Securing Internet Communication: TLS

CS 161: Computer Security

Prof. David Wagner

March 11, 2016

Today’s Lecture

- Applying crypto technology in practice
- Two simple abstractions cover 80% of the use cases for crypto:
  - “Sealed blob”: Data that is encrypted and authenticated under a particular key
  - Secure channel: Communication channel that can’t be eavesdropped on or tampered with
- Today: SSL – a secure channel

Today's Lecture

- Goal #1: overview of SSL/TLS, the most prominent Internet security protocol
  - Secures the web via HTTPS
- Goal #2: cement understanding of crypto building blocks & how they're used together

Building Secure End-to-End Channels

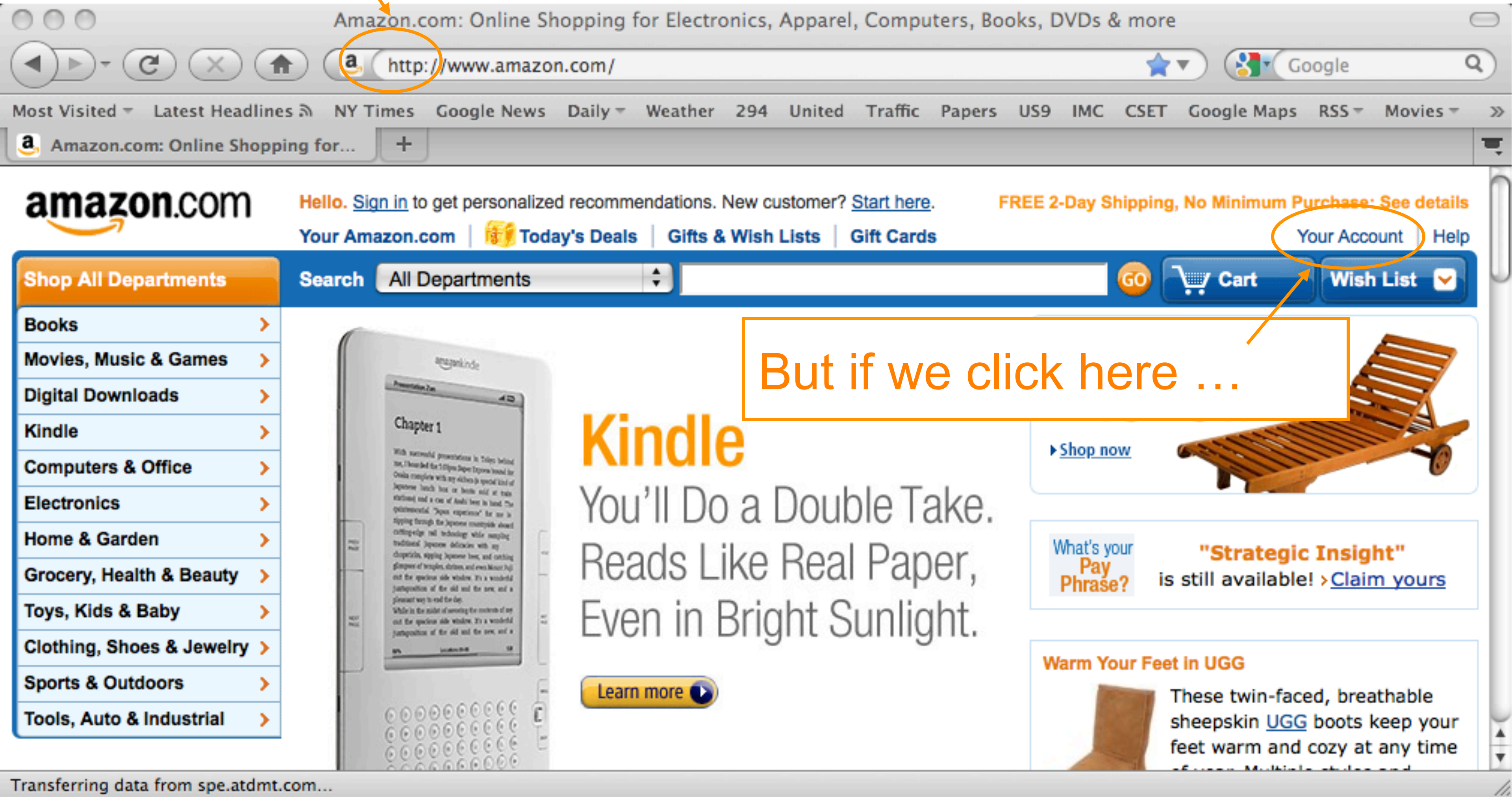
- *End-to-end* = communication protections achieved all the way from originating client to intended server
  - – With no need to trust intermediaries
- Dealing with threats:
  - – Eavesdropping?
    - Encryption (including session keys)
  - – Manipulation (injection, MITM)?
    - Integrity (use of a MAC); *replay protection*
  - – Impersonation?
    - Signatures

(What's missing?
Availability …)

Building A Secure End-to-End Channel: SSL/TLS

- SSL = *Secure Sockets Layer* (predecessor)
- TLS = *Transport Layer Security* (standard)
  - Both terms used interchangeably
- Security for *any* application that uses TCP
  - Secure = encryption/confidentiality + integrity + authentication (of server, but *not* of client)
  - E.g., puts the ‘s’ in “https”

Regular web surfing - http: URL



Hello. Sign in to get personalized recommendations. New customer? Start here.

FREE 2-Day Shipping, No Minimum Purchase: See details

You'll Do a Double Take. Reads Like Real Paper, Even in Bright Sunlight.

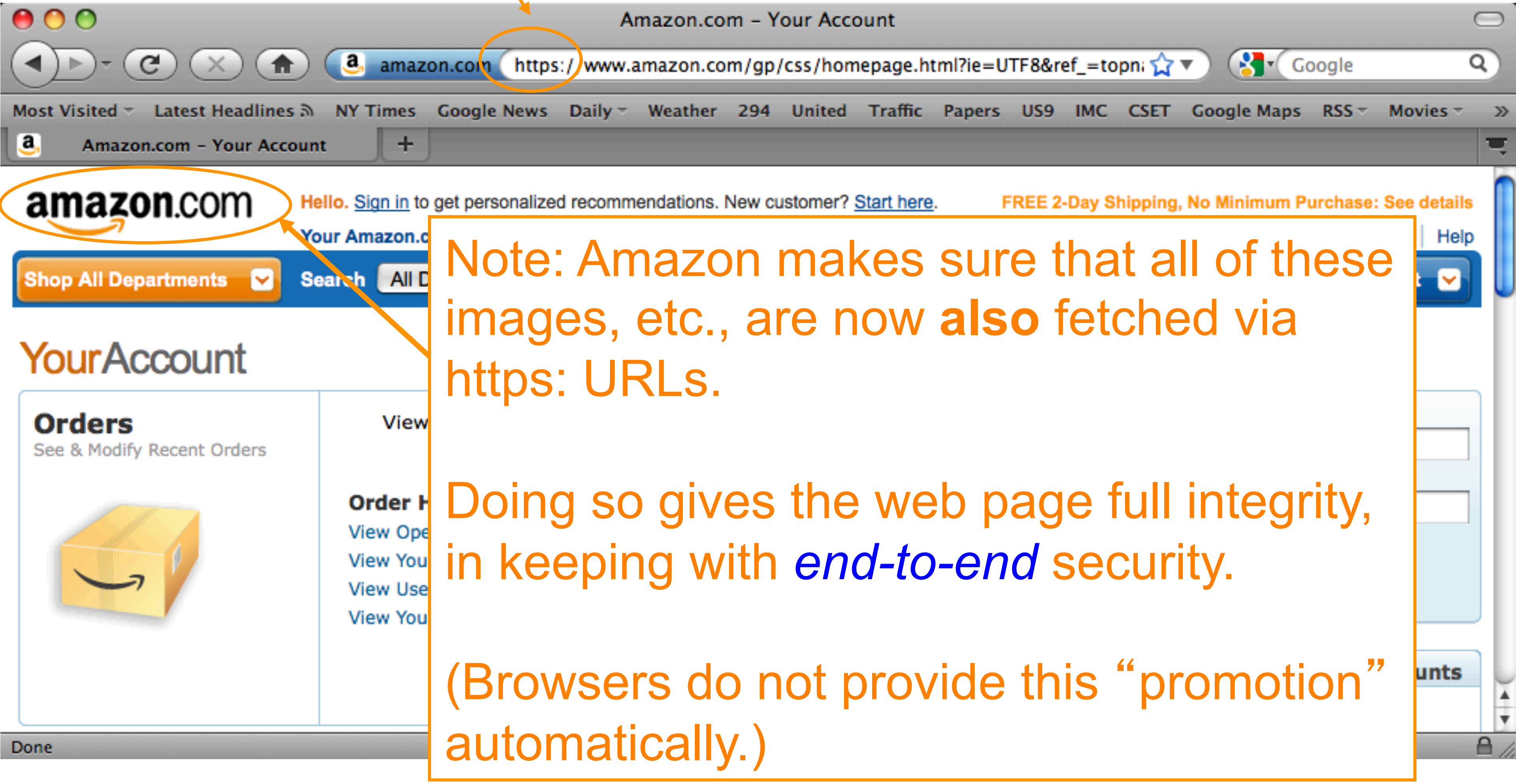
"Strategic Insight" is still available! › Claim yours

These twin-faced, breathable sheepskin UGG boots keep your feet warm and cozy at any time

Transferring data from spe.atdmt.com...

But if we click here …

Web surfing with TLS/SSL - https: URL



Hello. Sign in to get personalized recommendations. New customer? Start here.

FREE 2-Day Shipping, No Minimum Purchase: See details

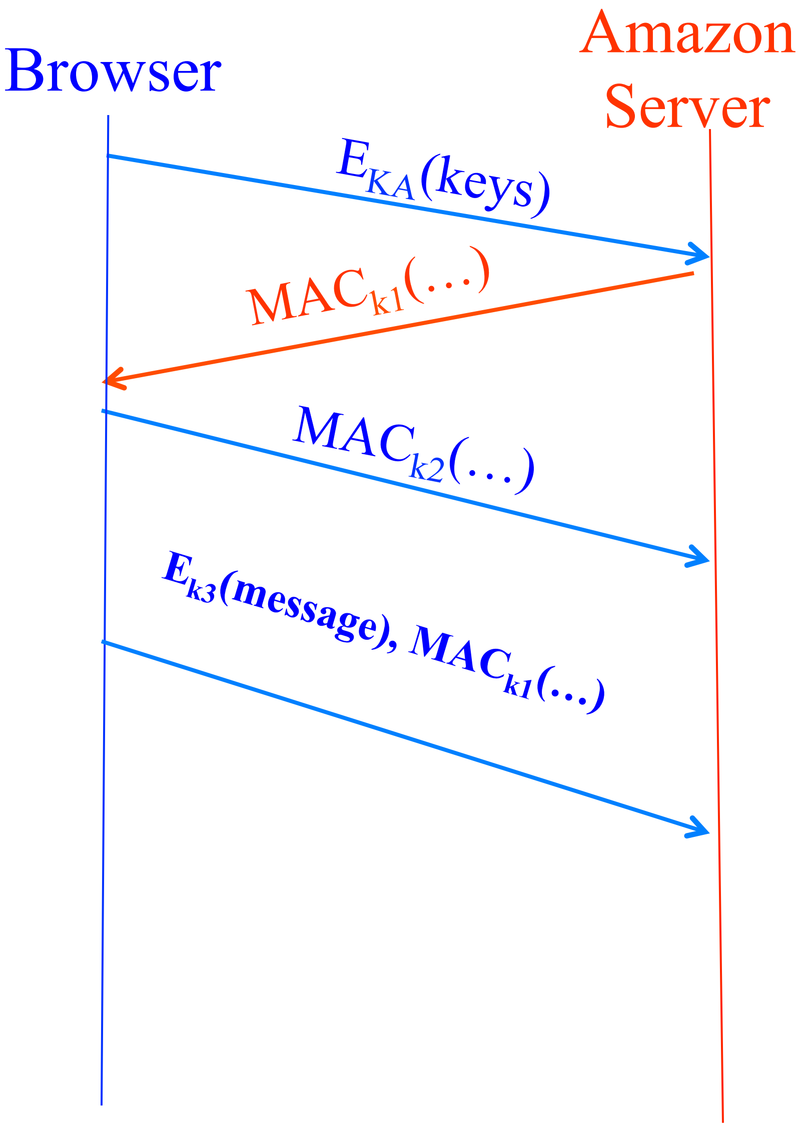
Note: Amazon makes sure that all of these images, etc., are now **also** fetched via https: URLs.

Doing so gives the web page full integrity, in keeping with *end-to-end* security.

(Browsers do not provide this “promotion” automatically.)

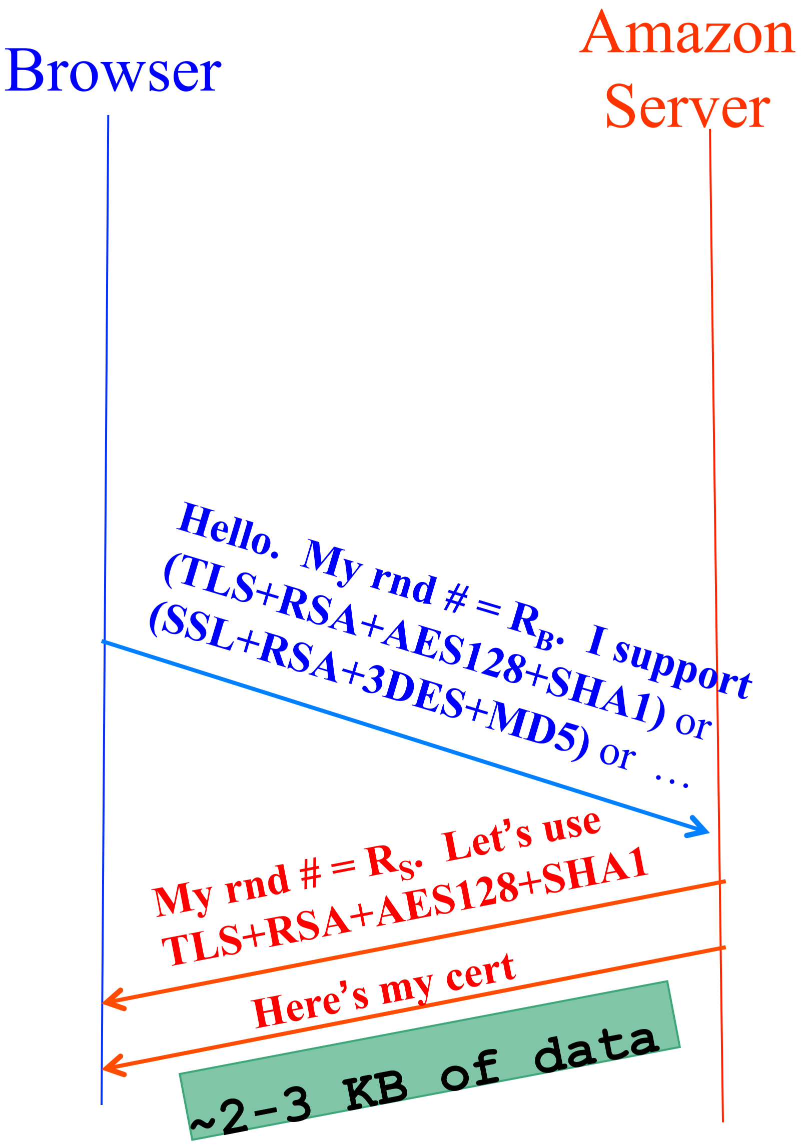
Basic idea

- Browser (client) picks some symmetric keys for encryption + authentication
- Client sends them to server, encrypted using RSA public-key encryption
- Both sides send MACs
- Now they use these keys to encrypt and authenticate all subsequent messages, using symmetric-key crypto



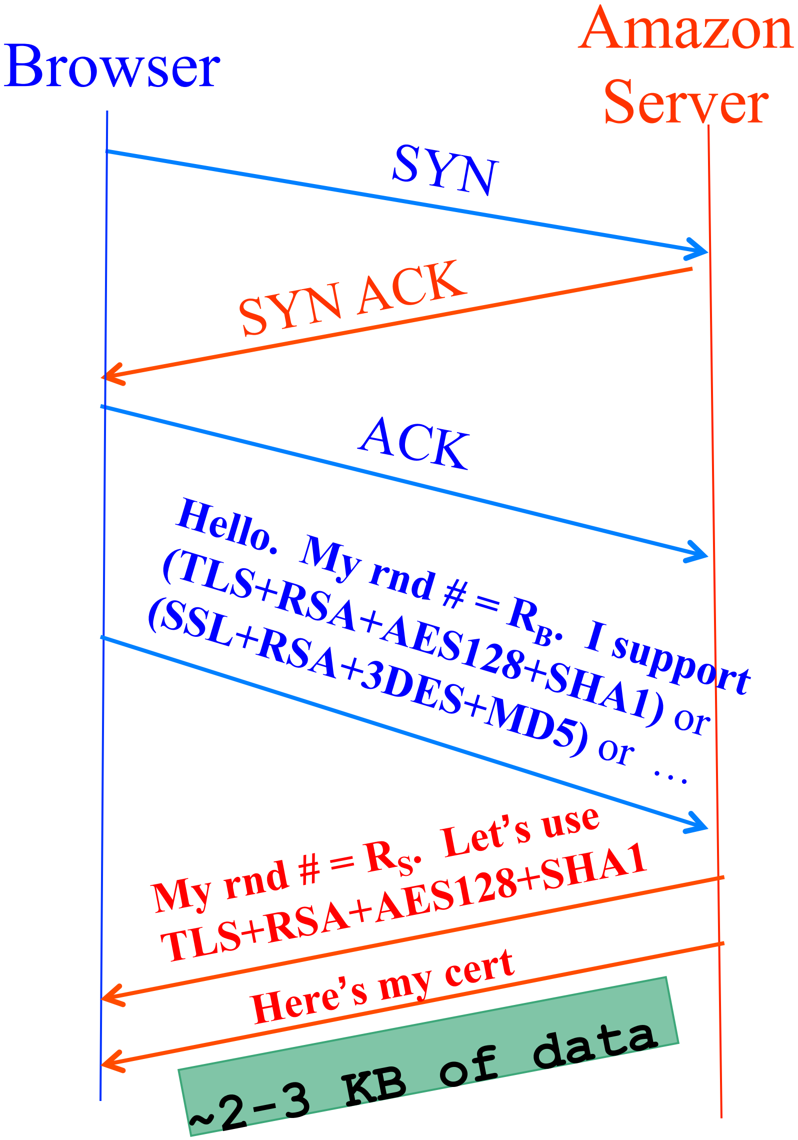
HTTPS Connection (SSL / TLS)

- Browser (client) connects to Amazon's **HTTPS** server
- Client picks 256-bit random number R_B, sends over list of crypto algorithms it supports
- Server picks 256-bit random number R_S, selects algorithms to use for this session
- Server sends over its certificate
- (all of this is in the clear)
- ***Client now validates cert***


Browser
Amazon Server
Hello. My rnd # = R_B. I support (TLS+RSA+AES128+SHA1) or (SSL+RSA+3DES+MD5) or …
My rnd # = R_S. Let's use TLS+RSA+AES128+SHA1
Here's my cert
~2-3 KB of data

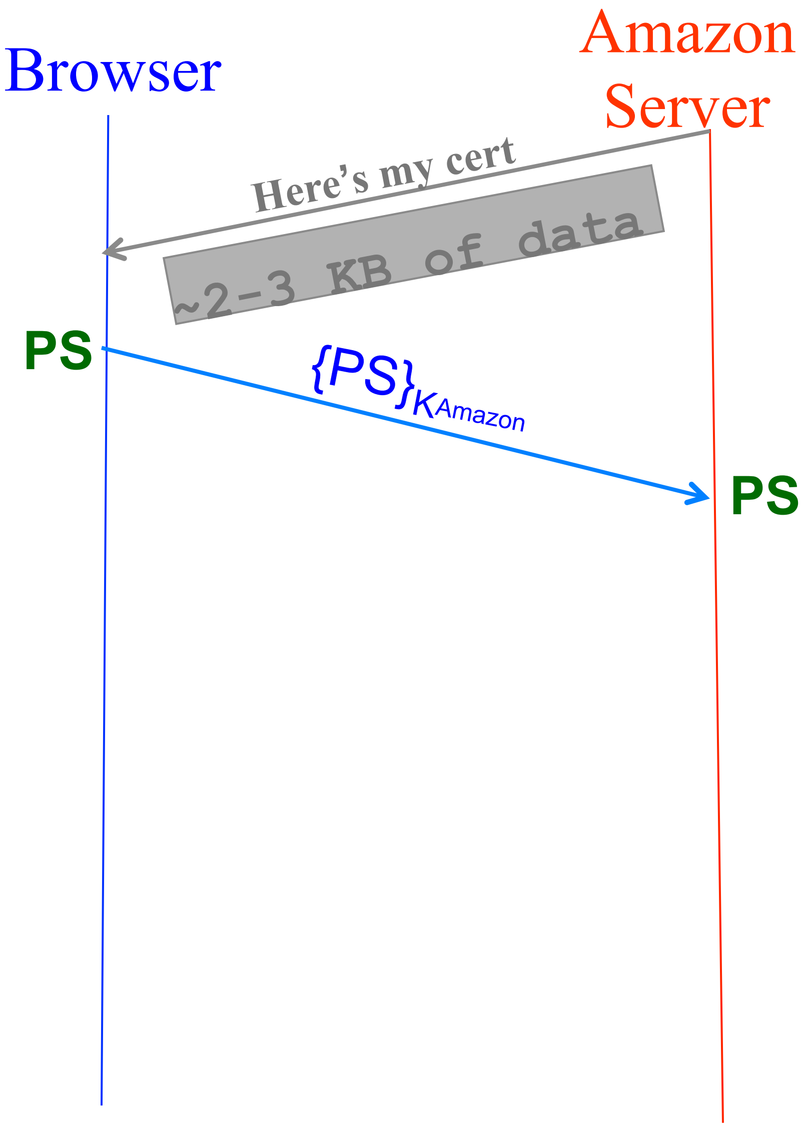
HTTPS Connection (SSL / TLS)

- Browser (client) connects via TCP to Amazon's **HTTPS** server
- Client picks 256-bit random number R_B, sends over list of crypto protocols it supports
- Server picks 256-bit random number R_S, selects protocols to use for this session
- Server sends over its certificate
- (all of this is in the clear)
- ***Client now validates cert***


Browser
Amazon Server
SYN
SYN ACK
ACK
Hello. My rnd # = R_B. I support (TLS+RSA+AES128+SHA1) or (SSL+RSA+3DES+MD5) or …
My rnd # = R_S. Let's use TLS+RSA+AES128+SHA1
Here's my cert
~2-3 KB of data

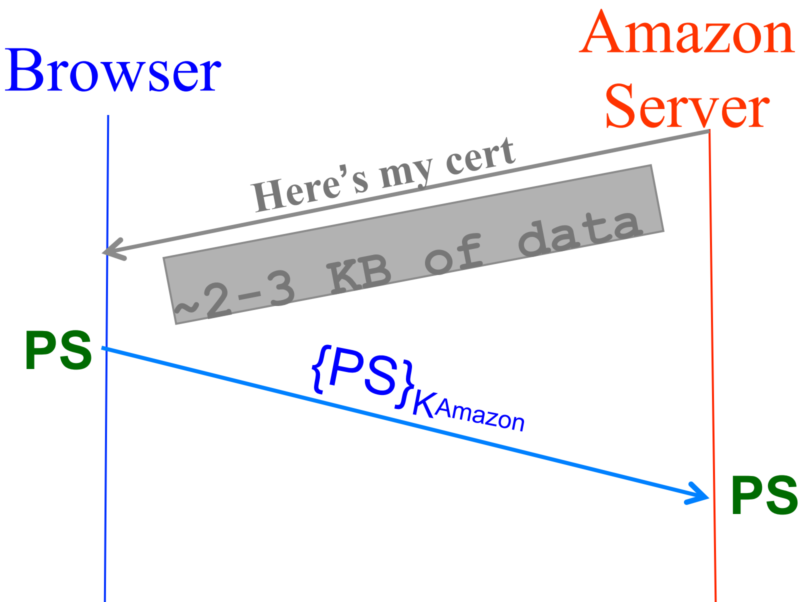
`HTTPS` Connection (SSL / TLS), cont.

- For RSA, browser constructs "Premaster Secret" **PS**
- Browser sends PS encrypted using Amazon's public RSA key K_{Amazon}
- Using PS, R_B, and R_S, browser & server derive symm. *cipher keys* (C_B, C_S) & MAC *integrity keys* (I_B, I_S)
  - One pair to use in each direction



`HTTPS` Connection (SSL / TLS), cont.

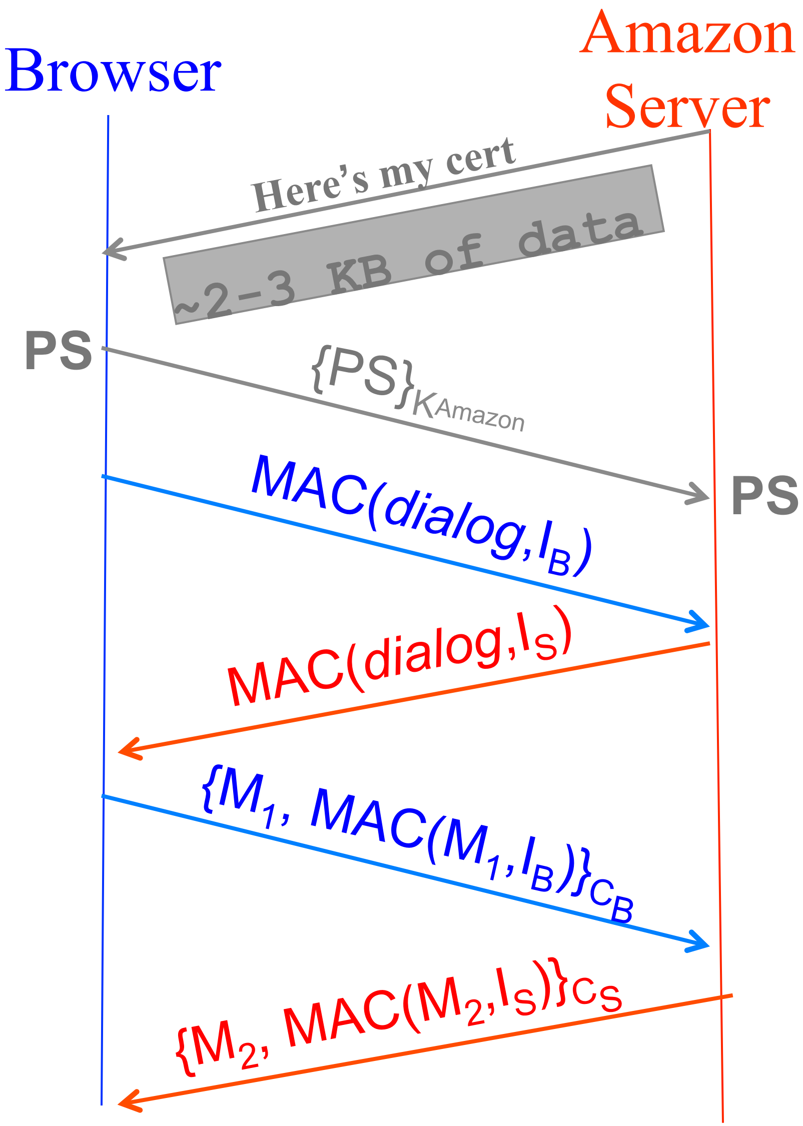
- For RSA, browser constructs “Premaster Secret” **PS**
- Browser sends PS encrypted using Amazon’s public RSA key K_{Amazon}
- Using PS, R_B, and R_S, browser & server derive symm. *cipher keys* (C_B, C_S) & MAC *integrity keys* (I_B, I_S)
  - One pair to use in each direction



These seed a cryptographically strong pseudo-random number generator (PRNG). Then browser & server produce C_B, C_S, *etc.*, by making repeated calls to the PRNG.

HTTPS Connection (SSL / TLS), cont.

- For RSA, browser constructs "Premaster Secret" **PS**
- Browser sends PS encrypted using Amazon's public RSA key K_{Amazon}
- Using PS, R_B, and R_S, browser & server derive symm. *cipher keys* (C_B, C_S) & MAC *integrity keys* (I_B, I_S)
  - One pair to use in each direction
- Browser & server exchange MACs computed over entire dialog so far
- If good MAC, Browser displays 🔒
- All subsequent communication encrypted w/ symmetric cipher (e.g., AES128) cipher keys, MACs
  - Sequence #'s thwart replay attacks



Browser

Amazon Server

Here's my cert

~2-3 KB of data

PS

$\{PS\}_{K_{Amazon}}$

PS

$MAC(dialog, I_B)$

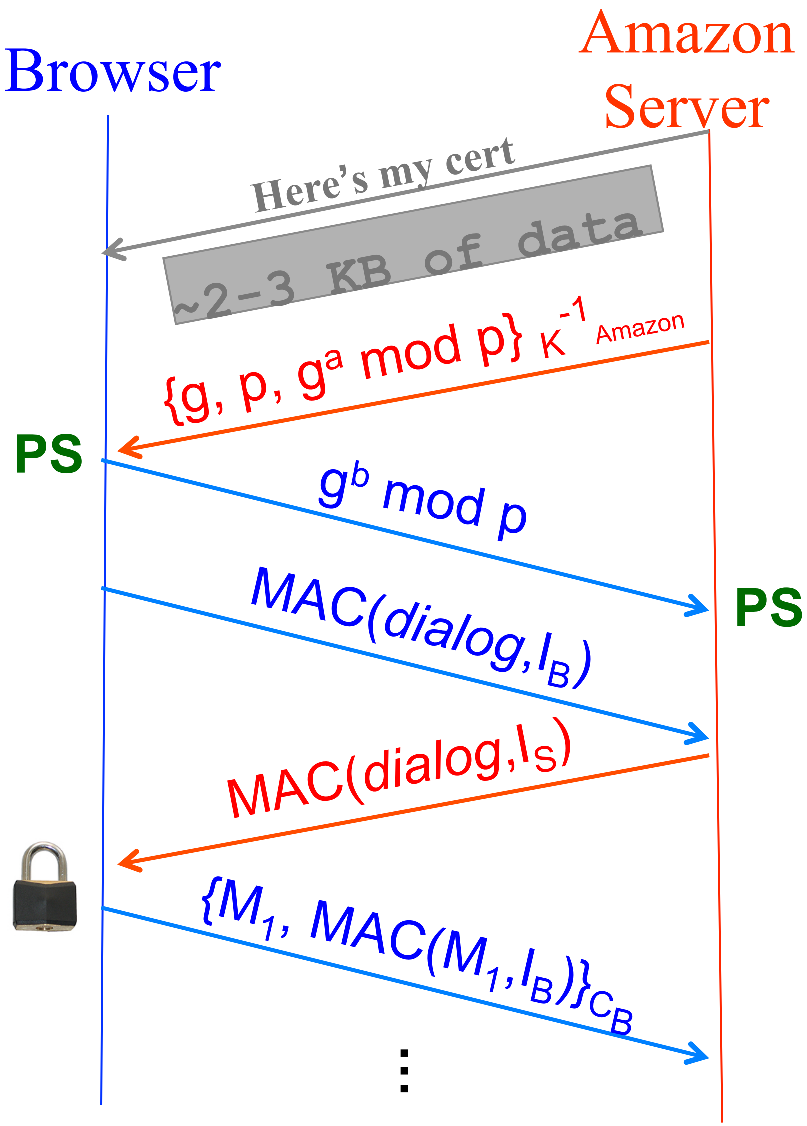
$MAC(dialog, I_S)$

$\{M_1, MAC(M_1, I_B)\}_{C_B}$

$\{M_2, MAC(M_2, I_S)\}_{C_S}$

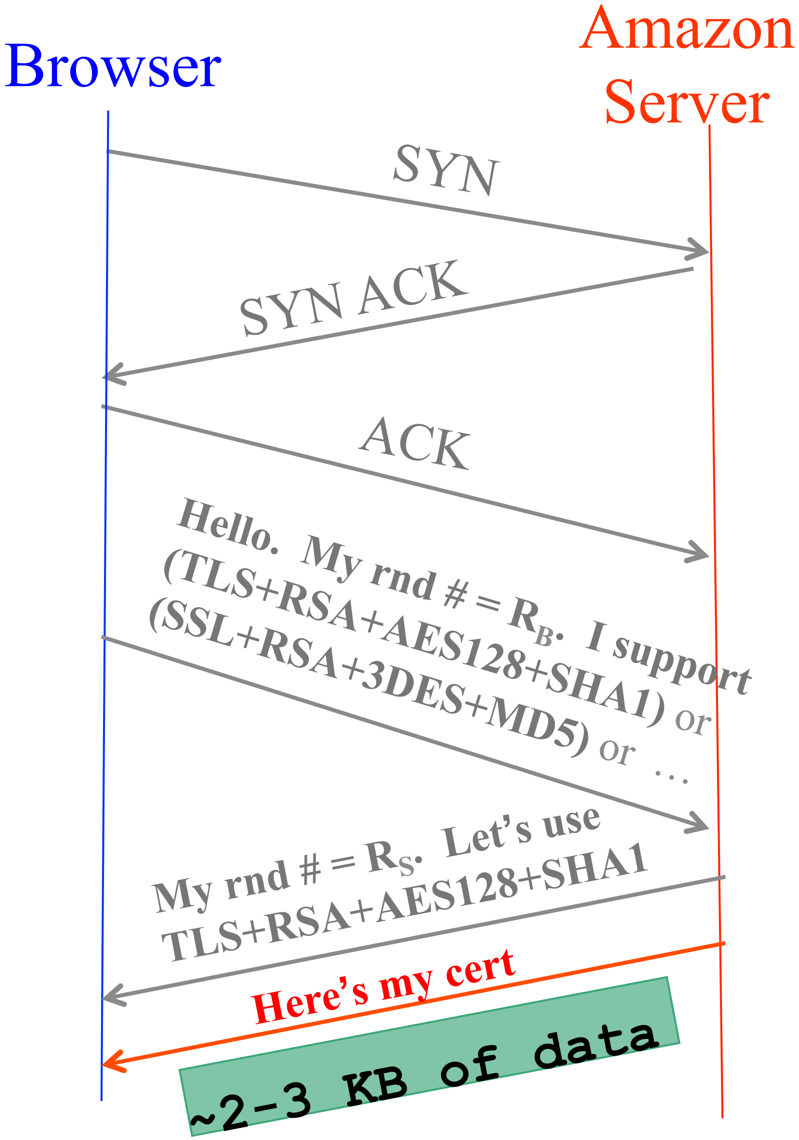
Alternative: Key Exchange via Diffie-Hellman

- For Diffie-Hellman, server generates random a, sends public params and g^a mod p
  - Signed with server's private key
- Browser verifies signature
- Browser generates random b, computes **PS** = g^{ab} mod p, sends to server
- Server also computes **PS** = g^{ab} mod p
- Remainder is as before: from PS, R_B, and R_S, browser & server derive symm. *cipher keys* (C_B, C_S) and MAC *integrity keys* (I_B, I_S), etc…



`HTTPS` Connection (SSL / TLS)

- Browser (client) connects via TCP to Amazon's `HTTPS` server
- Client picks 256-bit random number R_B, sends over list of crypto protocols it supports
- Server picks 256-bit random number R_S, selects protocols to use for this session
- Server sends over its certificate
- (all of this is in the clear)
- ***Client now validates cert***


Browser
Amazon Server
SYN
SYN ACK
ACK
Hello. My rnd # = R_B. I support (TLS+RSA+AES128+SHA1) or (SSL+RSA+3DES+MD5) or …
My rnd # = R_S. Let's use TLS+RSA+AES128+SHA1
Here's my cert
~2-3 KB of data

Certificates

- Cert = signed statement about someone's public key
  - Note that a cert does not say anything about the identity of who **gives** you the cert
  - It simply states a given public key K_{Bob} belongs to Bob …
    - … and backs up this statement with a digital signature made using a different public/private key pair, say from Verisign
- Bob then can prove his identity to you by *you sending him* something encrypted with K_{Bob} …
  - … which he then demonstrates he can read
- … or by *signing* something he demonstrably uses
- Works provided you trust that you have a valid copy of Verisign's public key …
  - … and you trust Verisign to use prudence when she signs other people's keys

Validating Amazon's Identity

- Browser compares domain *name* in cert w/ URL
  - Note: this provides an end-to-end property (as opposed to say a cert associated with an IP address)
- Browser accesses *separate* cert belonging to **issuer**
  - These are hardwired into the browser – and **trusted!**
  - There could be a *chain* of these …
- Browser applies issuer's public key to verify signature **S**, obtaining hash of what issuer signed
  - Compares with its own SHA-1 hash of Amazon's cert
- Assuming hashes match, now have high confidence it's indeed Amazon …
  - ***assuming signatory is trustworthy***

= assuming didn't lose private key; assuming didn't sign thoughtlessly

End-to-End ⇒ Powerful Protections

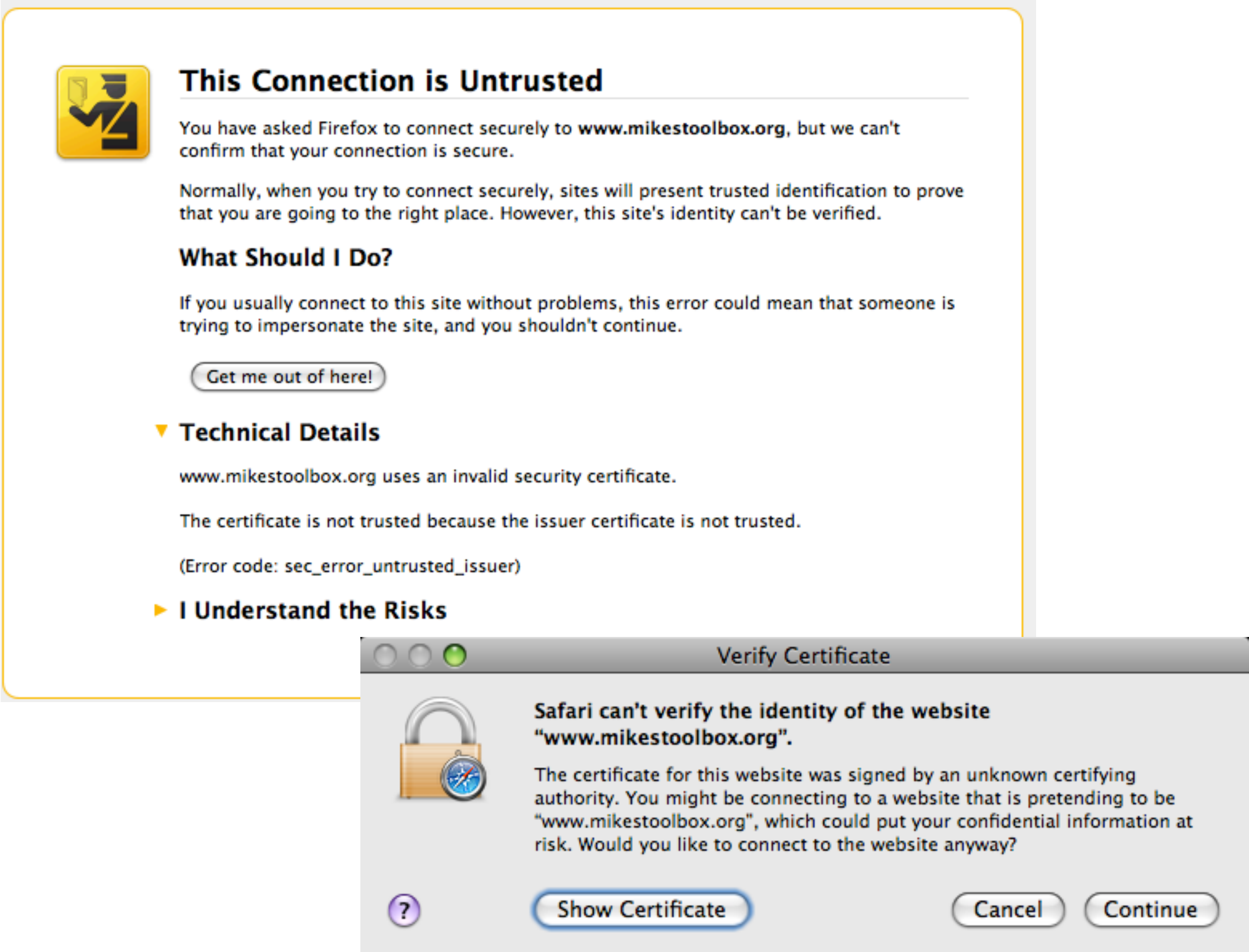
- Attacker runs a sniffer to capture our WiFi session?
  - (maybe by breaking crummy WEP security)
  - But: encrypted communication is unreadable
    - No problem!
- DNS cache poisoning?
  - Client goes to wrong server
  - But: detects impersonation
    - No problem!
- Attacker hijacks our connection, injects new traffic
  - But: data receiver rejects it due to failed integrity check
    - No problem!

Powerful Protections, cont.

- DHCP spoofing?
  - Client goes to wrong server
  - But: detects impersonation
    - No problem!
- Attacker manipulates routing to run us by an eavesdropper or take us to the wrong server?
  - But: they can’t read; we detect impersonation
    - No problem!
- Attacker slips in as a Man In The Middle?
  - But: they can’t read, they can’t inject
  - They can’t even replay previous encrypted traffic
  - **No problem!**

Validating Amazon’s Identity, cont.

- Browser retrieves cert belonging to the **issuer**
  - These are hardwired into the browser – and **trusted!**
- What if browser can’t find a cert for the issuer?



This Connection is Untrusted

You have asked Firefox to connect securely to **www.mikestoolbox.org**, 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.

▼ Technical Details

www.mikestoolbox.org uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is not trusted.

(Error code: sec_error_untrusted_issuer)

▶ I Understand the Risks

Safari can't verify the identity of the website "www.mikestoolbox.org".

The certificate for this website was signed by an unknown certifying authority. You might be connecting to a website that is pretending to be "www.mikestoolbox.org", which could put your confidential information at risk. Would you like to connect to the website anyway?

Validating Amazon's Identity, cont.

- Browser retrieves cert belonging to the **issuer**
  - These are hardwired into the browser – and **trusted!**
- What if browser can't find a cert for the issuer?
- If it can't find the cert, then warns the user that site has not been verified
  - Can still proceed, just without authentication
- Q: Which end-to-end security properties do we lose if we incorrectly trust that the site is whom we think?
- A: **All of them!**
  - Goodbye confidentiality, integrity, authentication
  - Active attacker can read everything, modify, impersonate

SSL / TLS Limitations

- Properly used, SSL / TLS provides powerful end-to-end protections
- So why not use it for *everything*??
- Issues:
  - Cost of public-key crypto (fairly minor)
    - Takes non-trivial CPU processing (but today a minor issue)
    - Note: *symmetric* key crypto on modern hardware is non-issue
  - Hassle of buying/maintaining certs (fairly minor)

SSL / TLS Limitations

- Properly used, SSL / TLS provides powerful end-to-end protections
- So why not use it for *everything*??
- Issues:
  - Cost of public-key crypto (fairly minor)
    - Takes non-trivial CPU processing (but today a minor issue)
    - Note: *symmetric* key crypto on modern hardware is non-issue
  - Hassle of buying/maintaining certs (fairly minor)
  - Integrating with other sites that don't use HTTPS
  - **Latency**: extra round trips ⇒ 1st page slower to load

SSL / TLS Limitations, cont.

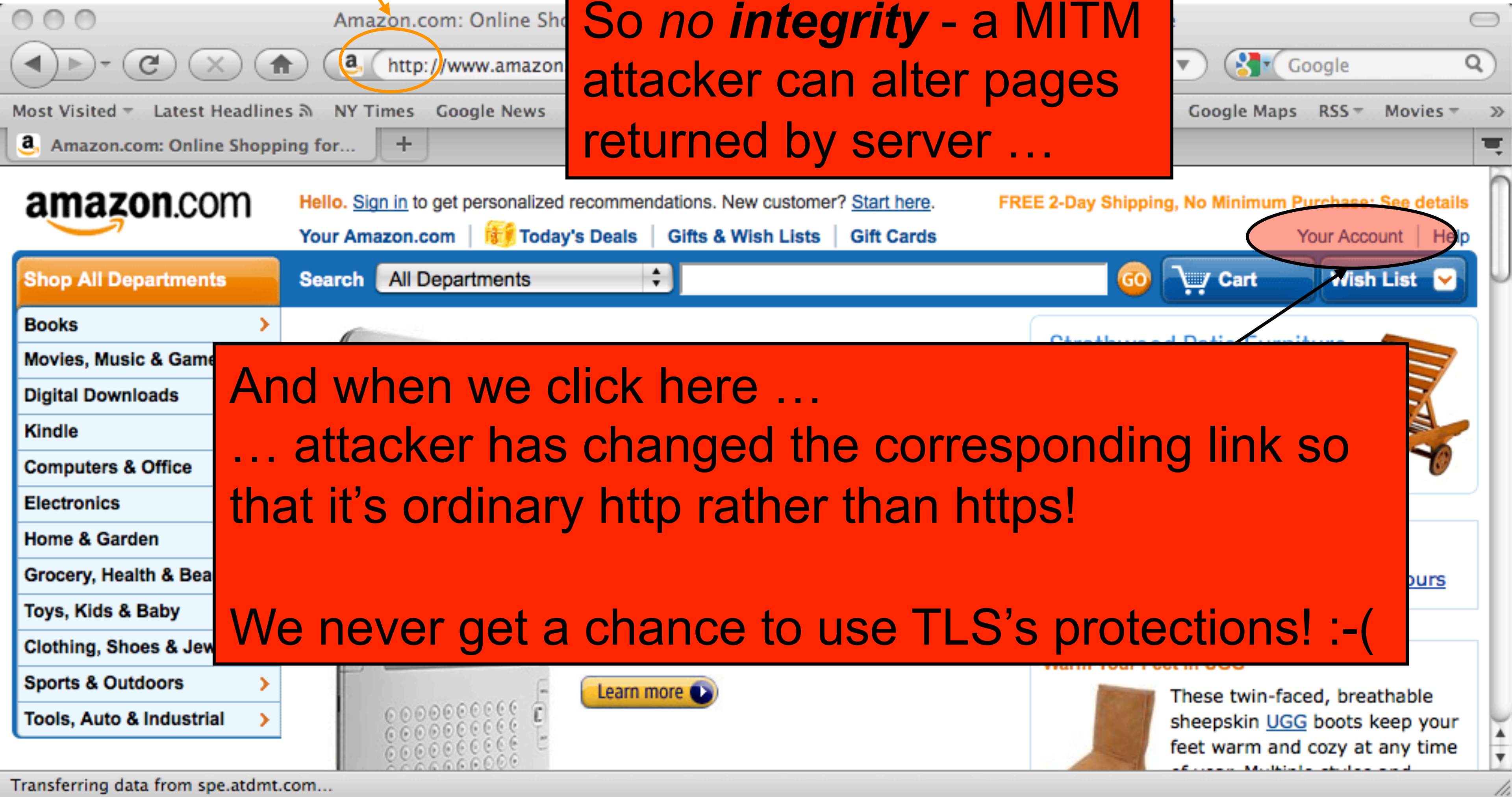
- Problems that SSL / TLS does **not** take care of ?
- TCP-level denial of service
  - SYN flooding
  - RST injection
    - (but does protect against data injection!)
- SQL injection / XSS / server-side coding/logic flaws
- Vulnerabilities introduced by server inconsistencies

SSL / TLS Limitations, cont.

- Problems that SSL / TLS does **not** take care of ?

- SQL injection / XSS / server-side coding/logic flaws
- Vulnerabilities introduced by server inconsistencies

Regular web surfing: http: URL



So *no* ***integrity*** - a MITM attacker can alter pages returned by server …

And when we click here …
… attacker has changed the corresponding link so that it's ordinary http rather than https!

We never get a chance to use TLS's protections! :-(

"sslstrip" attack

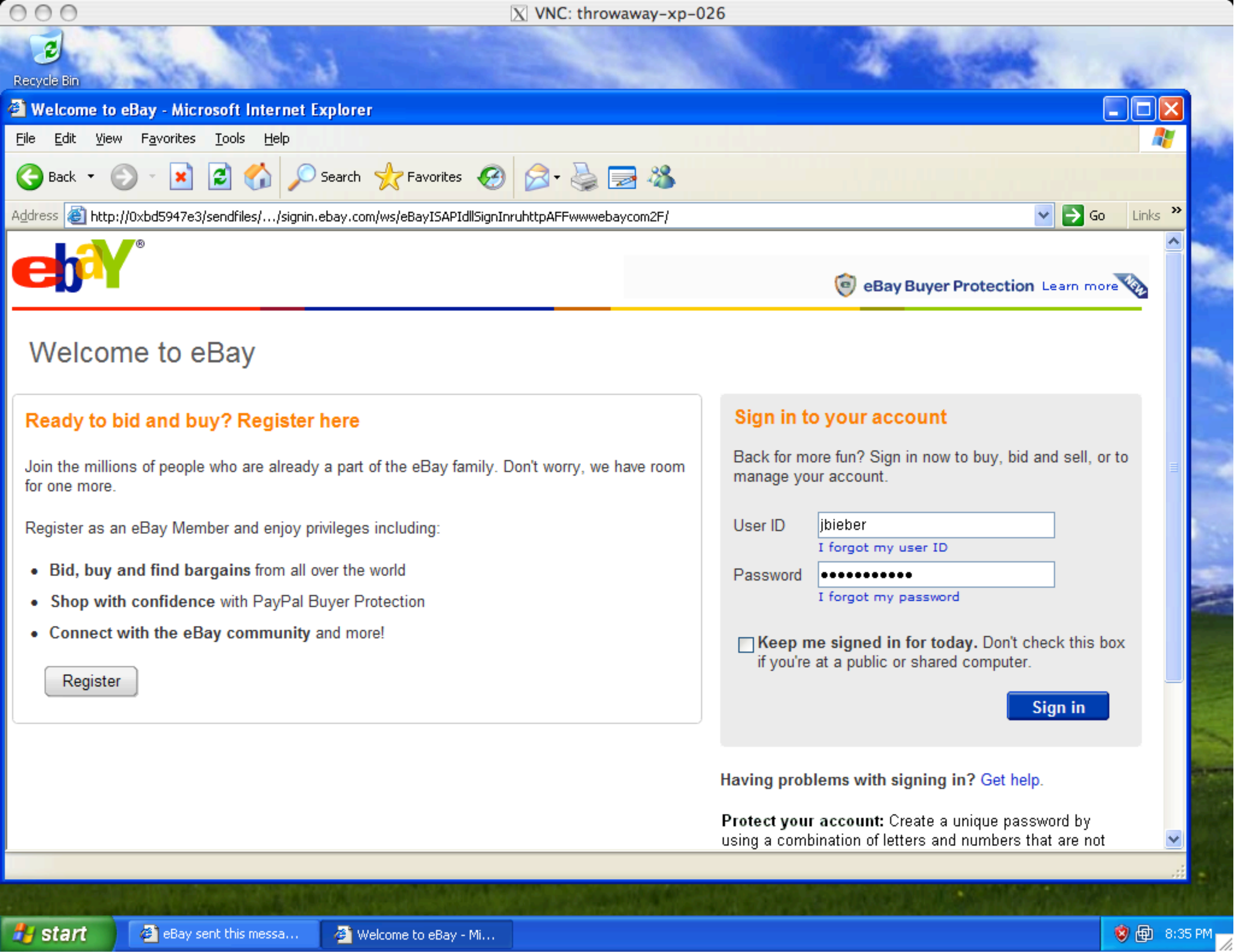
SSL / TLS Limitations, cont.

- Problems that SSL / TLS does **not** take care of ?

- SQL injection / XSS / server-side coding/logic flaws
- Vulnerabilities introduced by server inconsistencies
- Browser coding/logic flaws
- User flaws
  - Weak passwords
  - Phishing
- Issues of trust …

TLS/SSL Trust Issues

- User has to make correct trust decisions …



Welcome to eBay - Microsoft Internet Explorer

http://0xbd5947e3/sendfiles/…/signin.ebay.com/ws/eBayISAPIdllSignInruhttpAFFwwwebaycom2F/

Welcome to eBay

Ready to bid and buy? Register here

Join the millions of people who are already a part of the eBay family. Don't worry, we have room for one more.

Register as an eBay Member and enjoy privileges including:

- **Bid, buy and find bargains** from all over the world
- **Shop with confidence** with PayPal Buyer Protection
- **Connect with the eBay community** and more!

Sign in to your account

Back for more fun? Sign in now to buy, bid and sell, or to manage your account.

User ID: jbieber

I forgot my user ID

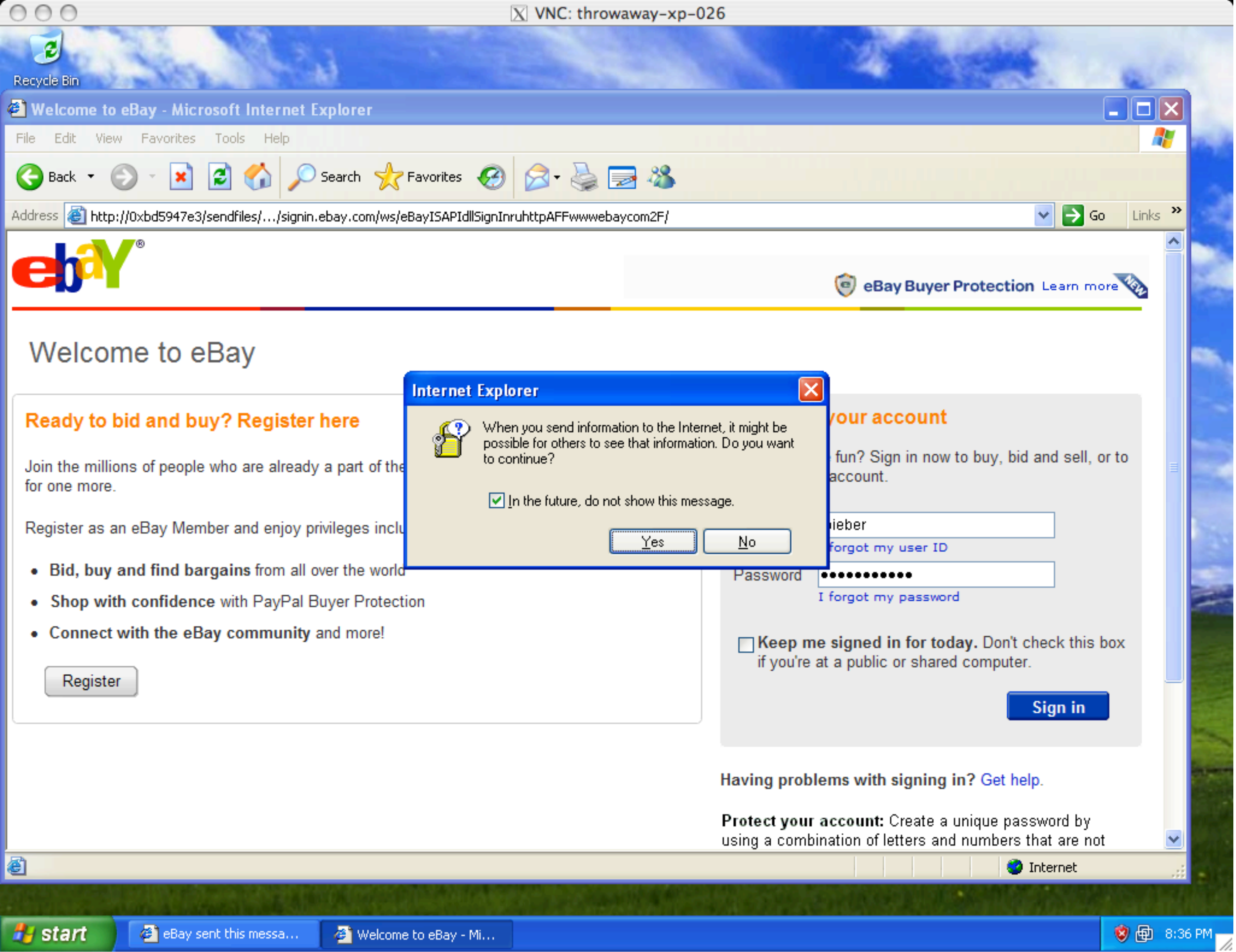
Password: ●●●●●●●●●●●

I forgot my password

□ **Keep me signed in for today.** Don't check this box if you're at a public or shared computer.

Having problems with signing in? Get help.

Protect your account: Create a unique password by using a combination of letters and numbers that are not



http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPIdllSignInruhttpAFFwwwebaycom2F/

eBay Buyer Protection Learn more

Welcome to eBay

Ready to bid and buy? Register here

Join the millions of people who are already a part of the
for one more.

Register as an eBay Member and enjoy privileges inclu

- **Bid, buy and find bargains** from all over the world
- **Shop with confidence** with PayPal Buyer Protection
- **Connect with the eBay community** and more!

Register

Internet Explorer

When you send information to the Internet, it might be possible for others to see that information. Do you want to continue?

☑ In the future, do not show this message.

Yes No

your account

fun? Sign in now to buy, bid and sell, or to
account.

ieber

forgot my user ID

Password ●●●●●●●●●●●

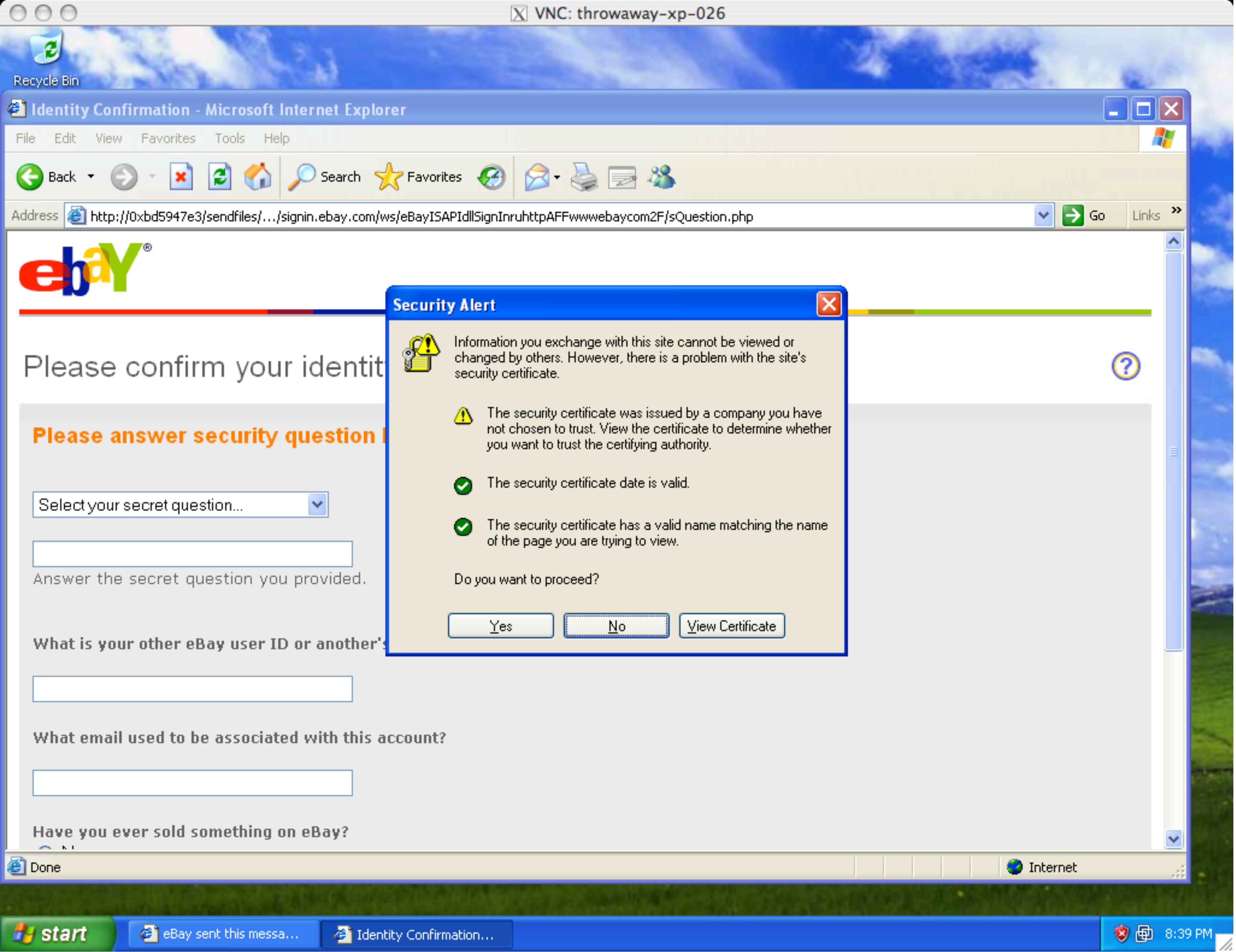
I forgot my password

□ **Keep me signed in for today.** Don't check this box if you're at a public or shared computer.

Sign in

Having problems with signing in? Get help.

Protect your account: Create a unique password by using a combination of letters and numbers that are not



VNC: throwaway-xp-026

Identity Confirmation - Microsoft Internet Explorer

Address http://0xbd5947e3/sendfiles/…/signin.ebay.com/ws/eBayISAPIdllSignInruhttpAFFwwwebaycom2F/sQuestion.php

Please confirm your identit

Please answer security question

Select your secret question...

Answer the secret question you provided.

What is your other eBay user ID or another's

What email used to be associated with this account?

Have you ever sold something on eBay?

Security Alert

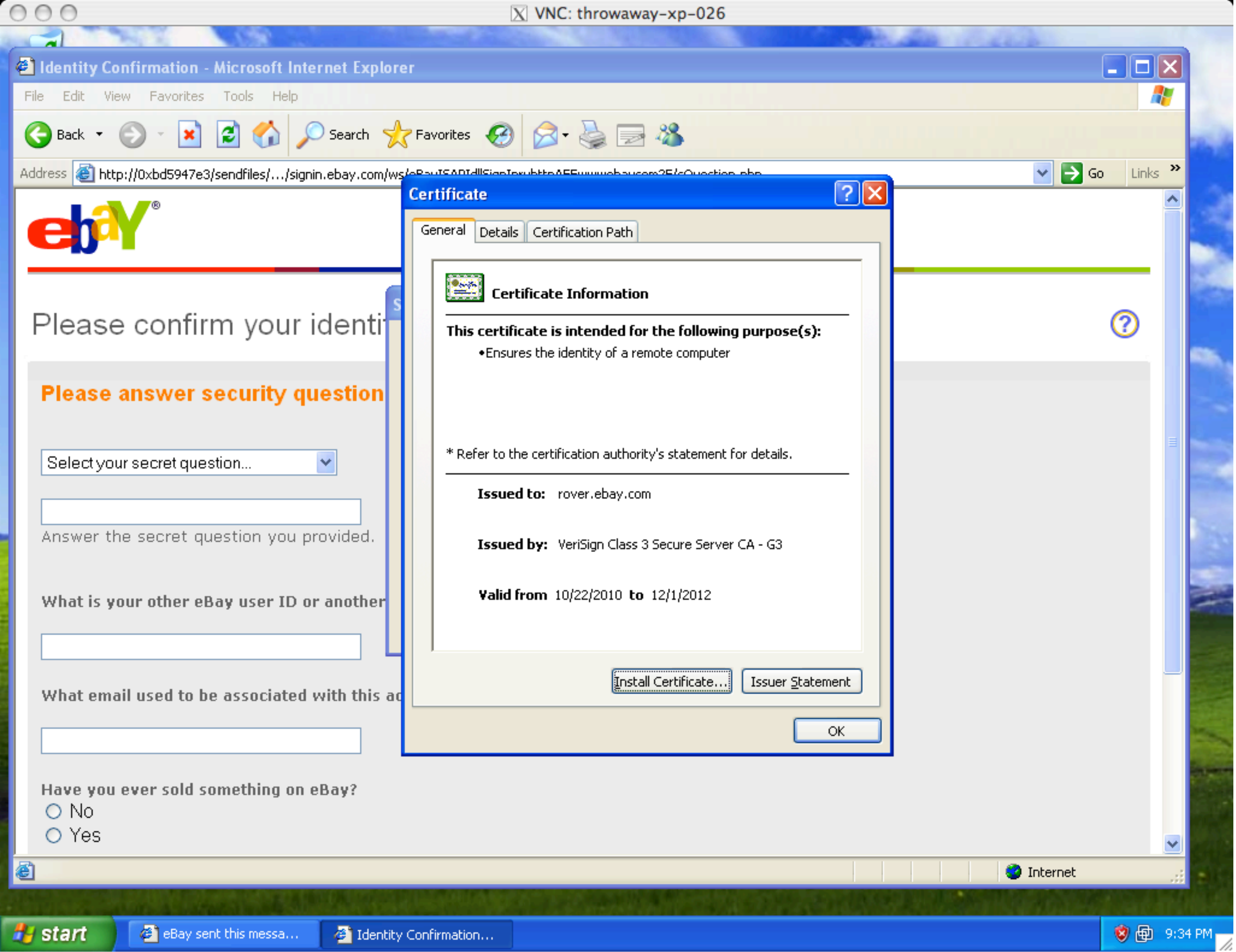
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?



http://0xbd5947e3/sendfiles/…/signin.ebay.com/ws

Please confirm your identi

Please answer security question

Select your secret question...

Answer the secret question you provided.

What is your other eBay user ID or another

What email used to be associated with this ac

Have you ever sold something on eBay?

○ No

○ Yes

Certificate Information

This certificate is intended for the following purpose(s):

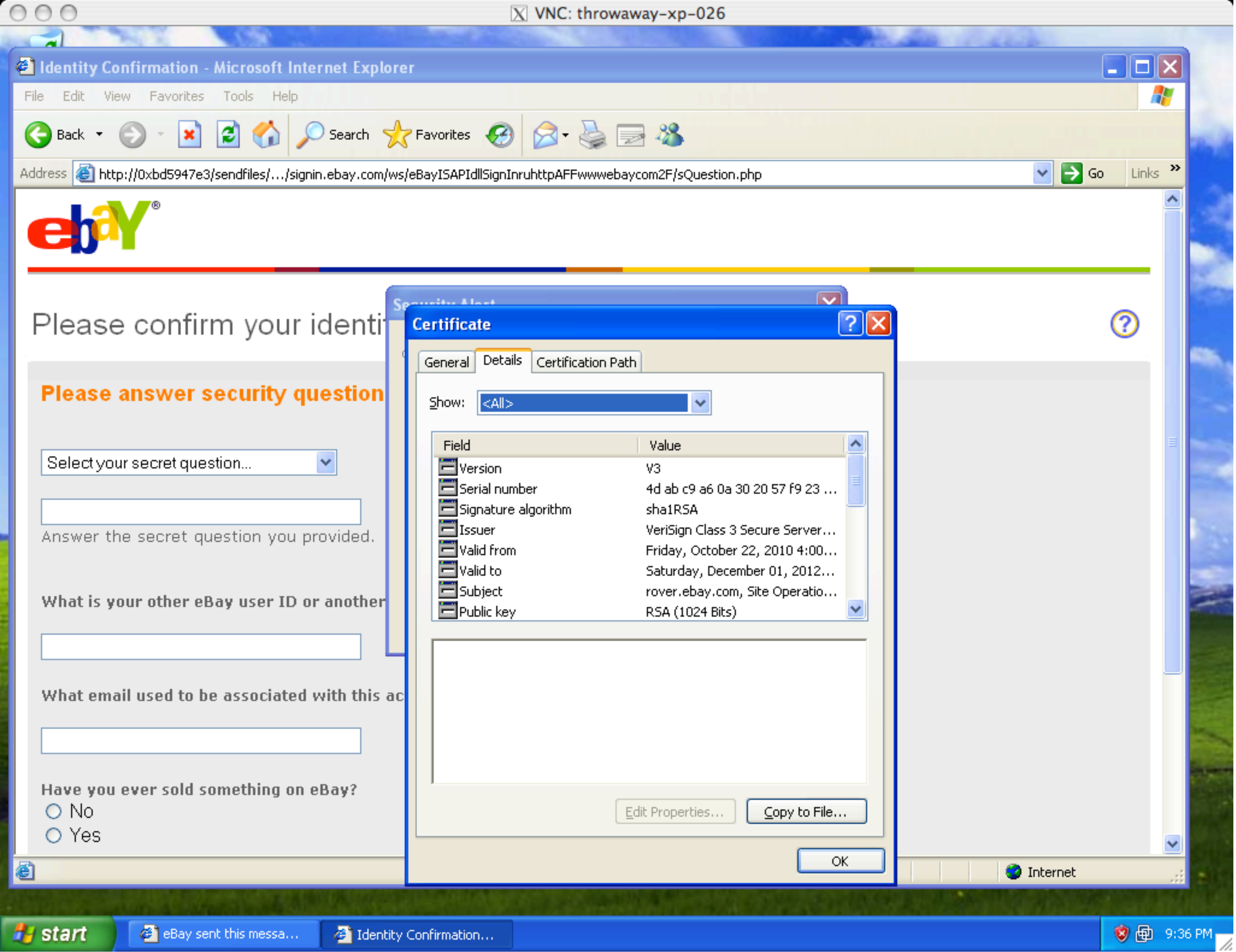
- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: rover.ebay.com

Issued by: VeriSign Class 3 Secure Server CA - G3

Valid from 10/22/2010 **to** 12/1/2012



VNC: throwaway-xp-026

Identity Confirmation - Microsoft Internet Explorer

Address http://0xbd5947e3/sendfiles/…/signin.ebay.com/ws/eBayISAPIdllSignInruhttpAFFwwwebaycom2F/sQuestion.php

Please confirm your identi

Please answer security question

Select your secret question...

Answer the secret question you provided.

What is your other eBay user ID or another

What email used to be associated with this ac

Have you ever sold something on eBay?

○ No

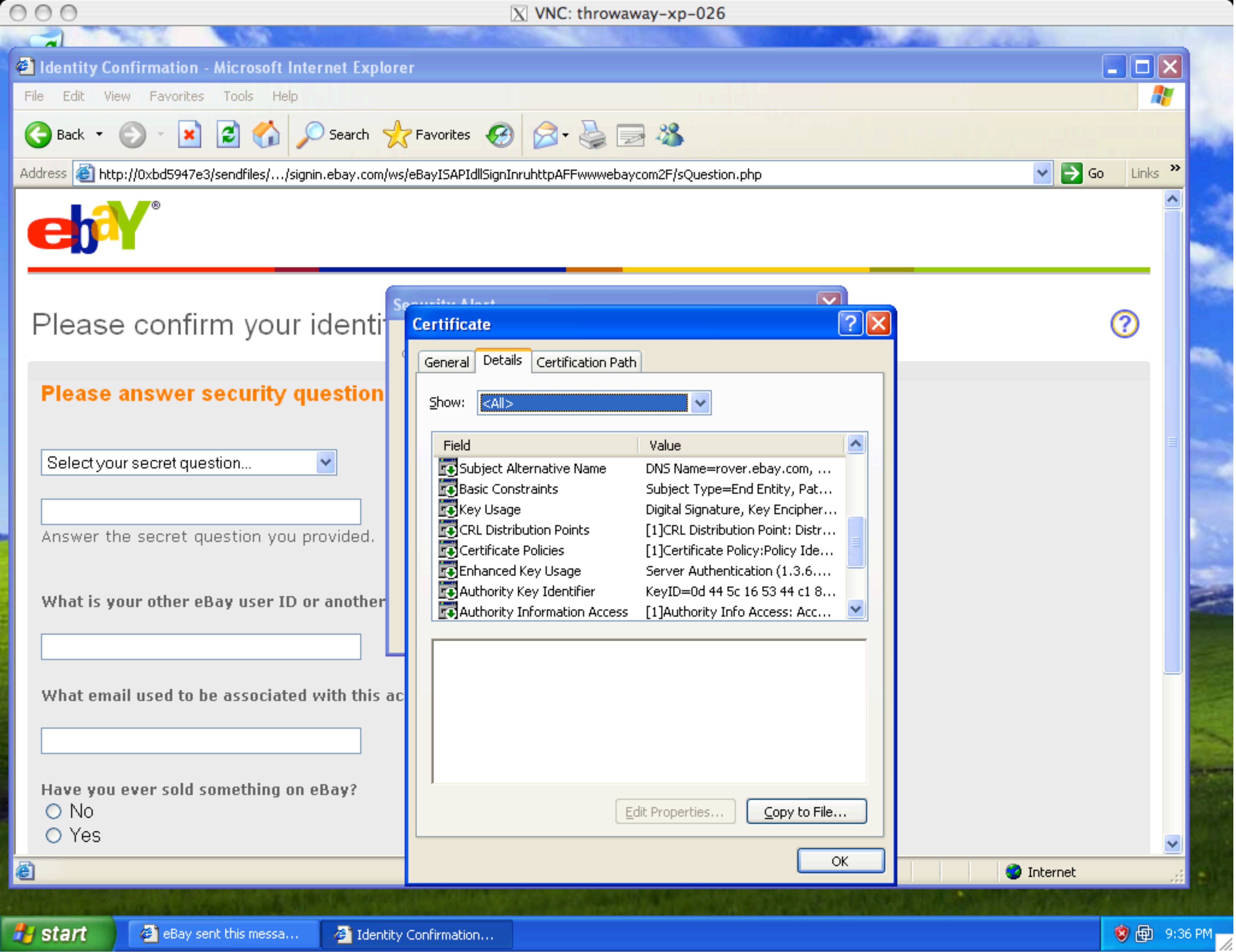
○ Yes

Security Alert

Certificate

Show: <All>

Field	Value
Version	V3
Serial number	4d ab c9 a6 0a 30 20 57 f9 23 …
Signature algorithm	sha1RSA
Issuer	VeriSign Class 3 Secure Server…
Valid from	Friday, October 22, 2010 4:00…
Valid to	Saturday, December 01, 2012…
Subject	rover.ebay.com, Site Operatio…
Public key	RSA (1024 Bits)



Identity Confirmation - Microsoft Internet Explorer

http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPIdllSignInruhttpAFFwwwebaycom2F/sQuestion.php

Please confirm your identi

Please answer security question

Select your secret question...

Answer the secret question you provided.

What is your other eBay user ID or another

What email used to be associated with this ac

Have you ever sold something on eBay?

○ No

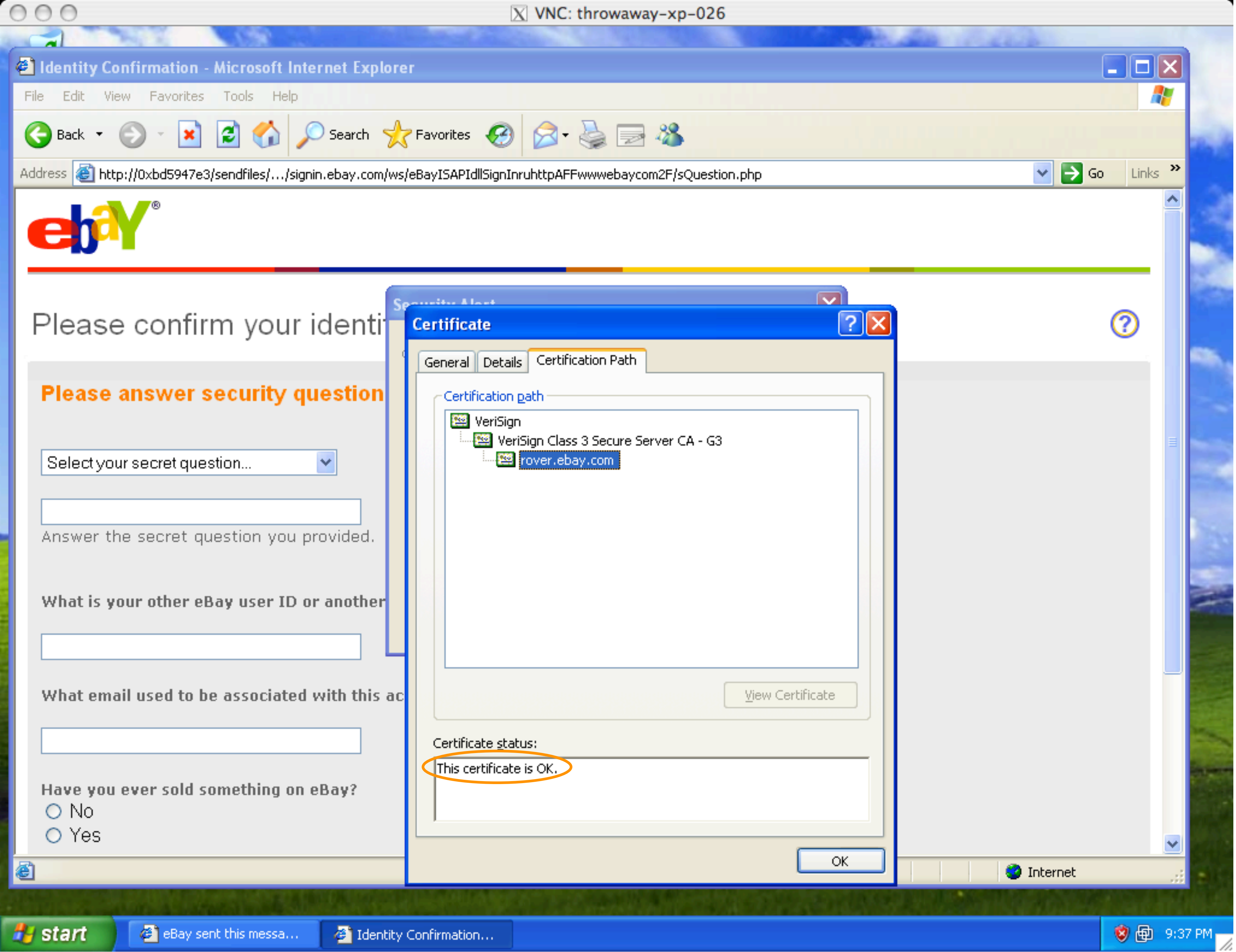
○ Yes

Security Alert

Certificate

Show: <All>

Field	Value
Subject Alternative Name	DNS Name=rover.ebay.com, ...
Basic Constraints	Subject Type=End Entity, Pat...
Key Usage	Digital Signature, Key Encipher...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Enhanced Key Usage	Server Authentication (1.3.6....
Authority Key Identifier	KeyID=0d 44 5c 16 53 44 c1 8...
Authority Information Access	[1]Authority Info Access: Acc...



http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPIdllSignInruhttpAFFwwwebaycom2F/sQuestion.php

Please confirm your identi

Please answer security question

Select your secret question...

Answer the secret question you provided.

What is your other eBay user ID or another

What email used to be associated with this ac

Have you ever sold something on eBay?

○ No
○ Yes

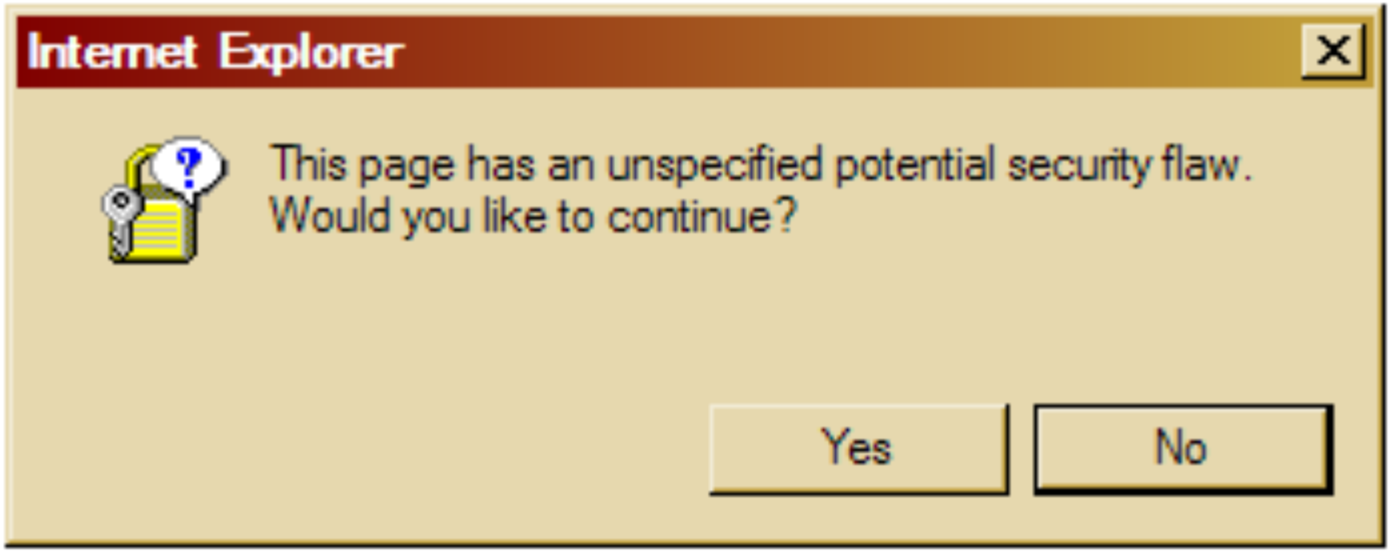
Certification path

- VeriSign
  - VeriSign Class 3 Secure Server CA - G3
    - rover.ebay.com

Certificate status:

This certificate is OK.

The equivalent as seen by most Internet users:

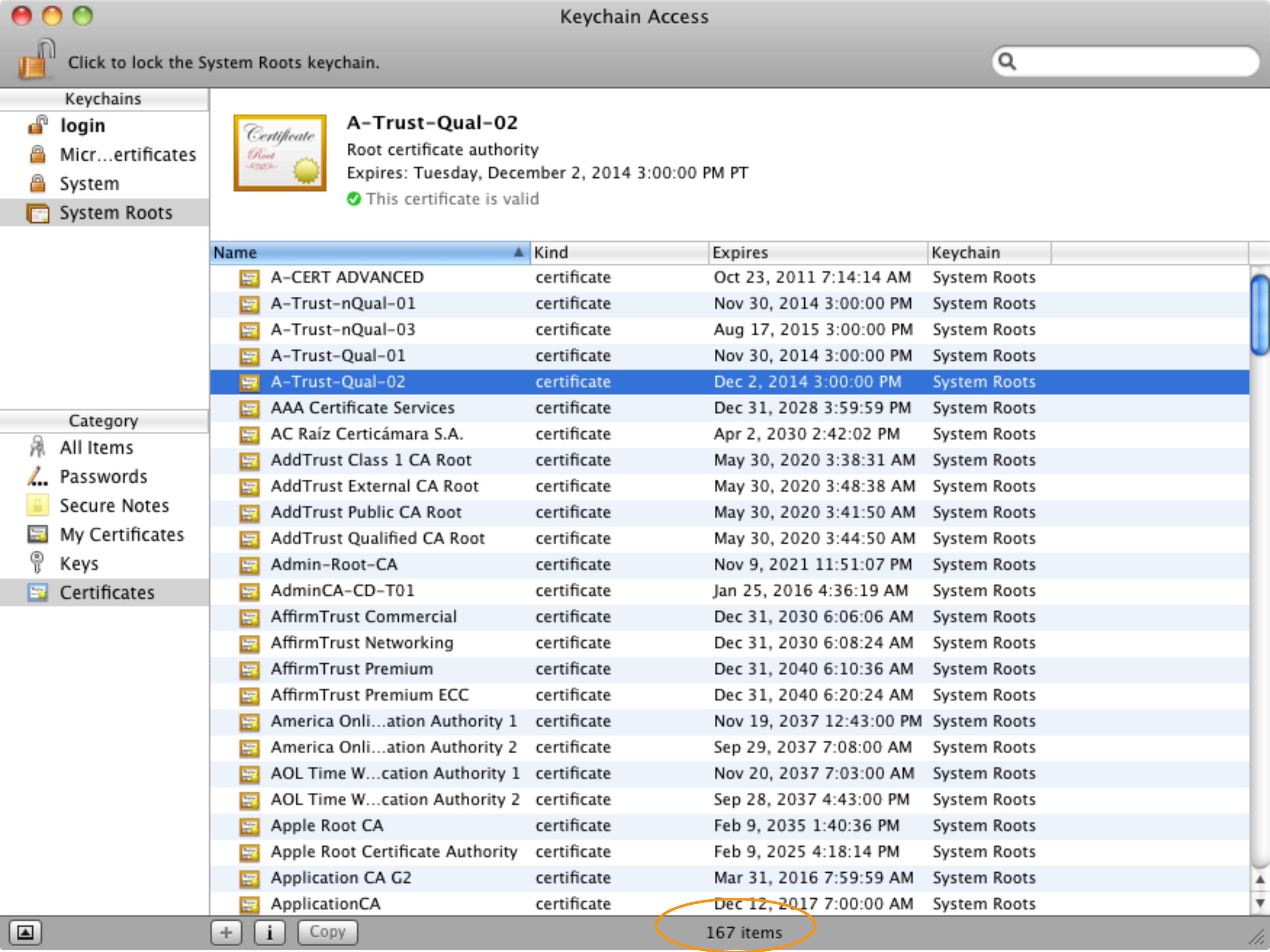


This page has an unspecified potential security flaw.
Would you like to continue?

(note: an actual Windows error message!)

TLS/SSL Trust Issues, cont.

- "*Commercial certificate authorities protect you from anyone from whom they are unwilling to take money.*"
  - – Matt Blaze, circa 2001
- So how many CAs do we have to worry about, anyway?



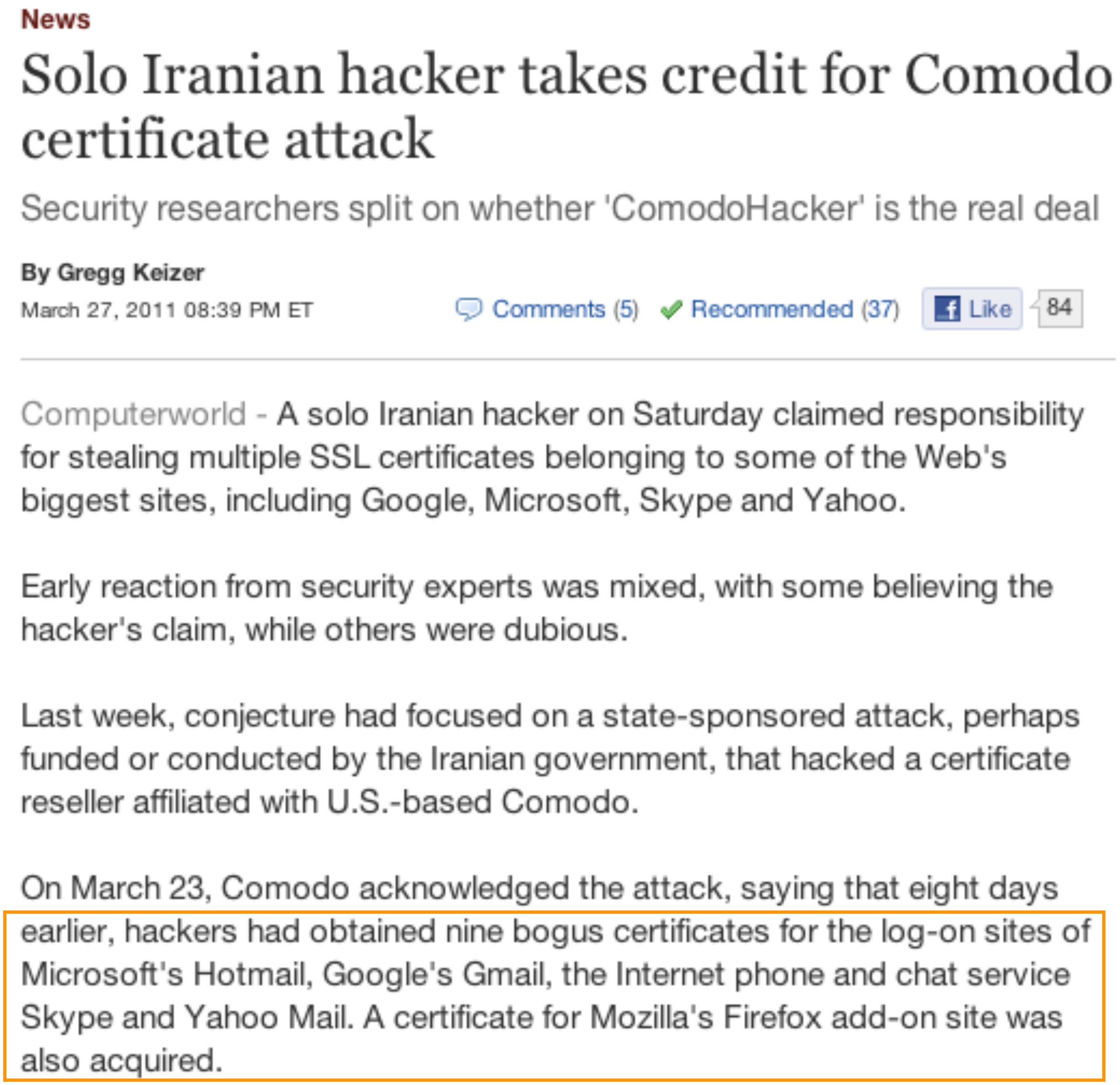
A-Trust-Qual-02
Root certificate authority
Expires: Tuesday, December 2, 2014 3:00:00 PM PT
✓ This certificate is valid

Name	Kind	Expires	Keychain
A-CERT ADVANCED	certificate	Oct 23, 2011 7:14:14 AM	System Roots
A-Trust-nQual-01	certificate	Nov 30, 2014 3:00:00 PM	System Roots
A-Trust-nQual-03	certificate	Aug 17, 2015 3:00:00 PM	System Roots
A-Trust-Qual-01	certificate	Nov 30, 2014 3:00:00 PM	System Roots
A-Trust-Qual-02	certificate	Dec 2, 2014 3:00:00 PM	System Roots
AAA Certificate Services	certificate	Dec 31, 2028 3:59:59 PM	System Roots
AC Raíz Certicámara S.A.	certificate	Apr 2, 2030 2:42:02 PM	System Roots
AddTrust Class 1 CA Root	certificate	May 30, 2020 3:38:31 AM	System Roots
AddTrust External CA Root	certificate	May 30, 2020 3:48:38 AM	System Roots
AddTrust Public CA Root	certificate	May 30, 2020 3:41:50 AM	System Roots
AddTrust Qualified CA Root	certificate	May 30, 2020 3:44:50 AM	System Roots
Admin-Root-CA	certificate	Nov 9, 2021 11:51:07 PM	System Roots
AdminCA-CD-T01	certificate	Jan 25, 2016 4:36:19 AM	System Roots
AffirmTrust Commercial	certificate	Dec 31, 2030 6:06:06 AM	System Roots
AffirmTrust Networking	certificate	Dec 31, 2030 6:08:24 AM	System Roots
AffirmTrust Premium	certificate	Dec 31, 2040 6:10:36 AM	System Roots
AffirmTrust Premium ECC	certificate	Dec 31, 2040 6:20:24 AM	System Roots
America Onli…ation Authority 1	certificate	Nov 19, 2037 12:43:00 PM	System Roots
America Onli…ation Authority 2	certificate	Sep 29, 2037 7:08:00 AM	System Roots
AOL Time W…cation Authority 1	certificate	Nov 20, 2037 7:03:00 AM	System Roots
AOL Time W…cation Authority 2	certificate	Sep 28, 2037 4:43:00 PM	System Roots
Apple Root CA	certificate	Feb 9, 2035 1:40:36 PM	System Roots
Apple Root Certificate Authority	certificate	Feb 9, 2025 4:18:14 PM	System Roots
Application CA G2	certificate	Mar 31, 2016 7:59:59 AM	System Roots
ApplicationCA	certificate	Dec 12, 2017 7:00:00 AM	System Roots

167 items

TLS/SSL Trust Issues

- *"Commercial certificate authorities protect you from anyone from whom they are unwilling to take money."*
  - Matt Blaze, circa 2001
- So how many CAs do we have to worry about, anyway?
- Of course, it's not just their greed that matters …



News

Solo Iranian hacker takes credit for Comodo certificate attack

Security researchers split on whether 'ComodoHacker' is the real deal

By Gregg Keizer

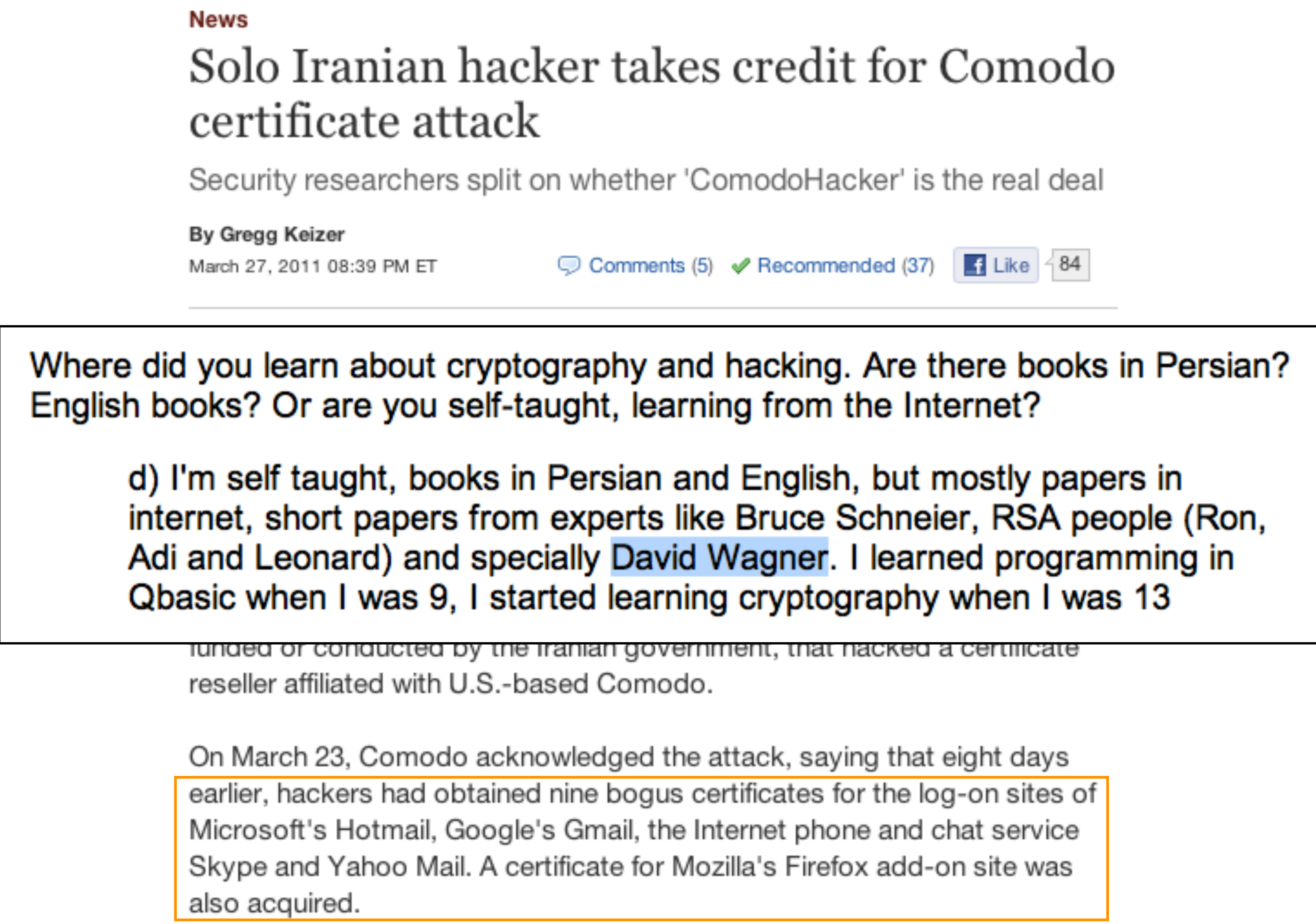
March 27, 2011 08:39 PM ET

Computerworld - A solo Iranian hacker on Saturday claimed responsibility for stealing multiple SSL certificates belonging to some of the Web's biggest sites, including Google, Microsoft, Skype and Yahoo.

Early reaction from security experts was mixed, with some believing the hacker's claim, while others were dubious.

Last week, conjecture had focused on a state-sponsored attack, perhaps funded or conducted by the Iranian government, that hacked a certificate reseller affiliated with U.S.-based Comodo.

On March 23, Comodo acknowledged the attack, saying that eight days earlier, hackers had obtained nine bogus certificates for the log-on sites of Microsoft's Hotmail, Google's Gmail, the Internet phone and chat service Skype and Yahoo Mail. A certificate for Mozilla's Firefox add-on site was also acquired.



News

Solo Iranian hacker takes credit for Comodo certificate attack

Security researchers split on whether 'ComodoHacker' is the real deal

By Gregg Keizer

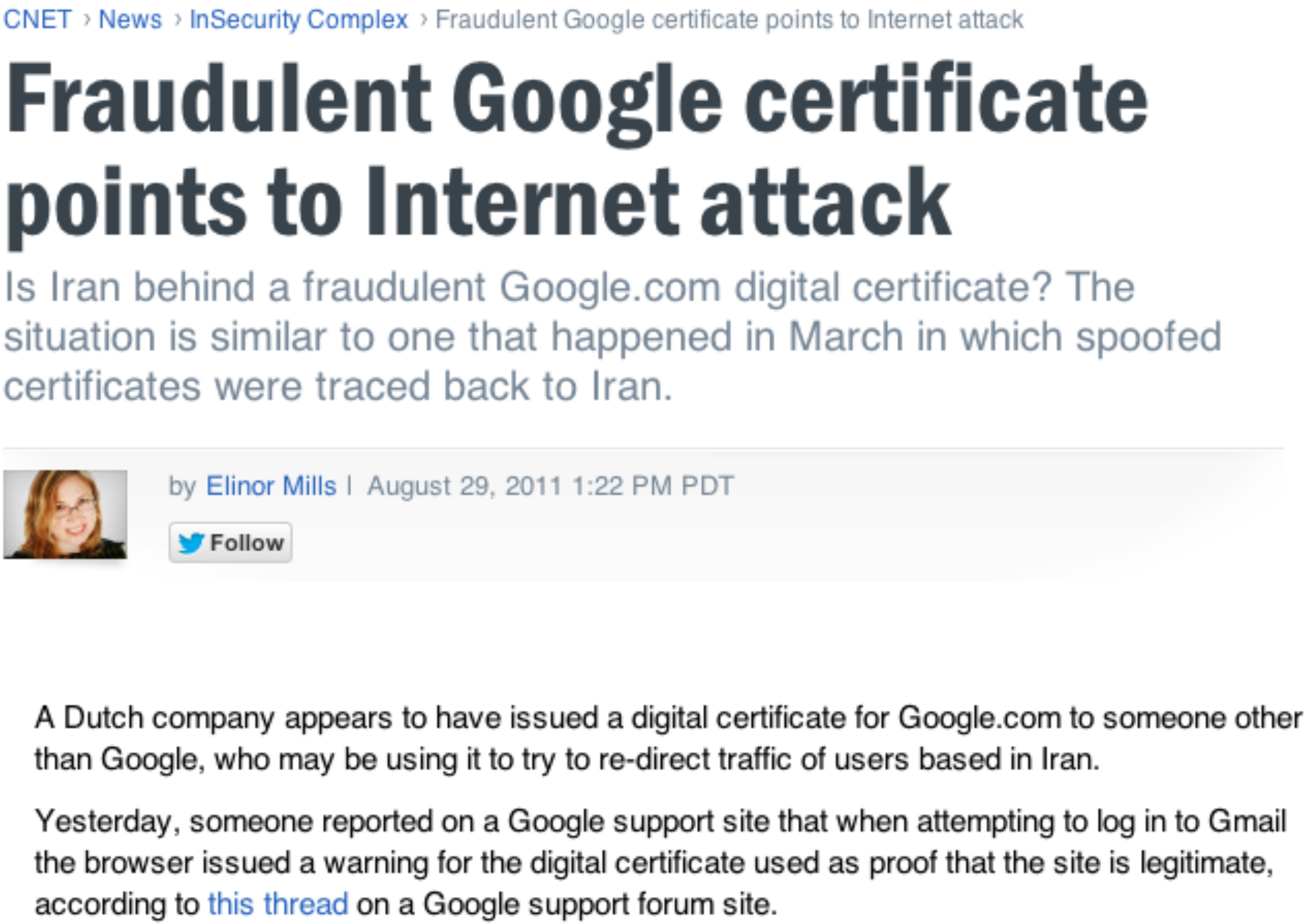
March 27, 2011 08:39 PM ET

Where did you learn about cryptography and hacking. Are there books in Persian? English books? Or are you self-taught, learning from the Internet?

> d) I'm self taught, books in Persian and English, but mostly papers in internet, short papers from experts like Bruce Schneier, RSA people (Ron, Adi and Leonard) and specially David Wagner. I learned programming in Qbasic when I was 9, I started learning cryptography when I was 13

funded or conducted by the Iranian government, that hacked a certificate reseller affiliated with U.S.-based Comodo.

On March 23, Comodo acknowledged the attack, saying that eight days earlier, hackers had obtained nine bogus certificates for the log-on sites of Microsoft's Hotmail, Google's Gmail, the Internet phone and chat service Skype and Yahoo Mail. A certificate for Mozilla's Firefox add-on site was also acquired.



CNET › News › InSecurity Complex › Fraudulent Google certificate points to Internet attack

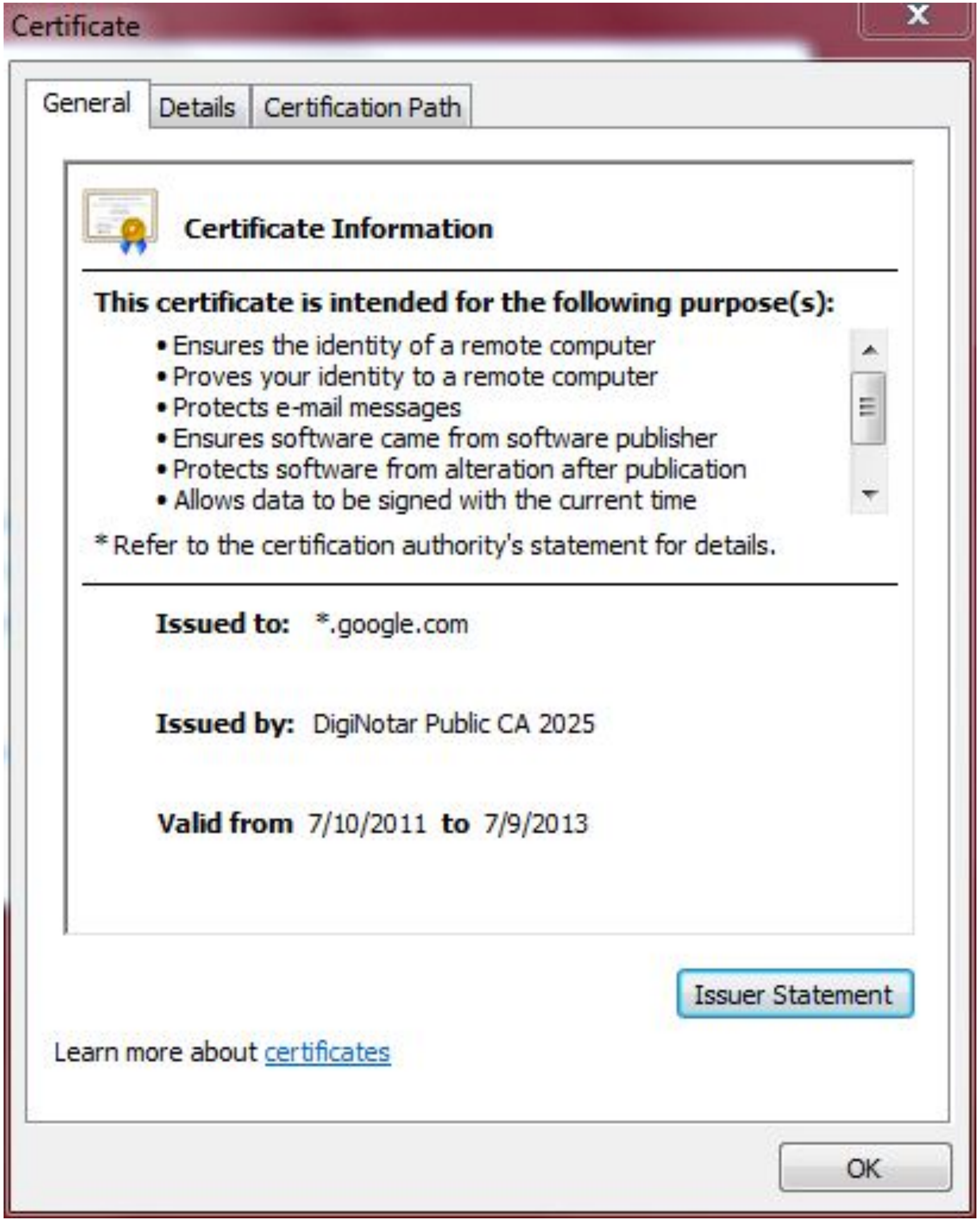
Fraudulent Google certificate points to Internet attack

Is Iran behind a fraudulent Google.com digital certificate? The situation is similar to one that happened in March in which spoofed certificates were traced back to Iran.

by Elinor Mills | August 29, 2011 1:22 PM PDT

A Dutch company appears to have issued a digital certificate for Google.com to someone other than Google, who may be using it to try to re-direct traffic of users based in Iran.

Yesterday, someone reported on a Google support site that when attempting to log in to Gmail the browser issued a warning for the digital certificate used as proof that the site is legitimate, according to this thread on a Google support forum site.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- Allows data to be signed with the current time

* Refer to the certification authority's statement for details.

Issued to: *.google.com

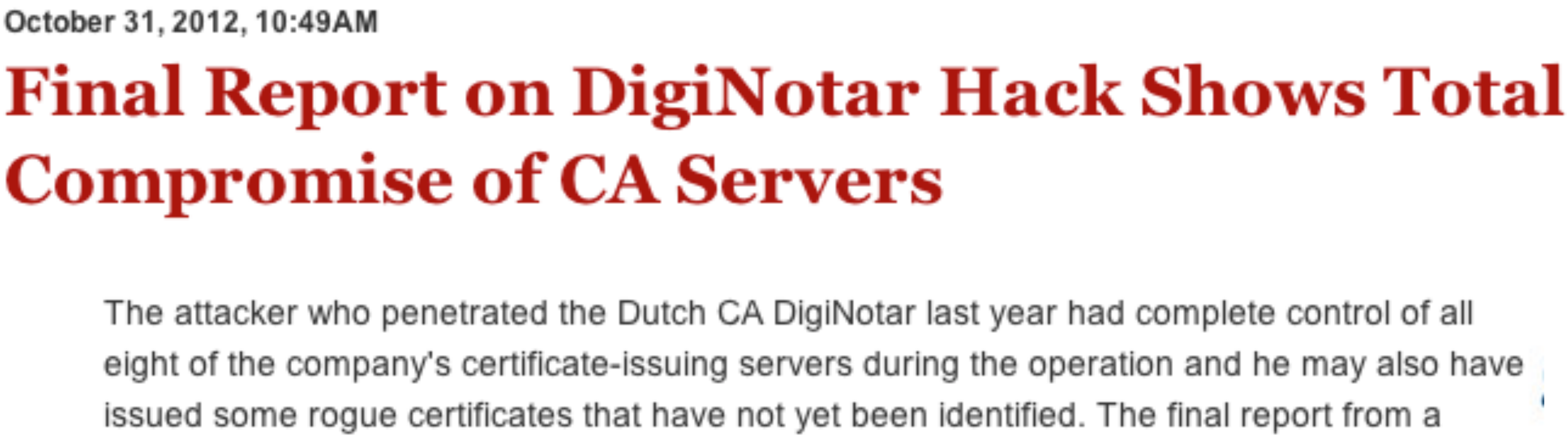
Issued by: DigiNotar Public CA 2025

Valid from 7/10/2011 **to** 7/9/2013

Learn more about certificates

This appears to be a fully valid cert using normal browser validation rules.

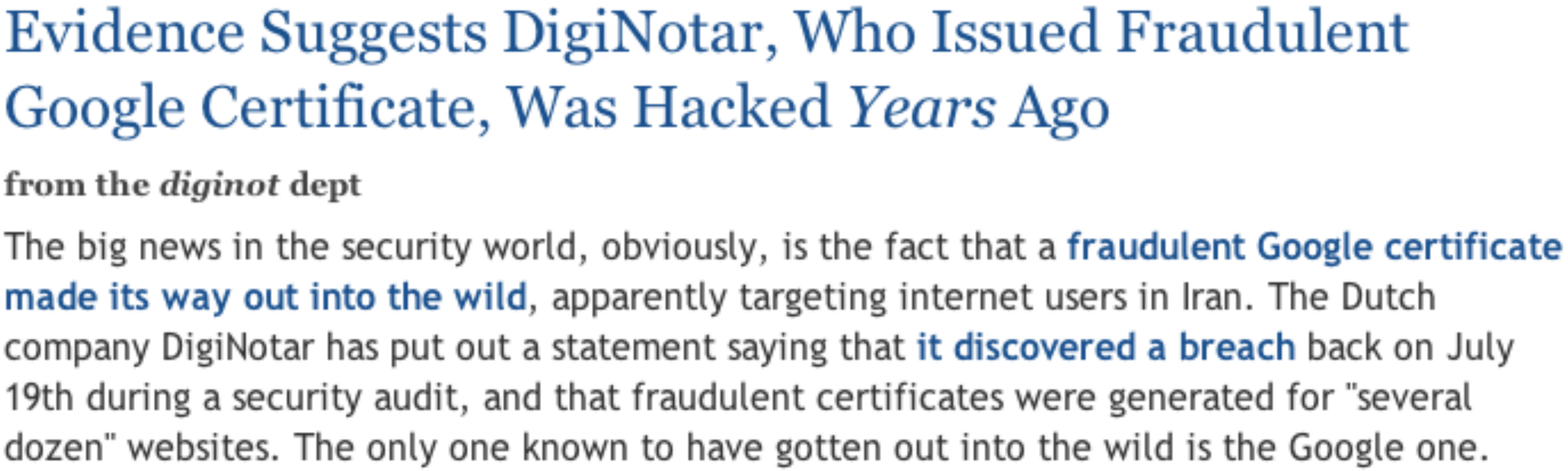
Only detected by Chrome due to its recent introduction of cert “pinning” – requiring that certs for certain domains **must** be signed by specific CAs rather than any generally trusted CA



October 31, 2012, 10:49AM

Final Report on DigiNotar Hack Shows Total Compromise of CA Servers

The attacker who penetrated the Dutch CA DigiNotar last year had complete control of all eight of the company's certificate-issuing servers during the operation and he may also have issued some rogue certificates that have not yet been identified. The final report from a



Evidence Suggests DigiNotar, Who Issued Fraudulent Google Certificate, Was Hacked *Years* Ago

from the *diginot* dept

The big news in the security world, obviously, is the fact that a **fraudulent Google certificate made its way out into the wild**, apparently targeting internet users in Iran. The Dutch company DigiNotar has put out a statement saying that **it discovered a breach** back on July 19th during a security audit, and that fraudulent certificates were generated for "several dozen" websites. The only one known to have gotten out into the wild is the Google one.

TLS/SSL Trust Issues

- “*Commercial certificate authorities protect you from anyone from whom they are unwilling to take money.*”
  - Matt Blaze, circa 2001
- So how many CAs do we have to worry about, anyway?
- Of course, it’s not just their greed that matters …
- … and it’s not just their diligence & security that matters …
  - “*A decade ago, I observed that commercial certificate authorities protect you from anyone from whom they are unwilling to take money. That turns out to be wrong; they don't even do that much.*” - Matt Blaze, circa 2010

BONUS SLIDES

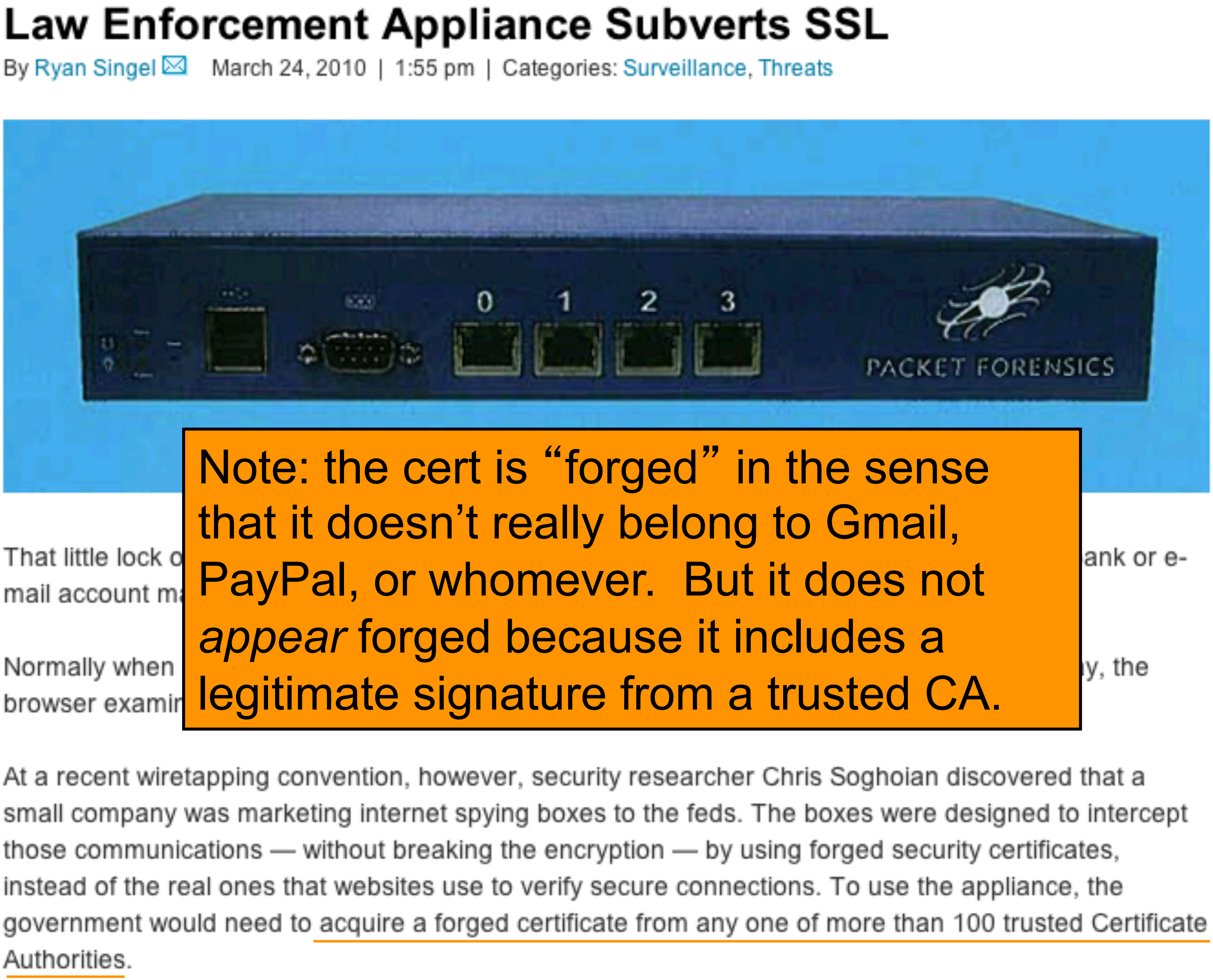
Law Enforcement Appliance Subverts SSL

By Ryan Singel ✉ March 24, 2010 | 1:55 pm | Categories: Surveillance, Threats

That little lock on your browser window indicating you are communicating securely with your bank or e-mail account may not always mean what you think its means.

Normally when a user visits a secure website, such as Bank of America, Gmail, PayPal or eBay, the browser examines the website's certificate to verify its authenticity.

At a recent wiretapping convention, however, security researcher Chris Soghoian discovered that a small company was marketing internet spying boxes to the feds. The boxes were designed to intercept those communications — without breaking the encryption — by using forged security certificates, instead of the real ones that websites use to verify secure connections. To use the appliance, the government would need to acquire a forged certificate from any one of more than 100 trusted Certificate Authorities.



Law Enforcement Appliance Subverts SSL

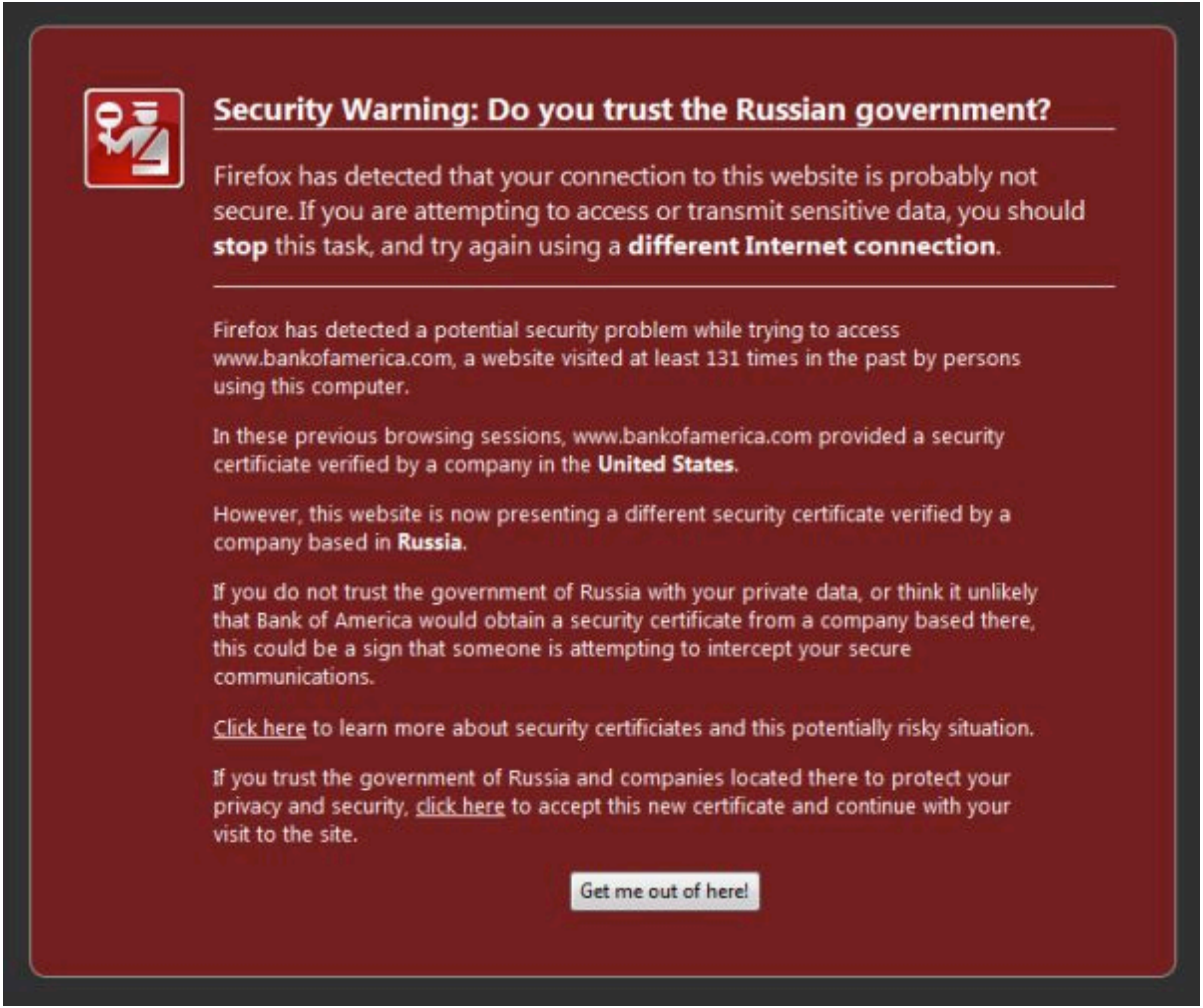
By Ryan Singel March 24, 2010 | 1:55 pm | Categories: Surveillance, Threats

That little lock o ank or e-
mail account m

Normally when y, the
browser examir

At a recent wiretapping convention, however, security researcher Chris Soghoian discovered that a small company was marketing internet spying boxes to the feds. The boxes were designed to intercept those communications — without breaking the encryption — by using forged security certificates, instead of the real ones that websites use to verify secure connections. To use the appliance, the government would need to acquire a forged certificate from any one of more than 100 trusted Certificate Authorities.

Note: the cert is “forged” in the sense that it doesn’t really belong to Gmail, PayPal, or whomever. But it does not *appear* forged because it includes a legitimate signature from a trusted CA.



Security Warning: Do you trust the Russian government?

Firefox has detected that your connection to this website is probably not secure. If you are attempting to access or transmit sensitive data, you should **stop** this task, and try again using a **different Internet connection**.

Firefox has detected a potential security problem while trying to access www.bankofamerica.com, a website visited at least 131 times in the past by persons using this computer.

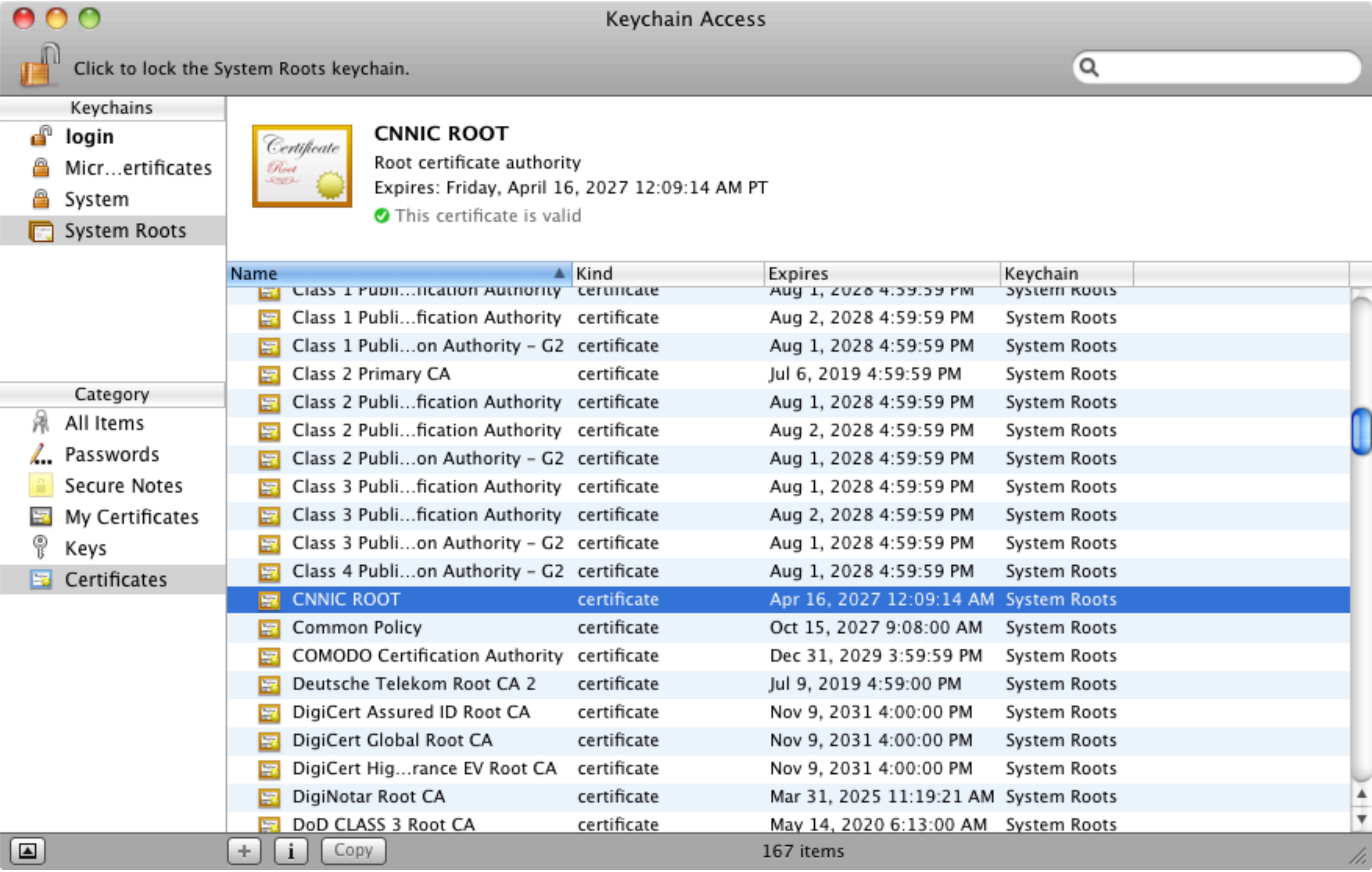
In these previous browsing sessions, www.bankofamerica.com provided a security certificiate verified by a company in the **United States**.

However, this website is now presenting a different security certificate verified by a company based in **Russia**.

If you do not trust the government of Russia with your private data, or think it unlikely that Bank of America would obtain a security certificate from a company based there, this could be a sign that someone is attempting to intercept your secure communications.

Click here to learn more about security certificiates and this potentially risky situation.

If you trust the government of Russia and companies located there to protect your privacy and security, click here to accept this new certificate and continue with your visit to the site.



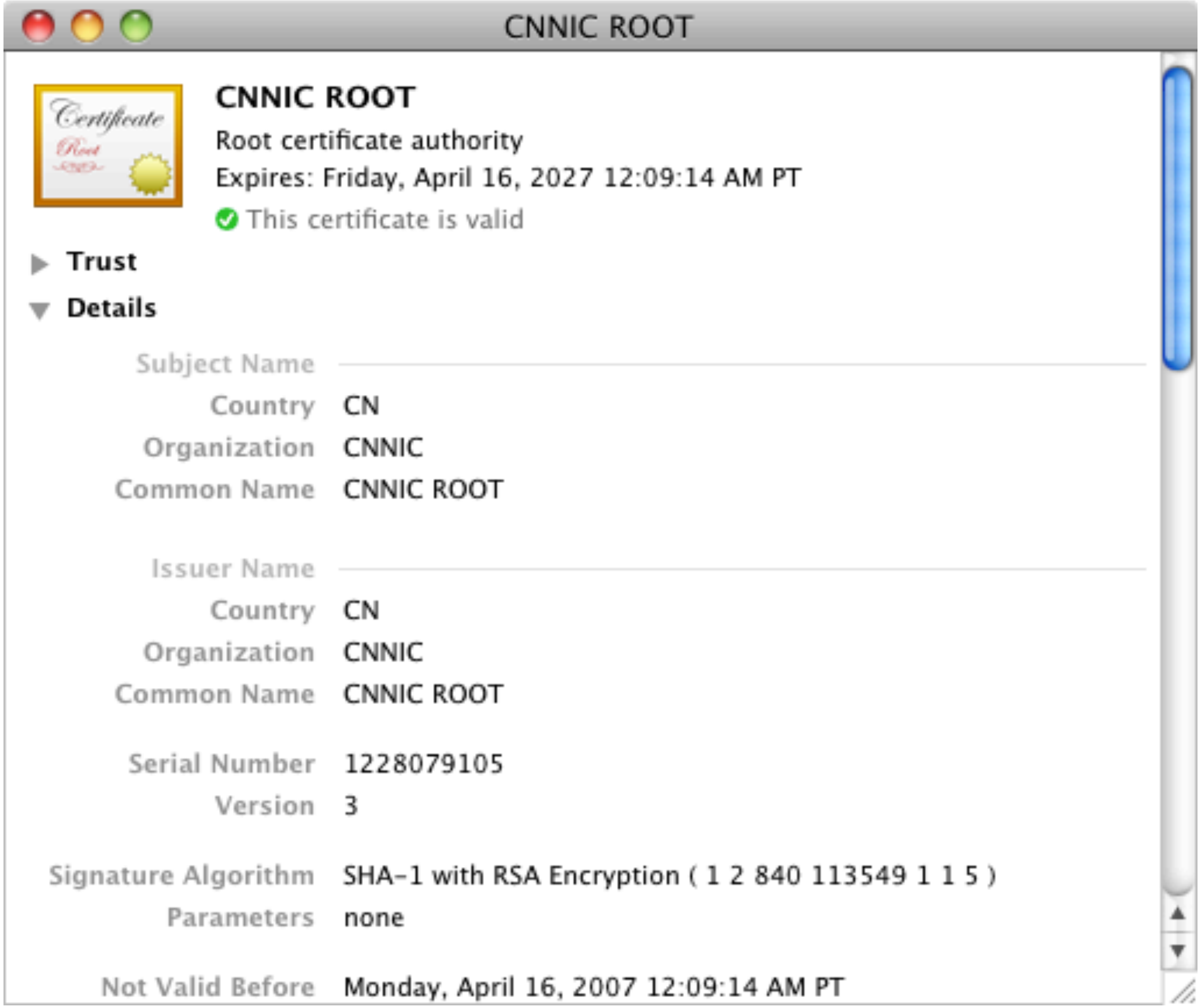
CNNIC ROOT

Root certificate authority

Expires: Friday, April 16, 2027 12:09:14 AM PT

✓ This certificate is valid

Name	Kind	Expires	Keychain
Class 1 Publi…fication Authority	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 1 Publi…fication Authority	certificate	Aug 2, 2028 4:59:59 PM	System Roots
Class 1 Publi…on Authority – G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 2 Primary CA	certificate	Jul 6, 2019 4:59:59 PM	System Roots
Class 2 Publi…fication Authority	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 2 Publi…fication Authority	certificate	Aug 2, 2028 4:59:59 PM	System Roots
Class 2 Publi…on Authority – G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 3 Publi…fication Authority	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 3 Publi…fication Authority	certificate	Aug 2, 2028 4:59:59 PM	System Roots
Class 3 Publi…on Authority – G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 4 Publi…on Authority – G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
CNNIC ROOT	certificate	Apr 16, 2027 12:09:14 AM	System Roots
Common Policy	certificate	Oct 15, 2027 9:08:00 AM	System Roots
COMODO Certification Authority	certificate	Dec 31, 2029 3:59:59 PM	System Roots
Deutsche Telekom Root CA 2	certificate	Jul 9, 2019 4:59:00 PM	System Roots
DigiCert Assured ID Root CA	certificate	Nov 9, 2031 4:00:00 PM	System Roots
DigiCert Global Root CA	certificate	Nov 9, 2031 4:00:00 PM	System Roots
DigiCert Hig…rance EV Root CA	certificate	Nov 9, 2031 4:00:00 PM	System Roots
DigiNotar Root CA	certificate	Mar 31, 2025 11:19:21 AM	System Roots
DoD CLASS 3 Root CA	certificate	May 14, 2020 6:13:00 AM	System Roots



CNNIC ROOT

Root certificate authority

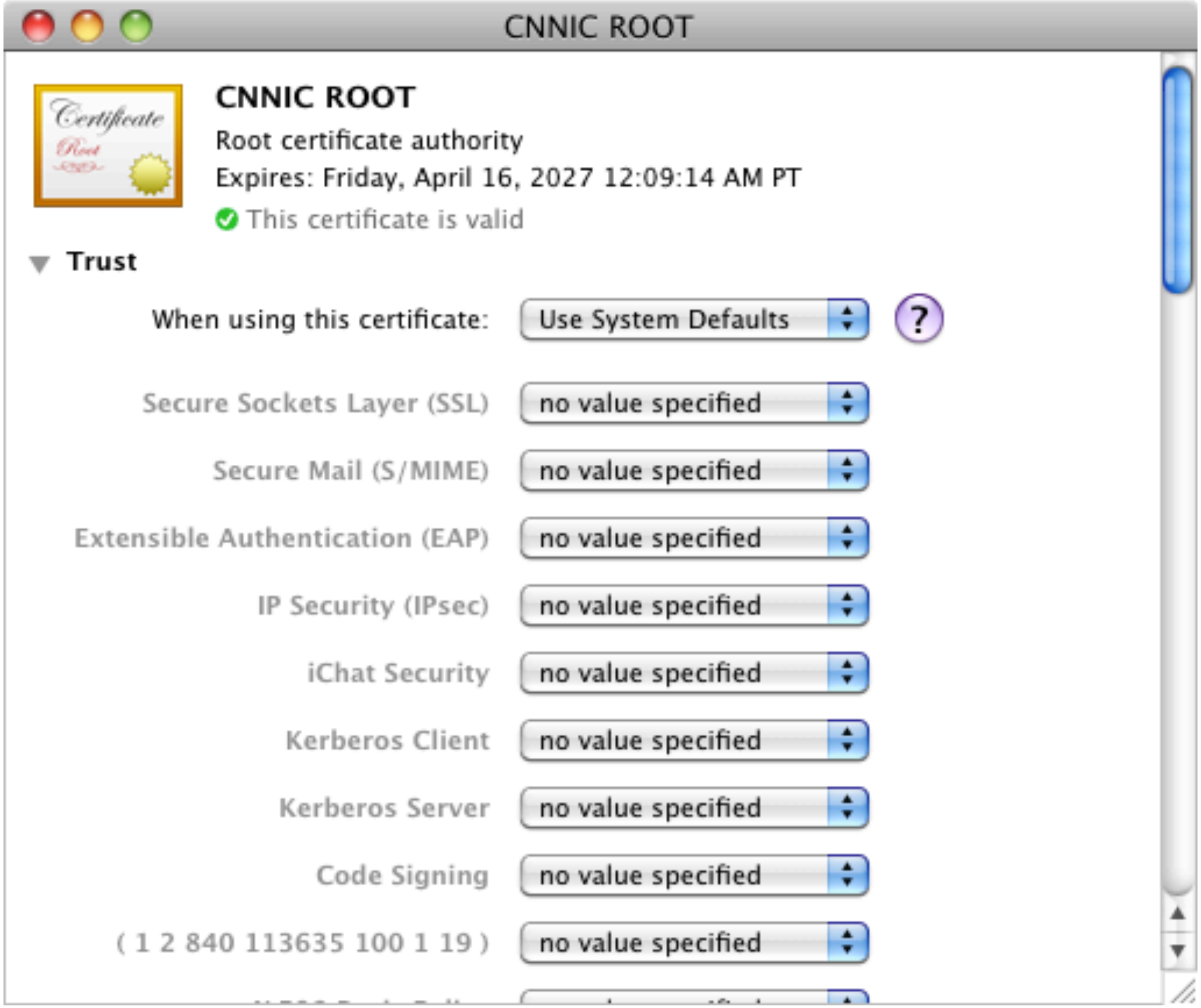
Expires: Friday, April 16, 2027 12:09:14 AM PT

✓ This certificate is valid

▶ Trust

▼ Details

Subject Name	
Country	CN
Organization	CNNIC
Common Name	CNNIC ROOT
Issuer Name	
Country	CN
Organization	CNNIC
Common Name	CNNIC ROOT
Serial Number	1228079105
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1 2 840 113549 1 1 5)
Parameters	none
Not Valid Before	Monday, April 16, 2007 12:09:14 AM PT



CNNIC ROOT

CNNIC ROOT

Root certificate authority

Expires: Friday, April 16, 2027 12:09:14 AM PT

✓ This certificate is valid

▼ **Trust**

When using this certificate: Use System Defaults

Secure Sockets Layer (SSL): no value specified

Secure Mail (S/MIME): no value specified

Extensible Authentication (EAP): no value specified

IP Security (IPsec): no value specified

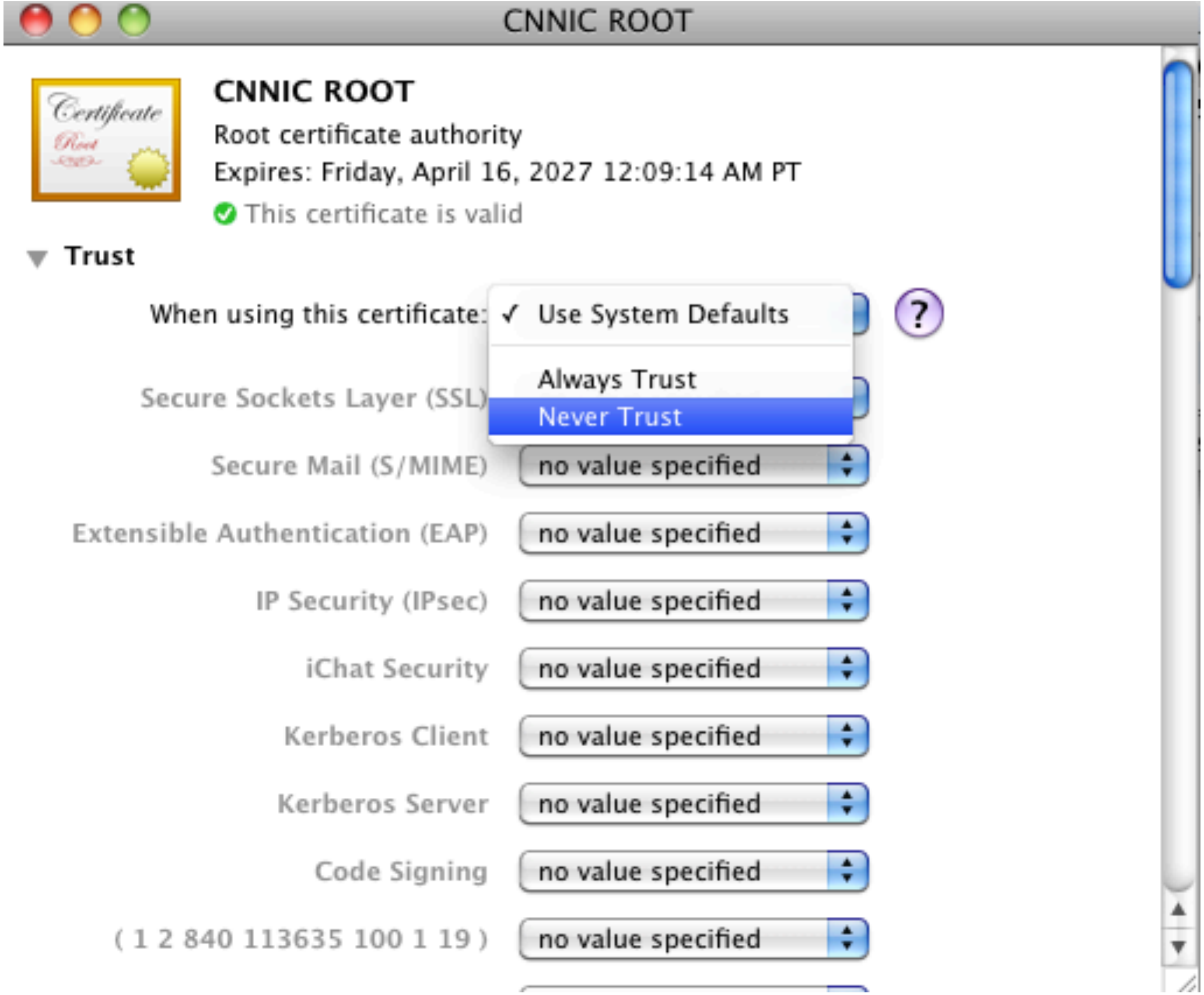
iChat Security: no value specified

Kerberos Client: no value specified

Kerberos Server: no value specified

Code Signing: no value specified

(1 2 840 113635 100 1 19): no value specified



CNNIC ROOT

CNNIC ROOT

Root certificate authority

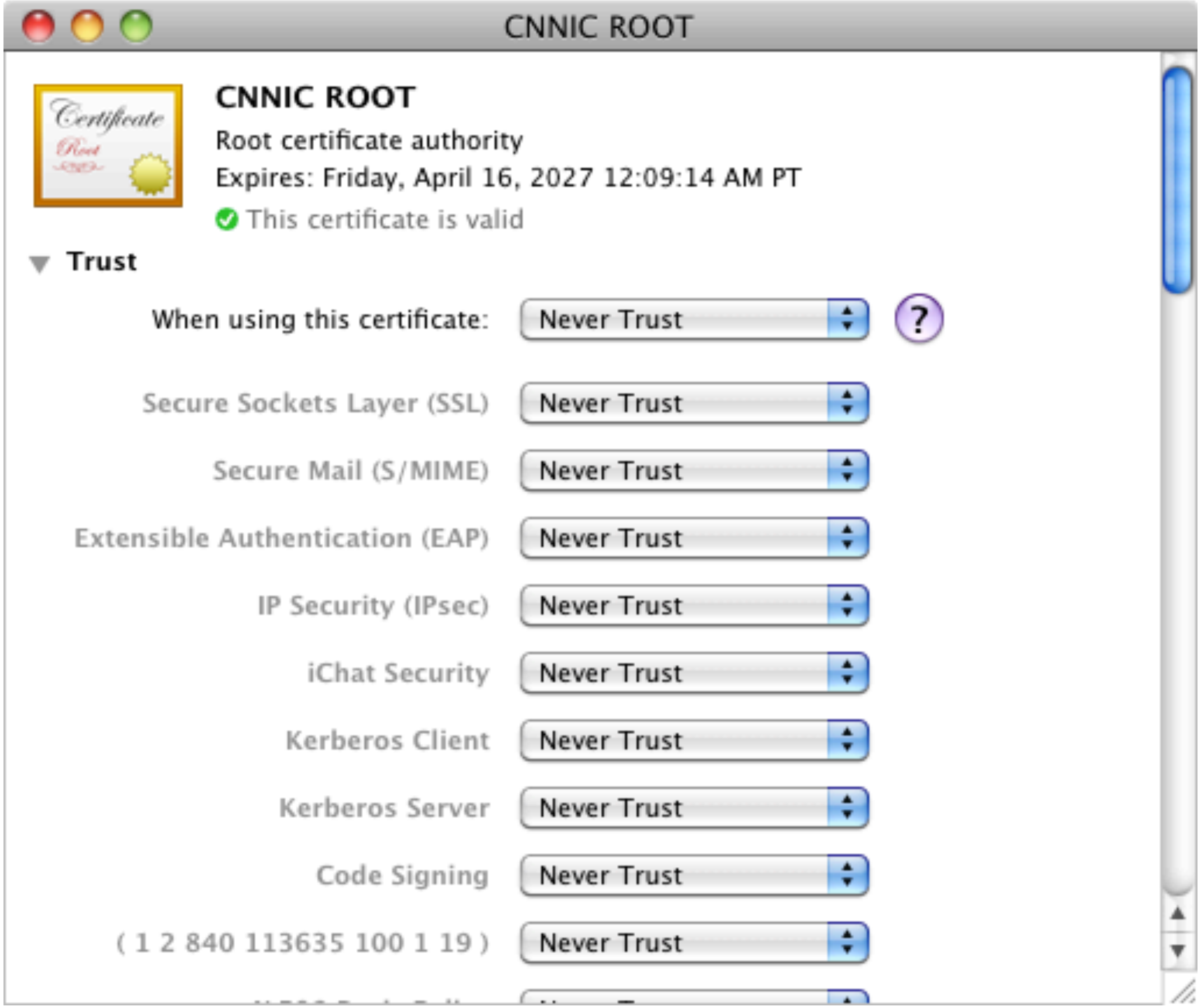
Expires: Friday, April 16, 2027 12:09:14 AM PT

✓ This certificate is valid

▼ Trust

When using this certificate: ✓ Use System Defaults

Secure Sockets Layer (SSL)	
Secure Mail (S/MIME)	no value specified
Extensible Authentication (EAP)	no value specified
IP Security (IPsec)	no value specified
iChat Security	no value specified
Kerberos Client	no value specified
Kerberos Server	no value specified
Code Signing	no value specified
(1 2 840 113635 100 1 19)	no value specified



CNNIC ROOT

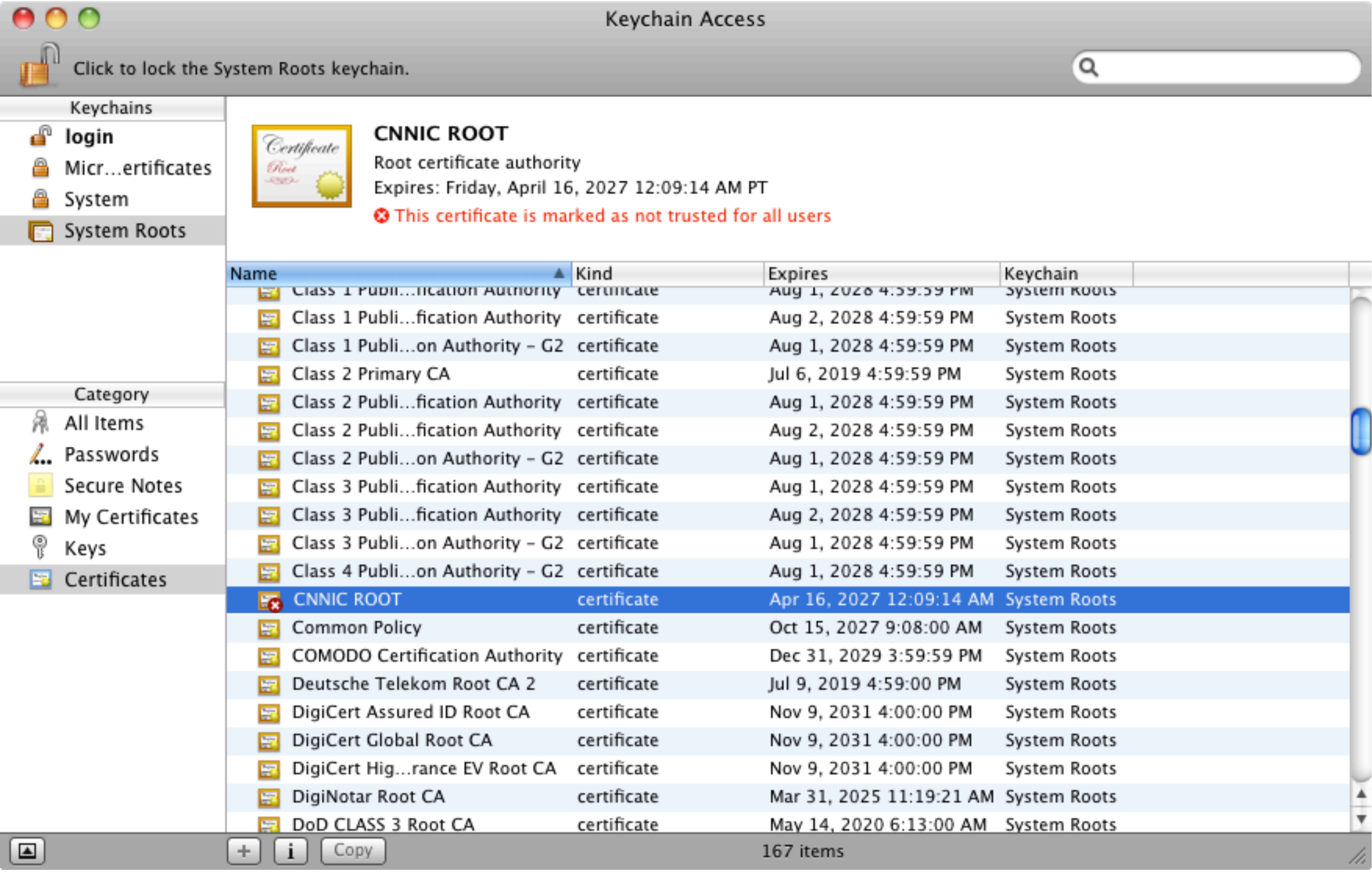
Root certificate authority

Expires: Friday, April 16, 2027 12:09:14 AM PT

✓ This certificate is valid

▼ Trust

When using this certificate:	Never Trust
Secure Sockets Layer (SSL)	Never Trust
Secure Mail (S/MIME)	Never Trust
Extensible Authentication (EAP)	Never Trust
IP Security (IPsec)	Never Trust
iChat Security	Never Trust
Kerberos Client	Never Trust
Kerberos Server	Never Trust
Code Signing	Never Trust
(1 2 840 113635 100 1 19)	Never Trust



CNNIC ROOT

Root certificate authority

Expires: Friday, April 16, 2027 12:09:14 AM PT

⊗ This certificate is marked as not trusted for all users

Name	Kind	Expires	Keychain
Class 1 Publi…fication Authority	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 1 Publi…fication Authority	certificate	Aug 2, 2028 4:59:59 PM	System Roots
Class 1 Publi…on Authority – G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 2 Primary CA	certificate	Jul 6, 2019 4:59:59 PM	System Roots
Class 2 Publi…fication Authority	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 2 Publi…fication Authority	certificate	Aug 2, 2028 4:59:59 PM	System Roots
Class 2 Publi…on Authority – G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 3 Publi…fication Authority	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 3 Publi…fication Authority	certificate	Aug 2, 2028 4:59:59 PM	System Roots
Class 3 Publi…on Authority – G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 4 Publi…on Authority – G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
CNNIC ROOT	certificate	Apr 16, 2027 12:09:14 AM	System Roots
Common Policy	certificate	Oct 15, 2027 9:08:00 AM	System Roots
COMODO Certification Authority	certificate	Dec 31, 2029 3:59:59 PM	System Roots
Deutsche Telekom Root CA 2	certificate	Jul 9, 2019 4:59:00 PM	System Roots
DigiCert Assured ID Root CA	certificate	Nov 9, 2031 4:00:00 PM	System Roots
DigiCert Global Root CA	certificate	Nov 9, 2031 4:00:00 PM	System Roots
DigiCert Hig…rance EV Root CA	certificate	Nov 9, 2031 4:00:00 PM	System Roots
DigiNotar Root CA	certificate	Mar 31, 2025 11:19:21 AM	System Roots
DoD CLASS 3 Root CA	certificate	May 14, 2020 6:13:00 AM	System Roots

Securing DNS Lookups

- Topic for next time:
  How can we ensure that when clients look up names with DNS, they can trust the answers they receive?

Think about these before Friday

- **Problem 1.** We have a database $D = \{d_1, d_2, \ldots, d_n\}$ of strings. A client anywhere in the world wants to be able to query it with a string s and determine whether $s \in D$; if the answer is "yes", client should get a proof of this fact. We want to store copies of D on untrusted mirror servers. How do we do it securely?
- **Problem 2.** Same as Problem 1, but now if the answer is "no", we also want a proof of that fact. How do we do it securely?