Applied informatics

Protecting access to freely available data, secure remote data access, protection and security of data storage.

ZEMÁNEK, Z. – PLUSKAL,D. – SMETANA, B.

esf european social fund in the czech republic
EUROPEAN UNION
MINISTRY OF EDUCATION, YOUTH AND SPORTS
OP Education for Competitiveness
UNIVERSITY OF DEFENCE
INVESTMENTS IN EDUCATION DEVELOPMENT

Protecting access to freely available data, secure remote data access, protection and security of data storage.

1. Access Methods to freely available data
2. Secure remote access to data
3. Data storage and protection
4. Assignments

Aims of the lecture

1. Provide the students with information on methods of approaching freely available data.
2. To explain the importance of secure remote access to data.
3. Characterising data storage and protection.

european social fund in the czech republic
EUROPEAN UNION
MINISTRY OF EDUCATION, YOUTH AND SPORTS
OP Education for Competitiveness
UNIVERSITY OF DEFENCE
INVESTMENTS IN EDUCATION DEVELOPMENT

Access to freely available data

- More than 150 million users on the Internet
- Still viruses are a big danger - but malware world is changing.
- 1983 - Fred. Cohen at the University of Pennsylvania used the code which is able to destroy itself - Calling it the term virus.

[1]

Remote data access

VPN - (Virtual Private Network)

The name for a group of technologies, respectively protocols for the implementation of private data transmissions

VPN is used for both:

- a remote client to the LAN
- Interconnect multiple LAN networks

VPN connects two points and securely transmits encrypted data.

Goal: to prevent changes in the transmission & the impossibility of interception of original data. [2]

Data access

Weak points on the way

= Number of intermediate nodes

= Can be infected or otherwise compromised

Transmission media

= Tapped

Threats

= Interception of communication and sniffing passwords

= Public wi-fi

Protection

= Encrypted connection (HTTPS)

= Encrypted transmission (SSL) vs certificate

[1]

[1]

HTTP protocol

HTTP (Hypertext Transfer Protocol) is an Internet protocol used for the interchange of hypertext documents.

Usually uses port TCP/80. Version 1.1 protocol is defined in RFC 2616. This protocol, along with e-mail the most widely used and contributed to the tremendous growth of the Internet in recent years.

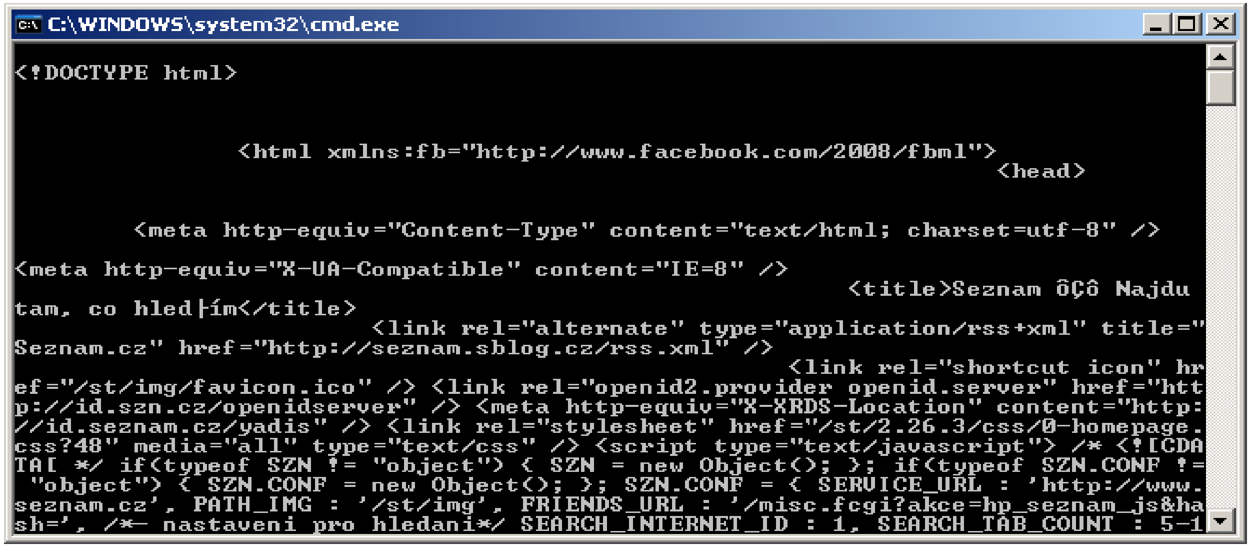
esf european social fund in the czech republic
EUROPEAN UNION
MINISTRY OF EDUCATION, YOUTH AND SPORTS
OP Education for Competitiveness
UNIVERSITY OF DEFENCE
INVESTMENTS IN EDUCATION DEVELOPMENT

HTTP communication

- By default HTTP request or response from server not encrypted
- This includes:
  - Usernames and passwords
  - Personal data that you insert into the form:
    - address
    - date of birth
    - Personal identification number
- If anyone has access to the network infrastructure through which data passes, he can eavesdrop.
- This also applies to hackers, who came to the switches, routers, etc. along the way ...

HTTP communication

- ❑ Start/run/cmd
- ❑ Telnet www.seznam.cz 80
- ❑ GET / [enter] [enter]



```
<!DOCTYPE html>


               <html xmlns:fb="http://www.facebook.com/2008/fbml">
                                                                  <head>


        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<meta http-equiv="X-UA-Compatible" content="IE=8" />
                                                        <title>Seznam ôÇô Najdu
tam, co hled├ím</title>
                        <link rel="alternate" type="application/rss+xml" title="
Seznam.cz" href="http://seznam.sblog.cz/rss.xml" />
                                                    <link rel="shortcut icon" hr
ef="/st/img/favicon.ico" /> <link rel="openid2.provider openid.server" href="htt
p://id.szn.cz/openidserver" /> <meta http-equiv="X-XRDS-Location" content="http:
//id.seznam.cz/yadis" /> <link rel="stylesheet" href="/st/2.26.3/css/0-homepage.
css?48" media="all" type="text/css" /> <script type="text/javascript"> /* <![CDA
TA[ */ if(typeof SZN != "object") { SZN = new Object(); }; if(typeof SZN.CONF !=
 "object") { SZN.CONF = new Object(); }; SZN.CONF = { SERVICE_URL : 'http://www.
seznam.cz', PATH_IMG : '/st/img', FRIENDS_URL : '/misc.fcgi?akce=hp_seznam_js&ha
sh=', /*— nastaveni pro hledani*/ SEARCH_INTERNET_ID : 1, SEARCH_TAB_COUNT : 5-1
```

HTTP communication

Request

Headers

- GET / HTTP/1.0
- Connection: Keep-Alive
- User-Agent: Mozilla/4.7 [en]
- (X11; U; FreeBSD 3.4-STABLE i386)
- Host: www.rtfm.com
- Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
- Accept-Encoding: gzip
- Accept-Language: en
- Accept-Charset: iso-8859-1,*,utf-8
- *(blank line)*

Empty line

HTTPS communication

HTTPS (Hypertext Transfer Protocol Secure) is an extension HTTP network protocol that enables secure connection between the Web browser and the Web server from eavesdropping, spoofing data and also allows you to verify the identity of the counterparty.

HTTPS uses HTTP protocol, the transmitted data is encrypted using SSL or TLS and standard port on the server side is 443

Basics for current form dates back to the 90th.

At that time, the company Netscape Communications came up with the first version of the SSL protocol, which they created for their Web browser.

HTTPS communication

- ***HTTPS = HTTP + SSL***
- HTTPS communication is secured by SSL/TLS.
- SSL/TLS provides for:
  - ***Data confidentiality***
    - Data is symmetrically encrypted
  - ***Data integrity***
    - Data is protected by MAC (Message Authentication Code)
  - ***Autentication***
    - Server authentication is mandatory by default

SSL/TLS

❑Protocol Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL) are cryptographic protocols, providing the opportunity for secure communications on the Internet for services such as WWW, electronic mail, Internet fax and other data transfers.

❑ There are only minor differences among the protocols SSL 3.0 and TLS 1.0.

european social fund in the czech republic
EUROPEAN UNION
MINISTRY OF EDUCATION, YOUTH AND SPORTS
OP Education for Competitiveness
UNIVERSITY OF DEFENCE
INVESTMENTS IN EDUCATION DEVELOPMENT

HTTPS authentication

- The default of HTTPS is compulsory authentication of the server. I.e. when a client (eg web browser) connects to the (web) server, it can be sure that it connected to the correct server.
    - This is important when entering passwords, credit card numbers ...
    - Dangerous Phishing ...

HTTPS authentication

- Server sends the server certificate.
- The certificate states the name of the server, and public key of the server.
- SSL / TLS also verifies that the server has access to the private key corresponding to the certified public key.
- Data encrypted with the public key of the server, can be decrypted only by the correct server.

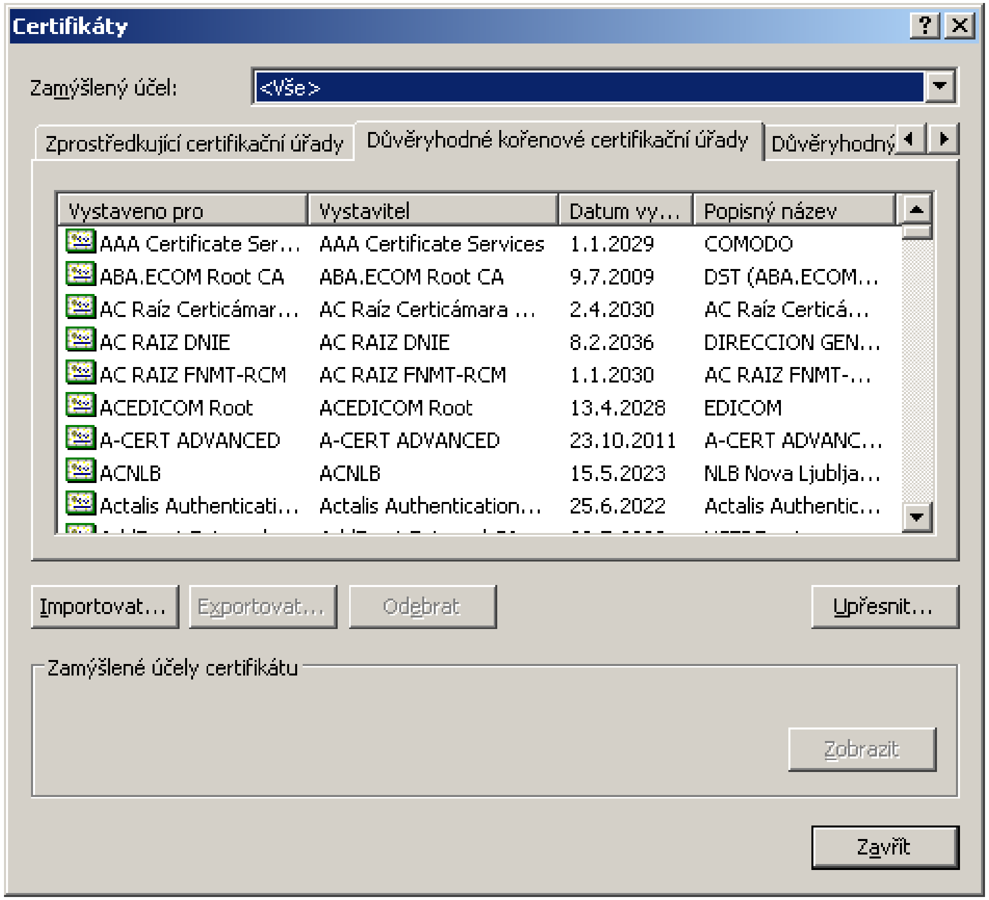
HTTPS authentication

- The server certificate is signed by the issuing certification authority (CA).
- The signing CA must be trusted.
- A CA certificate is a must be stored in the list of trusted CA ...

HTTPS communication

- Lists are saved in browsers.
  (IE takes a list from OS)
- Initially there are tens of CAs you've never heard of ...
- These lists can be configured.
- You automatically trust all of them

List of trusted CAs in Windows



Certifikáty

Zamýšlený účel: <Vše>

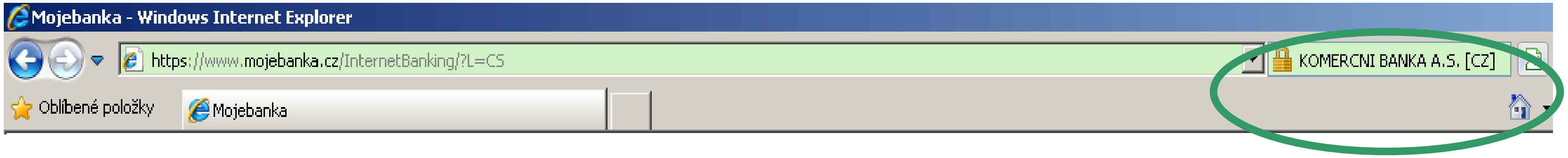
Vystaveno pro	Vystavitel	Datum vy...	Popisný název
AAA Certificate Ser...	AAA Certificate Services	1.1.2029	COMODO
ABA.ECOM Root CA	ABA.ECOM Root CA	9.7.2009	DST (ABA.ECOM...
AC Raíz Certicámar...	AC Raíz Certicámara ...	2.4.2030	AC Raíz Certicá...
AC RAIZ DNIE	AC RAIZ DNIE	8.2.2036	DIRECCION GEN...
AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM	1.1.2030	AC RAIZ FNMT-...
ACEDICOM Root	ACEDICOM Root	13.4.2028	EDICOM
A-CERT ADVANCED	A-CERT ADVANCED	23.10.2011	A-CERT ADVANC...
ACNLB	ACNLB	15.5.2023	NLB Nova Ljublja...
Actalis Authenticati...	Actalis Authentication...	25.6.2022	Actalis Authentic...

?
Zprostředkující certifikační úřady
Důvěryhodné kořenové certifikační úřady
Důvěryhodný
Importovat...
Exportovat...
Odebrat
Upřesnit...
Zamýšlené účely certifikátu
Zobrazit
Zavřít

SSL/TLS

EV certificate signed by trusted CA

- ❑ EV (Extended Validation) certificate has a higher degree of confidence in conformity with the Web domain owner.
- ❑ Technically the same X.509 (with a slight note). But the CA does a thorough check of identity.



https://www.mojebanka.cz/InternetBanking/?L=CS

- ❑ If the certificate is not signed by a trusted CA, it does not necessarily mean the site is bad/malicious.
- ❑ On the contrary, a certificate signed by a trusted CA does not mean that there’s no malware on the website etc.
- ❑ Simple solutions / recommendations to remain secure do not exist.

Remote data storage – sharing of large files

- ❑ Hand in hand with increasing the speed and quality of Internet connections the size of the average document is increasing, too.
- ❑ Large attachments cannot be sent by email (email is typically limited to 10MB)
- ❑ The most convenient way is to use anonymous data sharing through web stores.

[4]

european social fund in the czech republic
EUROPEAN UNION
MINISTRY OF EDUCATION, YOUTH AND SPORTS
OP Education for Competitiveness
UNIVERSITY OF DEFENCE
INVESTMENTS IN EDUCATION DEVELOPMENT

Remote data storage

- Service ***Uloz.to*** provided by Nodus Technologies.
- Free use of up to 800MB without registration.

NAS

- ***NAS*** = **N**etwork **A**ttached **S**torage
- Data storage that can be provided for various users.
- NAS may not only have the file server functionality, but may have other specialized functions.
- It usually contains an embedded computer whose task is sharing of data and protocol support.

NAS

- NAS devices have gained popularity since 2010, when it began to be used to share data among multiple computers.
- In comparison with other network storage options they are easier to administer and to set up.
- NAS contains one or more hard drives that can merged into larger data structures, or they can create a RAID array.
- RAID (Redundant Array of Inexpensive / Independent Disks) is a method of data protection against a hard disk failure.

[6]

Web surfing hints

1. Internet is an anonymous environment (the one with whom you are communicating might not be who he says – he might have created an alternative identity).
2. Information to which you have access may not be credible, it may be a misinformation, not only in terms of obsolescence.
3. On the web you are not anonymous, there are identification mechanisms - through the IP address. Interception of transmitted data & communication can also be possible.
4. Providers are required to keep certain data on the activities of their users and in case of a legal requirement they will provide them to law enforcement authorities.
5. Also, employers monitor their ICT environment.

[1]

Assignments

1. Access Methods to freely available data
2. Secure remote access to data
3. Data storage and protection

Resources:

1. KÁBRT, Filip. *Bezpečnost na Internetu* [online]. [cit. 2013-12-25]. Studijní materiály MFF UK. Dostupné z: www.liveonline.cz/docs/lol_prednaska_bezpecnost.ppt
2. *Co je VPN?* [online]. © 2013 Microsoft. [cit. 2013-12-26]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc731954(v=ws.10).aspx
3. ČEKAN, Lukáš. *Podniková informatika - přednáška* [online]. 2013-04-07. [cit. 2013-12-25]. Studijní materiály z FEI UPCE, obor Informační technologie. Dostupné z: http://fei.pepiczech.cz/?p=136
4. *Přehled českých webových služeb pro snadné sdílení dat.* [online]. 2013 [cit. 2013-12-16]. Dostupné z: http://www.zive.cz/clanky/prehled-ceskych-webovych-sluzeb-pro-snadne-sdileni-dat/sc-3-a-141698/default.aspx
5. Jak stahovat z ulozto.cz ZADARMO!! [online]. 2013 [cit. 2013-12-16]. Dostupné z: http://www.youtube.com/watch?v=SxO2O2SNosM
6. Chytrá datová úložiště (NAS) [online]. 2013 [cit. 2013-12-16]. Dostupné z: http://www.alza.cz/servery/diskove-stanice/