

Secure Communication



Agenda

- Aspects of Secure Communication
- Cryptography
- Trust
- Lines of Communication
- Risks and Mitigation
- About DeepSec IDSC

Aspects of Secure Communication

Information Networks

- Messengers
- Plain Old Telephone Service (POTS)
- Radio Communication
- Internet
- GSM family (2G/3G)
- Private / closed networks (wired/wireless)

Information Security

- Confidentiality
 - Does someone else know?
- Integrity
 - Did someone tamper with the message?
- Authenticity
 - Are you real?
- Non-repudiation
 - Can you deny having sent the message?
- *Pick any three.* ☺

Cryptography

- Origin of the term
 - κρυπτός, kryptos - „hidden”, „secret”
 - γράφω, gráphō - „I write”
- Mix of computer science, mathematics, engineering
- Used for 4500+ years
- Driven by military and governments
- Widespread today
 - Computers, PDAs, cell phones, ...

Basic Cryptography

- Requirements
 - I. Algorithm
 - II. Cryptographic key
 - III. Message (plaintext \rightleftarrows ciphertext)
- Attacker usually knows algorithm or ciphertext
- Key must be protected

Basic Cryptography

- **Symmetric encryption**
 - Encryption/decryption use the same key
 - Key per sender/recipient pair
- **Asymmetric encryption**
 - Encryption uses public key
 - Decryption uses private key
 - Recipient retains private key
 - Senders receive public key of recipients

Applied Cryptography

- Confidentiality
- Integrity
- Authenticity
- Non-repudiation
- Encryption
- Hashes, checksums
- Digital signatures
- Digital signatures

Steganography

- Focus on hiding information
- Message appears to be „normal”
 - Video, audio, text
 - Avoids attracting attention
- Uses methods of cryptography for protection

Possible Goals

- Hide the content of the transmission
 - Encryption, steganography
 - Couple message to identities
- Hide the parties of a conversation
 - Anonymisation, use „crowds”
 - Use hard to trace methods
- Hide the fact that communication takes place
 - Use covers
 - Create random traffic

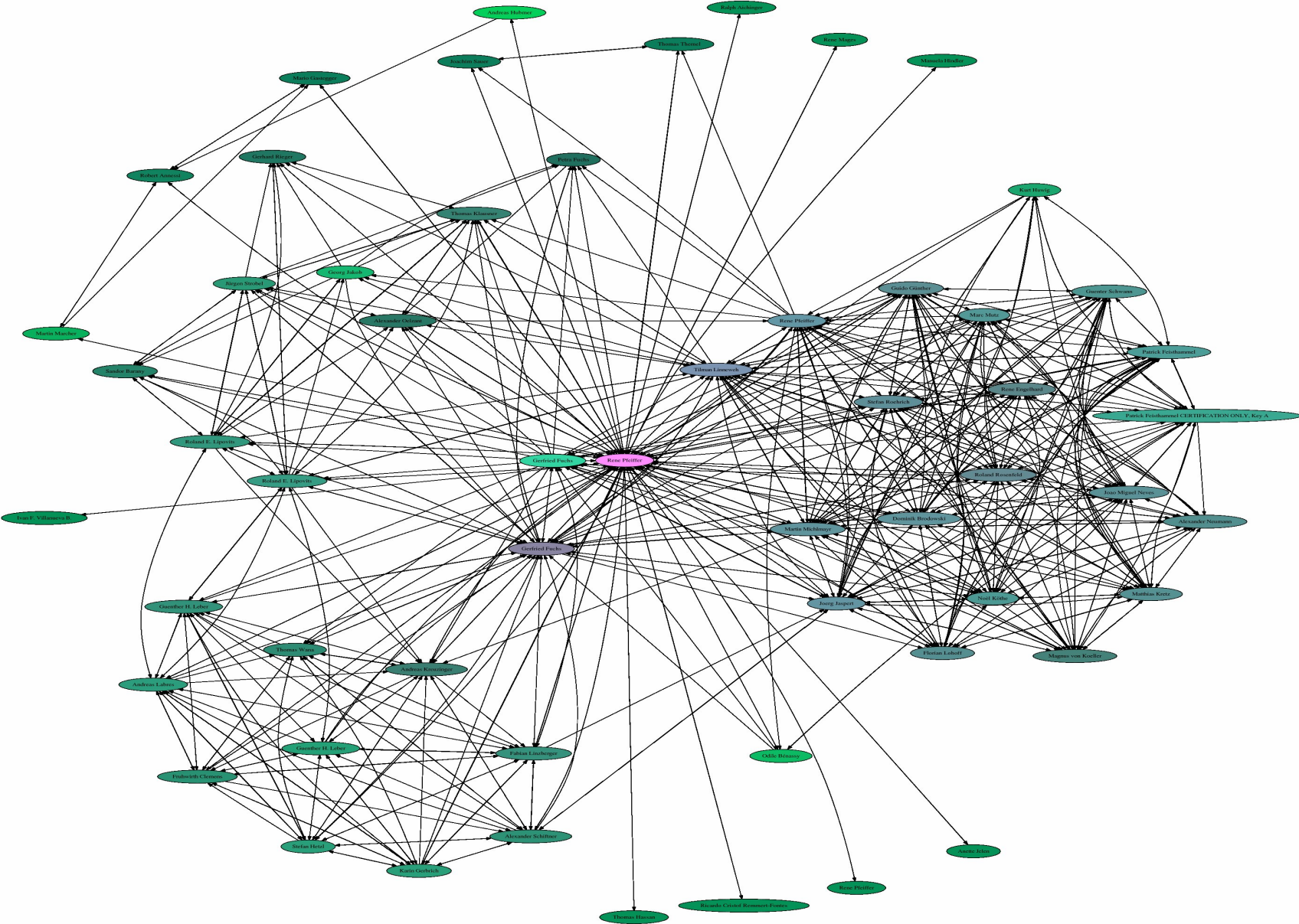
Trust Relationships

- Trust precedes secure communication
 - I. Determine identities*
 - II. Establish a secure channel*
 - III. Communicate*
- Basic methods
 - Public Key Infrastructure (PKI) - centralised
 - Web of Trust - decentralised

Public Key Infrastructure

- Requires central infrastructure
 - X.509 PKIs require signatures from single party (CA)
 - CA is crucial to trust relationship
 - Commercial CAs may be affected by bankruptcy
- Requires strict work flow
 - Verification of identity / certificates
 - Renewal of certificates
 - Revoking certificates

Web of Trust



DeepSec IDSC

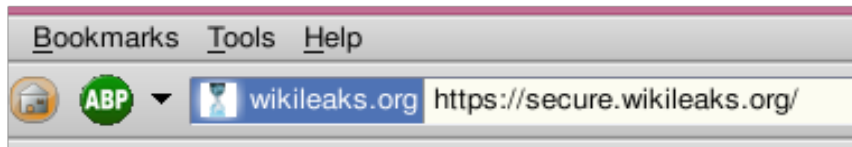
Web of Trust

- Key management done by users
 - Certification, key generation, key revocation
 - Implies to trust all users in trust chain
 - *Key Signing Parties*
- Possibly no common rules for certification
- Trusted CA possible, but not widely used

Secure Socket Layer (SSL)

- Designed by Netscape
 - Known as „HTTPS”
 - Widely deployed apart from the WWW
- Now called Transport Layer Security (TLS)
- Uses symmetric & asymmetric encryption
 - Collection of different algorithms
 - Variable key sizes
- Uses X.509 PKI

SSL/TLS in Action



Secure Connection Failed

www.wikileaks.org uses an invalid security certificate.

The certificate is only valid for secure.wikileaks.org

(Error code: ssl_error_bad_cert_domain)

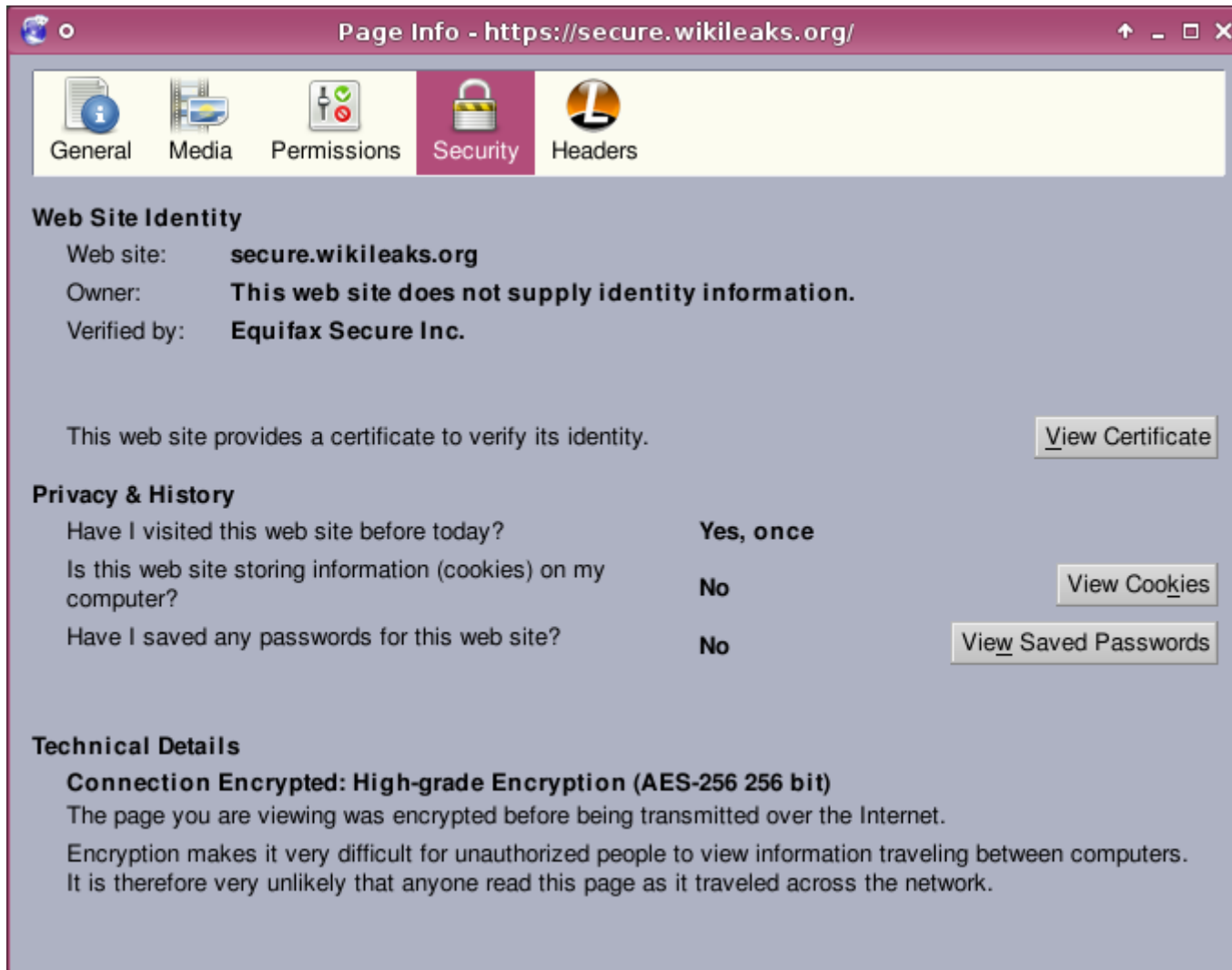
- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

You should not add an exception if you are using an internet connection that you do not trust completely or if you are not used to seeing a warning for this server.

Get me out of here!

Add Exception...

SSL/TLS Information



The screenshot shows a browser window titled "Page Info - https://secure.wikileaks.org/". The "Security" tab is selected, displaying the following information:

Web Site Identity

- Web site: **secure.wikileaks.org**
- Owner: **This web site does not supply identity information.**
- Verified by: **Equifax Secure Inc.**

This web site provides a certificate to verify its identity. [View Certificate](#)

Privacy & History

Have I visited this web site before today?	Yes, once	
Is this web site storing information (cookies) on my computer?	No	View Cookies
Have I saved any passwords for this web site?	No	View Saved Passwords

Technical Details

Connection Encrypted: High-grade Encryption (AES-256 256 bit)

The page you are viewing was encrypted before being transmitted over the Internet. Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

SSL/TLS Certificate

Certificate Viewer: "secure.wikileaks.org"

General Details

This certificate has been verified for the following uses:

- SSL Server Certificate

Issued To

Common Name (CN)	secure.wikileaks.org
Organization (O)	secure.wikileaks.org
Organizational Unit (OU)	GT46622659
Serial Number	08:AB:C2

Issued By

Common Name (CN)	Equifax Secure Global eBusiness CA-1
Organization (O)	Equifax Secure Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

Validity

Issued On	11/06/08
Expires On	12/06/10

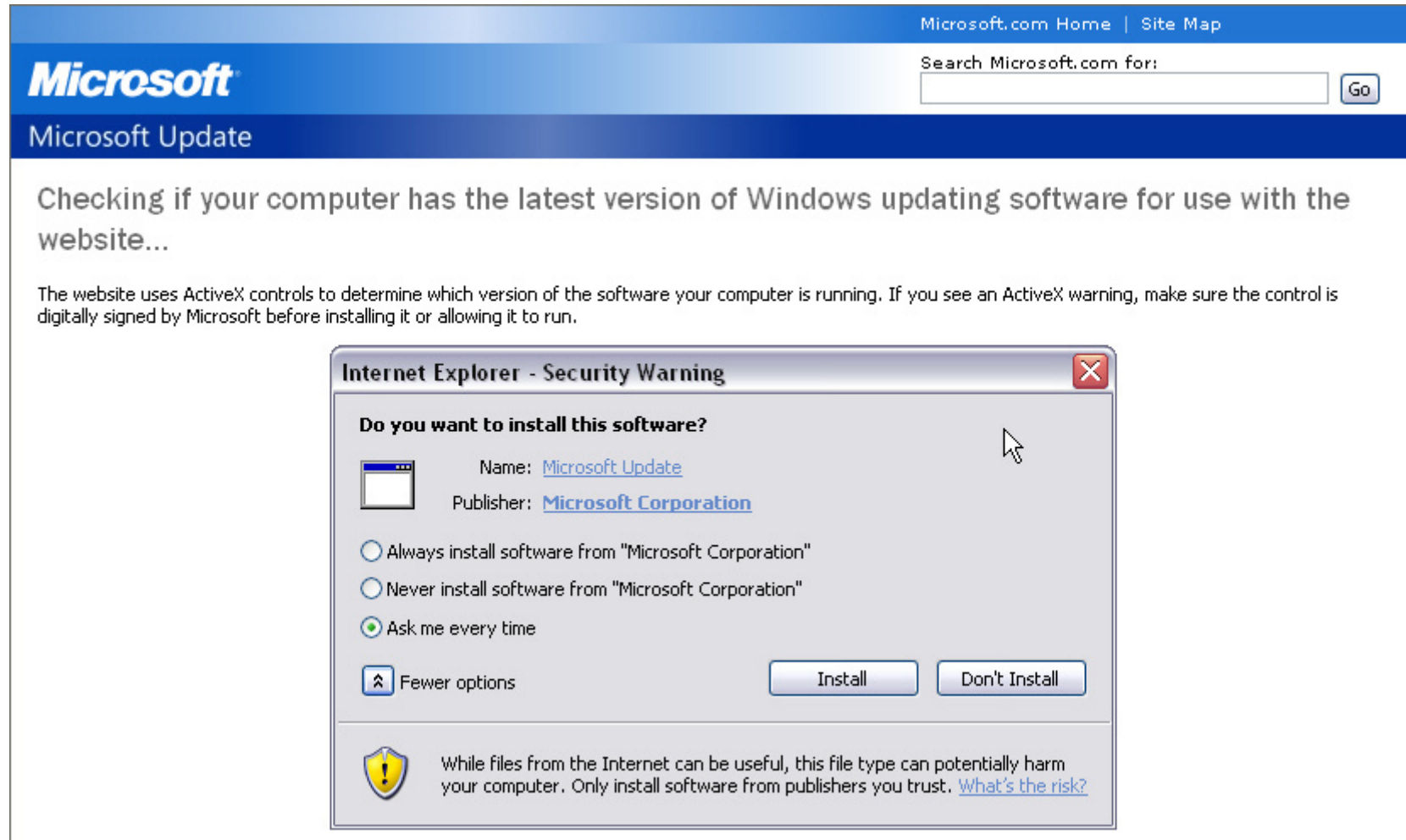
Fingerprints

SHA1 Fingerprint	88:CC:EE:8C:4F:87:3F:5D:8A:88:F1:43:2D:A9:7D:EA:8B:70:B9:07
MD5 Fingerprint	36:64:C6:A0:45:AA:BA:58:F2:79:A3:89:C6:C4:CD:9A

SSL/TLS Automatic Trust

Certificate Name	Security Device
▼ (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.	
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	Builtin Object Token
▼ ABA.ECOM, INC.	
ABA.ECOM Root CA	Builtin Object Token
▼ AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token
▼ AddTrust AB	
AddTrust External CA Root	Builtin Object Token
AddTrust Class 1 CA Root	Builtin Object Token
AddTrust Public CA Root	Builtin Object Token
AddTrust Qualified CA Root	Builtin Object Token
▼ America Online Inc.	
America Online Root Certification Authority 1	Builtin Object Token
America Online Root Certification Authority 2	Builtin Object Token
▼ AOL Time Warner Inc.	
AOL Time Warner Root Certification Authority 1	Builtin Object Token
AOL Time Warner Root Certification Authority 2	Builtin Object Token
▼ Autoridad de Certificacion Firmaprofesional CIF A62634068	
Autoridad de Certificacion Firmaprofesional CIF A62634068	Builtin Object Token
▼ Baltimore	
Baltimore CyberTrust Root	Builtin Object Token
▼ beTRUSTed	
beTRUSTed Root CA	Builtin Object Token

SSL/TLS outside the Web



The screenshot shows a Microsoft website page with a blue header. The header contains the Microsoft logo, a search bar with the text "Search Microsoft.com for:", and a "Go" button. Below the header, the page title is "Microsoft Update". The main content area displays the text "Checking if your computer has the latest version of Windows updating software for use with the website..." followed by a paragraph: "The website uses ActiveX controls to determine which version of the software your computer is running. If you see an ActiveX warning, make sure the control is digitally signed by Microsoft before installing it or allowing it to run."

Overlaid on the page is an "Internet Explorer - Security Warning" dialog box. The dialog box has a title bar with a close button (X). The main text asks "Do you want to install this software?". Below this, there is a small icon of a window, the name "Microsoft Update", and the publisher "Microsoft Corporation". There are three radio button options: "Always install software from 'Microsoft Corporation'", "Never install software from 'Microsoft Corporation'", and "Ask me every time" (which is selected). At the bottom left, there is a "Fewer options" button with an upward-pointing arrow. At the bottom right, there are "Install" and "Don't Install" buttons. At the very bottom, there is a warning icon (a shield with an exclamation mark) and a text block: "While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. [What's the risk?](#)"

SSL/TLS in Practice

- Who verifies certificates?
 - Check URL?
 - Check domain(s)?
 - Check digital fingerprints (hashes)?
- What do you do when your browser warns you?
- Do all devices issue proper warnings?
- Do all CAs follow proper procedures?
- Is your SSL software free of bugs?

SSL/TLS Bugs

- 25C3: [Attacking MD5](#)
 - Create a rogue CA
 - MITM
- [Null bytes](#) in certificate identity
 - [www.paypal.com\0thoughtcrime.org](#)
 - [*\0thoughtcrime.org](#)

Well...

- Secure communication can be hard
 - You don't own the key(s)? *You're not safe!*
 - Third party CA? Own CA?
 - Web of trust must be build
- Most technologies protect from passive attacks
- DNS is not secured (no DNS-SSL yet)
- Old protocols still in use (DES, RC4, SSLv2, ...)

Questions?



DeepSec IDSC

The [DeepSec IDSC](#) is an annual European two-day in-depth conference on computer, network, and application security. The mission statement is to bring together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. DeepSec aims to be a strictly neutral platform and a meeting point for everyone involved in security.

Contact: Michael Kafka & René Pfeiffer, deepsec@deepsec.net

Copyright Information

- Some rights reserved. / Einige Rechte vorbehalten.
- [DeepSec GmbH](#), Vienna, Austria.
- You may freely use, distribute and modify this work under the following agreement:
 - Authors must be referenced (also for modification) / Autoren müssen genannt werden (auch bei Bearbeitung)
 - Only for non-commercial use / nur für nichtkommerzielle Nutzung
 - Derivative work under the same license / Derivative Arbeit unter derselben Lizenz



Secure Communication



DEEPSEC
In-Depth Security Conference

DeepSec IDSC

1

Secure communication is a major component of commercial, governmental and military information networks. The Internet and the rise of ubiquitous computing has enabled secure communication technologies for the private sector, too. However the implementation of secure communication channels is very difficult and requires strict planning. In addition the communication partners need a fundamental knowledge about what can go wrong and how to verify the security of a communication. This presentation tries to address the problems and discusses experiences from Real Life™.

The images shows a collection of aerials in Graz, Austria.

Agenda

- Aspects of Secure Communication
- Cryptography
- Trust
- Lines of Communication
- Risks and Mitigation
- About DeepSec IDSC

We do not delve deeply into the wonderful world of cryptography and mathematics. For an in-depth discussion you are advised to consult other sources.

Aspects of Secure Communication

Information Networks

- Messengers
- Plain Old Telephone Service (POTS)
- Radio Communication
- Internet
- GSM family (2G/3G)
- Private / closed networks (wired/wireless)

Networks transporting information can assume many shapes. Messengers carrying letters, optical storage, hard-disks or USB-sticks can form an information network. Modern communication usually resorts to the POTS, radio communication (also used for satellite uplinks), the Internet or mobile telephone networks. Apart from public networks there are private networks operated by governments, global corporations, individuals, NGOs or the military (we use this term in its broadest sense and include paramilitary groups as well).

Information Security

- Confidentiality
 - Does someone else know?
- Integrity
 - Did someone tamper with the message?
- Authenticity
 - Are you real?
- Non-repudiation
 - Can you deny having sent the message?
- *Pick any three.* ☺

5

DeepSec IDSC

Most people who think of information security only think of confidentiality. This not even half of the story. Secure communication has more components and the requirements for it go beyond confidentiality. The list shows the major four building blocks of information security.

Cryptography

- Origin of the term
 - κρυπτός, kryptos - „hidden”, „secret”
 - γράφω, gráphō - „I write”
- Mix of computer science, mathematics, engineering
- Used for 4500+ years
- Driven by military and governments
- Widespread today
 - Computers, PDAs, cell phones, ...

To quote from the corresponding [Wikipedia article](#): *Modern cryptography intersects the disciplines of mathematics, computer science, and engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.*

Development of cryptographic methods was often motivated by military applications. The business sector now uses cryptography extensively.

Basic Cryptography

- Requirements
 - I. Algorithm
 - II. Cryptographic key
 - III. Message (plaintext \rightleftharpoons ciphertext)
- Attacker usually knows algorithm or ciphertext
- Key must be protected

7

DeepSec IDSC

Every message starts out as the *plaintext* in decrypted form. By use of an algorithm and one or multiple keys the plaintext is transformed into the *ciphertext*. The ciphertext is usually transmitted over untrusted networks. Thus an attacker has knowledge of the encrypted message and knows probably the algorithm that was used for encryption. The keys are protected from any third party not involved in the trusted communication.

It is common practice to publish every strong cryptographic algorithm in order to find possible flaws through peer review. This is the scientific approach, and every high-quality algorithm in use today is published.

Basic Cryptography

- **Symmetric encryption**
 - Encryption/decryption use the same key
 - Key per sender/recipient pair
- **Asymmetric encryption**
 - Encryption uses public key
 - Decryption uses private key
 - Recipient retains private key
 - Senders receive public key of recipients

8

DeepSec IDSC

We mentioned that encryption/decryption can use one or multiple keys.

Symmetric encryption uses the same key for encryption and decryption. This means that you need one key for all sender/recipient pair (if you want to avoid creating groups that can see all correspondence) and that this key must be safely distributed among all communication partners.

Asymmetric encryption uses one key for encryption and one key for decryption. The encryption key is called the *public key*, and the decryption key is called the *private key*. Communication partners only need to (safely) distribute their public key. This facilitates key management, but it doesn't quite solve the problem of secure key exchange.

The **Diffie–Hellman–Merkle key exchange** is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. It is widely used to exchange parameters for subsequent encryption/decryption algorithms. It is a corner stone for securing data transmissions. Despite the key exchange the parties still have to make sure that their identity is correct.

Applied Cryptography

- Confidentiality
- Integrity
- Authenticity
- Non-repudiation
- Encryption
- Hashes, checksums
- Digital signatures
- Digital signatures

The tables shows how the requirements for secure communication can be addressed by the use of cryptography. Encryption was already discussed. The integrity can be verified by the use of checksums or cryptographic hash functions. These hashes transform any amount of data into a unique value that can be used as a digital fingerprint. The modification of a single bit of information leads to a different hash value. Any changes can be detected by this method.

Authenticity and non-repudiation can be achieved by digital signatures. In essence these signatures are hashes tied to the content of the message, the (private) key of the sender and possibly the date/time of the message's creation. Recipients can then verify the authenticity by means of the sender's (public) key.

Steganography

- Focus on hiding information
- Message appears to be „normal”
 - Video, audio, text
 - Avoids attracting attention
- Uses methods of cryptography for protection

Steganography's primary goal is to hide messages in other messages. The idea is to use plausible cover data such as pictures, text collections, audio or video files. This way the ciphertext doesn't attract much attention and may be overlooked. In other respects the protection of the message is done by cryptographic means.

Possible Goals

- Hide the content of the transmission
 - Encryption, steganography
 - Couple message to identities
- Hide the parties of a conversation
 - Anonymisation, use „crowds“
 - Use hard to trace methods
- Hide the fact that communication takes place
 - Use covers
 - Create random traffic

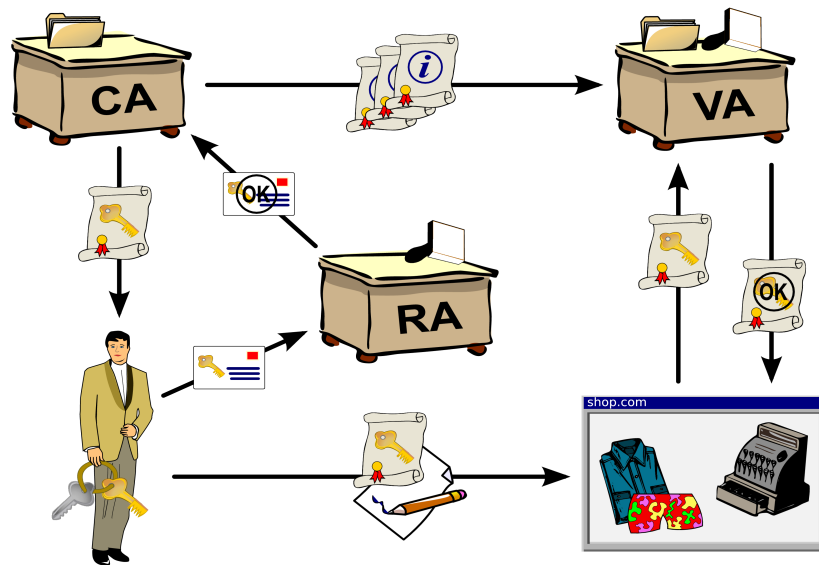
Before thinking about the implementation it is wise to have some idea what to protect against. Depending on the requirements the solutions are different.

Trust Relationships

- Trust precedes secure communication
 - I. Determine identities*
 - II. Establish a secure channel*
 - III. Communicate*
- Basic methods
 - Public Key Infrastructure (PKI) - centralised
 - Web of Trust - decentralised

Trust relationships are a very important component of secure communication. In order to avoid *man-in-the-middle* attacks (MITM) the identity of the communication partners needs to be verified. In case of one-way communication the sender must take care to use the correct key of the recipient. Essentially this requires a secure and trusted key exchange in advance of the communication.

Public Key Infrastructure



13

DeepSec IDSC

A Public Key Infrastructure (PKI) consists of a *Registration Authority (RA)*, a *Certificate Authority (CA)* and a *Verification Authority (VA)*. Every user wishing to take part in the communication network needs to register at the RA where the identity of the user is verified. The request is forwarded to the CA who issues a certificate of the user's cryptographic key(s). The key(s) in combination with the certificate are used for secure communication (the key(s) for encryption, the certificate for identity checks).

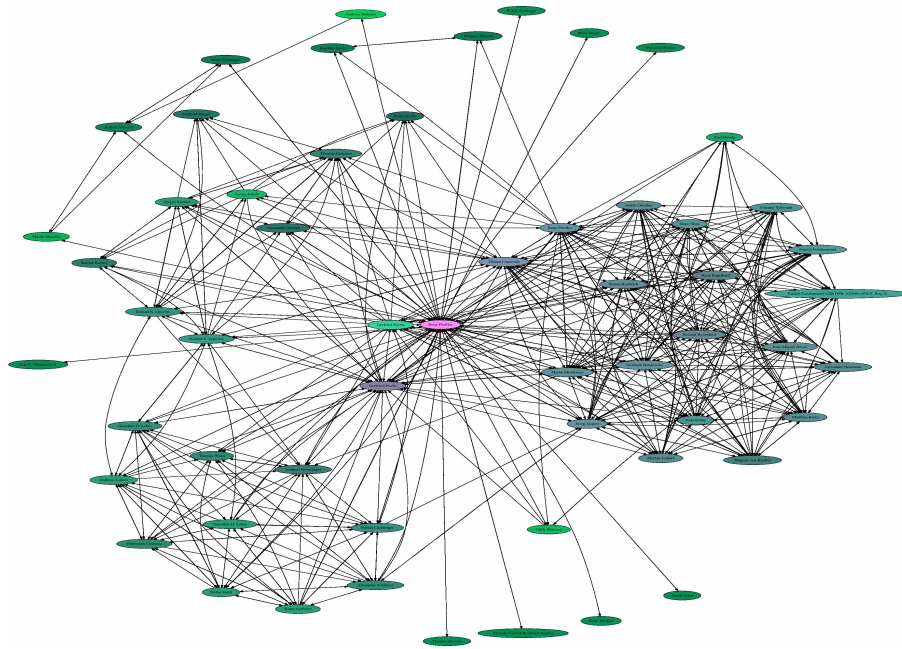
The illustration shows an example data transmission with a digital shop system. The shop server can check the user's certificate and verify if it was really issued by the PKI's own CA. This is done by the VA which in turn is supplied by the CA with information about valid and revoked certificates.

Public Key Infrastructure

- Requires central infrastructure
 - X.509 PKIs require signatures from single party (CA)
 - CA is crucial to trust relationship
 - Commercial CAs may be affected by bankruptcy
- Requires strict work flow
 - Verification of identity / certificates
 - Renewal of certificates
 - Revoking certificates

A PKI has its advantages and disadvantages.

Web of Trust



DeepSec IDSC

15

The graphic shows the web of trust for the author's [GPG](#) key (shown in pink). Every line depicts a trust relationship between GPG key owners. It is created by certificates signed by individual users after a meeting and verification of trust criteria. Trust can be expressed in varying degrees since it is possible to trust the authenticity of a public key if someone else trusts it. Despite its local nature the web of trust can also use the concept of certificate authorities (CAs). These CAs must be represented by keys and can issue trust certificates just like any other user.

Web of Trust

- Key management done by users
 - Certification, key generation, key revocation
 - Implies to trust all users in trust chain
 - *Key Signing Parties*
- Possibly no common rules for certification
- Trusted CA possible, but not widely used

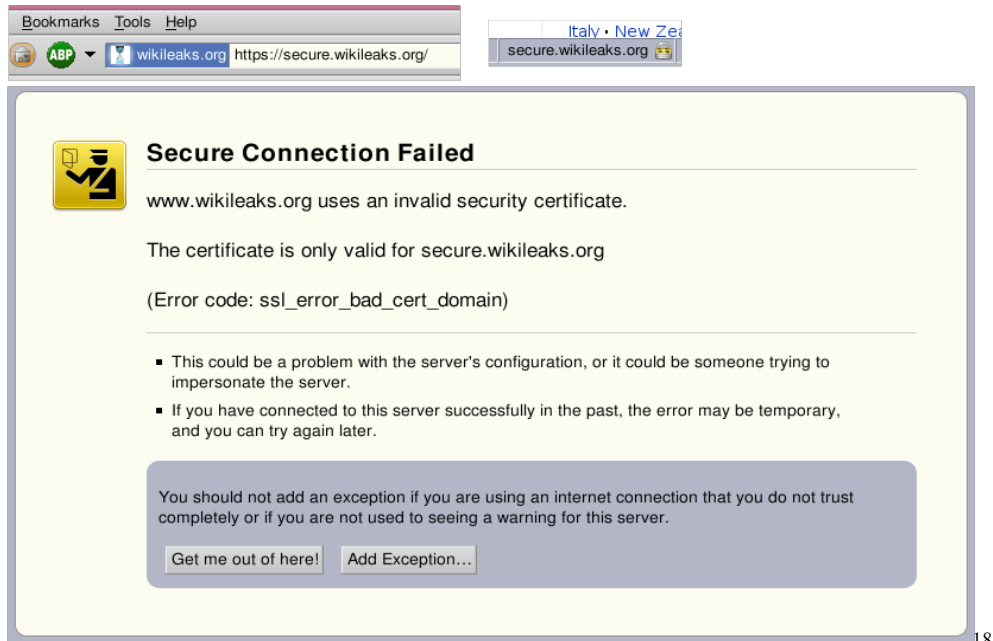
The main problem of the web of trust is the lack of unified criteria for key certification. If someone is sloppy or makes a mistake, then MITM attacks are possible (similar to introducing informers into groups). Another problem might be the visibility of the signatures. It might be a sign that users have met, thus compromising anonymity or relationships between individuals.

Secure Socket Layer (SSL)

- Designed by Netscape
 - Known as „HTTPS”
 - Widely deployed apart from the WWW
- Now called Transport Layer Security (TLS)
- Uses symmetric & asymmetric encryption
 - Collection of different algorithms
 - Variable key sizes
- Uses X.509 PKI

Transport Level Security (TLS) consists of a collection of cryptographic protocols that provide secure communication over networks. It is the most used standard for web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP). Communication partners need a private key, a certificate from a CA for this key and certificates from other CAs in order to verify the identity.

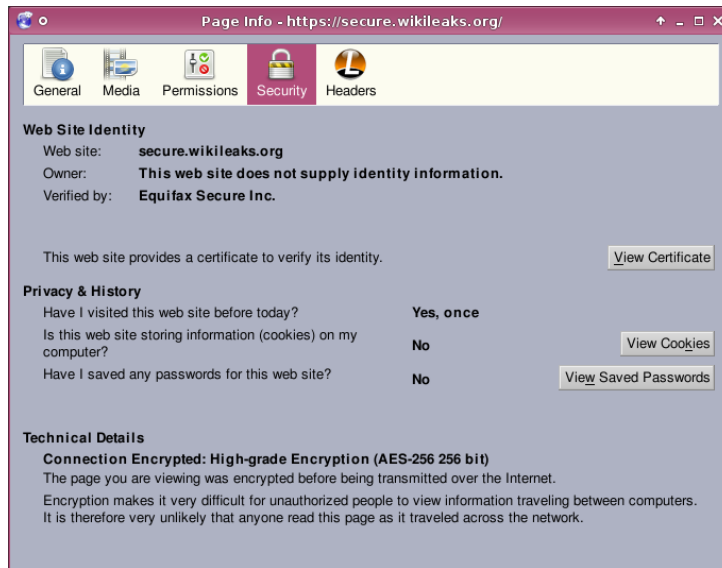
SSL/TLS in Action



DeepSec IDSC

The screen shots show two different scenarios when using SSL/TLS in the Mozilla Firefox / Debian Iceweasel web browser. The first two pictures show a properly encrypted connection with a verified identity. The field next to the URL <https://secure.wikileaks.org/> shows the domain, and in the bottom right corner the lock symbol shows the certified name secure.wikileaks.org. If you use <https://www.wikileaks.org/> instead, then the browser issues a warning because www.wikileaks.org does not correspond to the name secure.wikileaks.org in the cryptographic certificate. The user can bypass the warning and accept the connection by overruling the check. This can be exploited by social engineering attacks, and users can be led to malicious web sites. Encryption alone doesn't protect you if you ignore the warnings about the web site's identity.

SSL/TLS Information



19

DeepSec IDSC

Inspection of the secure.wikileaks.org certificate provides no insight into the ownership of the domain, web site or server. The certificate was issued by Equifax Secure Inc. The connection uses the best encryption mode (AES with 256 bit symmetric key).

SSL/TLS Certificate



20

DeepSec IDSC

The details of the certificate reveal a serial number, the CA that has issued the certificate (Equifax Secure Global Business CA-1), the date when it was issued, the expiration date and two digital fingerprints (MD5 and SHA-1). You can use this information in order to contact the CA and verify if this information is correct and was processed by the CA.

Expired certificates should never be used and trusted (yet people do).

SSL/TLS Automatic Trust

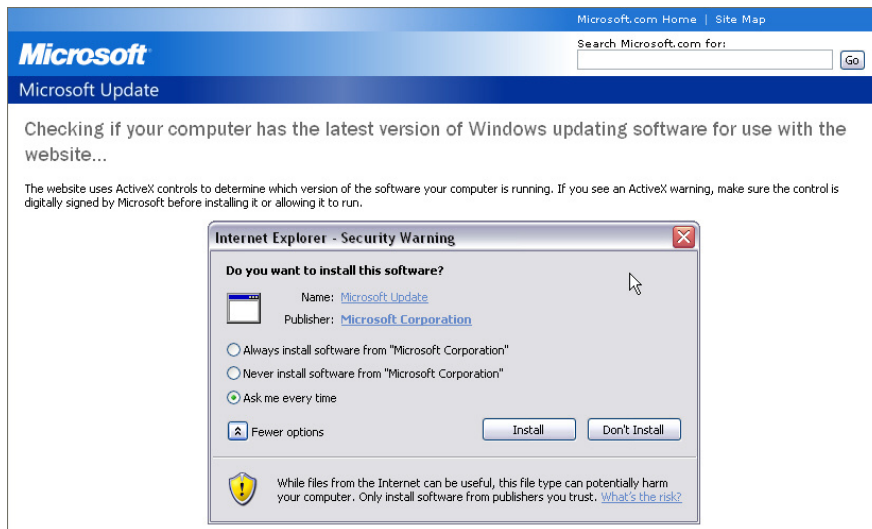
Certificate Name	Security Device
▼ (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.	
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	Built-in Object Token
▼ ABA.ECOM, INC.	
ABA.ECOM Root CA	Built-in Object Token
▼ AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Built-in Object Token
Global Chambersign Root	Built-in Object Token
▼ AddTrust AB	
AddTrust External CA Root	Built-in Object Token
AddTrust Class 1 CA Root	Built-in Object Token
AddTrust Public CA Root	Built-in Object Token
AddTrust Qualified CA Root	Built-in Object Token
▼ America Online Inc.	
America Online Root Certification Authority 1	Built-in Object Token
America Online Root Certification Authority 2	Built-in Object Token
▼ AOL Time Warner Inc.	
AOL Time Warner Root Certification Authority 1	Built-in Object Token
AOL Time Warner Root Certification Authority 2	Built-in Object Token
▼ Autoridad de Certificación Firmaprofesional CIF A62634068	
Autoridad de Certificación Firmaprofesional CIF A62634068	Built-in Object Token
▼ Baltimore	
Baltimore CyberTrust Root	Built-in Object Token
▼ beTRUSTed	
beTRUSTed Root CA	Built-in Object Token

21

DeepSec IDSC

The screen shot shows a part of the list of CAs your Mozilla Firefox automatically trusts. These CA certificates are present to facilitate the use of SSL/TLS, but the list doesn't explain the level of trust or the procedures used by the CA for verification of the certificate request.

SSL/TLS outside the Web



22

DeepSec IDSC

SSL/TLS can also be used to digitally sign software. This is very useful for authenticity verification. GNU/Linux distributions use GPG for this. The screen shot shows a requester asking the user what to do with software digitally signed by Microsoft®.

SSL/TLS in Practice

- Who verifies certificates?
 - Check URL?
 - Check domain(s)?
 - Check digital fingerprints (hashes)?
- What do you do when your browser warns you?
- Do all devices issue proper warnings?
- Do all CAs follow proper procedures?
- Is your SSL software free of bugs?

23

DeepSec IDSC

As soon as cryptography enters the stage, some tasks get a bit more complex. As we have seen from the certificate warning messages and the certificate properties, you'll need some knowledge of what's going on and how things work. This is more complicated than picking up the phone and start talking.

Another issue are the many CAs in operation. Vendors sell certificates with varying levels of trust (i.e. varying levels of quality). Procedures of verification are not the same, often a single phone call is sufficient (more often verification is done by automated systems without human interaction on the side of the CA).

We just saw what a web browser does. What does a cell phone, a PDA, a VoIP phone, a washing machine, a refrigerator or a TV set do?

SSL/TLS Bugs

- 25C3: [Attacking MD5](#)
 - Create a rogue CA
 - MITM
- [Null bytes](#) in certificate identity
 - [www.paypal.com\0thoughtcrime.org](#)
 - [*\0thoughtcrime.org](#)

The bugs are quite recent and not the only weaknesses. MD5 is an aging hash algorithm and should not be used anymore. The null byte bug was present in the Microsoft® CryptoAPI, a fundamental code library providing cryptographic functions. The bug was published in July 2009, and it was fixed in October 2009. In between every client using the CryptoAPI was vulnerable.

Well...

- Secure communication can be hard
 - You don't own the key(s)? *You're not safe!*
 - Third party CA? Own CA?
 - Web of trust must be build
- Most technologies protect from passive attacks
- DNS is not secured (no DNS-SSL yet)
- Old protocols still in use (DES, RC4, SSLv2, ...)

Questions?



DeepSec IDSC

The [DeepSec IDSC](#) is an annual European two-day in-depth conference on computer, network, and application security. The mission statement is to bring together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. DeepSec aims to be a strictly neutral platform and a meeting point for everyone involved in security.

Contact: Michael Kafka & René Pfeiffer, deepsec@deepsec.net

Copyright Information

- Some rights reserved. / Einige Rechte vorbehalten.
- [DeepSec GmbH](#), Vienna, Austria.
- You may freely use, distribute and modify this work under the following agreement:
 - Authors must be referenced (also for modification) / Autoren müssen genannt werden (auch bei Bearbeitung)
 - Only for non-commercial use / nur für nichtkommerzielle Nutzung
 - Derivative work under the same license / Derivative Arbeit unter derselben Lizenz

