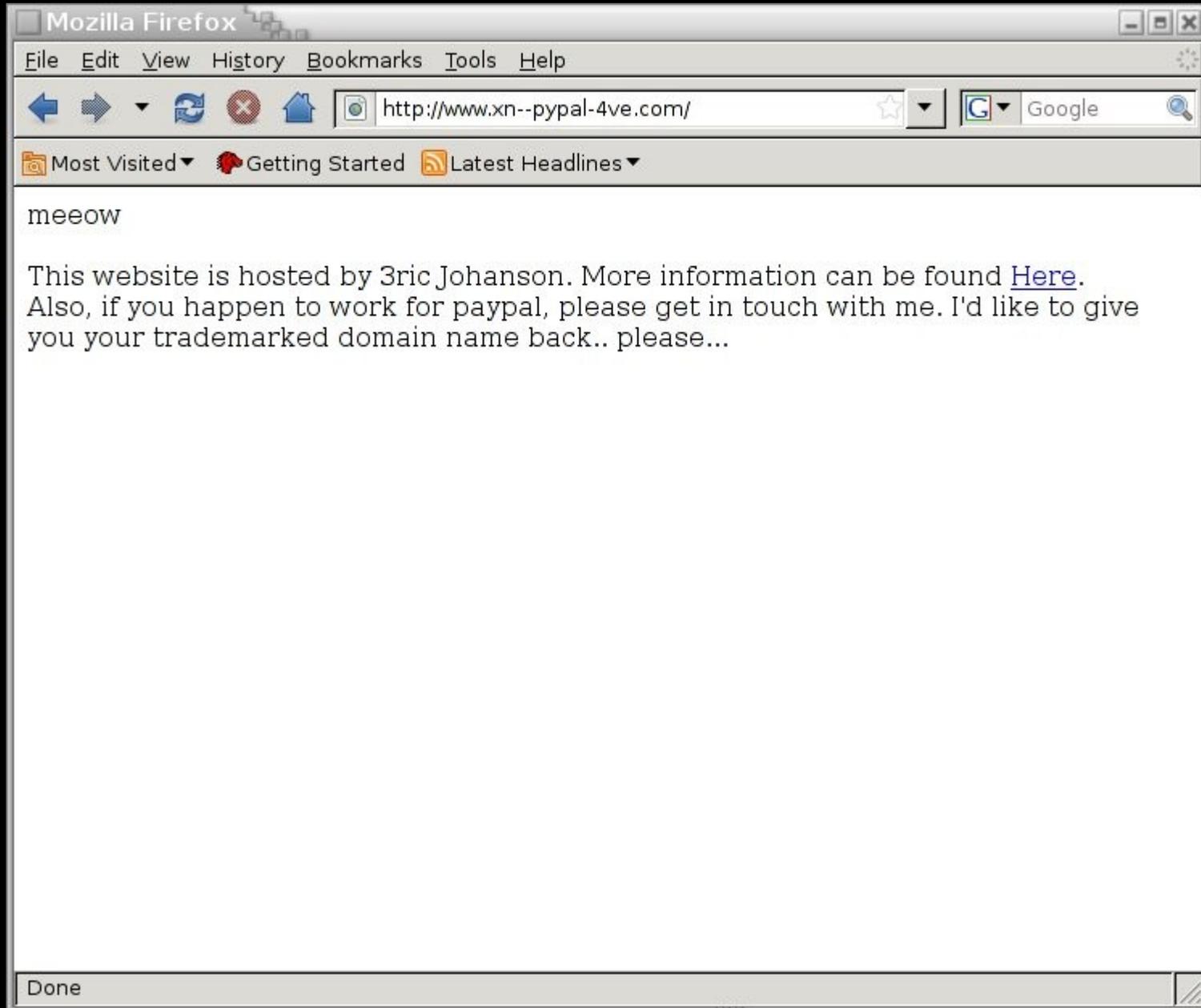
What I don't like about the standard attack:

The attack vector has to be targeted. By registering p#1072;ypal.com, all we can attack is paypal.com

Phishing is really just too much work. It'd be nicer if we could just MITM a network and get whatever people are doing.

The IDN stuff has been fixed. For TLDs like .com, Firefox renders the IDN characters as punycode both in the URL bar and the status bar.

# p&#1072;ypal.com today



# So how can we reinvent this to attack SSL?

We can't use .com or any TLD that Firefox will render into punycode.

We want something that we can generalize, not just a simple substitution for some particular character in a domain.

So, what's in most URLs? . / & ?

# one trick

Register a domain like ijjk.cn

Get a domain-validated SSL wildcard cert for \*.ijjk.cn

Use IDN-valid characters that look very similar to '/' and '?' to create false URLs.

MITM HTTP and swap out the HTTPS links as usual.

But this time, instead of just stripping the HTTPS links, we swap them out for our own look-alikes.

# one trick

<https://www.gmail.com/accounts/ServiceLogin>  
becomes

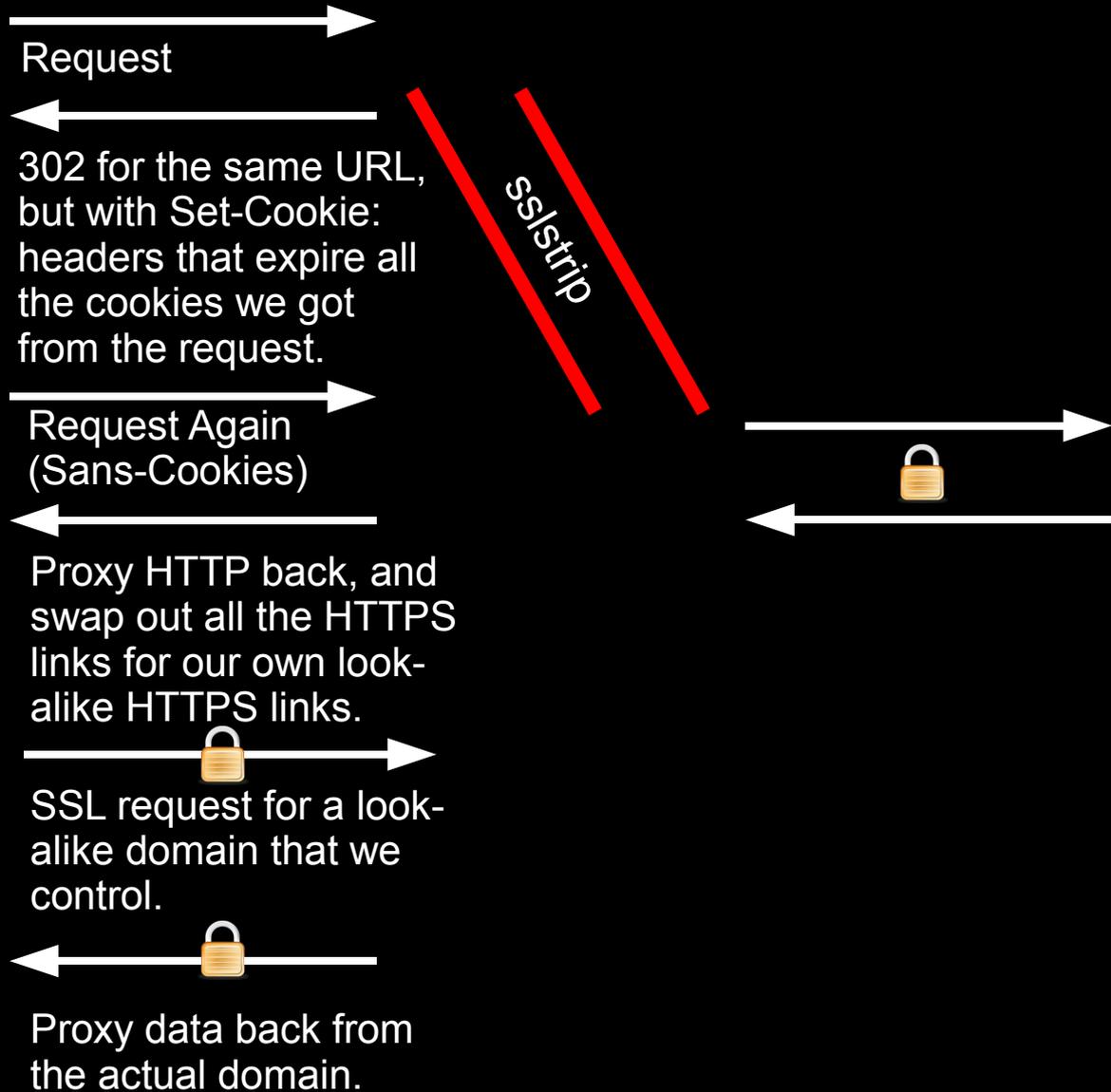
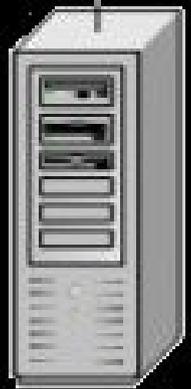
<https://www.gmail.com/accounts/ServiceLogin?!f.ijj>

The latter does not display as punycode in the status bar or the URL bar.

When resolved, it becomes `www.google.xn--comaccountsservicelogin-5j9pia.f.ijjk.cn`

When we MITM these connections, we do SSL on both ends, but are able to present our own valid `*.ijjk.cn` cert to the client.

# Here We Go



# An Example

Personal Banking - PNC Bank - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.pnc.com/webapp/unsec/Homepage

Most Visited Getting Started Latest Headlines

**PNC**  
LEADING THE WAY

HOME SECURITY ASSURANCE LOCATE PNC CONTACT US CUSTOMER SERVICE

Search

PERSONAL SMALL BUSINESS CORPORATE & INSTITUTIONAL ABOUT PNC

**Online Banking Sign On**

User ID:  **SIGN ON**

▶ Forgot Your User ID or Password?

New to Online Banking? ▶ Learn More  
▶ Get Started Now! ▶ View Demo

Sign On to Other Services:  
Select Service

**PNC Bank Select Reward Visa® Platinum Card**

Take advantage of a 0.99% Introductory APR through March 31, 2010 on Balance Transfers

Learn More

1 2 3 4

▶ PNC Security Assurance

Products and Services Solutions

**Important FDIC Information**

PNC Bank is participating in the FDIC's Transaction Account Guarantee Program. [more ▶](#)

**Two of America's best-known banks. Now simply one of America's best.**

Making the transition to PNC as easy as possible for you.

PNC's wide range of services can make banking easier, and more convenient than ever. See why PNC's the smart choice for help in meeting your financial goals.

- ▶ Online Banking and Bill Pay
- ▶ Checking
- ▶ Savings
- ▶ Loans and Lines of Credit
- ▶ Cards

Whatever challenges and opportunities lie ahead, PNC can help. See why working with PNC to plan for life's greatest milestones is the smart choice.

- ▶ Making the Most of Your Money
- ▶ Virtual Wallet
- ▶ Planning for Retirement
- ▶ Saving for Education
- ▶ Buying a Home

Done

www.pnc.com

# An Example

Personal Banking - PNC Bank - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.pnc.com/webapp/unsec/homepage

Most Visited Getting Started Latest Headlines

**PNC**  
LEADING THE WAY

HOME SECURITY ASSURANCE LOCATE PNC CONTACT US CUSTOMER SERVICE

Search

PERSONAL SMALL BUSINESS CORPORATE & INSTITUTIONAL ABOUT PNC

**Online Banking Sign On**

User ID:  **SIGN ON**

▶ Forgot Your User ID or Password?

New to Online Banking? ▶ Learn More  
▶ Get Started Now! ▶ View Demo

Sign On to Other Services:  
Select Service

**PNC Bank Select Reward Visa® Platinum Card**

Take advantage of a 0.99% Introductory APR through March 31, 2010 on Balance Transfers

Learn More

1 2 3 4

▶ PNC Security Assurance

Products and Services Solutions

**Important FDIC Information**

PNC Bank is participating in the FDIC's Transaction Account Guarantee Program. [more ▶](#)

**Two of America's best-known banks. Now simply one of America's best.**

Making the transition to PNC as easy as possible for you.

PNC's wide range of services can make banking easier, and more convenient than ever. See why PNC's the smart choice for help in meeting your financial goals.

- ▶ Online Banking and Bill Pay
- ▶ Checking
- ▶ Savings
- ▶ Loans and Lines of Credit
- ▶ Cards

Whatever challenges and opportunities lie ahead, PNC can help. See why working with PNC to plan for life's greatest milestones is the smart choice.

- ▶ Making the Most of Your Money
- ▶ Virtual Wallet
- ▶ Planning for Retirement
- ▶ Saving for Education
- ▶ Buying a Home

Done

www.pnc.com/webapp/unsec/homepage.var.cn

# Nice thing about this...

Happens in real-time.

Generalized:

- Targets whatever secure sites people are browsing to at any moment.

- Doesn't require multiple certificates or restricting ourselves to popular sites.

Once we get a secure POST, we can switch them back to a normal traffic stream.

# Lessons...

Lots of times the security of HTTPS comes down to the security of HTTP, and HTTP is not secure.

If we want to avoid the dialogs of death, start with HTTP not HTTPS.

Once we've got control of that, we can do all kinds of stuff to re-introduce the positive indicators people might miss.

Other tricks...

sslstrip

<http://www.thoughtcrime.org>