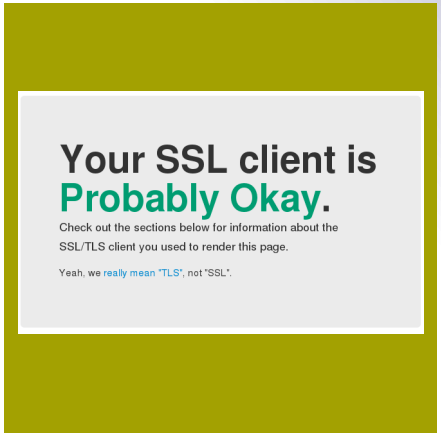


Certificates | SSL/TLS | PGP

INGI2347: COMPUTER SYSTEM SECURITY (Spring 2016)

Marco Canini

UCL
Université
catholique
de Louvain

Lecture slides adapted from Upenn CSE331 by Steve Zdancewic and UC Berkeley CS161 by Vern Paxson
Reproduced with permission

Certificates

Certificates

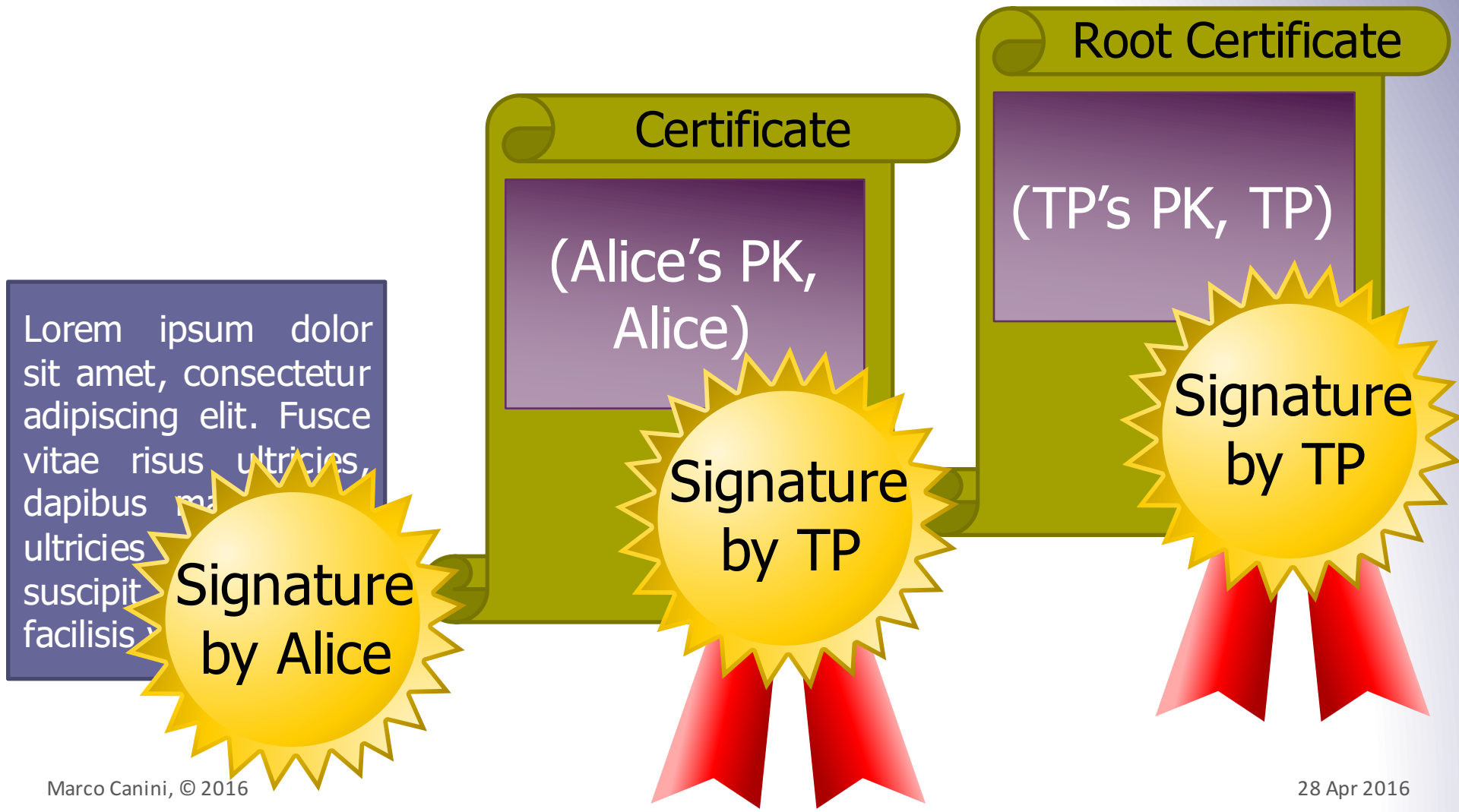
- Cert = signed statement about someone's public key
  - Note that a cert does not say anything about the identity of who **gives** you the cert
  - It simply states a given public key K_{Bob} belongs to Bob …
    - … and backs up this statement with a digital signature made using a different public/private key pair, say from Alice
- 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 Alice's public key …
  - … and you trust Alice to use prudence when she signs other people's keys, such as Bob's

What is the goal?

Certificate's goal is to **link** a public key (PK) with its owner

- The pair (PK, owner) is signed by a trusted party (TP)
- The TP is named **Certification Authority** (CA)
- To check the signature, the CA's PK is needed
  - **Root certificate**: the pair (CA's PK, CA) is self-signed
  - The authenticity of the root certificate is fundamental (included in browsers)

Illustration



X.509 Certificates

X.509

- Standard from International Telecommunication Union (ITU), 1988
- Also IETF RFC-2459 (and updates)

Three required fields:

- TBS Certificate (TBS = "To Be Signed")
  - The useful payload of the certificate
- CA signature algorithm
  - Identifier for the crypto algorithm used by the CA to sign this certificate
- CA signature value
  - Signature of the certificate by the CA

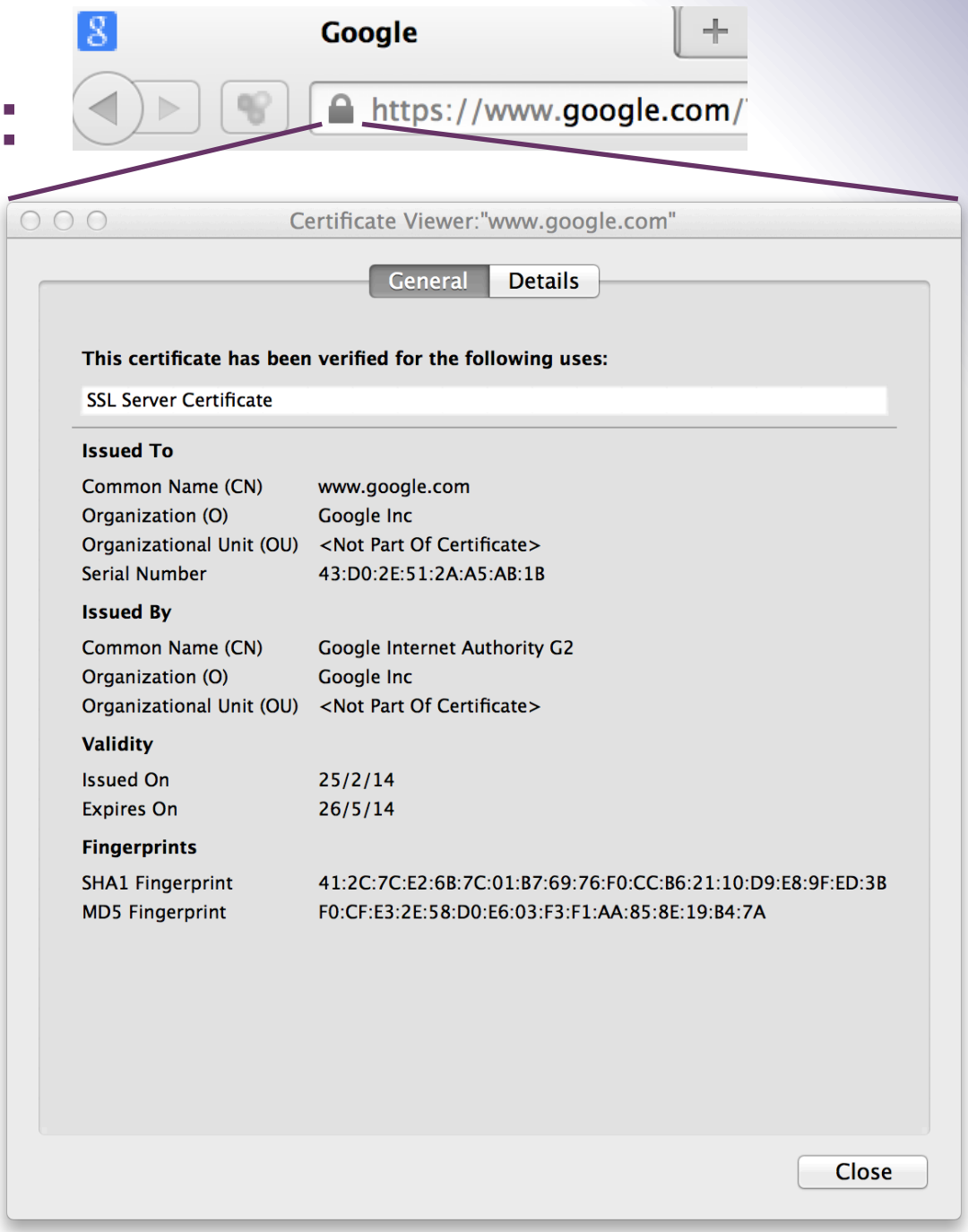
X.509 TBS

- Serial number
  - Unique number assigned by the CA to the certificate
- Issuer field
  - Identifies the entity who has signed and issued the certificate
- Subject
  - Identifies the entity associated with the public key
    - O: organization, C: country, OU: organization unit, CN: common name, ST: state, L: city, etc. no IP address

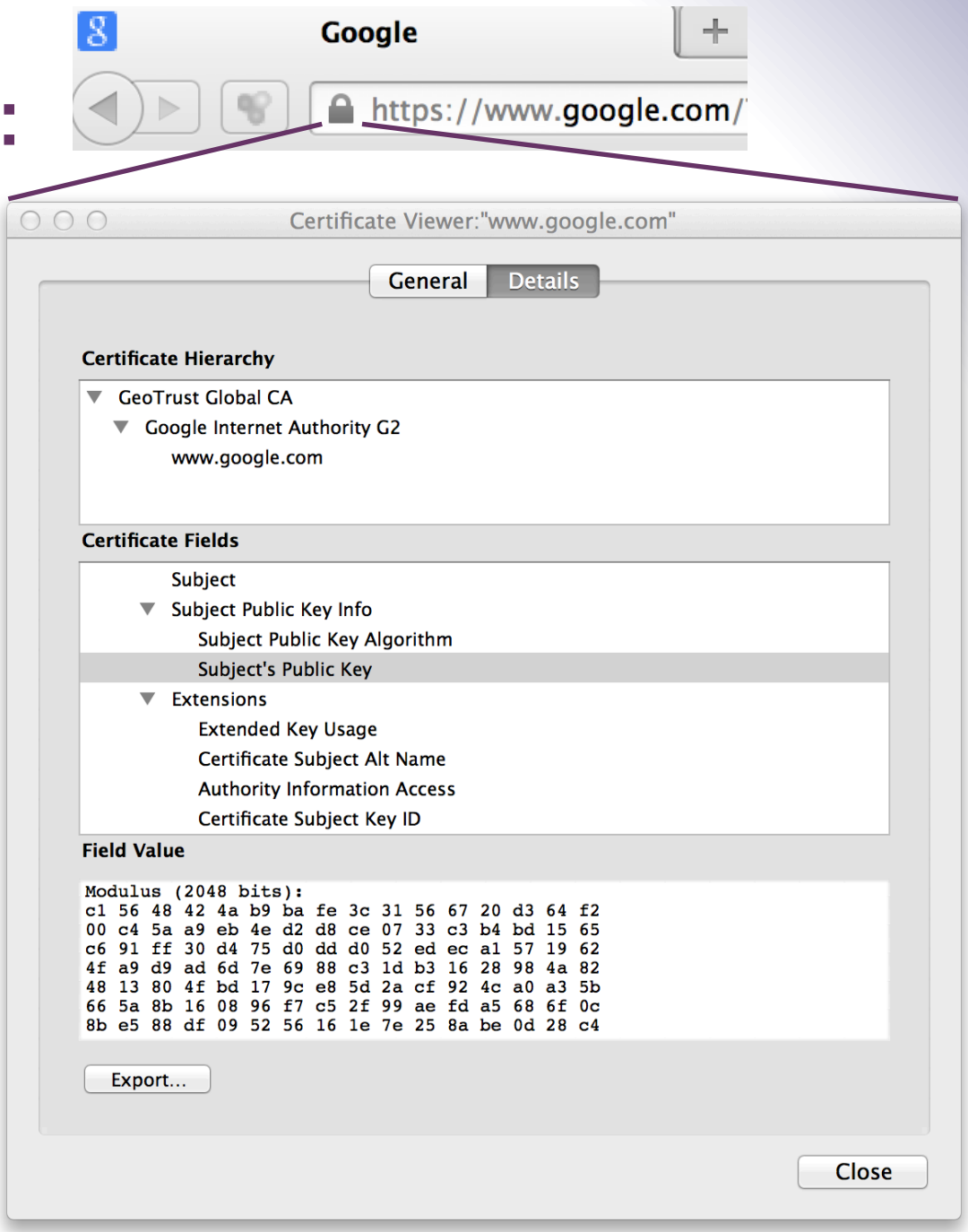
X.509 TBS (Continued)

- Validity
  - Not before
  - Not after
- Subject Public Key Info
  - Public key
  - Identifies the algorithm with which the key is used
    - e.g., RSA, DSA, or DH
- Etc.

Example:


Google
https://www.google.com/
Certificate Viewer:"www.google.com"
General
Details
This certificate has been verified for the following uses:
SSL Server Certificate
Issued To
Common Name (CN) www.google.com
Organization (O) Google Inc
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 43:D0:2E:51:2A:A5:AB:1B
Issued By
Common Name (CN) Google Internet Authority G2
Organization (O) Google Inc
Organizational Unit (OU) <Not Part Of Certificate>
Validity
Issued On 25/2/14
Expires On 26/5/14
Fingerprints
SHA1 Fingerprint 41:2C:7C:E2:6B:7C:01:B7:69:76:F0:CC:B6:21:10:D9:E8:9F:ED:3B
MD5 Fingerprint F0:CF:E3:2E:58:D0:E6:03:F3:F1:AA:85:8E:19:B4:7A
Close

Example:


Google
https://www.google.com/
Certificate Viewer:"www.google.com"
General
Details
Certificate Hierarchy
GeoTrust Global CA
Google Internet Authority G2
www.google.com
Certificate Fields
Subject
Subject Public Key Info
Subject Public Key Algorithm
Subject's Public Key
Extensions
Extended Key Usage
Certificate Subject Alt Name
Authority Information Access
Certificate Subject Key ID
Field Value
Modulus (2048 bits):
c1 56 48 42 4a b9 ba fe 3c 31 56 67 20 d3 64 f2
00 c4 5a a9 eb 4e d2 d8 ce 07 33 c3 b4 bd 15 65
c6 91 ff 30 d4 75 d0 dd d0 52 ed ec a1 57 19 62
4f a9 d9 ad 6d 7e 69 88 c3 1d b3 16 28 98 4a 82
48 13 80 4f bd 17 9c e8 5d 2a cf 92 4c a0 a3 5b
66 5a 8b 16 08 96 f7 c5 2f 99 ae fd a5 68 6f 0c
8b e5 88 df 09 52 56 16 1e 7e 25 8a be 0d 28 c4
Export...
Close

+

Working with Certificates

Certificate Authorities

- Issuers of certificates found on web servers

CA	Count [%]
GeoTrust	25.19
GoDaddy.com	13.65
Verisign	13.09
Thawte	9.79
Comodo Limited	7.12
Unknown	2.40
DigiCert	2.39
Network Solutions LLC	2.09
Comodo CA Limited	1.77
GlobalSign	1.64

NOTE: GeoTrust, Verisign, and Thawte are the same group

Source: https://secure1.securityspace.com/es/s_survey/data/man.201002/casurvey.html (Feb 2010)

How to obtain a certificate

- Applicant registers with a CA
- CA (physically) authenticates the applicant
- CA asks applicant to generate public/private keys
- CA creates a certificate with the applicant's identity, PK, expiration date, etc., and the CA's signature
- CA provides a copy of its own PK to applicant

Registration Authority (RA)

- CA can delegate the registration of an applicant to the **registration authority** (RA)
- RA does not have CA's private key
- CA trusts the RA to authenticate the applicants
- After applicant is authenticated, applicant generates a pair of keys and sends the public key to the CA to create the certificate
- Technically RA sends a signed Certificate Signing Request (CSR) to the CA

CSR in practice

- Generate a 1024-RSA key-pair
  - openssl genrsa 1024 > mykey.key
- Generate a CSR
  - openssl req -new -key mykey.key -out myreq.csr
- Verify a CSR
  - openssl req [-text] [-noout] -verify -in myreq.csr
- Online checkers
  - http://support.ecenica.com/ssl-certificates/csr-checker/
  - https://ssl-tools.verisign.com/checker/

Certificate without CA

- Everyone can self-sign a certificate
- Distribute the certificate through an authenticated channel
- Makes sense in enterprise intranet
- Not really for public-facing services
- Rather get a free certificate…

Certificates in practice

- Generate a certificate
  - openssl x509 -req -in myreq.csr -signkey mykey.key -out mycert.crt
- View a certificate
  - openssl x509 -text -in mycert.crt
- Verify a certificate
  - openssl verify mycert.crt

Key escrowing

Keys are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys

Example:

- A company can provide two key pairs and certificates to each of is employees
  - One for signing | One for encrypting
- CA escrows a copy of the private encryption key
- Only employees can sign, but company can decrypt

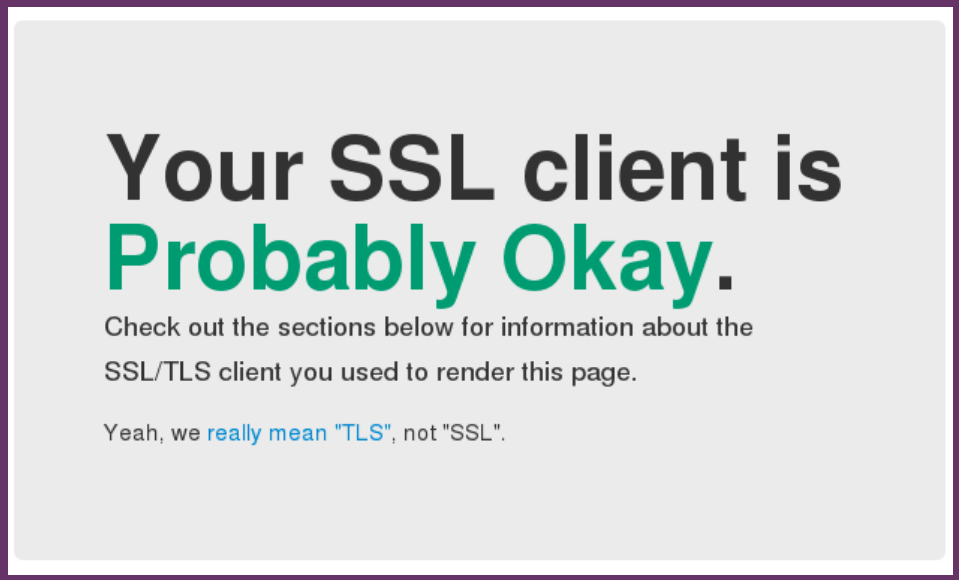
Verifying a certificate

1. Verify the **certification path**
   - Performed locally
   - Delegated to a server: SCVP (Server-based Certificate Validation Protocol)
2. Verify the **validity period**
3. Verify that the certificate is **not revoked**
   - Performed locally: CRL (certificate revocation lists)
   - Delegated to a server: OCSP (Online Certificate Status Protocol)
   - Supported by all major browsers ... but not implemented consistently
     - What is the risk?

Issues w/ compromised certificates

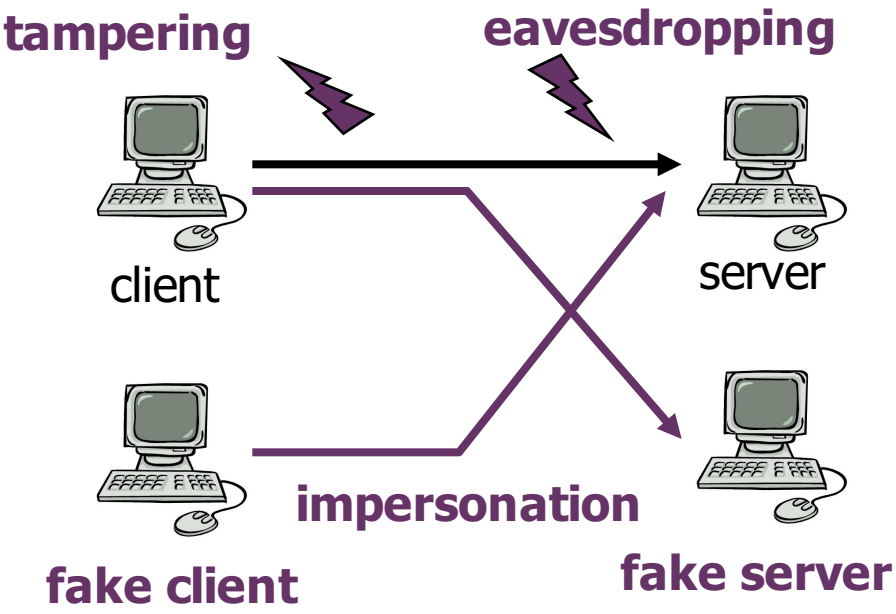
- A certificate might become compromised
  - For example, see Heartbleed bug: http://heartbleed.com/
- Even if the compromised certificate is revoked and replaced with a new one, a secure site could still be vulnerable
- Problem: browsers support revocation checking in different, inconsistent ways
  - e.g., when OCSP is not available only IE and Opera will check a URL pointing to a CRL in individual certificates
  - By default OCSP is disabled in Chrome (in part due to privacy concerns)
    - Chrome uses its own updating mechanism and is intended for most important certificates only
- Finally, CRLs are retrieved less frequently by browsers

Read more: http://news.netcraft.com/archives/2014/04/24/certificate-revocation-why-browsers-remain-affected-by-heartbleed.html


Your SSL client is
Probably Okay.
Check out the sections below for information about the
SSL/TLS client you used to render this page.
Yeah, we really mean "TLS", not "SSL".

SSL / TLS

SSL Primer



- Authentication of server based on public key
- Trusted third party: certification authority (CA)

Secure Sockets Layer (SSL)

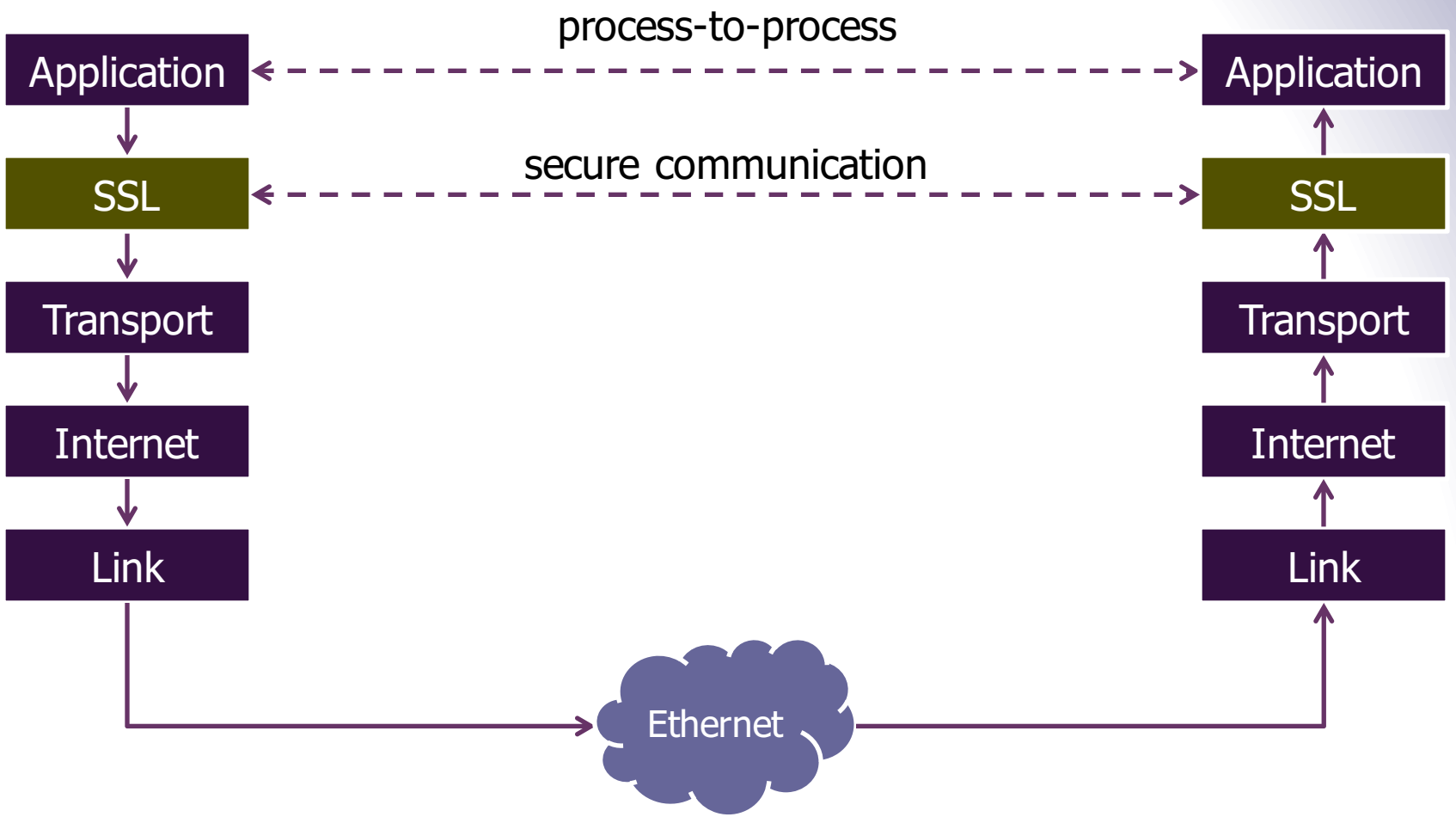
- Most widely deployed security protocol in the world
- SSL was developed by Netscape to offer secure access to web servers (HTTPS)
- History
  - SSL v1.0 never publicly released
  - SSL v2.0 released in 1994 (flawed)
  - SSL v3.0 released in 1996, leads to TLS 1.0 in 1999

Transport Layer Security (TLS)

- TLS is an IETF standard based on SSL v3.0
  - Slight modifications compared to SSL v3.0
  - TLS v1.0 and SSL v3.0 do not interoperate
  - TLS v1.0 sometimes called SSL v3.1
  - TLS v1.0 defined in RFC 2246
  - TLS v1.2 updated in RFC 5246 (August 2008)

- Current version (March 2011)
  - TLS v1.2 (prohibits SSL v2.0)
  - RFC 6176

SSL in the layered model



Approaches

Create a new protocol from an existing protocol

- Examples:
  HTTP (80) / HTTPS (443), FTP (21) / FTPS (990), SMTP (25) / SMTPS (995), POP3 (110) / POP3S (995), IMAP (143) / IMAPS (993)
- Disadvantage: only clients supporting TLS can connect
- Advantage: we are sure that communications are secure

Extend a protocol to negotiate SSL/TLS

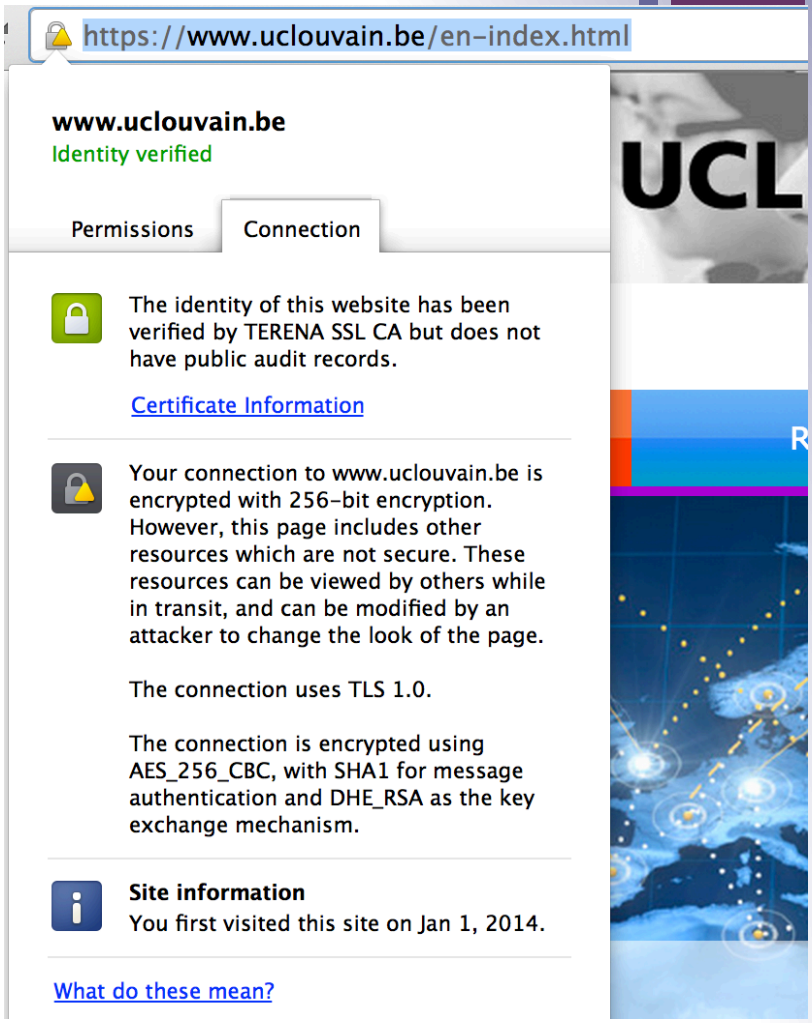
- Examples: (E)SMTP, POP3, IMAP, with the help of the STARTTLS command the client can ask to use TLS
- Advantage: the client is not required to support TLS to use the service

OpenSSL

```
bash$ openssl s_client -connect www.uclouvain.be:443
CONNECTED(00000003)
[...]
Certificate chain
 0 s:/C=BE/L=Louvain-la-Neuve/O=Universit\xC3\xA9 Catholique de Louvain/OU=Portail UCL/CN=www.uclouvain.be
   i:/C=NL/O=TERENA/CN=TERENA SSL CA
[...]
Server certificate
-----BEGIN CERTIFICATE-----
MIIErDCCA5SgAwIBAgIRAOjy08jirG7k+6k8Ln7bZxQwDQYJKoZIhvcNAQEFBQAw
[...]
-----END CERTIFICATE-----
[...]
SSL handshake has read 5258 bytes and written 328 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 2048 bit
[...]
SSL-Session:
    Protocol  : TLSv1
    Cipher    : DHE-RSA-AES256-SHA
    Session-ID: C0FE449DC7345355B4119A095C27DA72691326880FE52271FB2CB3B0DCF29FE0
    Master-Key: 7A8DE9425505930A2F11AFC241F9236ABA61DAC7BFC0A9709C6F887D819BAA42C5F1B7A9E01CC26945A[...]
```

Example: HTTPS

- TLS guarantees data confidentiality and authenticity (server, possibly client)
  - The server must have a certificate
  - The client can have one
    - e.g., e-banking, Belgian SPF Finances



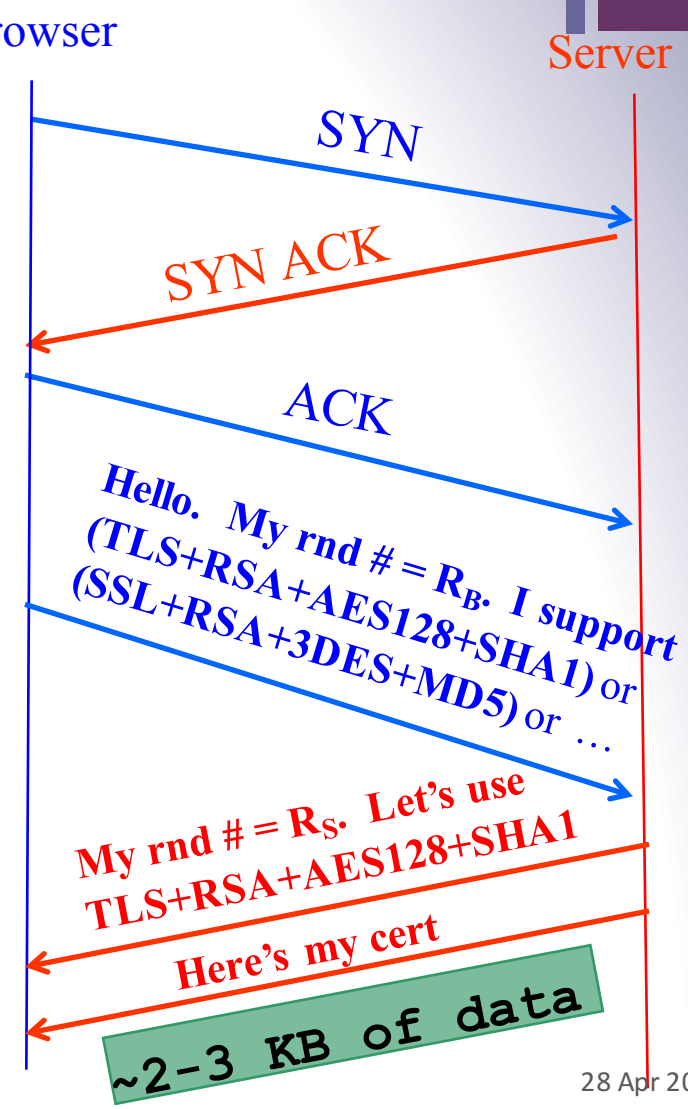
Example: Mail

- ESMTP (sending mail), POP3 (mailbox access), IMAP (better mailbox access)
  - TLS is implemented as a protocol extension
  - The use of TLS is optional (needs to be configured)
- By default these protocols send cleartext passwords
- TLS protects passwords and email contents

TLS Protocol

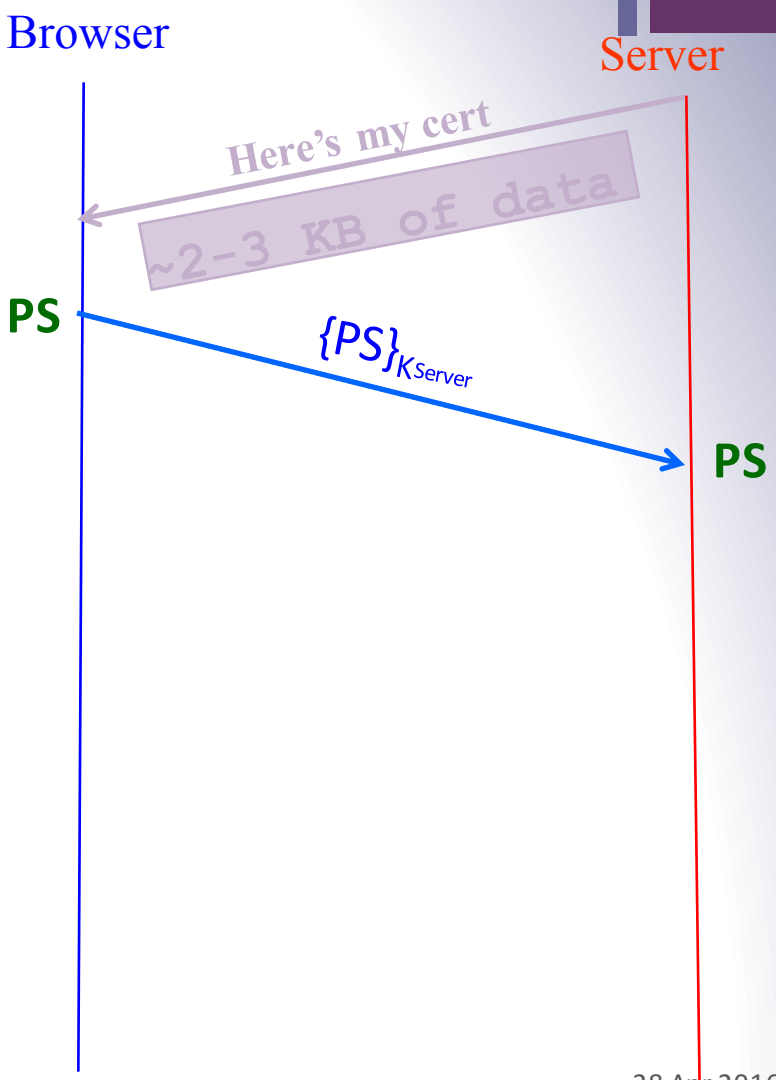
HTTPS Connection (SSL / TLS)

- Browser (client) connects via TCP to **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***



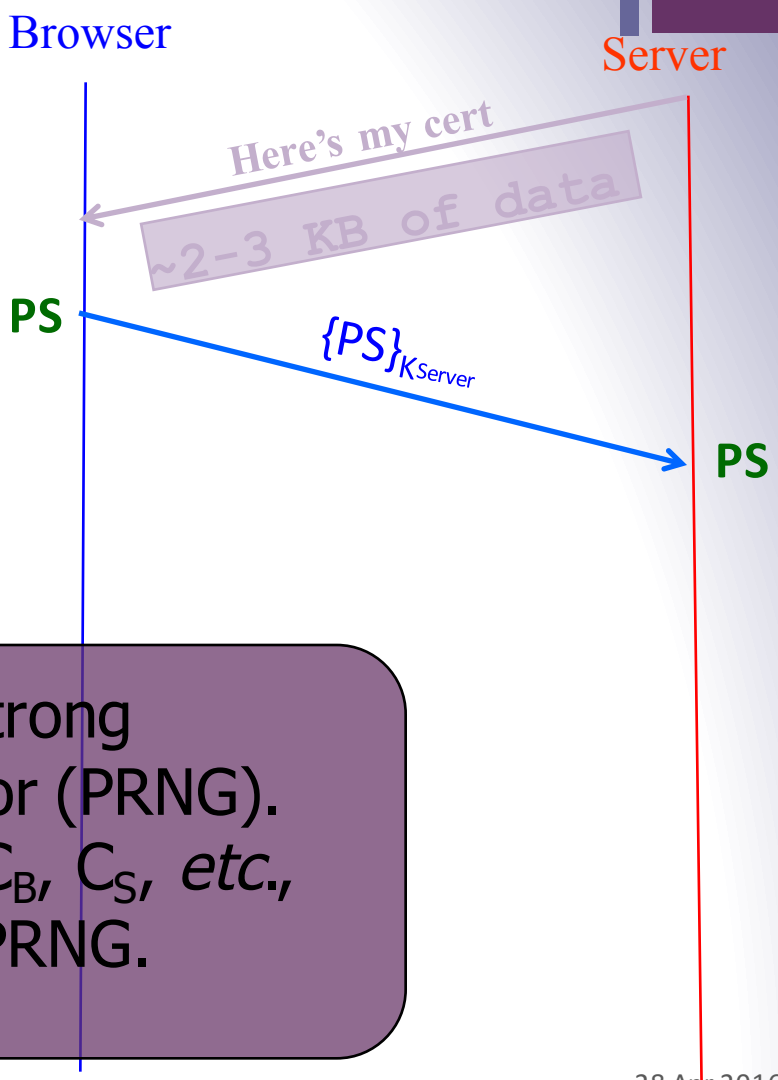
HTTPS Connection (SSL / TLS), con't

- For RSA, browser constructs long (368 bits) "Premaster Secret" **PS**
- Browser sends PS encrypted using server's public RSA key K_{Server}
- 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), con't

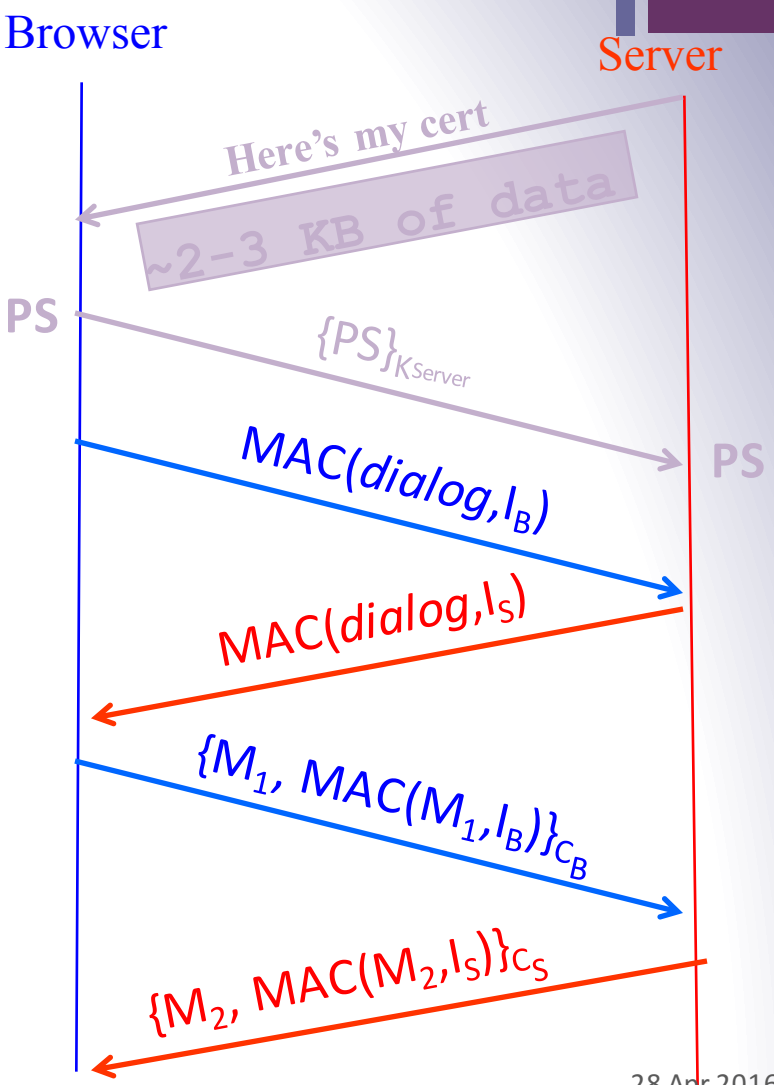
- For RSA, browser constructs long (368 bits) "Premaster Secret" **PS**
- Browser sends PS encrypted using server's public RSA key K_{Server}
- Using PS, R_B, and R_S, browser & server derive symm. *cipher keys* (C_B, C_S) & MAC *integrity keys* (I_B, I_S)
  - One pair to use in each direction



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

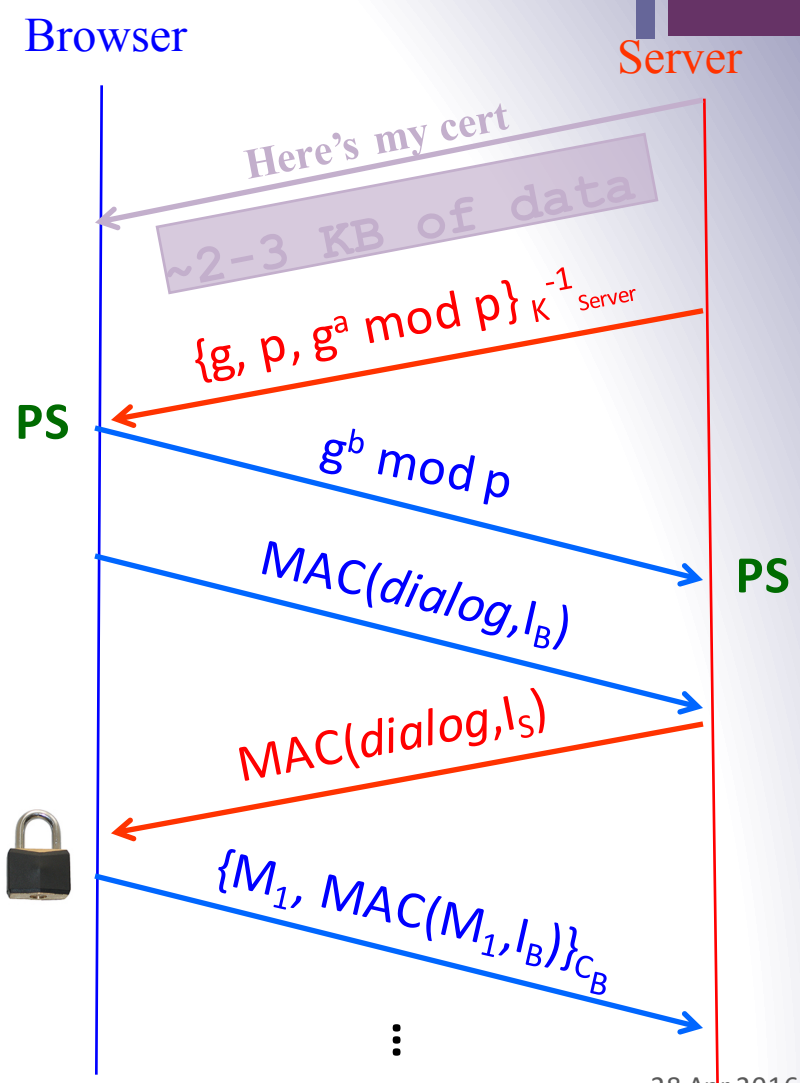
HTTPS Connection (SSL / TLS), con't

- For RSA, browser constructs long (368 bits) "Premaster Secret" **PS**
- Browser sends PS encrypted using server's public RSA key K_{Server}
- 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
  - Messages also numbered to thwart replay attacks



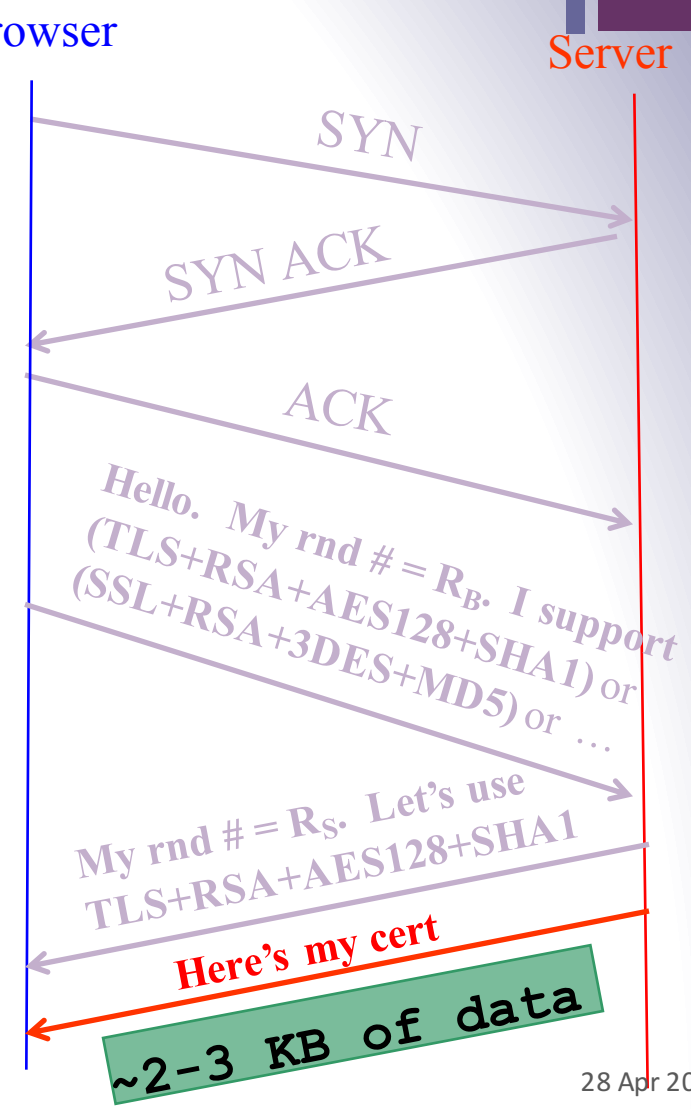
Alternative: Key Exchange via Diffie-Hellman

- For Diffie-Hellman, server generates random a, sends public params and g^a mod p
  - Signed with server's public 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 server'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***



+

Validating Certificates

Inside the Server's Certificate

- **Domain name** associated w/ cert
  - e.g., amazon.com
- Amazon's **public key** (e.g., 2048 bits for RSA)
- A bunch of auxiliary info (physical address, type of cert, expiration time)
- Name of certificate's **issuer** (e.g., Verisign)
- Optional URL to *revocation center* to check for revoked certs
- A public-key **signature** of a hash (SHA-1) of all this
  - Constructed using the *issuer's* private key
  - Call this signature **S**

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 - **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, con't

- 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, con't

- Browser retrieves cert belonging to the **issuer**
  - These are hardwired into the browser - **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.

Get me out of here!

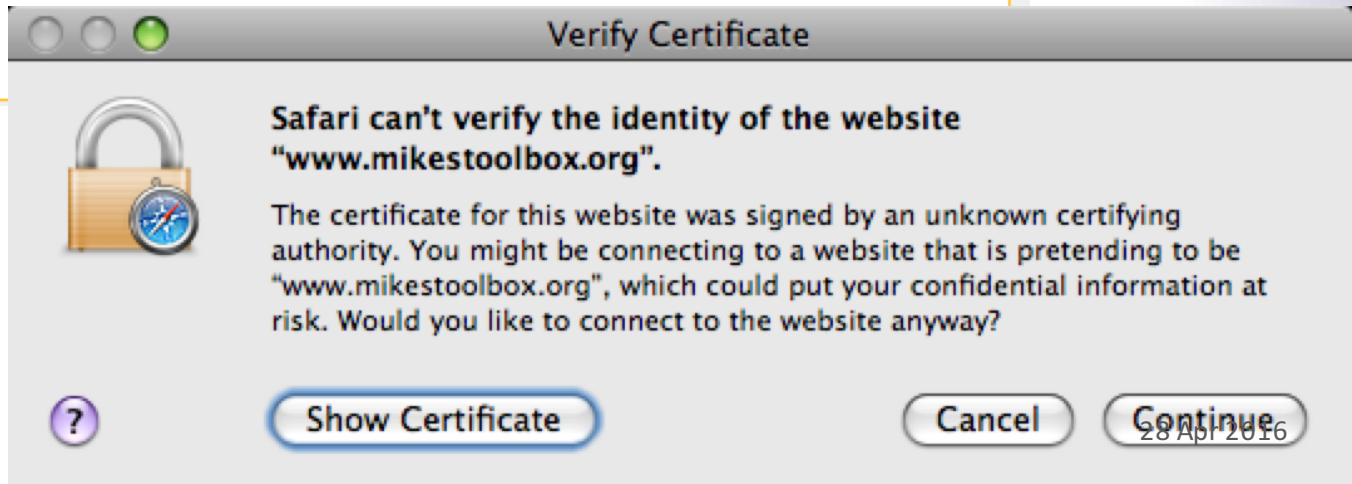
Technical Details

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



Validating Amazon's Identity, con't

- Browser retrieves cert belonging to the **issuer**
  - These are hardwired into the browser - **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
  - Note, 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
  - Attacker can read everything, modify, impersonate

+

SSL / TLS Limitations

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
    - 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)

Welcome to StartSSL™ PKI

StartSSL™ is the trade mark of the **StartCom® Certification Authority** - a leader of the digital certification industry. We provide you with everything from **free** low-assurance **SSL** certificates up to the most advanced PKI and security solutions for your business and personal use.

StartSSL™ Free (Class 1)

128/256-bit Encryption, **1 Year** Validity
Legitimate SSL/TLS + S.MIME Certificates
No Charge, Unlimited + 100 % Free

StartSSL™ Verified (Class 2)

128/256-bit Encryption, **2 Years** Validity
Legitimate SSL/TLS + S/MIME + Object Code
Wild Cards, Multiple Domain Names (UCC)
Unlimited Certificates - US$ 59.90

StartSSL™ Extended Validation

128/256-bit Encryption, **2 Years** Validity
Highest Level Third Party Assurance
Green Extended Trust Indicator
Multiple Domain Names (UCC)
Special Offer - US$ 199.90

High Protection

StartSSL™ High Level Protection
No MD5 Hashes, Weak Key Scans
Minimum 2048-bit Strong RSA Keys

Hardware

Aladdin® USB eToken Pro
Aladdin® Smart Cards + Reader
Original Driver Software + PKI Client
Enterprise PKI Customized Solutions

Authentication

StartSSL™ Authentication SSL Protected
Open Identity Authentication Provider
Click here to log into your
StartSSL™ Account

Internationally Recognized

WebTrust for CAs + WebTrust EV Certified
Recognized by major browsers + software vendors

Easy Enrollment

Sign-up and you will receive right away an S/MIME client-certificate and a digital StartSSL™ Open Identity without charge during the easy three-step enrollment!

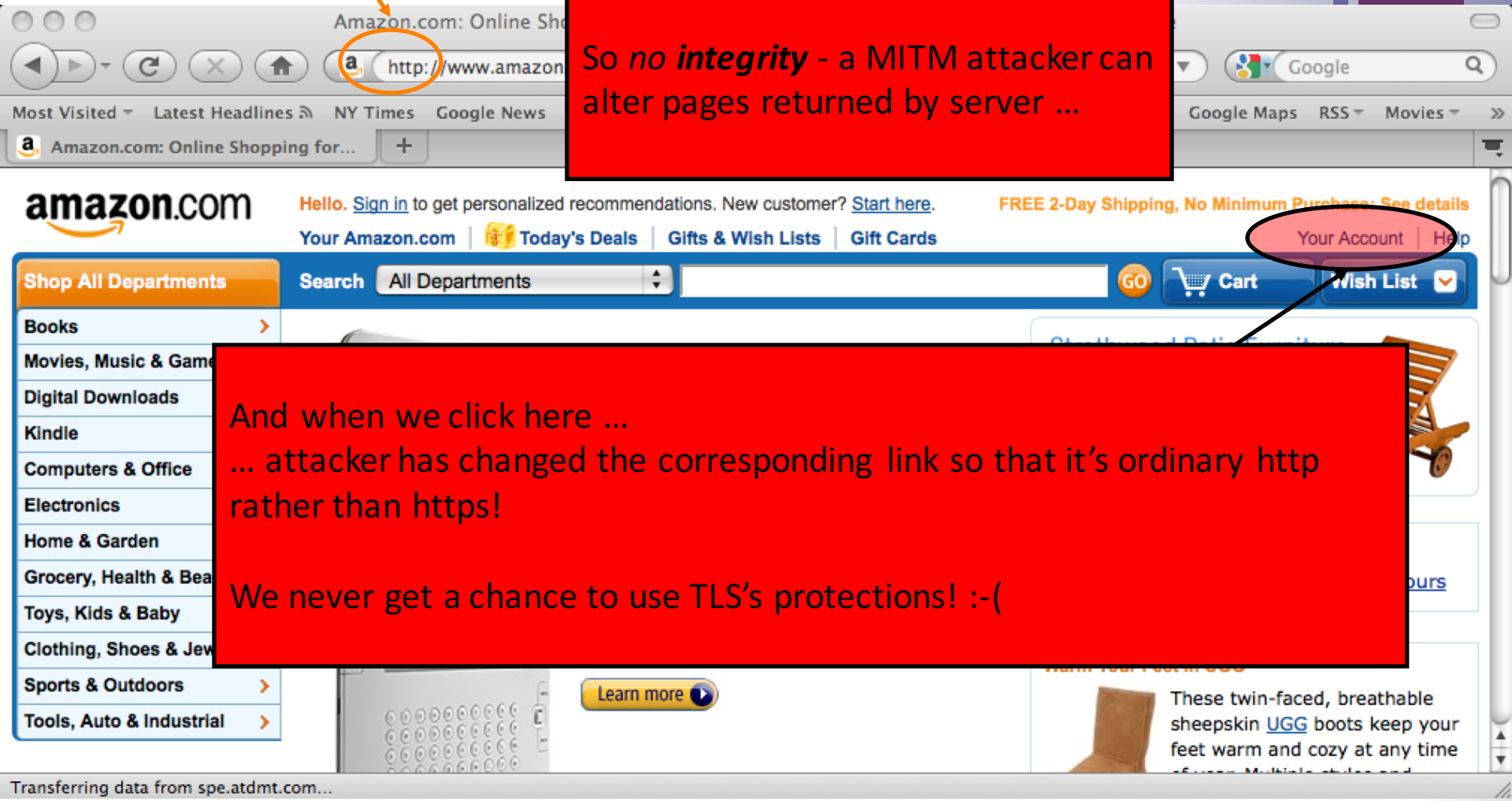
SSL / TLS Limitations

- Properly used, SSL / TLS provides powerful end-to-end protections
- So why not use it for *everything*??
- Issues:
  - Cost of public-key crypto
    - 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)
  - DoS amplification
    - Client can force server to undertake public key operations
    - But: requires established TCP connection, and given that, there are other juicy targets like back-end databases
  - Integrating with other sites that don't use HTTPS
  - **Latency**: extra round trips ⇒ pages take longer to load

SSL / TLS Limitations, con't

- 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

Regular web surfing - http: URL



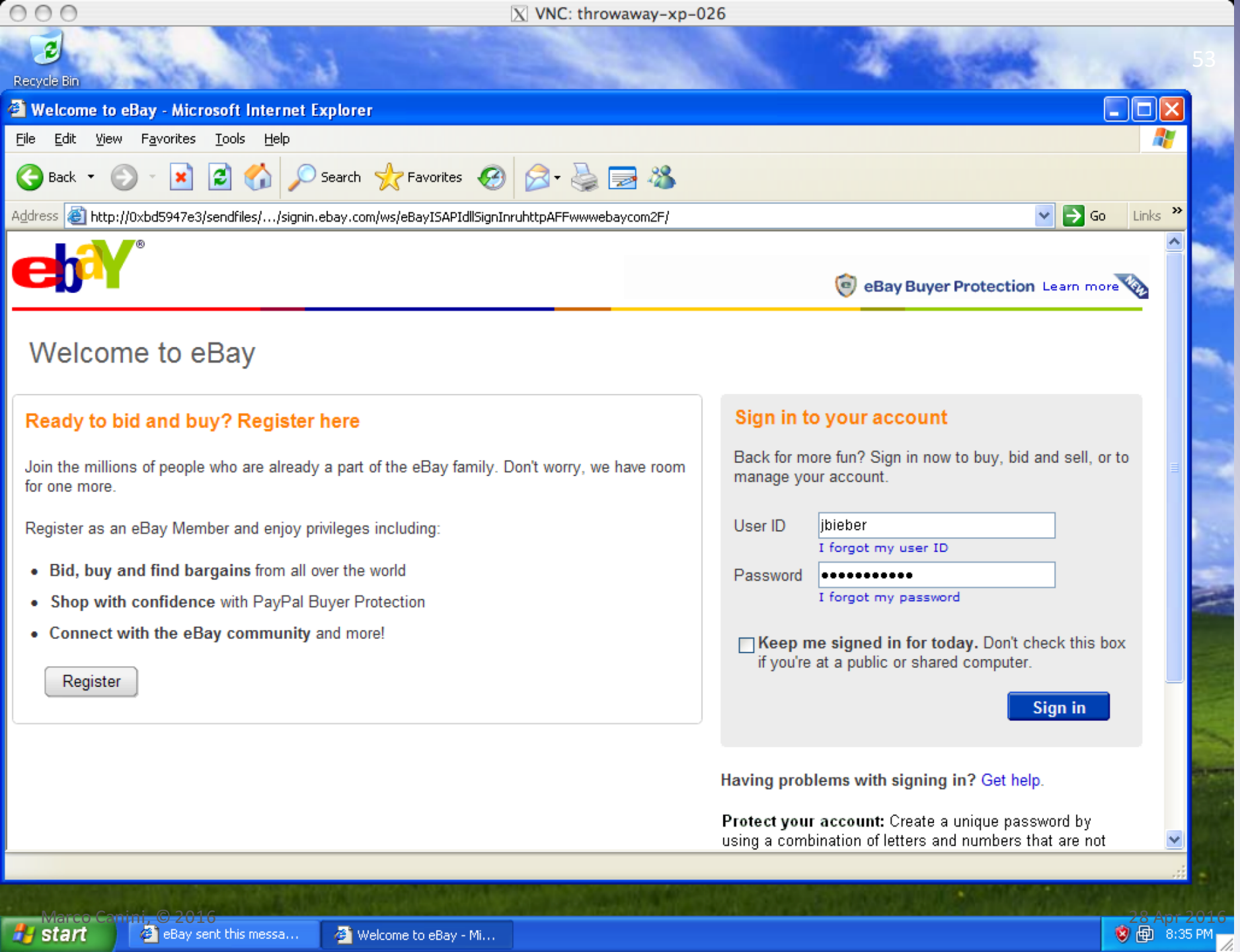
"sslstrip" attack

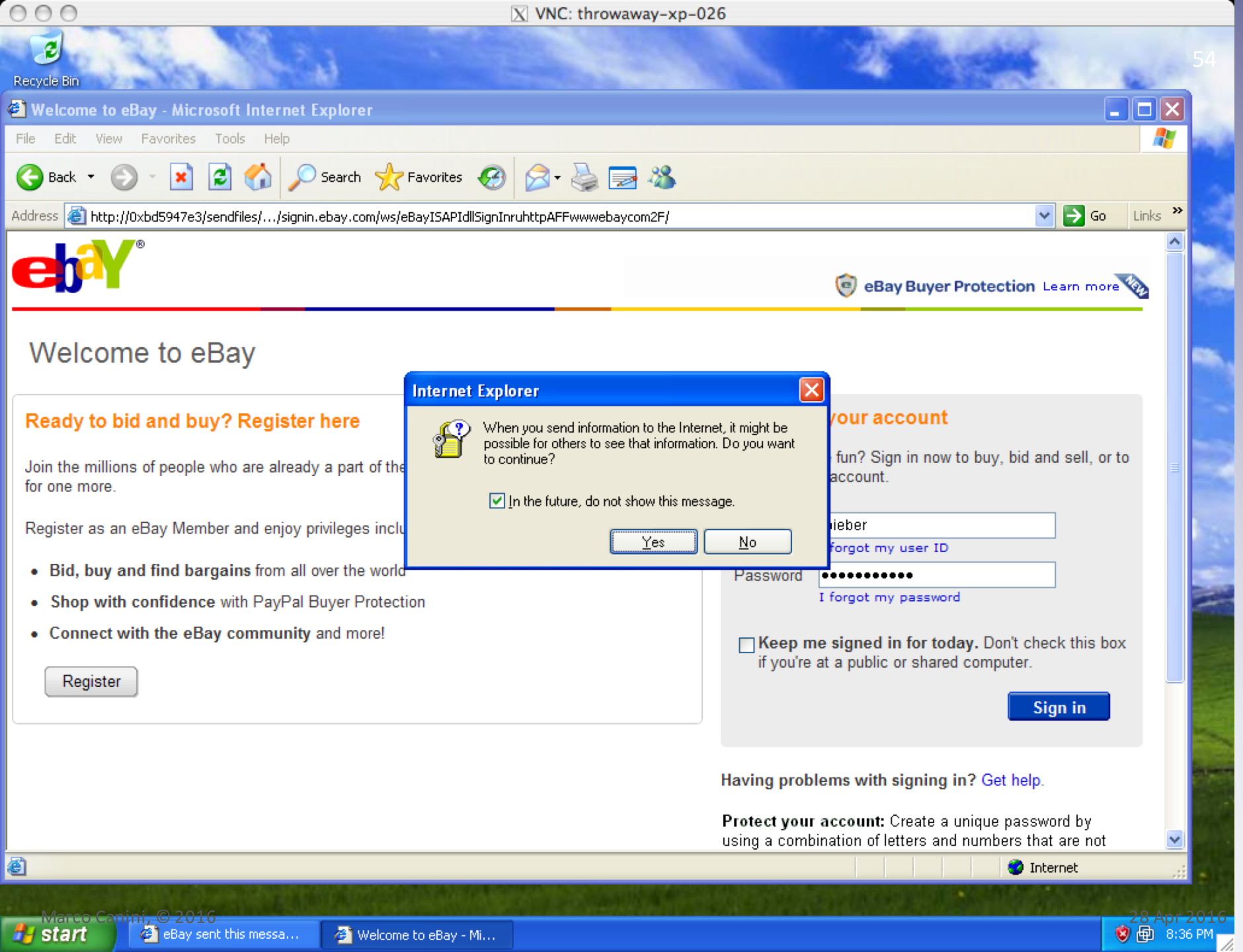
SSL / TLS Limitations, con't

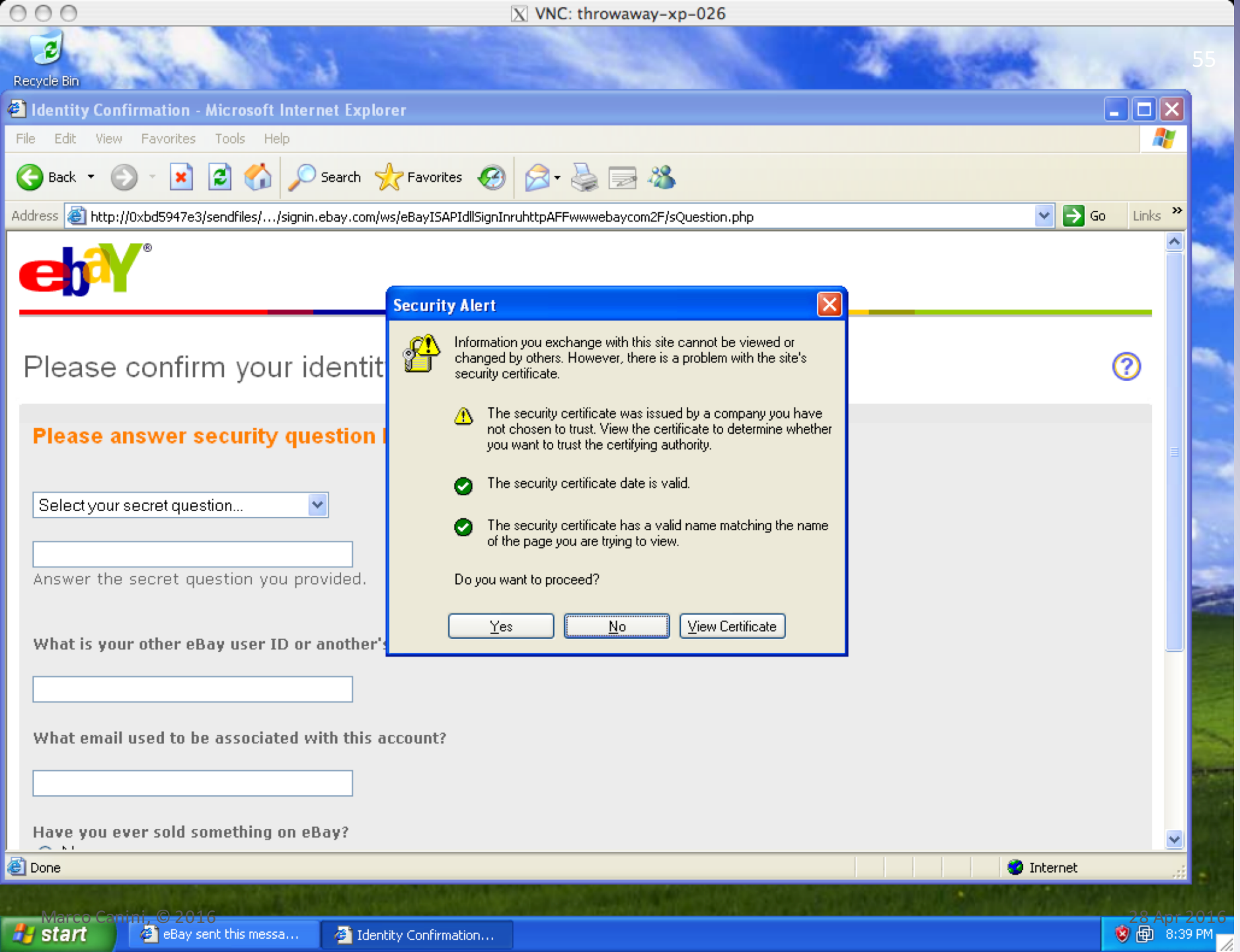
- Problems that SSL / TLS does **not** take care of ?
- TCP-level denial of service
  - SYN flooding
  - RST injection
    - (but does protect against data injection!)
- SQL injection / XSS / server-side coding/logic flaws
- Vulnerabilities introduced by server inconsistencies
- Browser coding/logic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

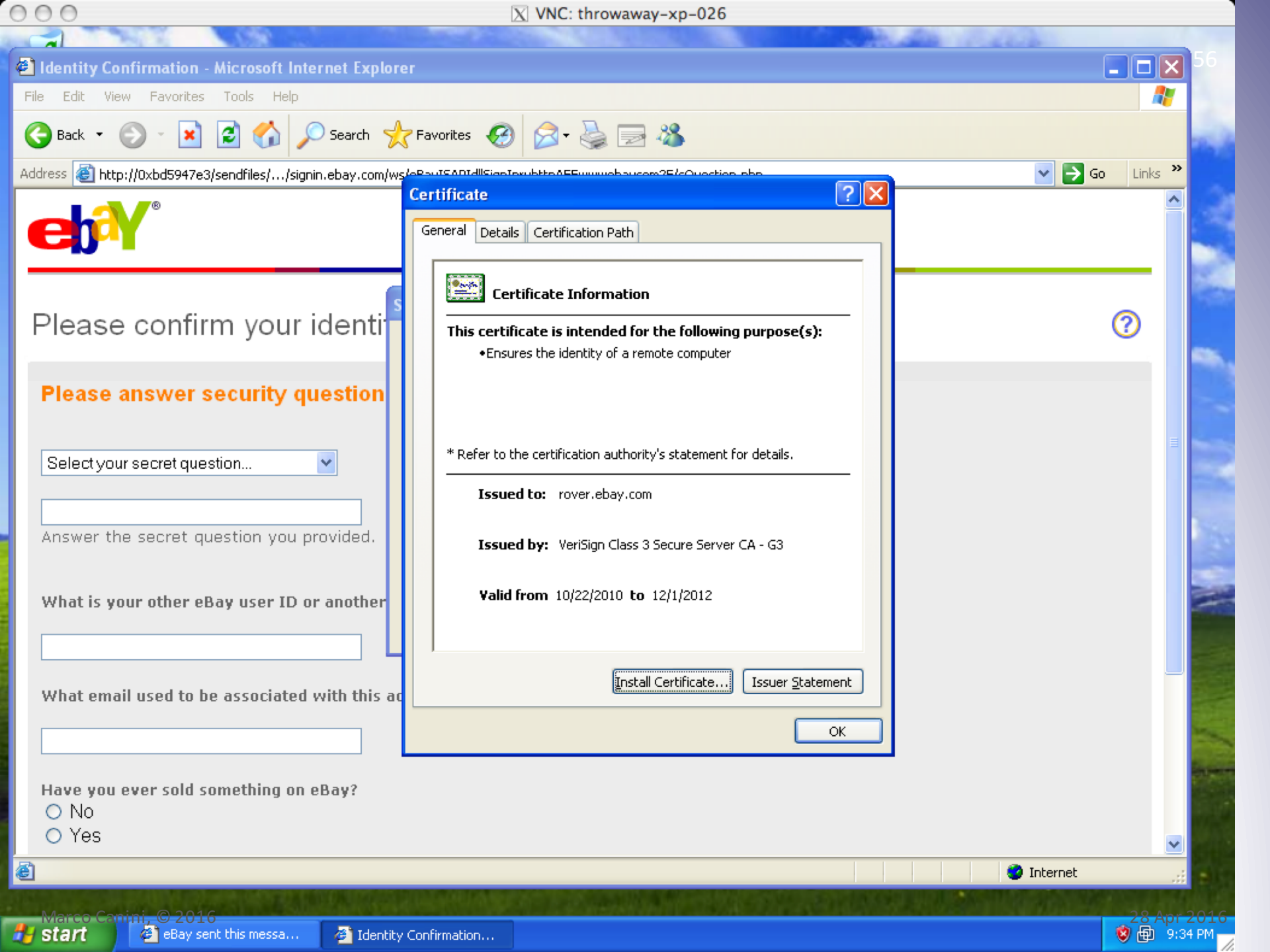
TLS/SSL Trust Issues

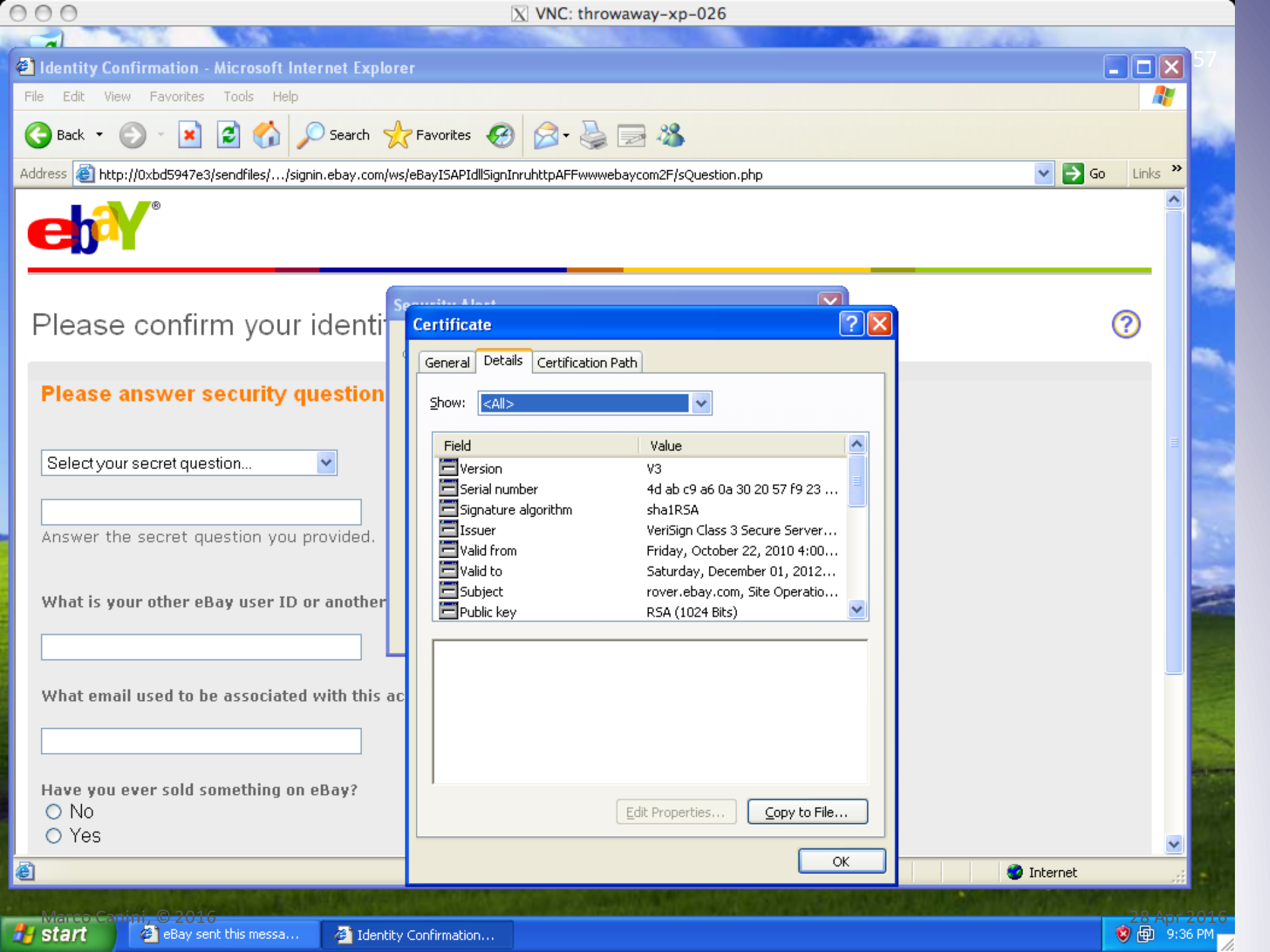
- User has to make correct trust decisions …

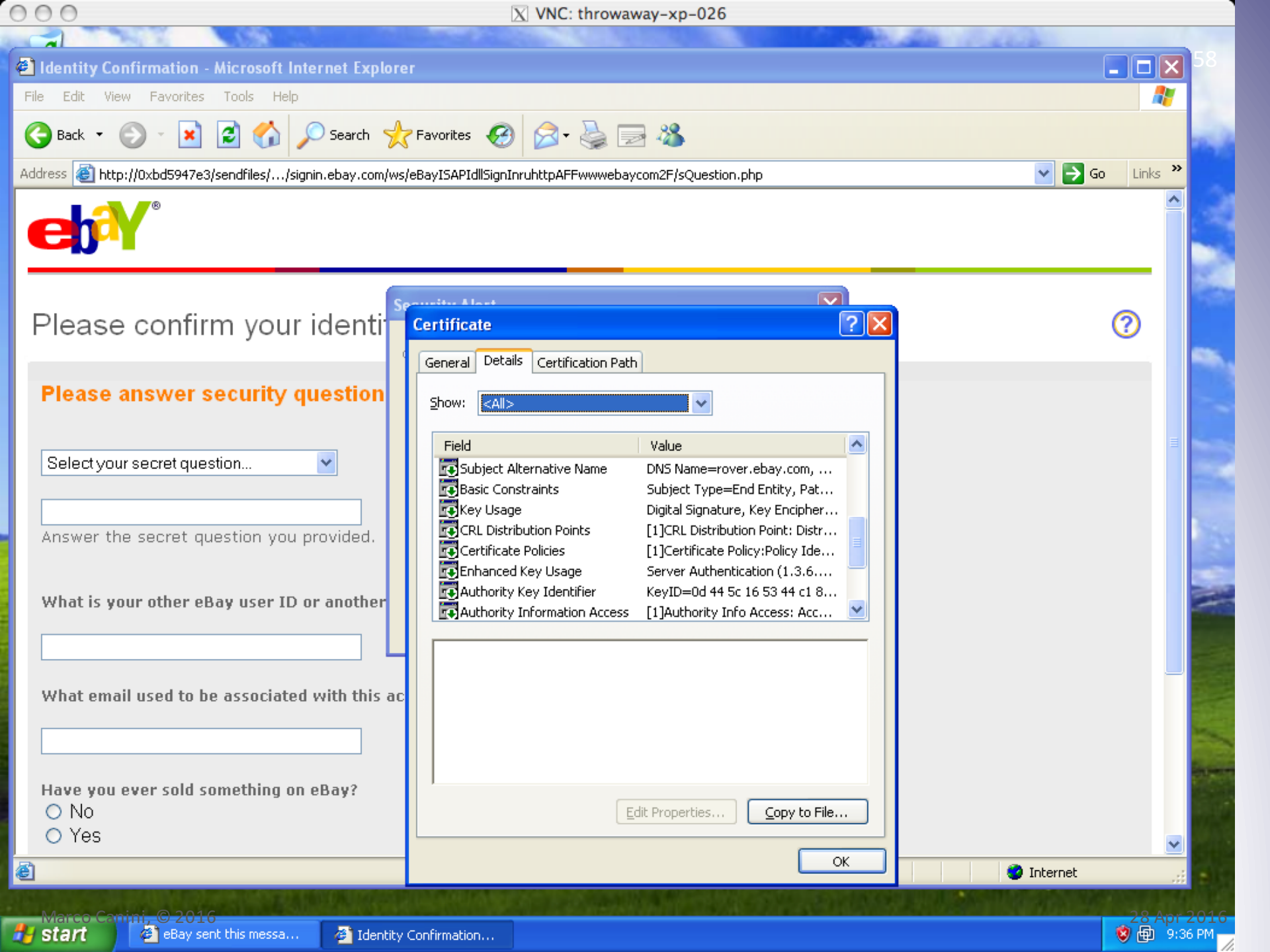

VNC: throwaway-xp-026
Recycle Bin
Welcome to eBay - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPIdllSignInruhttpAFFwwwebaycom2F/
Go Links
eBay Buyer Protection Learn more NEW
Welcome to eBay
Ready 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!
Register
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.
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
start
eBay sent this messa...
Welcome to eBay - Mi...
8:35 PM

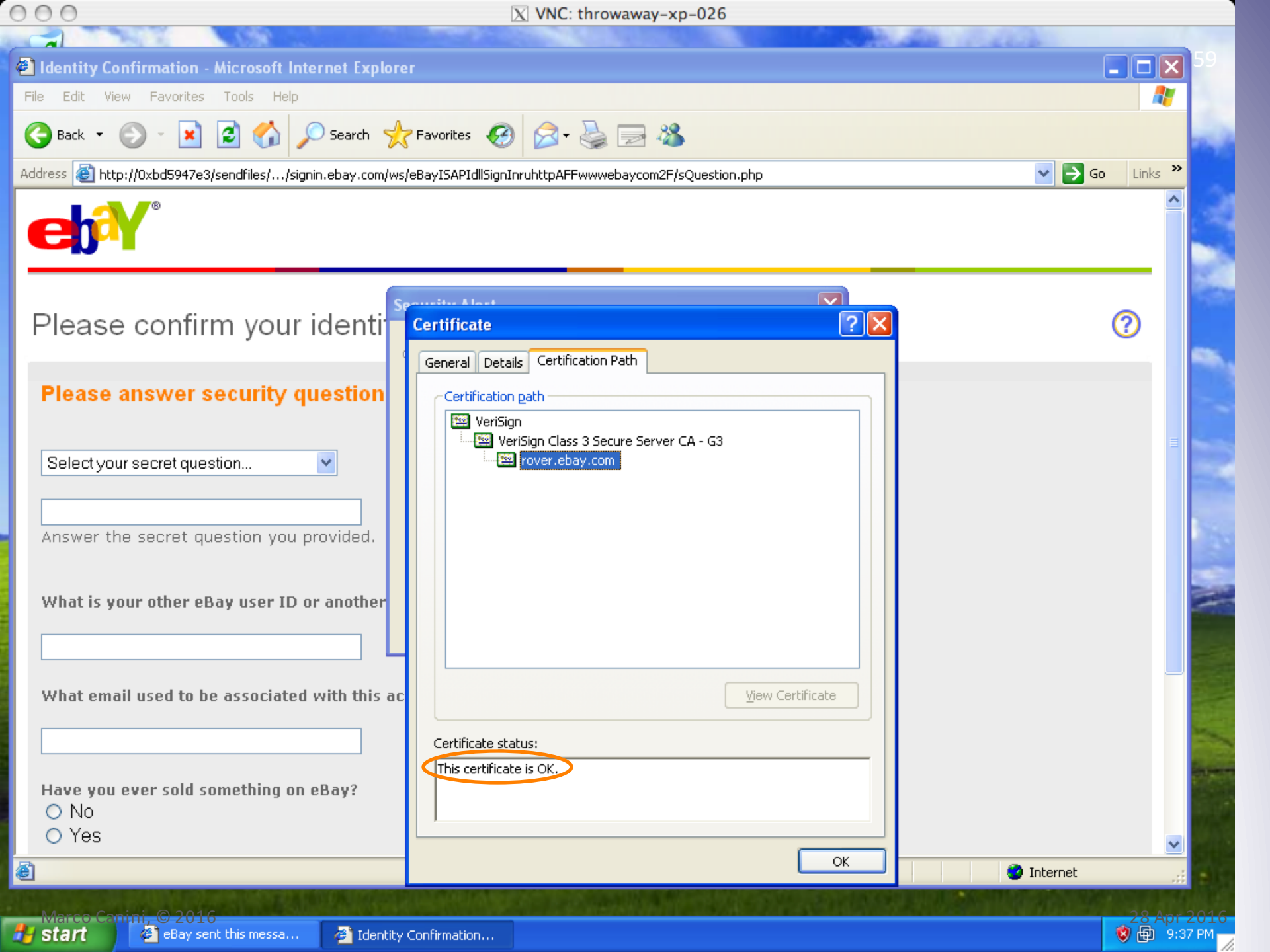

VNC: throwaway-xp-026
Recycle Bin
Welcome to eBay - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPIdllSignInruhttpAFFwwwebaycom2F/
Go Links
eBay Buyer Protection Learn more NEW
Welcome to eBay
Ready 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
Internet
start
eBay sent this messa...
Welcome to eBay - Mi...
8:36 PM


VNC: throwaway-xp-026
Recycle Bin
Identity Confirmation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPIdllSignInruhttpAFFwwwebaycom2F/sQuestion.php
Go Links
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?
Yes
No
View Certificate
Done
Internet
start
eBay sent this messa...
Identity Confirmation...
8:39 PM

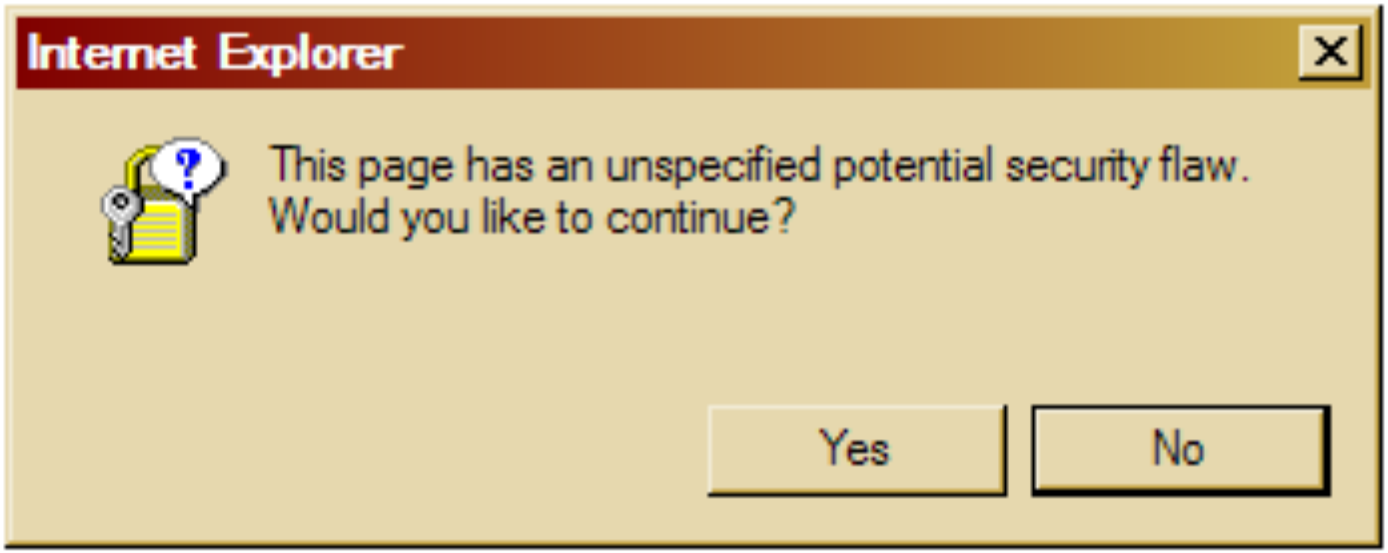

VNC: throwaway-xp-026
Identity Confirmation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPI.dll?SignIn&ruhttpAFEwwwebayscm2F&sQuestion.php
Go Links
Please confirm your identi
Please answer security 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
General Details Certification Path
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
Install Certificate...
Issuer Statement
OK
Internet
Marco Cannini, © 2016
28 Apr 2016
start
eBay sent this messa...
Identity Confirmation...
9:34 PM


VNC: throwaway-xp-026
Identity Confirmation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPIdllSignInruhttpAFFwwwebaycom2F/sQuestion.php
Go Links
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
General Details Certification Path
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)
Edit Properties... Copy to File...
OK
Internet
Marco Cannini, © 2016
28 Apr 2016
start
eBay sent this messa...
Identity Confirmation...
9:36 PM


VNC: throwaway-xp-026
Identity Confirmation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://0xbd5947e3/sendfiles/.../signin.ebay.com/ws/eBayISAPIdllSignInruhttpAFFwwwebaycom2F/sQuestion.php
Go Links
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
General Details Certification Path
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...
Edit Properties... Copy to File...
OK
Internet
Marco Cannini, © 2016
28 Apr 2016
start
eBay sent this messa...
Identity Confirmation...
9:36 PM



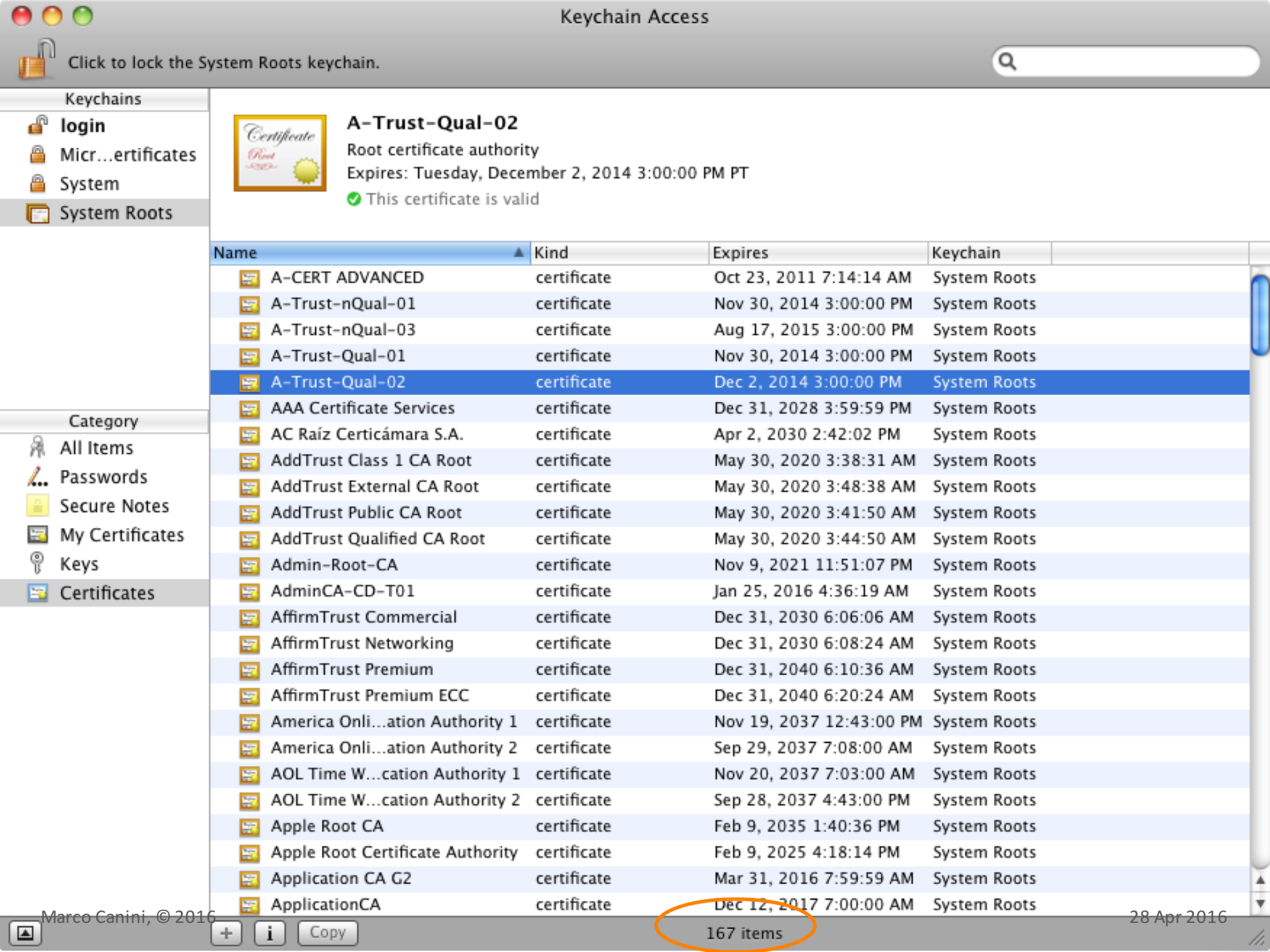
The equivalent as seen by most Internet users:



(note: an actual Windows error message!)

TLS/SSL Trust Issues, con't

- "*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?



28 Apr 2016

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

Comments (5) Recommended (37) Like 84

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

Comments (5) Recommended (37) Like 84

Computerworld - A solo Iranian hacker on Saturday claimed responsibility

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

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.

Fraudulent Google certificate points to Internet attack

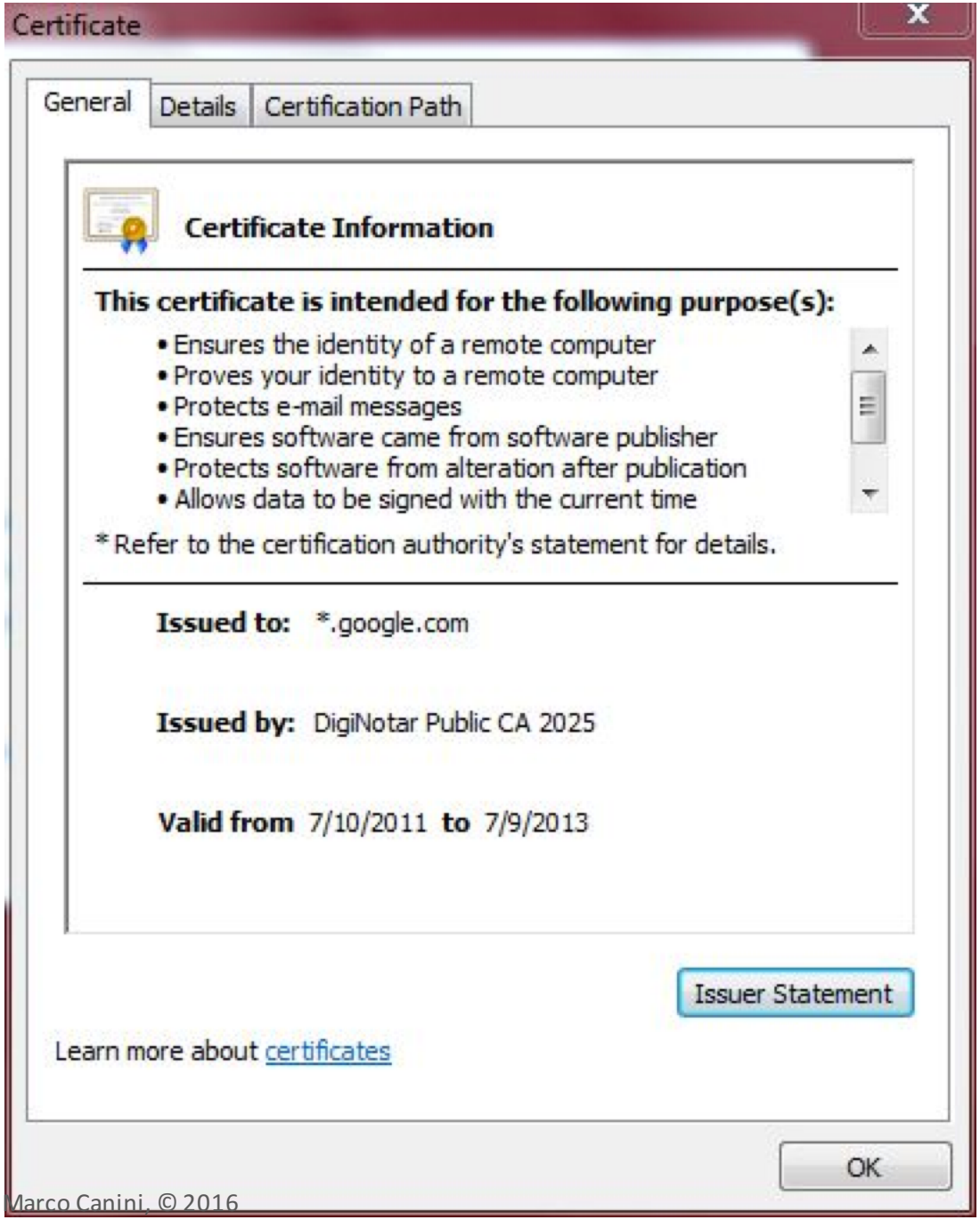
Is Iran behind a fraudulent Google.com digital certificate? The situation is similar to one that happened in March in which spoofed certificates were traced back to Iran.

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

Follow

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.



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

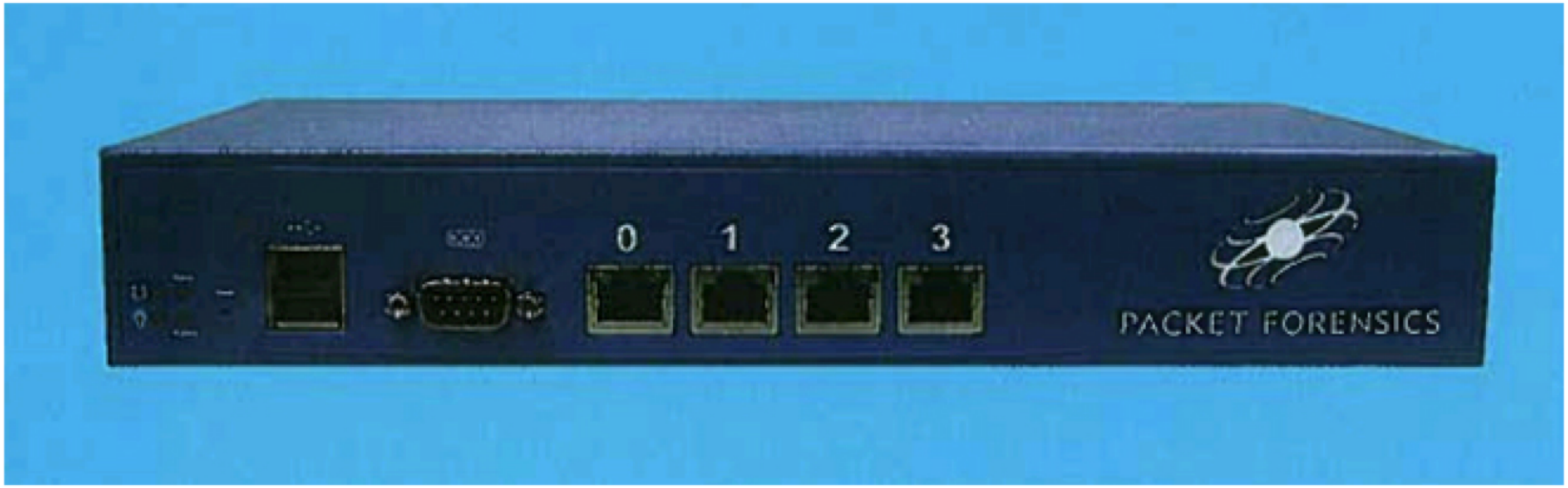
The big news in the security world, obviously, is the fact that a **fraudulent Google certificate made its way out into the wild**, apparently targeting internet users in Iran. The Dutch company DigiNotar has put out a statement saying that **it discovered a breach** back on July 19th during a security 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

Law Enforcement Appliance Subverts SSL

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



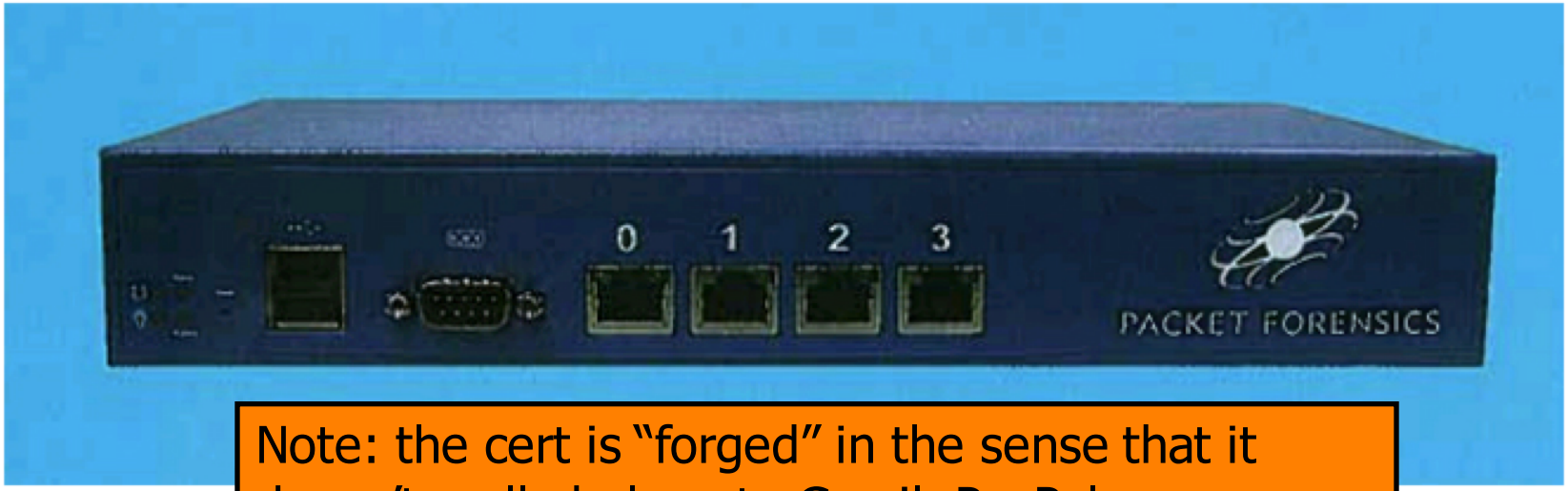
That little lock on your browser window indicating you are communicating securely with your bank or e-mail account may not always mean what you think its means.

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

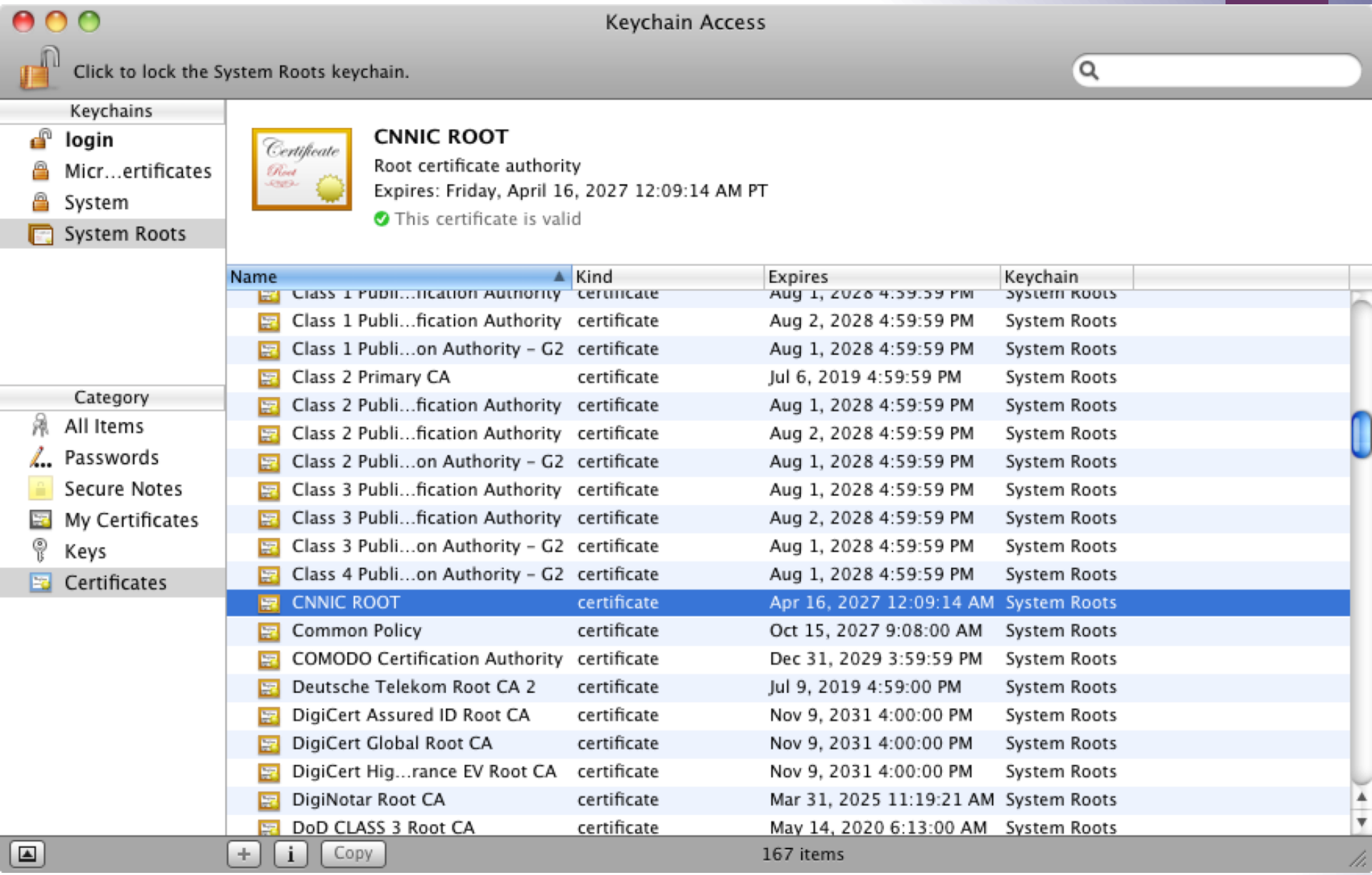


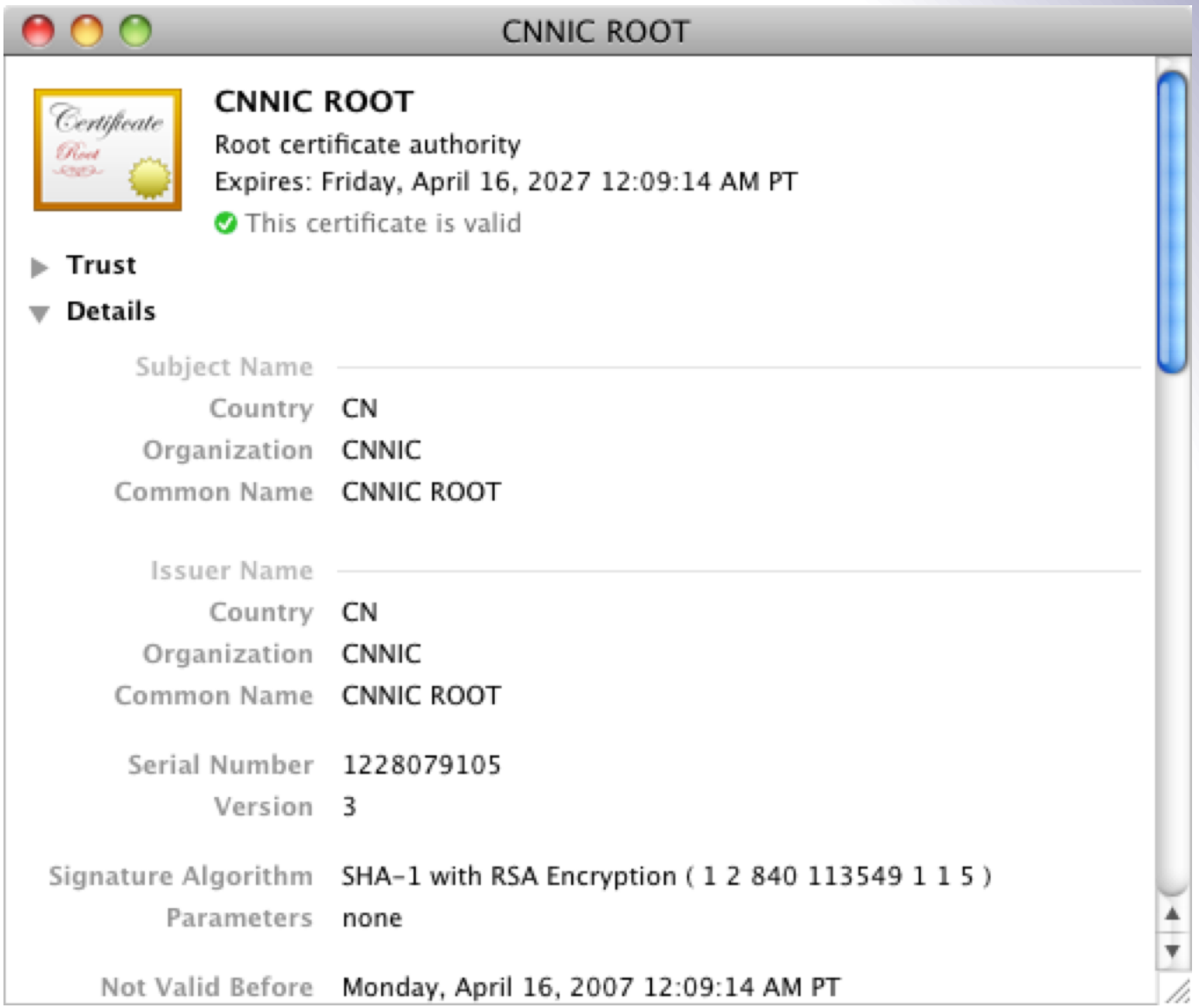
Note: the cert is "forged" in the sense that it doesn't really belong to Gmail, PayPal, or whomever. But it does not *appear* forged because it includes a legitimate signature from a trusted CA.

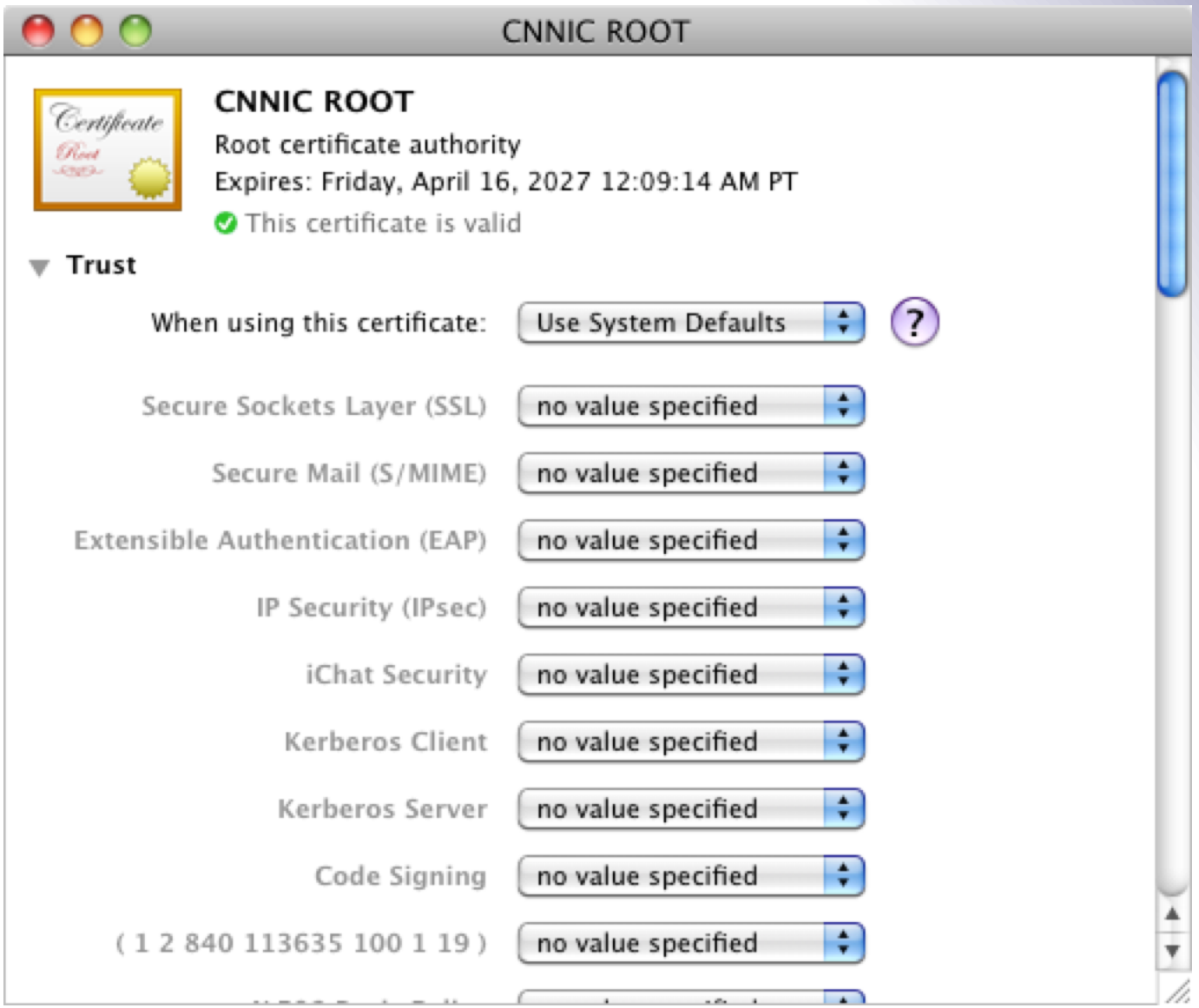
That little lock o ank or e-mail account ma

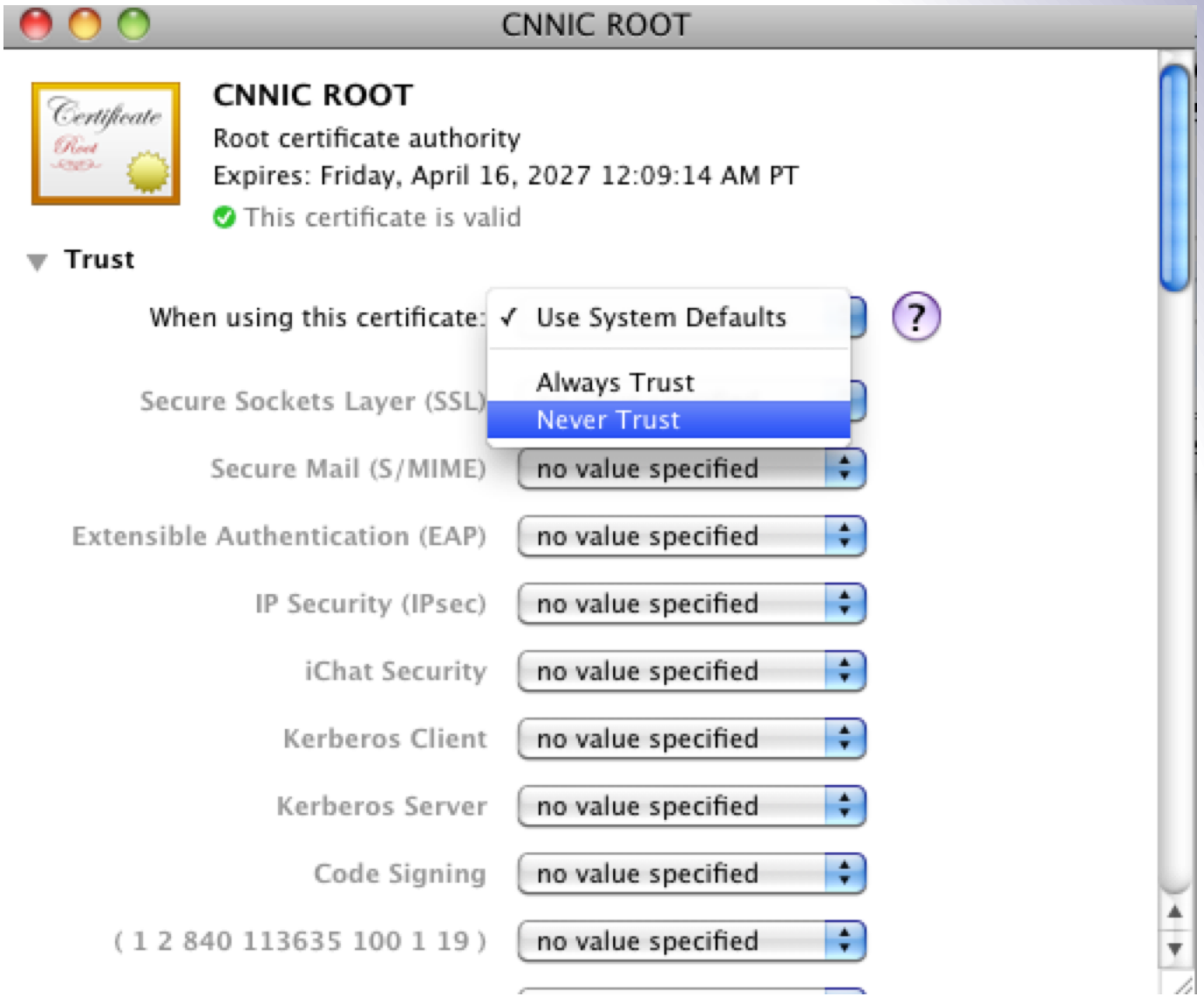
Normally when y, the browser examines the website's certificate to verify its authenticity.

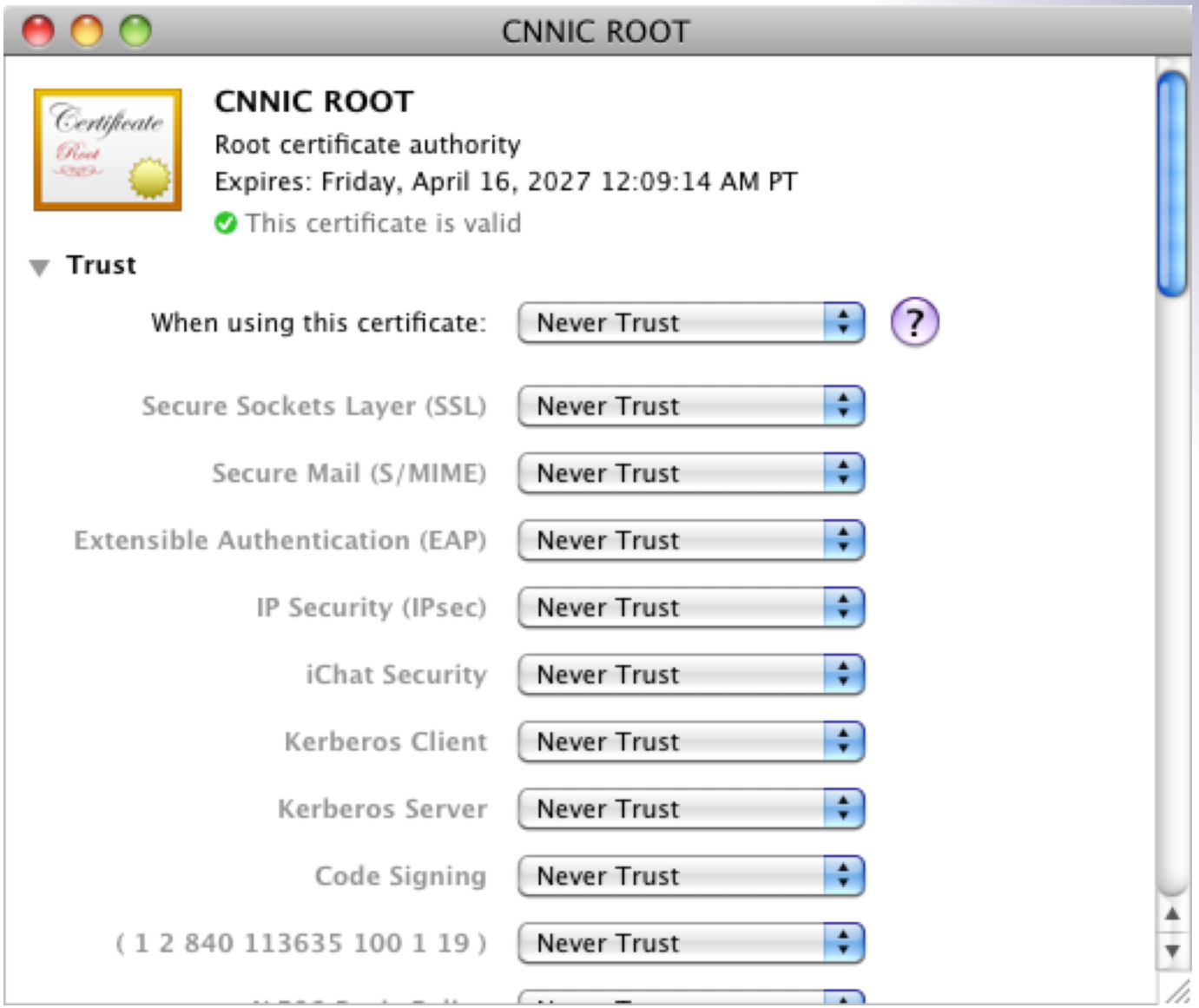
At a recent wiretapping convention, however, security researcher Chris Soghoian discovered that a small company was marketing internet spying boxes to the feds. The boxes were designed to intercept those communications — without breaking the encryption — by using forged security certificates, instead 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.

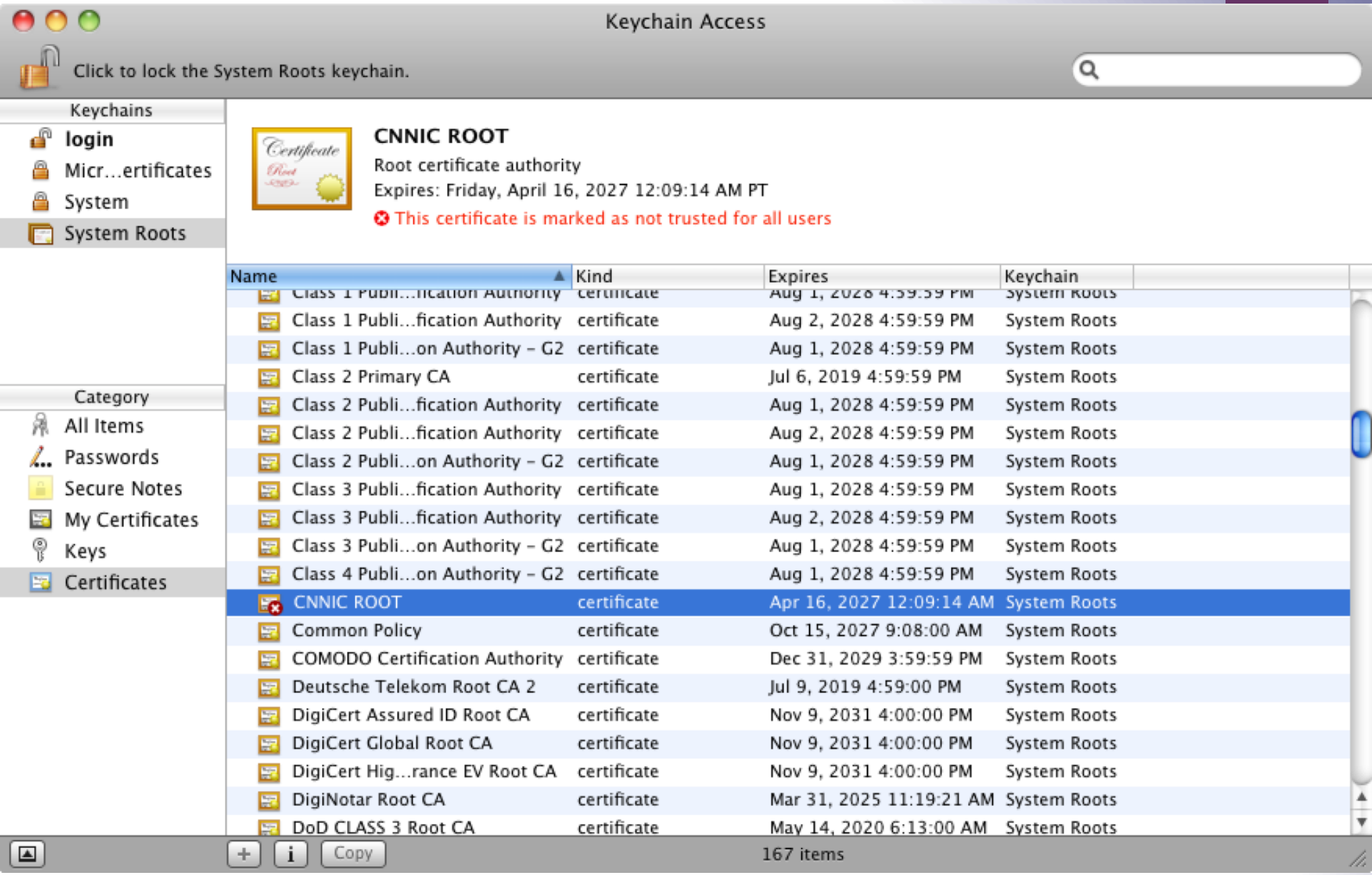

Keychain Access
Click to lock the System Roots keychain.
Keychains
login
Micr...ertificates
System
System Roots
Category
All Items
Passwords
Secure Notes
My Certificates
Keys
Certificates
CNNIC ROOT
Root certificate authority
Expires: Friday, April 16, 2027 12:09:14 AM PT
This certificate is valid
Name
Kind
Expires
Keychain
Class 1 Publi...fication Authority certificate Aug 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
Copy
167 items


CNNIC ROOT
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
Always Trust
Never Trust
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
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


Keychain Access
Click to lock the System Roots keychain.
Keychains
login
Micr...ertificates
System
System Roots
Category
All Items
Passwords
Secure Notes
My Certificates
Keys
Certificates
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 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
Copy
167 items

+

Pretty Good Privacy (PGP)

PGP History

- PGP = Pretty Good Privacy
- Several flavors: PGP, PGPi, GPG

PGP

- Published by Philip Zimmermann in 1991
- Portable software initially containing classical algorithms MD5, IDEA, RSA
- First software allowing anybody to completely protect their documents and messages
- 3 years of enquiry and harassment by the American government
  - Patented algorithms (RSA patented in the US until 2000)
  - Suspicion of violating export regulations

PGP History

1996-97:

- Selling of PGP Inc. to McAffee (Network Associates)
  - Code no longer public
- During the 39th IETF meeting at Munich, Zimmermann and Callas requested the IETF to setup a working group on the standardization of PGP (OpenPGP [RFC1991, Aug 96], [RFC2440, Nov 98], [RFC4880, Nov 07])
- Richard Stallman at the Individual-Network Betriebstagung at Aachen requested the European hackers to implement public key software (US citizens were not allowed to do so outside the US)

2001:

- Zimmermann leaves Network Associates
- Network Associates abandons PGP

PGP History

2002:

- PGP Corporation is created, buys back PGP rights www.pgp.com
- Code is again public
- Free trial version
- Basic functionalities remain available after 30 days, but not the additional functionalities, e.g., disk encryption
- Complete system compliant with OpenPGP

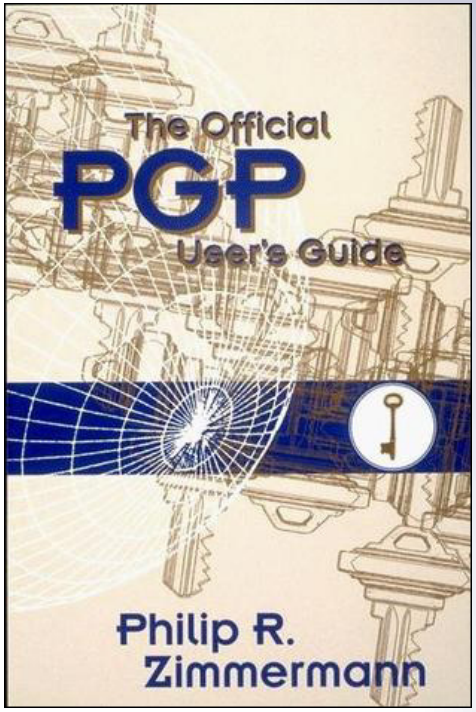
2010:

- Symantec acquired PGP

PGP History

PGPi

- Developed by Ståle S. Ytteborg (Norway) to counter the US export regulations
- Maintained from 1997 to 2000
- Obtained from the printed source code of PGP
- MIT Press thus published a book with the PGP source code
- www.pgpi.org



PGP History

GPG = GnuPG = GNU Privacy Guard

- GnuPG is the GNU GPL version of PGP www.gnupg.org
- Initially, used ElGamal and Blowfish instead of RSA and IDEA
- Follow the Open PGP Standard
- Version 0.0.0 released in December 1997

- GUI Frontends:
  - http://www.gnupg.org/related_software/frontends.en.html

+

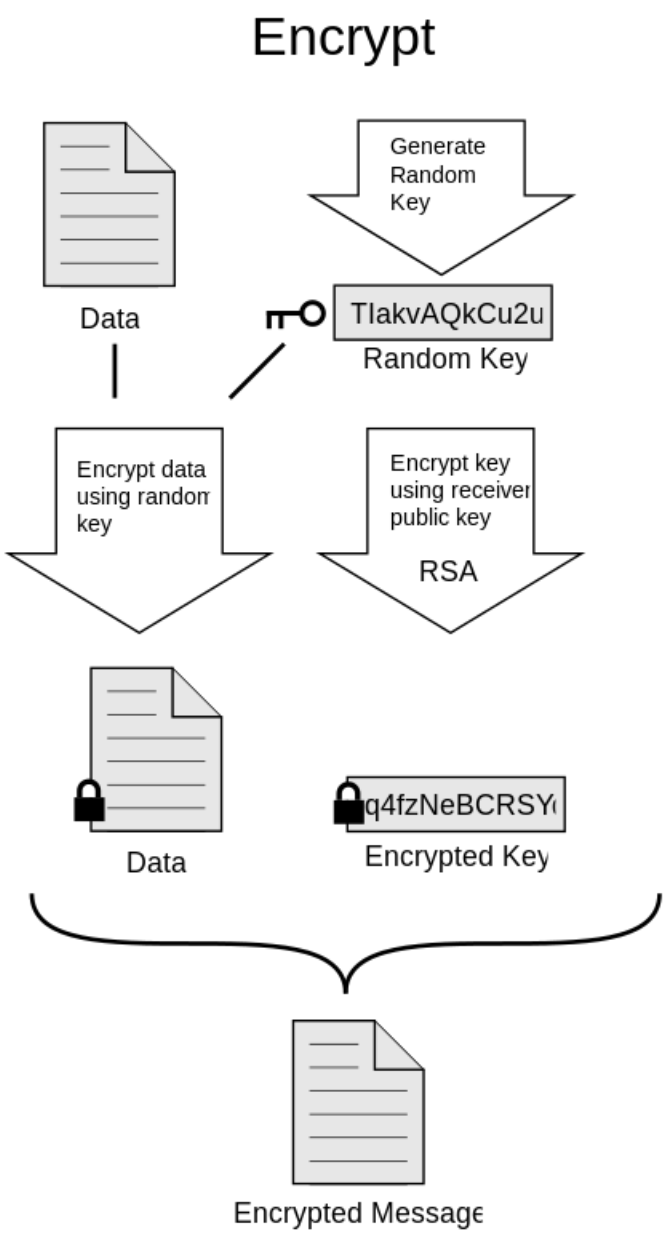
Basics

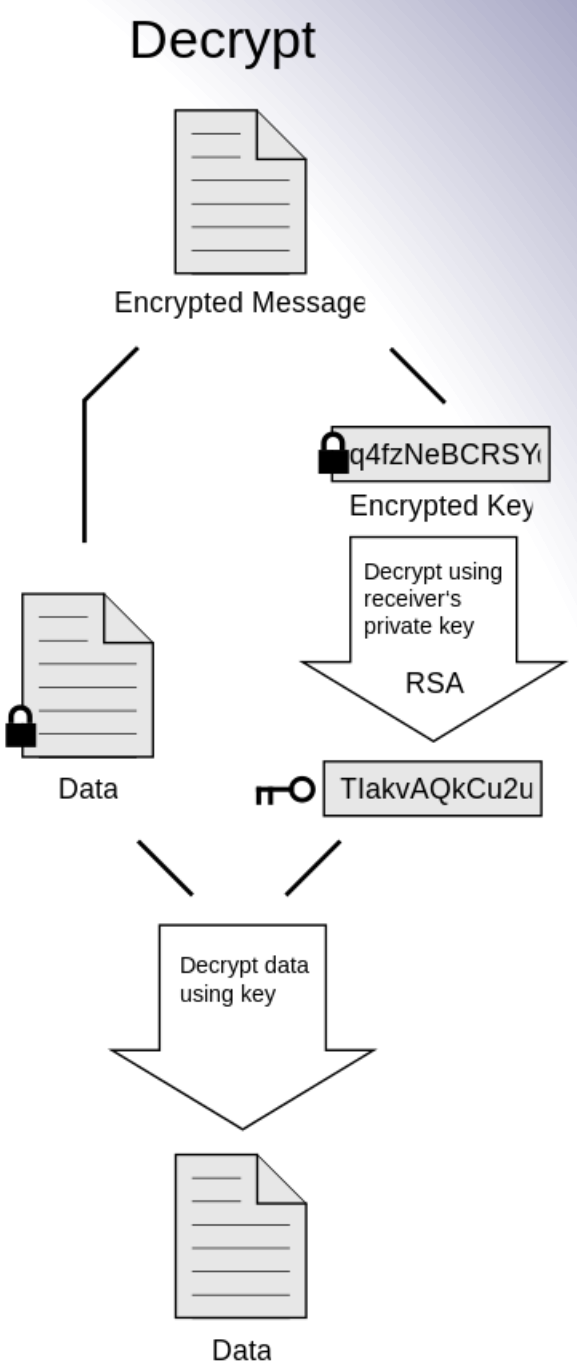
PGP Features

- Signature

- Encryption
  - Hybrid crypto: combine symmetric and public-key crypto
  - Session key is symmetric; encrypt session key with public-key of recipient

- Key management
  - What is called a PGP key is actually a PGP certificate
  - Web of trust





Example

```
This is an example of signed message

-----BEGIN PGP SIGNATURE-----

iQIcBAEBCgAGBQJTcWJaAAoJEChyd2euJIo/aYYP/0Vl/+u5zNkFw9lgvCd4UYdu
88aTImx+KmP8loFnu0Q6EC8UCuYCd8q/CHNPVq9k+pBE3Szolt6L3EIO6hDwRjJn
lnODZVoAWBgy5S5+BEgTA6OI3ixsmySacjkfYKbSprgLCKRklgesVl9Lo+5/ZTXJ
gQRhqePkYEmsfMKnTmLi9jiS/TqfXBcKOiuZ2Y/ihhNULIP4mnIDKw7k2AI8d27/
rAV2uMEi2XKDwxn9ziJ31yAM6IUhKvEKFwAjHf63rETZM3QrlgHaG/U128S5pqzS
JCkXFMhXnyCVRXmVDaoq9drzWXJ7EU8YHYDZnw6cuuYXPkGQC83T8XM+ZDIXFeQz
o0uFXcKUPyO+Ns6D2HrPKv+yxi8PbmBTOZs8nKIj843BzWFr3etnR19N1f/+zV+X
VMaNRW/i67Of8uD4dJlkA8PYDgBmglBn8oRiU0L5bqOWoXJFJKXQiYz62lZvtPwS
PBDAfM2NfGkdBV4ypOoqydTzwhd8ZO26PICKAKFhW+AfEeQu7a7tOD0+m/3L74Mf
ljbTTalyctgTY/slDiP/bHS8NCgIIhvjsJYdfrMCuc+t29bh5FwMnyemU07Ynqa2
vo4L/Jq1qJ3Cy2h+kyW4MZlh6ADauacbHH1pVLKvHOnH5mT4FsP0rsI/F73oZSN2
RQZwQdrjHsIihP02ERCX
=FyhH
-----END PGP SIGNATURE-----
```

Symmetric Encryption [RFC4880]

All of them seem to be secure.

- TDES [Mandatory]
  - Slow. Considered to be secure
- IDEA
  - Patented until 2010. Seem to be secure, resisted to all cryptanalysis for 17 years…
- CAST5 (128 bit-key) [should impl. CAST5]
  - Less studied than the other algorithms
- Blowfish (128 bit-key)
  - Less studied than the other algorithms
- Twofish (256 bit-key) (AES contest top-5 finalists)
  - Rather new
- AES (128/192/256 bit-key) [should impl. AES128]
  - The standard since 2000

Public-Key Encryption [RFC4880]

- RSA
- ElGamal [Mandatory]

(Public-Key) Signature [RFC4880]

- RSA
- DSA [Mandatory]
- ElGamal no longer recommended for signature
  - Attack by Phong Nguyen (2003) when ElGamal keys used for both encryption and signature.
  - *"[…] We show that as soon as one (GPG-generated) ElGamal signature of an arbitrary message is released, one can recover the signer's private key in less than a second on a PC. As a consequence, ElGamal signatures and the so-called ElGamal sign+encrypt keys have recently been removed from GPG"* (Nguyen, 2003)
  - The flaw was exploitable during 4 years…

Hash Functions [RFC4880]

- MD5
  - Deprecated
- SHA-1 [Mandatory]
  - Should be avoided
- SHA-224/256/384/512
  - Seem Ok
- RIPEMD-160
  - Seem Ok
- Tiger
  - Seem Ok

Protection of the Private Key

- The private key cannot be memorized by the user
- **How can we protect the private key?**
- Stored on the hard drive
  - Encrypted with a password (no means to access it without the user's collaboration)
  - Once decrypted, it is in the computer's memory (dangerous)
- Stored on a smart card
  - Access to the card is protected by a password
  - The key never leaves the card, it's the data that transits through the card to get encrypted, decrypted or signed
- The passphrase must be as strong as the key (i.e., same entropy at least)

Key Size [Lenstra, Verheul, 01]

sym. key (bits)	public key (bits)
71	1024
80	1536
87	2048
99	3072

Help choosing an appropriate key size:
http://www.keylength.com/en/1/

+

Public-key Validity

Getting the Recipient's Key

- How to be sure that the key we use to encrypt a message is the correct one?

- Directory
  - Who put the key into the directory?
  - Fake identity associated to the key?
  - Is the directory a legitimate one?

- Face to face, check the ID, check the hash of the key, sign the key
- Certificates

Certificates

- Peer-to-peer
- Users trust some other users
- One or several signatures on each certificate

+

Public-key Distribution

Validity and Trust in PGP

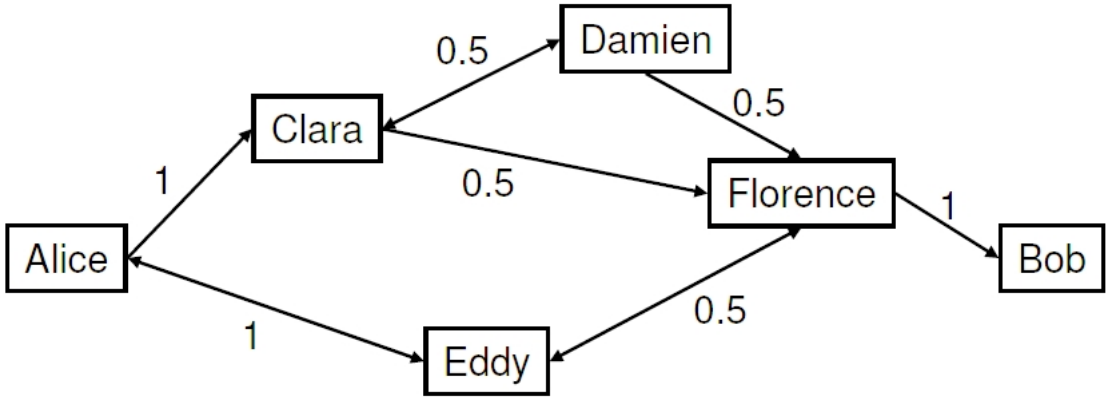
- Two important notions in PGP

- Validity: I know that this key belongs to Bob
- Trust: I know that Bob does not sign keys arbitrarily

- When we sign a key, we declare its validity

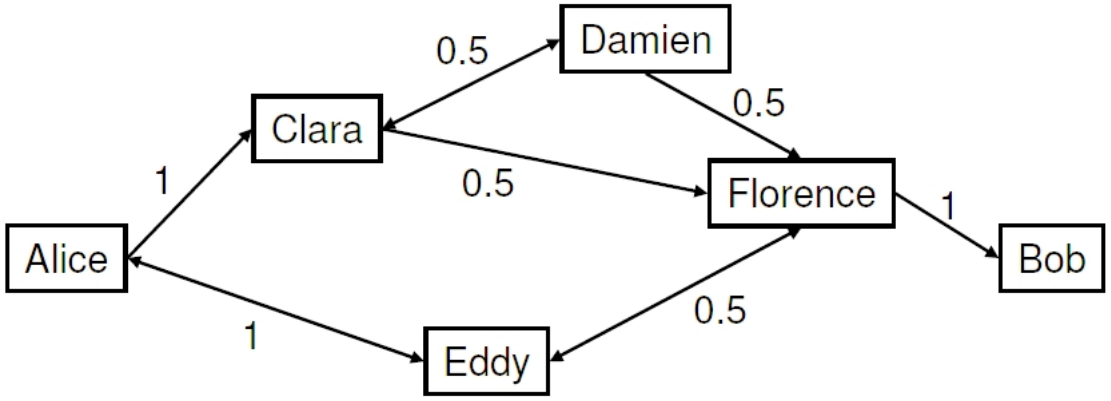
Validity and Trust in PGP

- We can also declare a full or partial trust
- A key is valid if the sum of the partial trusts of its valid signatures is at least 1



The Web of Trust

- Clara and Eddy are valid since Alice has signed them
- Alice has full trust in Clara and Eddy:
  - Damien, Florence, and Eddy are valid
- Clara and Eddy each have a partial trust in Florence:
  - Alice trusts Florence and Bob is valid



Key Signing Party

- Each participant's public key is published in advance and downloaded by everybody
- Each participant identifies himself (with passport) and reads aloud his key fingerprint
- Everybody signs that key and uploads it on a key servers

Key Publication

- Several PGP key servers exist across the world
  - http://pgp.mit.edu/
- They contain keys of all PGP users that want to publish their key
- If Alice is sure that the key associated to Clara belongs to Clara, she can sign Clara's key and re-submit it to the servers
- If Eddy trusts Alice, he can accept Clara's key

+

Public-key Revocation

Key Revocation

- How can we revoke a key published on a server?
- Servers are replicated: deleting a key from one server is useless because another server will duplicate it again
- How can we prove that we are allowed to revoke a key if we lost it?
- We generate a key revocation certificate when we generate the key
- We put a validity deadline to the key when we generate it

Any questions?

Stay tuned

+

Next time you will learn about

Bitcoin