

IT 4823

Information Security Administration

Cryptography III



Notice: This session is
being recorded.

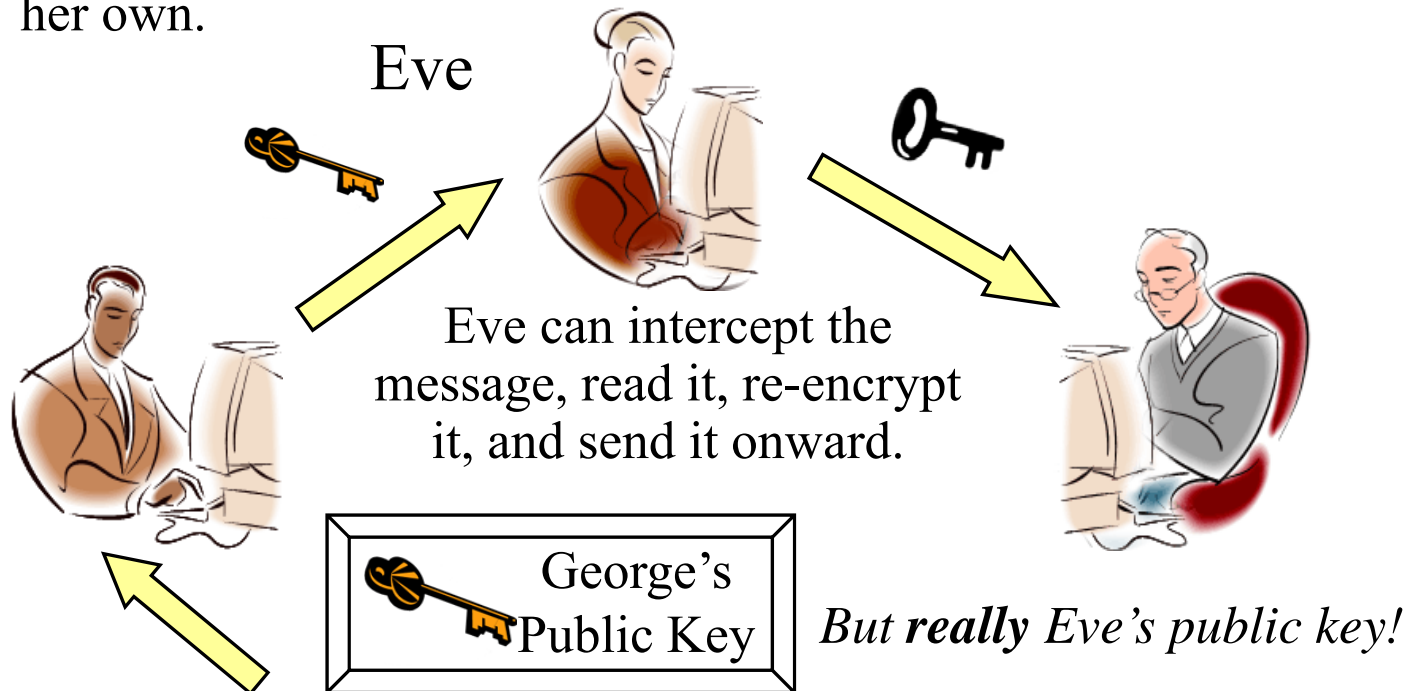


Copyright © 2016 by Bob Brown



Man-in-the-Middle Attack

Evil Eve the Eavesdropper (and the man in the middle) sneakily replaces George's public key in the repository with her own.



Public Key Infrastructure

- Goal: **bind identity to a public key**
 - Principals must be identified by an acceptable name.
 - Often a domain name or email address will do.
- Binding is necessary to mitigate man-in-the-middle attacks.
- Erroneous binding compromises confidentiality
- The alternative to the PKI is the Web of Trust

Certificate Authorities

- A CA is a trusted organization (*Verisign!?!)* that exists to issue digital certificates.
 - Carefully verify the identity of the principal
 - Keep their signing (private) key private
- A principal creates a digital certificate with an identity and a public key...
- The CA verifies the identity...
- And signs the certificate with its own private key.
- The CA's public key is “well-known” and can be used to verify the signature

Reminder: Digital Certificate

Contains:

- Principal's identity
- Principal's public key
- Identity of signer and other info
- Digital Signature

Everything is plain text except the digital signature, which is a cryptographic hash (digest) encrypted by the signer's *private* key.

Principal's Identity Amazon.com
Principal's Public Key mQGIBD9aAvwRB
Hash, other information SHA-256
Signer's Identity Verisign
Digital Signature B157 ACE3 9788

Changing the Public Key

- Evil Eve substitutes her public key for Amazon's, a man-in-the-middle attack.
- The digital signature is no longer valid (because the data have changed.)
- Evil Eve must gain access to the signer's private key (signing key) to forge a new digital signature. We hope this is hard!

Principal's Identity
Amazon.com

Eve's Public Key
DfIZOkhURN

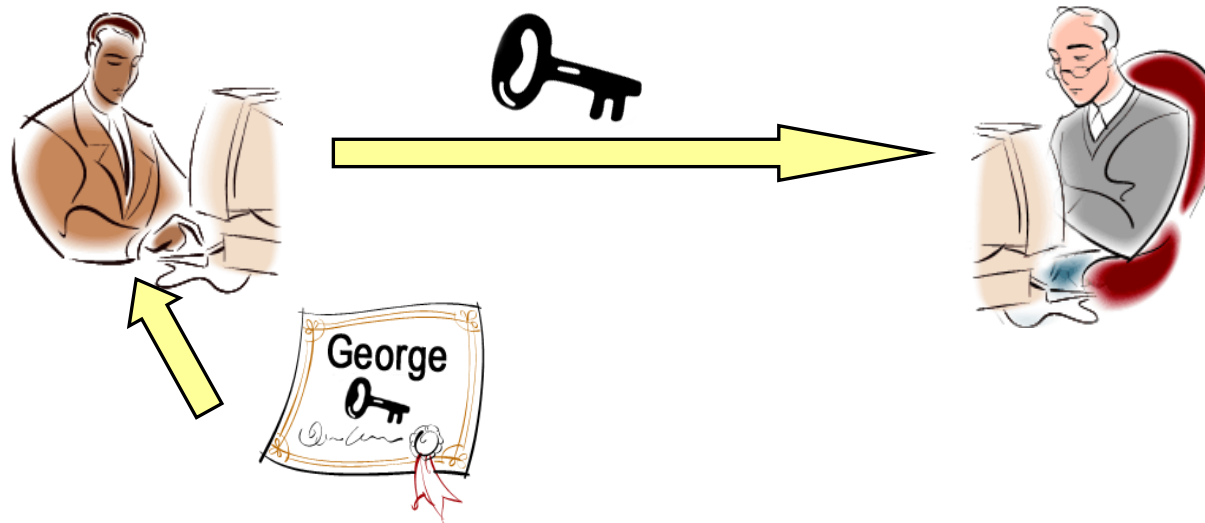
Hash, other information
SHA-256

Signer's Identity
Verisign

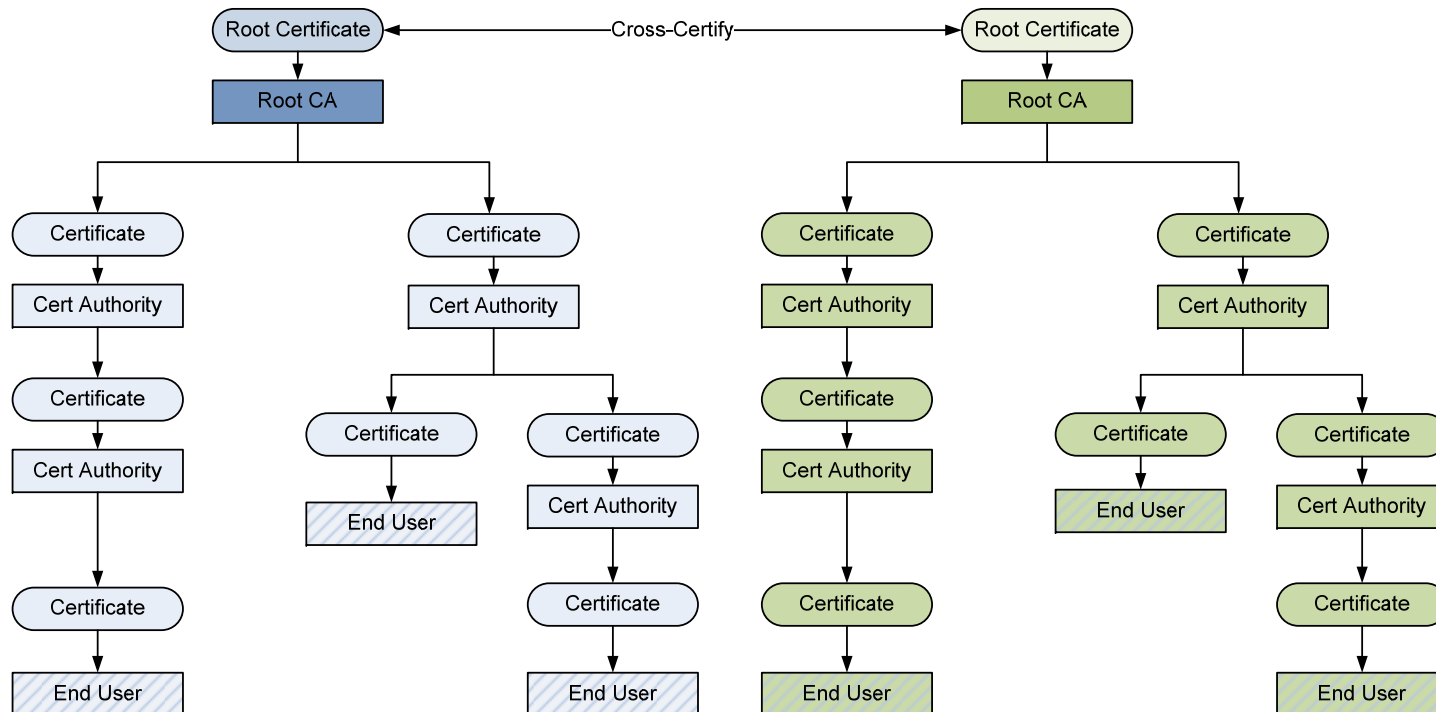
Digital Signature
B157 ACE3 9788

Public Key in a Certificate

If George's public key is contained in a certificate, digitally signed with a private key, it is *much harder* to tamper with the public key in the certificate.



Hierarchy of Certificate Authorities



Trusting “Things”

- We trust that DDS has correctly identified the individual.
- We trust that this document is not a forgery.
- We trust that no one has compromised an employee at DDS to produce a “real” document with bogus information on it.



Trusting Digital Certificates

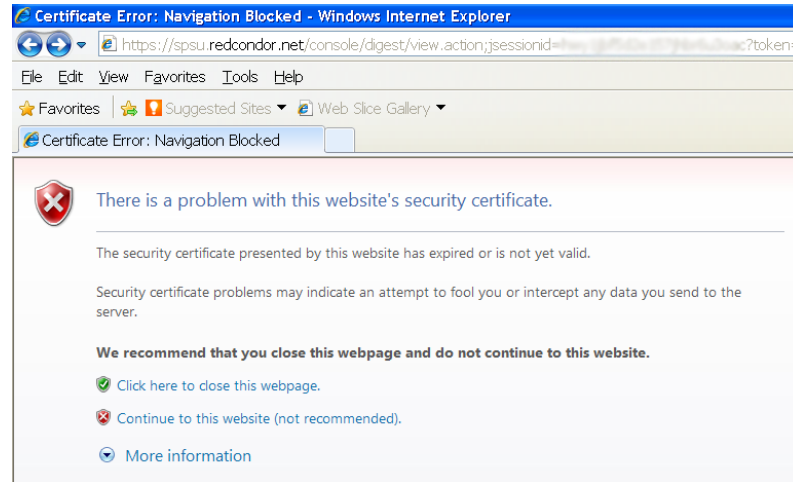
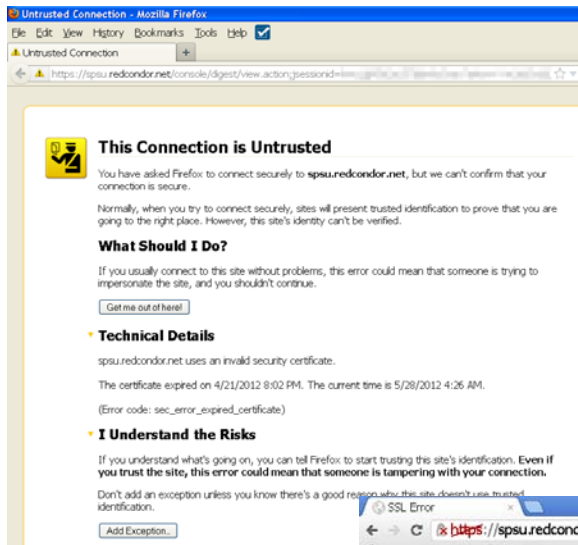
We must trust that:

- The CA has correctly identified the principal (not very hard)
- The CA's private key has not been compromised:
 - Theft of the key
 - Subversion of the CA's mechanisms
- This does not scale well... the more CAs there are the more opportunities for sub-version

Lifetimes of Certificates and Keys

- Trade off: security vs. overhead
- Renewal of certificate
 - Original keys, new certificate
 - New keys and certificate

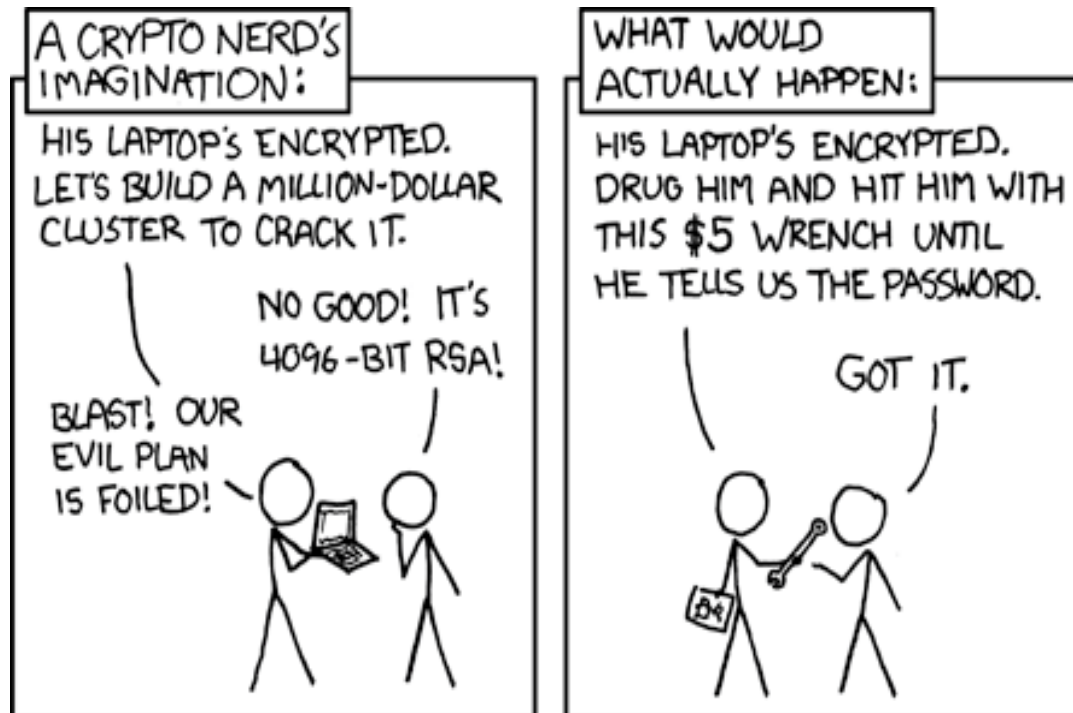
Expired Certificate



Revoked Certificates

- What happens if a private key is known to be compromised? (The digital certificate still looks OK, but is no longer safe, that's what!)
- Certificate authorities maintain *revocation lists* to revoke compromised keys.
- The client software using the certificate must check the revocation list.

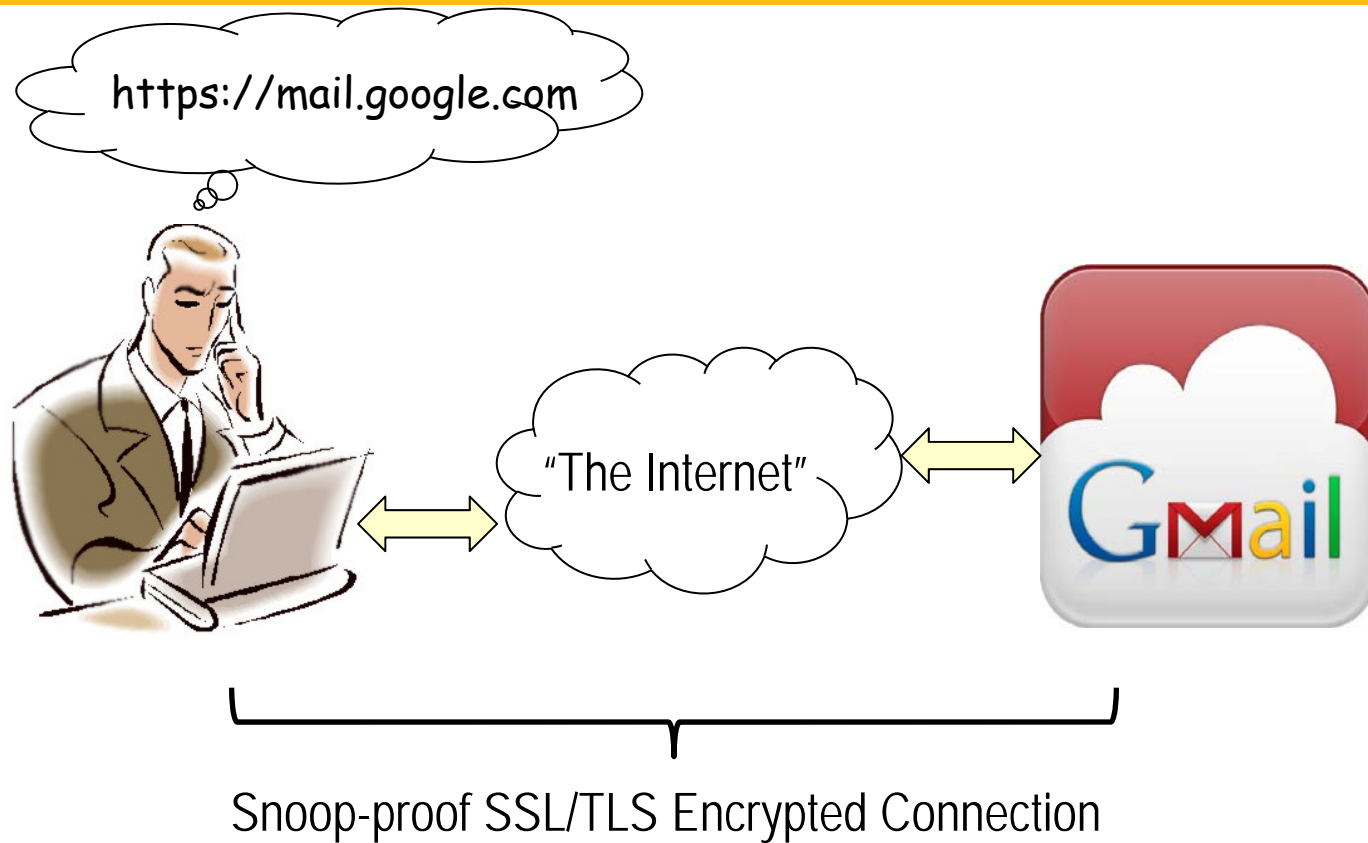
About Attacks on Cryptography



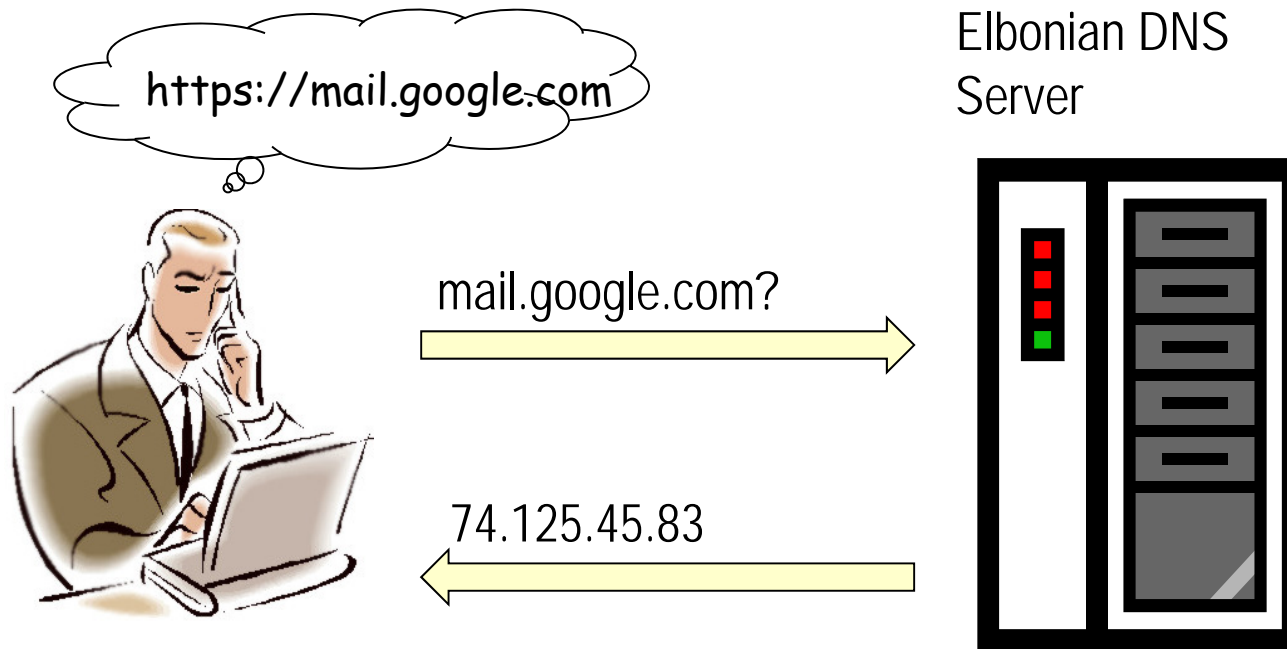
Man-in-the-Middle Scenario

- George lives in Elbonia and has a Gmail account.
- The Elbonian Minister of Peace and Benevolence suspects that radicals are using Gmail to upset the peaceful benevolence of Elbonia. He wants to catch them!
- There's only one ISP in Elbonia, and it is run by the government.

George Reads His Gmail

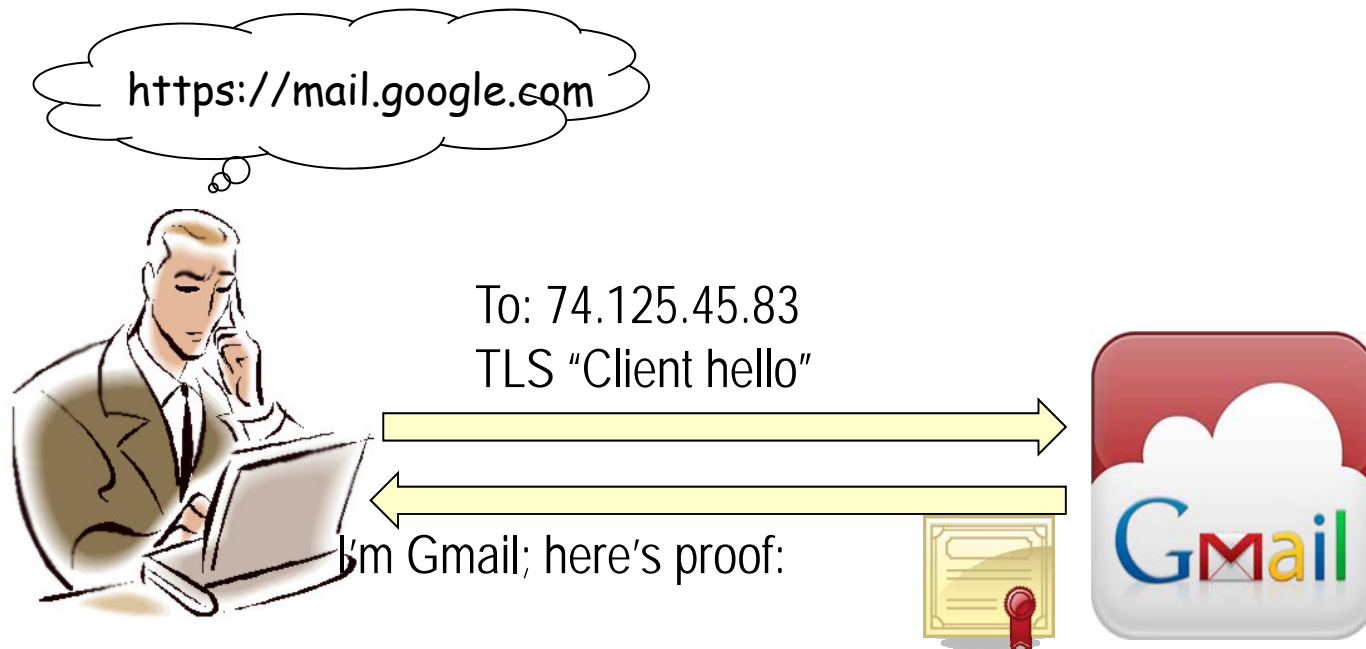


What Really Happens – Step 1



George's computer asks the Domain Name System for the IP address of `mail.google.com` and receives an answer.

What Really Happens – Step 2



George's browser contacts Gmail at the address from DNS and asks for an encrypted connection. Gmail replies with a digital certificate.

That Digital Certificate

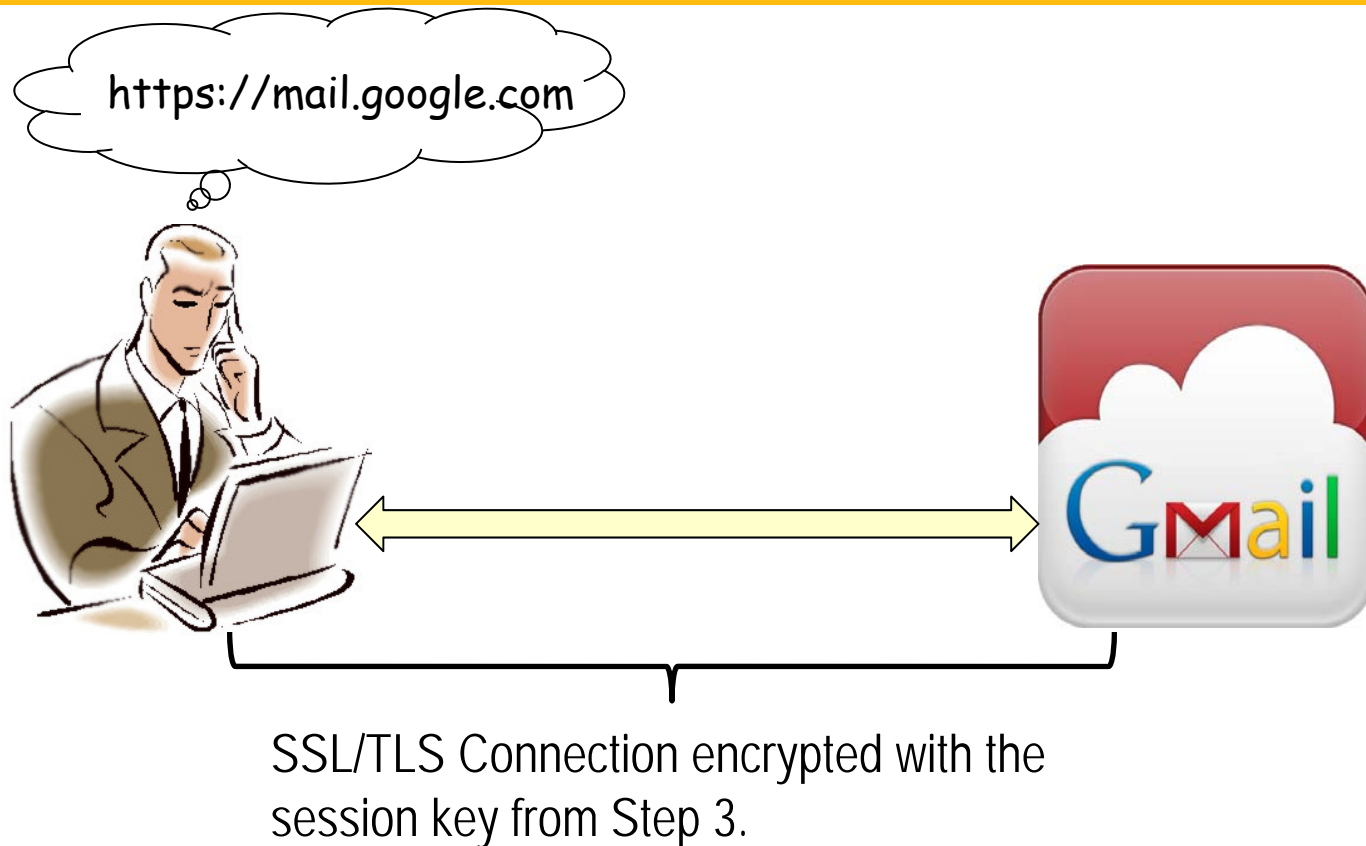
mail.google.com	Identifier
a47fk8smkkl2#*doru mnw\$gj&@mq^[poq ;?fghq	Public key (Google holds the corresponding private key.)
Verisign	Certificate Authority ID
Expiration, etc.	Other information
Digital Signature	Signed with CA's <i>private</i> key.

What Really Happens – Step 3



George's browser validates the digital certificate.
If all is OK, sends a "premaster secret" to Gmail.

What Really Happens – Step 4

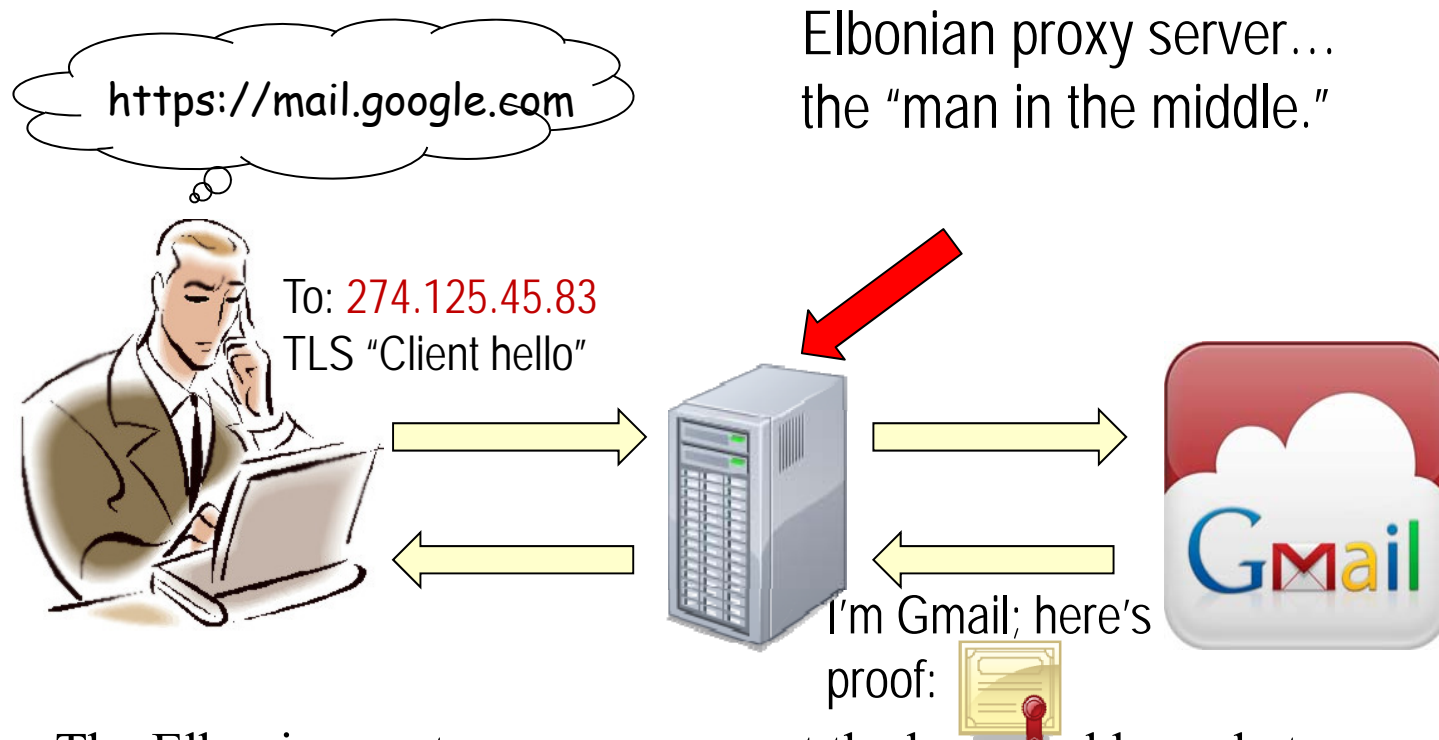


The Attack – Step 1



George's computer asks the Domain Name System for the IP address of mail.google.com and receives a bogus address from the Elbonian DNS server

The Attack – Step 2

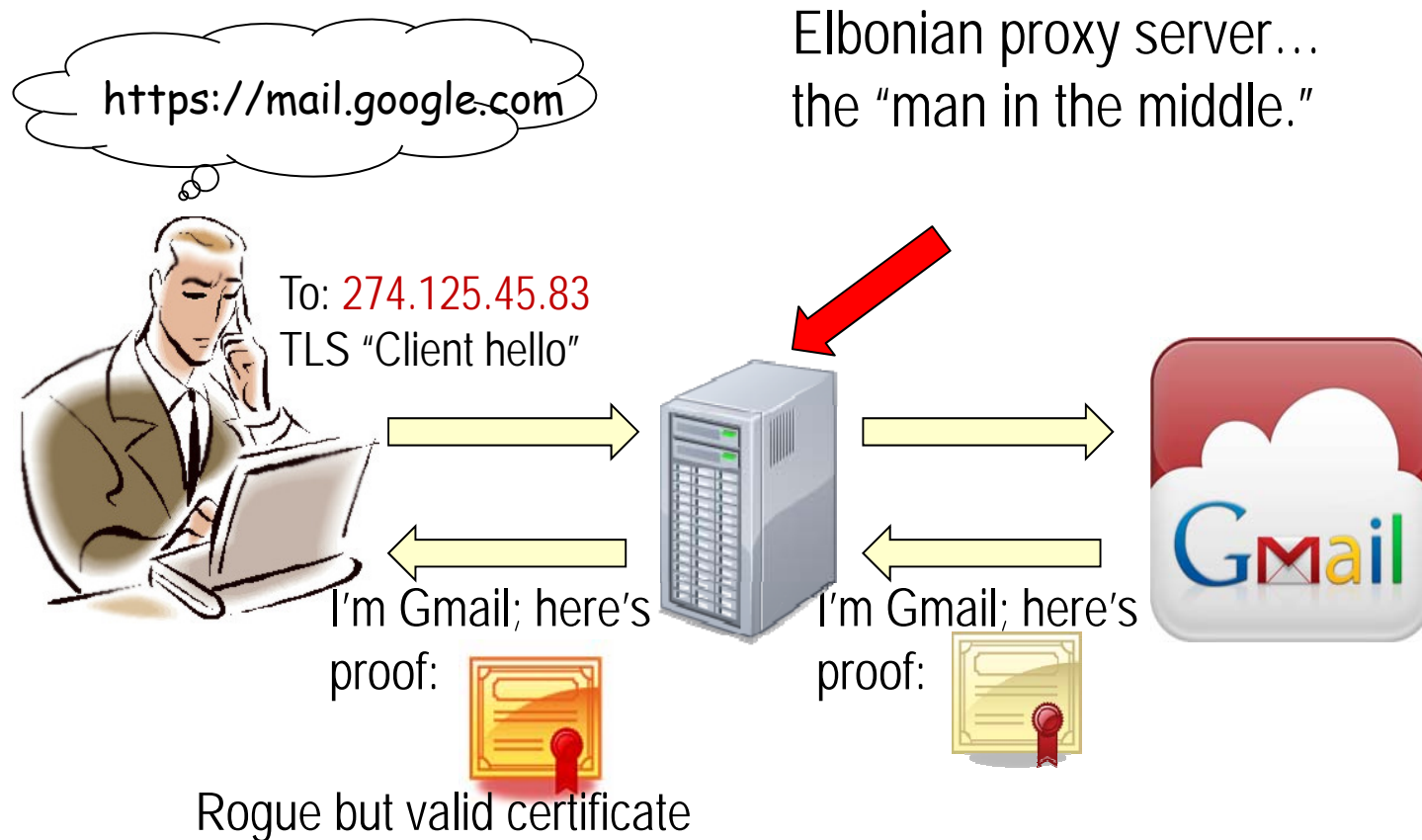


The Elbonians put a proxy server at the bogus address, between George and Gmail. Communication is still secure, though.

A Rogue (but “Valid”) Digital Certificate

mail.google.com	Identifier
b38fj6fgauki\$%utjlc] *8:!as8mmqwr&&*d gtlkyuzx	Public key (Elbonia holds the corresponding private key.)
DigiNotar	Certificate Authority ID
Expiration, etc.	Other information
Digital Signature	Signed with DigiNotar’s <i>private</i> key.

The Attack – Step 3



The Result

- George is talking to a proxy server that identifies itself as Gmail through a valid but rogue digital certificate.
- The proxy can decrypt all data on the connection to George, including George's password.
- The proxy server talks to Gmail, pretending to be George.
- The confidentiality of George's Gmail account is *completely* compromised.

Multi-Factor Authentication

- We will discuss the three factors that can prove identity:
 - Something you know
 - Something you have
 - Something you are.
- Google and others implement two-factor authentication.
- If a service you use has two-factor authentication, *turn it on!*

Certificate Pinning

- Certificate pinning and public key pinning are “trust on first use” measures that can help mitigate even a man in the middle attack by a government.
- The first time George’s browser connects to Gmail, it “pins” (saves) the digital certificate.
- If a rogue certificate is presented later, the browser can warn George.

Web of Trust

- A digital certificate signed by a CA has only one signature; if it's bad, security is toast.
- What if we could have a certificate signed by several trusted parties?
- They'd all have compromised to compromise a public key.
- That is Phil Zimmerman's "web of trust."

Brown's Public Key

Public Key Server -- Verbose Index ``0x203F73FE'' - Mozilla Firefox

http://pgp.mit.edu:11371/pks/lookup?op=vindex&search=0x203F73FE

Public Key Server -- Verbose Index ``0x203F73FE''

Type	bits /keyID	Date	User ID
pub	1024D/203F73FE	2003/09/06	Robert L. (Bob) Brown < bbrown@spsu.edu >
sig	CA57AD7C		PGP Global Directory Verification Key
sig	CA57AD7C		PGP Global Directory Verification Key
sig	CA57AD7C		PGP Global Directory Verification Key
sig	CA57AD7C		PGP Global Directory Verification Key
sig	CA57AD7C		PGP Global Directory Verification Key
sig	203F73FE		Robert L. (Bob) Brown < bbrown@spsu.edu >
			Robert L. (Bob) Brown < robebrow@nova.edu >
sig	CA57AD7C		PGP Global Directory Verification Key
sig	CA57AD7C		PGP Global Directory Verification Key
sig	CA57AD7C		PGP Global Directory Verification Key
sig	CA57AD7C		PGP Global Directory Verification Key
sig	CA57AD7C		PGP Global Directory Verification Key
sig	CA57AD7C		PGP Global Directory Verification Key
sig	CA57AD7C		PGP Global Directory Verification Key
sig	CA57AD7C		PGP Global Directory Verification Key
sig	CA57AD7C		PGP Global Directory Verification Key
sig	CA57AD7C		PGP Global Directory Verification Key
sig	9F6B4075		James Cannady < j.cannady@computer.org >
sig	203F73FE		Robert L. (Bob) Brown < bbrown@spsu.edu >

Transitive Trust

- Do you trust any entity that has signed the key?
- If so, you can trust that you have Brown's real key.
- No? Read on...

Do You Trust Any of These People?

Type	bits	/keyID	Date	User ID
pub	1024D	9F6B4075	2000/08/18	James Cannady <j.cannady@computer.org>
sig		8B4608A1		Peter Nai Wan <peter.wan@cc.gatech.edu>
sig		09590CFD		Peter Nai Wan KeyID: 09590CFD
sig		6916C873		Peter Nai Wan <peter.wan@cc.gatech.edu>
sig		603A8C1F		(Unknown signator, can't be checked)
sig		5E5850CC		(Unknown signator, can't be checked)
sig		0E7AC0C1		(Unknown signator, can't be checked)
sig		AB951161		(Unknown signator, can't be checked)
sig		2E53A2AA		Mercy M. Fung <fungmerc@nova.edu>
sig		1072F7A0		Merrick Wright <mwrwright@sprintmail.com>
sig		27B9EACB		Raymond E LaCasse <raymond.lacasse@prodigy.net>
sig		82558B15		Dinesh Khialani <khialani@nova.edu>
sig		E661281D		Xuansong Li <lixuanso@scis.nova.edu>
sig		F0B5772B		(Unknown signator, can't be checked)
sig		54FD9104		(Unknown signator, can't be checked)
sig		D37AF273		Cleo Cannady <cleo@kuiper.scis.nova.edu>
sig		DFB52ECA		William P. Cantor <cantorw@nova.edu>
sig		08576C19		Yehia Hamze <yehiahamze@hotmail.com>
sig		5288E079		Elizabeth Kay Hawthorne <ehawthorne@acm.org>
sig		CA64E927		(Unknown signator, can't be checked)
sig		F194EA37		Janice Swiatek-Kelley <swiatekk@nova.edu>

Transitive Trust

- Do you trust any of the people who have signed Dr. Cannady's key? If so, you can trust that you have Brown's real key.
- This is **transitive trust**.

Other Public Key Algorithms

- The public key algorithm we've studied is the RSA algorithm.
- In the RSA algorithm, the keys are cryptographic inverses of one another.
- There are other public key cryptography algorithms for which that is not the case.
- Those other algorithms cannot be used for digital signatures in the way we've discussed.

Cryptography, Keys, and the Law

Important points:

- I am not a lawyer.
- I cannot and will not give you legal advice.
- Good common-sense advice:
 - Do not possess illegal material.
 - If you think you need a lawyer, you do!

On Giving Up Encryption Keys

(The cases refer to these as “passwords.”)

- United States v. Kirschner, U.S. District Court, Eastern District of Michigan, Southern Division, March 30, 2010
- Defendant accused of receipt of child pornography, grand jury subpoena to provide all passwords for computer and any files.
- Subpoena quashed; defendant did not have to provide passwords.

The Other Side of the Coin

- In Re Boucher, United States District Court for the District of Vermont. Nov. 29, 2009.
- Boucher was stopped on entry to the U.S. and asked to turn on his laptop computer.
- Customs agents observed what appeared to be child pornography. Boucher arrested, laptop seized.
- A partition on the drive was encrypted; a subpoena demanded the password from Boucher. Boucher pleads the fifth.

The Other Side of the Coin

- Magistrate judge agreed; government appealed.
- The District Court ruled that the subpoena is valid and Boucher must provide the contents of the encrypted drive (partition.)
- Differences:
 - He had already allowed access once; the result was a “foregone conclusion.”
 - The demand was for the “contents, unencrypted” and not for the password.
- The Supreme Court will eventually decide.

The Other, Other Side

- Feds seized a laptop computer from Ramona Fricosu, who was accused of fraud.
- It's encrypted. (Surprise!)
- U.S. District Judge Robert Blackburn ordered Fricosu to decrypt, on penalty of contempt.
- Fricosu pleads the Fifth; Blackburn isn't moved and Ramona Fricosu goes to jail.
- The case appeared headed for a Federal Appeals Court, with Fricosu in jail.

However...

- The Feds “crack” the encryption on Fricosu’s computer, rendering the court order moot.
- Speculation: They probably didn’t really crack the encryption; Fricosu’s ex husband is a co-defendant and is cooperating with the prosecution. He either had or helped investigators guess the password or phrase.
- The government “became able” to “crack” the encryption just after the 11th U.S. Circuit Court of Appeals ruled that forcing a suspect to decrypt a hard drive is unconstitutional.

Still Another Side

- U.S. Magistrate Judge William Callahan (Wisconsin) ruled that requiring Jeffrey Feldman to decrypt data or hand over a pass phrase violated Feldman's First Amendment rights.
- Time passes... the Feds “crack” the encryption on one drive, find child porn.
- Judge Callahan then ordered Feldman to decrypt the rest of the drives under the “foregone conclusion” theory, May, 2013.
- June 4, 2013: District Judge Rudolph Randa temporarily stays Judge Callahan's order.

Still Another Side (Continued)

- August 16, 2013: Federal prosecutors withdraw the order compelling Feldman to decrypt his disk drives.
- Reason: the material on the drives they “cracked” is enough to prosecute Feldman.
- Speculation: The Feds did not “crack” the encryption; they guessed a password or passphrase.
- Prosecutors want to avoid another Fifth Amendment ruling if possible.

The 11th Circuit Case

- “John Doe” is suspected of possessing child pornography on several encrypted disk drives.
- A Florida Federal grand jury issued a subpoena ordering “Doe” to decrypt the material.
- “Doe” pleads the Fifth and refuses. He is sent to jail for contempt.
- The 11th Circuit Court of Appeals (Atlanta) rules that “Doe” is protected by the Fifth Amendment, March, 2011.

The End Result

- ... is not known.
- There will be an eventual appeal to the Supreme court, which will rule on whether passwords or passphrases are protected under the Fifth Amendment.
- Common sense advice:
 - Do not possess illegal material.
 - Use strong passwords.
 - Assume, at least for now, that you will go to jail for contempt if you do not give up the password.

Border Searches

- March 8, 2013: 9th Federal Circuit Court of Appeals upheld the conviction of Howard Cotterman for possession of child pornography.
- Customs agents performed a “forensic examination” of his computer upon his return from Mexico
- The Court ruled that the “presence of password protected files” (presumably encrypted) plus Cotterman’s earlier conviction provided “reasonable suspicion” to justify the search.

Search Incident to Arrest

- Objects in your “immediate possession” can be searched if you are arrested.
- “Immediate possession” includes the interior of a car, but not the trunk.
- Thus, your laptop could be searched if you are stopped for a traffic violation.
- Common sense advice:
 - Do not possess illegal material.
 - Keep your laptop in the trunk.
 - Use strong passwords.

Cell Phones

- In June, 2014, The Supremes ruled that a warrant is necessary to search a cell phone, even incident to arrest.
- The Supremes got involved when Federal appeals courts contradicted one another.
- You should *still* protect your phones with strong passwords.

Only in the United States

U.S. law does not apply in other countries.
Example, in the U.K., one *can* be required to
produce encryption keys.

Can “They” Crack *Your* Key?

- Yes, or at least they can try, just as (with a warrant), “they” can drill open your safe.
- However, “good” modern cryptosystems (*e.g.* TrueCrypt, GPG) are extremely difficult to crack.
- Not all cryptosystems are “good.” Example: most smart phones have well-known vulnerabilities.
- Passwords or phrases are the greatest vulnerability for “good” cryptosystems.
- Common sense advice:
 - Do not possess illegal material.
 - Use strong pass phrases.

Questions

