SSL And The Future Of Authenticity

Moving beyond Certificate Authorities
Comodo
Web Firm Suspects Iran Hacked Into It

Internet-Security Company Says It Was Tricked Into Authenticating Fake Sites, Opening Access to Data, Not Money
The Damage

- mail.google.com
- www.google.com
- login.yahoo.com
- login.skype.com
- addons.mozilla.org
- login.live.com
“This [attack] was extremely sophisticated and critically executed...it was a very well orchestrated, very clinical attack, and the attacker knew exactly what they needed to do and how fast they had to operate.”

-- Melih Abdulhayoglu, Comodo Founder
“All the IPs were from Iran…”

-- Melih Abdulhayoglu, Comodo Founder
cyber
“All of the above leads us to one conclusion only: that this was likely to be a state-driven attack.”

-- Melih Abdulhayoglu, Comodo Founder
hack --> war
“What does this mean?”
“How would they use them?”
sslsniff
The attack came from several IP addresses, but mainly from Iran.

<table>
<thead>
<tr>
<th>IP Address Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>City</td>
</tr>
<tr>
<td>State or Region</td>
</tr>
<tr>
<td>Country</td>
</tr>
<tr>
<td>ISP</td>
</tr>
<tr>
<td>Latitude &amp; Longitude</td>
</tr>
</tbody>
</table>
212.95.136.18 [16/Mar/2011:09:56:03 +0000] "GET http://www.thoughtcrime.org/software/sslsniff/index.html HTTP/1.1" 200 "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13 Gecko/20101203 Firefox/3.6.13 ( .NET CLR 3.5.30729; .NET4.0E)"

Wednesday, September 28, 2011
212.95.136.18 [16/Mar/2011:09:56:03 +0000] "GET http://www.thoughtcrime.org/software/sslsniff/index.html HTTP/1.1" 200 "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13 Gecko/20101203 Firefox/3.6.13 (.NET CLR 3.5.30729; .NET4.0E)"
www.thoughtcrime.org/software/sslsniff/index.html HTTP/1.1" 200
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13
Gecko/20101203 Firefox/3.6.13 ( .NET CLR 3.5.30729; .NET4.0E)"

Wednesday, September 28, 2011
212.95.136.18 [16/Mar/2011:09:56:03 +0000] "GET http://www.thoughtcrime.org/software/sslsniff/index.html HTTP/1.1" 200 "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13 Gecko/20101203 Firefox/3.6.13 ( .NET CLR 3.5.30729; .NET4.0E)"
referrer
Episode 610 – Man in the Middle fun with SSL Strip

Submitted by Darren Kitchen on October 21, 2009 – 6:49 am

This time on the show Darren’s having a little man-in-the-middle fun with a demonstration of SSLStrip, an epic tool for removing that pesky encryption from your victims browsing session.

Moxie Marlinspike’s SSLStrip, released at Blackhat/DEFCON this year, is a tool that transparently hijacks HTTP traffic and redirects HTTPS links to look-alike HTTP links. While this description barely scratches the surface, Darren’s segment takes a close look including a practical demonstration of a man-in-the-middle attack using openssl and a
"...it was a very well orchestrated, very clinical attack, and the attacker knew exactly what they needed to do and how fast they had to operate."

-- Melih Abdulhayoglu
And more embarrassing Google search referrers...

“SSL protocol mitm howto iptables prerouting”
1. Hello
2.
3. I'm writing this to all the world, so you'll know more about us.
4.
5. At first I want to give some points, so you'll be sure I'm the hacker:
6.
7. I hacked Comodo from InstantSSL.it, their CEO's e-mail address mfpenco@mfpenco.com
8. Their Comodo username/password was: user: gtadmin password: globaltrust
9. Their DB name was: globaltrust and instantsslcms
10.
11. Enough said, huh? Yes, enough said, someone who should know already knows...
12.
13. Anyway, at first I should mention we have no relation to Iranian Cyber Army, we don't change DNSes, we
14. just hack and own.
16.
17. I see Comodo CEO and other wrote that it was a managed attack, it was a planned attack, a group of
18. cyber criminals did it, etc.
20.
21. Let me explain:
22.
23. a) I'm not a group, I'm single hacker with experience of 1000 hacker, I'm single programmer with
24. experience of 1000 programmer, I'm single planner/project manager with experience of 1000 project
26. managers, so you are right, it's managed by 1000 hackers, but it was only I with experience of 1000
28. hackers.
30.
31. b) It was not really a managed hack. At first I decided to hack RSA algorithm, I did too much
He just wouldn’t shut up!

<table>
<thead>
<tr>
<th>NAME / TITLE</th>
<th>ADDED</th>
<th>EXPIRES</th>
<th>SIZE</th>
<th>SYNTAX</th>
<th>STATUS</th>
<th>OPTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROBLEM OF WORLD: MISSING EQUA...</td>
<td>Mar 31st, 11</td>
<td>Never</td>
<td>3.49 KB</td>
<td>None</td>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>Response to comments from Comodo...</td>
<td>Mar 29th, 11</td>
<td>Never</td>
<td>5.46 KB</td>
<td>None</td>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>Comodo Hacker: Mozilla Cert Re...</td>
<td>Mar 28th, 11</td>
<td>Never</td>
<td>2.40 KB</td>
<td>None</td>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>Just Another proof from Comodo...</td>
<td>Mar 28th, 11</td>
<td>Never</td>
<td>4.46 KB</td>
<td>None</td>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>Another proof of Hack from Comodo...</td>
<td>Mar 27th, 11</td>
<td>Never</td>
<td>12.54 KB</td>
<td>C#</td>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>A message from Comodo Hacker</td>
<td>Mar 26th, 11</td>
<td>Never</td>
<td>5.50 KB</td>
<td>None</td>
<td>Public</td>
<td></td>
</tr>
</tbody>
</table>
“If there were a Secure and Trusted DNS this issue would be a moot point! We need a Secure and Trusted DNS!”

-- Melih Abdulhayoglu, Comodo Founder
Comodo admits two more resellers pwned in SSL cert hack
How deep does the rabbit hole go?
New hack on Comodo reseller exposes private data
And then there were four
What happened to Comodo?
nothing
“Melih Abdulhayoglu named entrepreneur of the year at RSA 2011.”
problem
A Secure Protocol

- Secrecy
- Integrity
- Authenticity
early 90’s
Information
! e-commerce
! web applications
tiny
< 5 million
> 4 billion
< 10 “secure” sites
> 2 million
intense pressure
4am decisions == javascript
A Secure Protocol

✓ Secrecy
✓ Integrity
▷ Authenticity
A Secure Connection

Client

PayPal
A Secure Connection

Client

PayPal
entirely theoretical
certificates
and
certificate authorities
“...a bit of a hand wave.”
SSL Threat Model

- End Points
  - Attacks
    - Route hijacking (BGP)
    - Phishing
    - Corporate interception
    - XSS
  - DNS Cache Poisoning
    - LAN
    - MITM
    - Wireless
  - Users
    - Prevalence of self-signed certificates
    - Domain name spoofing
      - Internationalised domain names
      - Similar domain names
  - Implementation bugs
  - Usability
    - Prevalence of self-signed certificates

- Protocols
  - Specifications
    - Scope limitations
      - No IP layer protection
        - Not end-to-end
      - No certificate information protection
      - Hostname leakage (via SNI)
    - Downgrade attack (SSLv2)
    - Truncation attack (SSLv2)
    - Bleichenbacher adaptive chosen-ciphertext attack
    - Klima-Pokorny-Rosa adaptive chosen-ciphertext attack
    - etc.
cyber war
happening every day
login.live.com?
Mike Zussman just asked for it.
Eddy Nigg got mozilla.com
...with no validation

Wednesday, September 28, 2011
VeriSign issued
“Microsoft Corporation”
SSL-In-A-Box.com
These are the people securing the internet.
Maintenance

Due to a security breach that occurred at the 15th of June, issuance of digital certificates and related services has been suspended. Our services will remain offline until further notice.

Subscribers and holders of valid certificates are not affected in any form.

Visitors to web sites and other parties relying on valid certificates are not affected.

We apologize for the temporary inconvenience and thank you for your understanding.
FEATURES & BENEFITS

- Complete control over all RA functions for issuance of SSL server certs and client certs
- Globally recognized roots compatible with 99% of all browsers
- Build and maintain a trusted identity with privately-branded certificates
- Predictable and economical yearly costs
- Seamless integration with Microsoft IIS

PROTECT YOUR BUSINESS WITH YOUR OWN CERTIFICATE AUTHORITY
The growing demand for secure e-business environments makes user and transaction identity certification a necessity. One of the most important steps toward achieving enterprise-wide protection is to issue digital certificates through a Certificate Authority (CA). Yet, organizations that choose to run their own private CA often grapple with a common obstacle -- a lack of global recognition for their "self-signed" certificates.

GeoRoot is an ideal solution that allows enterprises to retain full control over Registration Authority (RA) functions for the issuance of SSL server certificates for domains and client certificates (x.509). With GeoRoot, your organization will gain the inherent security, confidence and recognition that result from being chained to one of GeoTrust’s trusted roots.

COMPATIBLE WITH 99% OF ALL BROWSERS
Lack of certificate recognition can be costly resulting in the loss of critical business or the denial of user access to vital information. If a certificate is not recognized, the result is that the recipient may receive an error message or complaint from the browser, and consequently not trust either the server or the source.
State Sponsored?
good news
“total ripoff”

“total ripoff and mostly worthless”
problem?
VeriSign?
20 --> 2,000,000
What happened to Comodo?
nothing
What could we have done?
trust
trustdb -= comodo
ideological
browser vendors
forever
trust agility
Trust Agility Properties

• A trust decision can be easily revised at any time.

• Individual users can decide where to anchor their trust.
A trust decision can be easily revised at any time.

- Individual users can decide where to anchor their trust.
• A trust decision can be easily revised at any time.

▷ Individual users can decide where to anchor their trust.
VeriSign

Facebook

Comodo
https?
one decision for everyone?
our data, our trust decision
Trust Agility Properties

• A trust decision can be easily revised at any time.

  Individual users can decide where to anchor their trust.
Trust Agility Properties

★ A trust decision can be easily revised at any time.

★ Individual users can decide where to anchor their trust.
DNSSEC
SSL Cert --> DNS Record
Client \quad \text{Lookup paypal.com} \quad \text{DNS Server}
Client → DNS Server

Lookup paypal.com

66.211.169.2

&&

SSL Certificate

Wednesday, September 28, 2011
distributed
information --> distributed
trust --> centralized
DNSSEC == CA System
Trust Requirements

• The Registrars.
• The TLDs.
• The root.
Trust Requirements

- The Registrars.
  - The TLDs.
  - The root.
sketchy++
Trust Requirements

• The Registrars.

  ▸ The TLDs.

• The root.
.com, .net
.org, .edu
ccTLDs
.io, .cc, .ly?
.ir, .cn?
domain seizures
Trust Requirements

• The Registrars.

• The TLDs.

  ▸ The root.
ICANN
Global --> California 501(c)(3)
COICA, PROTECT IP, etc...
Trust Requirements

✴ The Registrars.
✴ The TLDs.
✴ The root.
< trust agility
trustdb -= VeriSign
Trust Requirements

- The Registrars.
- The TLDs.
- The root.
forever
Perspectives

Dan Wendlandt, David G. Andersen, Adrian Perrig
Carnegie Mellon University
Perspectives: Improving SSH-style Host Authentication with Multi-Path Probing

Dan Wendlandt  David G. Andersen  Adrian Perrig
Carnegie Mellon University

Abstract

The popularity of “Trust-on-first-use” (Tofu) authentication, used by SSH and HTTPS with self-signed certificates, demonstrates significant demand for host authentication that is low-cost and simple to deploy. While Tofu-based applications are a clear improvement over completely insecure protocols, they can leave users vulnerable to even simple network attacks. Our system, PERSPECTIVES, thwarts many of these attacks by using a collection of “notary” hosts that observes a server’s public key via multiple network vantage points (detecting localized attacks) and keeps a record of the server’s key over time (recognizing short-lived attacks). Clients can download these records on-demand and compare them against an unauthenticated key, detecting many common attacks. PERSPECTIVES explores a promising part of the host authentication design space: Trust-on-first-use applications gain significant attack robustness without sacrificing their ease-of-use. We Furthermore, a study by Reis et al. used client-side measurements to confirm that real-time snooping and modification of web traffic is a reality in today’s networks [20].

In this paper, we examine a novel approach to authenticating a server’s public key. Traditional approaches to server key authentication, such as a public-key infrastructure (PKI) [7, 5], rely on trusted entities (e.g., Verisign) that grant certificates based on the validation of real-world identities. When done securely, such verification requires significant (often manual) effort. While some network hosts, primarily commercial websites, can afford to pay the high verification cost for these certificates, clients have no simple and effective means to authenticate connectivity to most other hosts on the Internet.

Because the high cost of creating and managing a host PKI presented a substantial barrier to the replacement of completely insecure protocols such as telnet, the SSH model of host authentication emerged as a pragmatic so-
perspective
Basic Premise
Basic Premise
Basic Premise
Basic Premise

Client

PayPal

Authority
Basic Premise

Client → Notaries → PayPal
Basic Premise
Basic Premise

Client

PayPal
Basic Premise

N

N

N

N

N

N

N
“perspective” is not new
The CA Version Of Perspective

VeriSign

Site Admin

PayPal
The CA Version Of Perspective

VeriSign

Site Admin

PayPal
The CA Version Of Perspective

VeriSign

Site Admin

PayPal
invert
user initiated
implementation
limited
self-signed certs
Perspectives Challenges

- Completeness
- Privacy
- Responsiveness
Perspectives Challenges

Completeness

Privacy

Responsiveness
initial connection
! eliminate CAs entirely
Perspectives Challenges

Completeness

Privacy

Responsiveness
Privacy Problems

Client — Notary — PayPal
Perspectives Challenges

- Completeness
- Privacy
- Responsiveness
notary lag
Notary Lag
Notary Lag

Client

Notary

PayPal

Wednesday, September 28, 2011
Notary Lag
• New Protocol
• New Client Implementation
• New Server Implementation
Perspectives Challenges

Completeness

Privacy

Responsiveness
! notary lag
Responsive: Eliminate Notary Lag
+ privacy
1) local caching
Local Caching

Client  

Notary

Local Cache

PayPal
Local Caching

Client -> Notary -> PayPal

Local Cache
Notary Bounce
Notary Bounce

Client

Bounce
Notary Bounce

Client

Bounce
Convergence : Firefox
Convergence: Extensible for the future.

Notary
Convergence: Extensible for the future.
Convergence: Extensible for the future.
Convergence: Extensible for the future.
Convergence: Extensible for the future.

Client → Notary → CA Signatures

Client

REST

PayPal
Convergence: Extensible for the future.

Client → Notary → SSL Observatory

REST

PayPal
Convergence: Extensible for the future.

Client → REST → Notary → Google Catalog → PayPal
Multiplicty and Agility

Client

Perspective

DNSSEC

CA Signatures

SSL Observatory

Bounce
Collective Trust

DNSSEC

CA Signatures

SSL Observatory

Consensus

Minority

Client

Perspective

Bounce
Collective Trust

DNSSEC

CA Signatures

SSL Observatory

Perspective

N

N

N

N

Client

Consensus

Minority

Bounce
Other Nice Things

Servers Do Nothing
Other Nice Things

!migrate internet
Other Nice Things

(1) Implement Convergence in the four major browsers.

(2) Be done.
Other Nice Things

no more self-signed certificate warnings
problems
“citibank problem”
This Connection is Untrusted

You have asked Firefox to connect securely to citibank.com, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

▸ Technical Details
▸ I Understand the Risks
captive portals
http://convergence.io
Leave with this:

Who do I have to trust?

...and for how long?
A prescribed set of people, forever.