SSL Eye Exam, One Million Websites, Banned in the Netherlands

...”

By Jay Graver [jgraver@gmail.com]
SSL Survey

- How to survey 1 Million websites using your Rogers Hi-Speed connection
Step 1: Find a list of 1M sites
Step 1: Find a list of 1M sites
Step 2: Avoid the hard work

Is my site safe?

Check your SSL certificate with our Site Check tool, to see if your site is really safe and secure. Verify whether your SSL certificate is correctly installed and which security options are in use.

The Site Check not only checks the presence of a SSL certificate, but also lists additional information which will give you an overall idea about the quality of the SSL connection. You will get information on the Certificate Authority, the expiry date, the encryption strength, EV support, SGC support and more.

Enter the url of your secured website or any other url like www.networking4all.com, to check how safe the connection to that site really is.

[Form input field] [Check site button]
SSL Certificate Details

- Expiration Date
- FQDN == CN
- Subject Alternate Names
- Organisation Details
- Key Size >= 1024-bit

- Strong Sig Algo
- Server Gated Crypto
- Extended Validation
- CA Security Issues
- Debian Weak Key
Step 3: Scan your list
It's all fun ...
Until someone gets BANNED
Holland still hates me
The Dutch like Freedom

Olympicproxy

With the Olympic Games in Beijing 2008, internet surfers face a big problem; a large majority of websites are blocked in China (coined “The Great Firewall Of China”), due to strict government censorship. If you are going over to Beijing to watch the olympics, or perhaps you’re a journalist, you can use our FREE service to unblock all websites without any technicalities, all you need to do is use the form on this web page and you will virtually reside in the USA.
Proxified SSL Survey

SSL Certificate correctly installed

This certificate should be trusted by all major web browsers

This website has the possibility to send data across a secure connection. This is no guarantee that this indeed will happen, it is however a good indication. To be sure we advise you, before you submit any personal information, to check if the url in the address bar starts with https:// instead of the insecure http://. The additional 's' stands for security.

- SSL Certificate is not expired
- Site is listed in the certificate
- Organisation details are listed
- Encryption strength is at least 1024-bit
- Signature Algorithm is strong
Back in Business
Proxy List

- http://privax.us/
Make your own API

- http://w2.hidemyass.com

&fqdn=www.cibc.com
Run Parallel Scripts
Get LOTS of data
Step 4: MySQL Time
Step 5: Now what?
Total Number of Certs

- 175,125 sites in the first 500,000
  - 35% of hosts have HTTPS

- 83,178 unique certificates found
  - 4560 intermediate certificates
Expired Certificates

- 593 Expired Certificates (0.7%)
Self Signed Certificates

- 589 sites found (0.33%)
Certs Expiring This Week
Certs Expiring Today

```
SELECT * FROM certificates
WHERE expire_date LIKE "%% 8 October 2009%%"
```
Certs Expiring Today

- 189 certificates expire today
<table>
<thead>
<tr>
<th>Key Size</th>
<th>Value</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
<td>2337</td>
<td>1.3%</td>
</tr>
<tr>
<td>768</td>
<td>1122</td>
<td>0.6%</td>
</tr>
<tr>
<td>1024</td>
<td>139363</td>
<td>80%</td>
</tr>
<tr>
<td>2048</td>
<td>31602</td>
<td>18%</td>
</tr>
<tr>
<td>4096</td>
<td>590</td>
<td>0.3%</td>
</tr>
</tbody>
</table>
Odd Key Sizes

- 511 (1)
- 1023 (92)
- 1028 (1)
- 1032 (1)
- 1042 (1)
- 1204 (1)
- 1536 (2)
- 2047 (2)
- 5120 (1)
- 8192 (1)
Weak Debian Keys in use!

- 410 sites discovered
Comodo still going strong

- 1429 Sites found
EV Numbers

- 2836 sites found (1.6%)
Use of the Wildcard *

- 5571 in Subject (7%)
  - *.oracle.com
  - Yes I did see Subject = *

- 18584 in Subject Alternate Names (10%)
  - google.com, *.google.com
SSL User Experience
Browsers Failing Users

1994 - 2004
✓ Little to no feedback system

2004 Firefox 1 released
✓ Positive Feedback system

2008 Firefox 3
✗ Negative Feedback system
Moxie Marlinspike’s sslstrip

http://www.thoughtcrime.org/software/sslstrip/
SSL Eye Exam
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/app](http://gmail.com/app)
  Learn more

- **Lots of space**
  Over 7377.126998 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: 

- Stay signed in

Sign in

Can’t access your account?

New to Gmail? It’s free and easy.
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/app](http://gmail.com/app).

- **Lots of space**
  Over 7377.126560 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: [ ]

[ ] Stay signed in

[Sign in]

Can't access your account?

New to Gmail? It's free and easy.
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/app](http://gmail.com/app).
  [Learn more](http://gmail.com/app)

- **Lots of space**
  Over 7,377,134,296 megabytes (and counting) of free storage so you’ll never need to delete another message.

Sign in to Gmail with your Google Account

- Username: [text field]
- Password: [text field]
- Stay signed in
- Sign in

New to Gmail? It’s free and easy.
IE7
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/app](http://gmail.com/app). Learn more

- Lots of space
  Over 7377.150628 megabytes (and counting) of free storage so you'll never need to delete another message.
IE8

Gmail: Email from Google - Windows Internet Explorer

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/app. Learn more

Lots of space
Over 7377.149401 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:

Stay signed in
Sign in

Can't access your account?

New to Gmail? It's free and easy.
Firefox 1

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/app](http://gmail.com/app).
  Learn more

- **Lots of space**
  Over 7377.125194 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: 
- Stay signed in
  - Sign in

Can't access your account?

New to Gmail? It's free and easy.
Firefox 1

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/app](http://gmail.com/app).
  [Learn more](http://gmail.com/app)

- **Lots of space**
  Over 7377.125923 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:
- Stay signed in

Can't access your account?

New to Gmail? It's free and easy.

Transferring data from mail.google.com...
Firefox 2

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/app](http://gmail.com/app).

- **Lots of space**
  Over 7377.127658 megabytes (and counting) of free storage so you'll never need to delete another message.
Firefox 2

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/app](http://gmail.com/app).

- **Lots of space**
  Over 7377.128177 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: 

Stay signed in

Sign in

Can't access your account?

New to Gmail? It's free and easy.
Firefox 3

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/app. Learn more

Lots of space
Over 7377.130446 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: 
Stay signed in

Can’t access your account?

New to Gmail? It’s free and easy.
Firefox 3

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/app](http://gmail.com/app). Learn more

- **Lots of space**: Over 7377.129144 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: [ ]

- Stay signed in

Sign in

Can't access your account?

New to Gmail? It’s free and easy.
Chrome

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/app](http://gmail.com/app). Learn more

- **Lots of space**
  Over 7377.151447 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: 

Stay signed in
Sign in

Can't access your account?

New to Gmail? It's free and easy.
Chrome

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/app](http://gmail.com/app). Learn more

- **Lots of space**
  Over 7377.151804 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: 

Toggle Stay signed in

Sign in

Can’t access your account?

New to Gmail? It’s free and easy.
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/app](http://gmail.com/app). [Learn more](http://gmail.com/help).

- **Lots of space**
  Over 7377.155681 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: 

- Stay signed in

[Sign in](http://gmail.com/signin)

Cant access your account?

New to Gmail? It’s free and easy.
Safari

Gmail: Email from Google

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/app](http://gmail.com/app).
  [Learn more](#)

- **Lots of space**
  Over 7377.155385 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: [ ]

- Stay signed in

[Sign in](#)

Can’t access your account?

New to Gmail? It's free and easy.
Innovation FAIL

- This attack would not have worked (as well) in 2007!
- Chrome still uses the yellow bar UI
- Safari is generally hopeless
SSLess Logins

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

Sign up

Windows Live ID gives you access to Microsoft services including MSN, Hotmail, Office Live, Xbox LIVE, and many more.

Don't have a Windows Live ID?

Sign in

Windows Live ID:

Password:

Forgot your password?

Remember me on this computer (?)

Remember my password (?)

Sign in

Use enhanced security

©2009 Microsoft Corporation About Privacy Trademarks Account Help Central Feedback
SSL == Failure?
Explain?
SSLv2 == PCI Fail
• Message integrity compromised. The SSLv2 message authentication uses the MD5 function, and is insecure.

• Man-in-the-middle attack. There is no protection of the handshake in SSLv2, which permits a man-in-the-middle attack.

• Truncation attack. SSLv2 relies on TCP FIN to close the session, so the attacker can forge a TCP FIN, and the peer cannot tell if it was a legitimate end of data or not.

• Weak message integrity for export ciphers. The cryptographic keys in SSLv2 are used for both message authentication and encryption, so if weak encryption schemes are negotiated (say 40-bit keys) the message authentication code use the same weak key, which isn't necessary.
4,096,000 Random IPs

168,620 Live Hosts

Port 80
67,366 Hosts

Ports 443/8443
29,269 Hosts

Port 993
6,705 Hosts

Port 995
7,127 Hosts

SSLv2
7,821 Hosts

26.2%

SSLv2
2,981 Hosts

44.5%

SSLv2
3,240 Hosts

45.5%
25% of Web Servers
&
~50% of Mail Servers

==

PCI Fail
But what runs SSLv2?
Microsoft Exchange – Outlook Web Access

118
Windows Small Business Server

207
Plesk & cPanel

163
Login / Logon / Authentication Required

1299
Finance / Bank / Mortgage / Insurance / Accountant
Health / Medical / Medicine

26
Firewall / VPN / Proxy / SECUREWORKS ezWall / ZyWALL / SonicWALL

142
Apache Install Test Pages

155
IIS 7

82
Remote Access / Citrix
City / County / State / Province / Country / Gov

186
There is a problem with this website’s security certificate.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

- Click here to close this webpage.
- Continue to this website (not recommended).
- More information
About

BeEF is a browser exploitation framework. Its purpose in life is to provide an easily integratable framework to demonstrate the impact of browser and Cross-site Scripting issues in real-time. The modular structure has allowed the development of new modules to be a simple process.

What's New

You will immediately notice the log summary on the main screen. This logs zombie details and module results. It provides access to the zombie pane by clicking on the date. There are two other logs - the zombie log and the raw log. The raw log contains more information than the log summary pane. For more detail refer to the CHANGELOG file.

Changes Summary:
* Integration with Metasploit via XMLRPC
* New browser functionality detection modules
* Command interface support added for Safari
* Filtered logging for module actions and results
* Viewing page content added to the zombie pane
* Add Autorun support added to each module

Copyright © 2006-2009, Wade Alcorn. All Rights Reserved.
SSL Survey

- Small survey using SurveyMonkey.com
- 112 responses to 10 questions
41% of respondents always check for SSL when entering a password
81% always check for SSL when entering credit card number

Studies say 33 – 66% of people use the same password everywhere
Less than 1/3 of respondents knew what EV SSL was and how it differs from SSL

How many people here know the difference?
90% of those surveyed are happy with browser error messages

How many people here are happy with them?
15% of responses indicated that those surveyed were annoyed with the error messages to the point that they automatically clicked through.

Looking at just the non-technical responses, 47% automatically click through.

YIKES!
Almost 20% of people that replied don’t know what a self-signed certificate is. That’s 1 in 5 people that these error messages have no meaning for.
The really scary one!

51% of people felt browser error messages made them more aware of flaws in website security.

Do these error messages really have anything to do with security?

Panelists?
Who do we blame?
Final Thoughts
One of my firm’s SaaS app vendors uses Akami with SSL offloading. The effect means that everything from us to Akami is encrypted, and everything from Akami to them is not. That was an interesting security risk to try to explain to senior management.

I think the security stuff is what made people so hostile to Vista – the constant “do you really want to do this?” messages. I was deleting duplicate MP3 files on a machine with Vista and those messages drove me totally mental, to the point where I stopped doing it and dug through Vista’s awful help files to find out how to turn the messages off. I assume things like the Rogers mismatch error are the result of some lazy web design person at Rogers screwing up. If the certificate pointed to stealyourself.ru, I’d be more concerned.

I like browser errors, but I don’t like the current brand of browser errors that render full pages rather than dialog boxes. Or that just break internally-signed certs for sites or appliances that you just inherently trust. The current errors are out of hand.

I’m a PKI professional and thus I’m not an “average” user. I know 99% of users do not care about warnings or alike. I would prefer a more radical solution (like some mobile browsers) where a SSL problem just prevents the user to access the site. Sounds hard but if that was the default behavior we won’t have gray areas as today.

because ssl certs perform the dual function of identifying the site and encrypting the data stream, the actions of mozilla are frustrating in the extreme. I know if I’m logging on to one of my servers that the cert is self-signed. I care that the stream is encrypted, which it still is.
Find our slides / data / scripts at:
http://www.sslfail.com/sector/
SSL == Failure?
Explain?
SSLv2 == PCI Fail
• Message integrity compromised. The SSLv2 message authentication uses the MD5 function, and is insecure.

• Man-in-the-middle attack. There is no protection of the handshake in SSLv2, which permits a man-in-the-middle attack.

• Truncation attack. SSLv2 relies on TCP FIN to close the session, so the attacker can forge a TCP FIN, and the peer cannot tell if it was a legitimate end of data or not.

• Weak message integrity for export ciphers. The cryptographic keys in SSLv2 are used for both message authentication and encryption, so if weak encryption schemes are negotiated (say 40-bit keys) the message authentication code use the same weak key, which isn't necessary.
4,096,000 Random IPs

168,620 Live Hosts

Port 80
67,366 Hosts

Ports 443/8443
29,269 Hosts

Port 993
6,705 Hosts

Port 995
7,127 Hosts

SSLv2
7,821 Hosts

SSLv2
2,981 Hosts

SSLv2
3,240 Hosts

26.2%

44.5%

45.5%
25% of Web Servers
&
~50% of Mail Servers

PCI Fail
But what runs SSLv2?
Microsoft Exchange – Outlook Web Access

118
Windows Small Business Server

207
Plesk & cPanel

163
Login / Logon / Authentication Required

1299
Finance / Bank / Mortgage / Insurance / Accountant

28
Health / Medical / Medicine

26
Firewall / VPN / Proxy / SECUREWORKS ezWall / ZyWALL / SonicWALL

142
Apache Install Test Pages

155
IIS 7

82
Remote Access / Citrix
There is a problem with this website's security certificate.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

- Click here to close this webpage.
- Continue to this website (not recommended).
- More information
BeEF is a browser exploitation framework. Its purpose in life is to provide an easily integratable framework to demonstrate the impact of browser and Cross-site Scripting issues in real-time. The modular structure has allowed the development of new modules to be a simple process.

What's New
You will immediately notice the log summary on the main screen. This logs zombie details and module results. It provides access to the zombie pane by clicking on the date. There are two other logs - the zombie log and the raw log. The raw log contains more information than the log summary pane. For more detail refer to the CHANGELOG file.

Changes Summary:
* Integration with Metasploit via kMATRPC
* New browser functionality detection modules
* Command interface support added for Safari
* Tinged logging for module actions and results
* Viewing page content added to the zombie pane
* Set autorun support added to each module

Copyright © 2006-2009, Wade Alcorn. All Rights Reserved.
SSL Survey

- Small survey using SurveyMonkey.com
- 112 responses to 10 questions
41% of respondents always check for SSL when entering a password
81% always check for SSL when entering credit card number

Studies say 33 – 66% of people use the same password everywhere
Less than 1/3 of respondents knew what EV SSL was and how it differs from SSL.

How many people here know the difference?
90% of those surveyed are happy with browser error messages

How many people here are happy with them?
15% of responses indicated that those surveyed were annoyed with the error messages to the point that they automatically clicked through.

Looking at just the non-technical responses, 47% automatically click through

YIKES!
Almost 20% of people that replied don’t know what a self-signed certificate is. That’s 1 in 5 people that these error messages have no meaning for.
The really scary one!

51% of people felt browser error messages made them more aware of flaws in website security.

Do these error messages really have anything to do with security?

Panelists?
Who do we blame?
Browser Vendors

Website Owners?

Everyone in this room?

End Users?

SSL CAs
Final Thoughts
One of my firm’s SaaS app vendors uses Akami with SSL offloading. The effect means that everything from us to Akami is encrypted, and everything from Akami to them is not. That was an interesting security risk to try to explain to senior management.

I think the security stuff is what made people so hostile to Vista – the constant “do you really want to do this?” messages. I was deleting duplicate MP3 files on a machine with Vista and those messages drove me totally mental, to the point where I stopped doing it and dug through Vista’s awful help files to find out how to turn the messages off. I assume things like the Rogers mismatch error are the result of some lazy web design person at Rogers screwing up. If the certificate pointed to stealyoursoul.ru, I’d be more concerned.

I like browser errors, but I don’t like the current brand of browser errors that render full pages rather than dialog boxes. Or that just break internally-signed certs for sites or appliances that you just inherently trust. The current errors are out of hand.

I’m a PKI professional and thus I’m not an “average” user. I know 99% of users do not care about warnings or alike. I would prefer a more radical solution (like some mobile browsers) where a SSL problem just prevents the user to access the site. Sounds hard but if that was the default behavior we won’t have gray areas as today.

Because ssl certs perform the dual function of identifying the site and encrypting the data stream, the actions of mozilla are frustrating in the extreme. I know if I’m logging on to one of my servers that the cert is self-signed. I care that the stream is encrypted, which it still is.
Find our slides / data / scripts at:
http://www.sslfail.com/sector/