

# Bezpečnostní protokoly a útoky v sítích

## Bezpečnost ICT 2

Lukáš Malina

Vysoké učení technické v Brně  
[malina@vut.cz](mailto:malina@vut.cz)  
[axe.vut.cz](http://axe.vut.cz)



2022



Informační bezpečnost

## 1 Bezpečnostní protokoly v sítích

- IPSec
- TLS
- VPN

## 2 Útoky v sítích

- Obecné útoky a obrana

## 3 Netechnické útoky v sítích

- Netechnické útoky v sítích
- Phishing

# Bezpečnostní protokoly v sítích

# Bezpečnost v TCP/IP komunikacích

- Aplikační vrstva (např. PGP, S/MIME - Secure/Multipurpose Internet Mail Extensions).
- Transportní vrstva (např. TLS 1.3, dříve SSL).
- Síťová vrstva (např. IPSec).
- Linková vrstva (např. WEP, WPA2, PPP-CHAP).

<b>User</b>	Fingerprint	PIN	SmartCard
<b>Application</b>	SNMPv3		S/MIME
	DNSSEC		Secure/Multipart
	XMLDigSign		OpenPGP
	AAA (VoIP etc.)		Routing Security
<b>Transport</b>	TLS		SSH
<b>Network</b>	IPSec AH/ESP (ISAKMP)		
	AAA (NAS, MobileIP etc.)		
	Firewall		
<b>Link</b>	Data link encryption		
<b>Physical</b>	Physical intactness		

# Zabezpečení linkové vrstvy

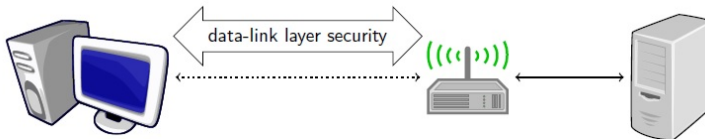


Figure : 2L bezpečnost [1]

- Komunikace bod - bod,
- např. protokoly: WEP, WPA, WPA2, autentizace PPP - PAP/CHAP/EAP, viz přednášky 2 a 3,
- šifrování po MAC adresu (data v Ethernet rámcích),
- Ethernet Encryptors (např. SAFENET CN4000 SERIES).

# Zabezpečení linkové vrstvy - autentizace PAP/CHAP

- PAP (Password Authentication Protocol) - autentizace v protokolu PPP. Autentizační data procházejí po síti nešifrovaná (v ASCII)!, struktura dat:
  - + Frame: Base frame properties
  - + PPP: Unknow Frame (0x0)
  - PPPPAP: Authenticate Request
  - PPPPAP: Code = Authenticate Request
  - PPPPAP ID = 5 (0x5)
  - PPPPAP Length = 27 (0x1B)
  - PPPPAP Peer ID Length = 13 (0xD)
  - PPPPAP Perr ID = Administrator
  - PPPPAP Password Length = 5 (0x5)
  - PPPPAP Password = **Heslo**
- **Challenge-Handshake Authentication Protocol (CHAP)** - oboustranná autentizace v protokolu PPP založena na sdíleném tajemství (heslu) - 3 zprávy (challenge, response, success/failure).

# Zabezpečení síťové vrstvy

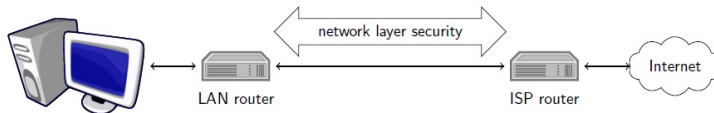


Figure : 3L bezpečnost [1]

- Komunikace v síti mezi dvěma zařízeními s IP adresou,
- např. protokol IPsec,
- šifrování po IP adresu (data v paketech, celé pakety).

# Protokol IPsec

## IPsec účel a princip:

- poskytuje end-to-end bezpečnost,
- šifrování a autentizace dat a stran na úrovni síťové vrstvy,
- chování uživatele či aplikace není třeba uzpůsobovat,
- lze pak tunelovat jak UDP tak i TCP datagramy,
- IPsec je popsán v mnoha RFC dokumentech.

## Součásti IPsec:

- **Authentication header (AH) protokol.**
- **Encapsulating Security Payloads (ESP) protokol.**
- **Security Association (SA)** - popis spojení.
- Popis hlavní architektury IPsec - RFC 4301 2005.



# Protokol IPsec - módy

## Transportní mód:

- **ochrana dat** (payloadu) v IP paketu.
- IP hlavička není šifrována,
- použití mezi hosty.

## Tunelující mód:

- ochrana **celého paketu** (IP hl. + data),
- paket se stane payloadem (data) v novém paketu s jinou IP hlavičkou,
- použití mezi hosty, bránami (překládají IP adresy).

# Protokol IPsec - Security Association (SA)

**SA** formálně **popisuje** unikátní jednocestné **spojení** mezi dvěma stranami a parametry použité pro zabezpečení. Aktivní spojení jsou uloženy v databázi Security Association Database (SAD). SA management a bezpečnostní pravidla je dále uloženo v Security Policy Database (SPD). Některé SA parametry v SAD (kompletní popis RFC 4301):

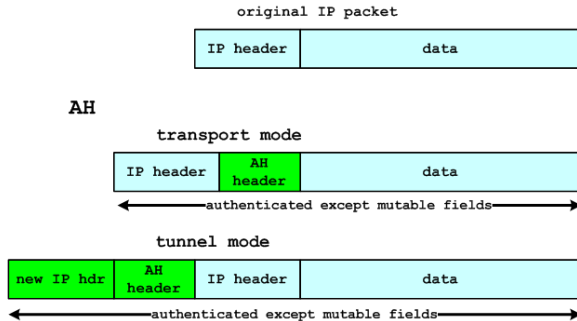
- Security Parameter Index (SPI) - 32-bit hodnota pro unikátní definici SA.
- sekvenční čísla: sequence number, sequence number overflow,
- parameter anti-replay window,
- AH informace: algoritmus pro autentizaci, klíč, životnost klíče, etc.,
- ESP informace: algoritmus šifrovací algorithm, klíč, životnost klíče etc.,
- životnost SA,
- IPsec protokol mód (tunel/transport),
- maximální velikost paketu.

# Protokol IPsec - Authentication header (AH) protokol

**AH protokol** poskytuje:

- **integritu a autentičnost IP paketů** (MAC funkce),
- chrání proti útoku opakováním zprávy (sekvenční číslo - counter 32b, okna, pravá hrana - nejvyšší přijaté s.č.).
- údaje AH jsou v hlavičce AH a autentizační tag (Integrity Check Value - ICV) je počítán ze všech dat (kromě proměnlivých parametrů).

# Protokol IPsec - AH protokol



# Protokol IPsec - Encapsulating Security Payloads (ESP) protokol

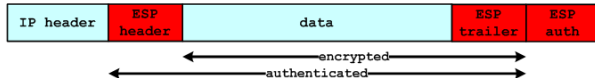
**ESP protokol** poskytuje

- zajištění **důvěrnosti dat** pomocí **šifrování** (např. AES-CBC-128b),
- ESP obsahuje ESP hlavičku, zašifrovaná data, ESP trailer,
- základní autentizace pouze ESP částí a dat, ne IP hlavičky,
- volitelně se přidává ochrana AH (přidává se AH hlavička).

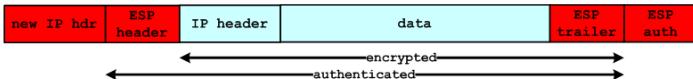
# Protokol IPsec - ESP

## ESP

### transport mode

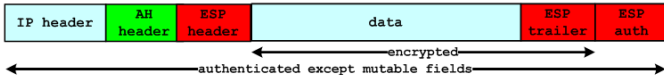


### tunnel mode

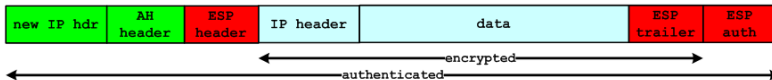


## AH & ESP

### transport mode



### tunnel mode



# Protokol IPsec - ustanovení klíče

Symetrické šifrování potřebuje klíče na obou stranách.

## Metody ustanovení klíče:

- **PSK** - Pre-shared Secret Key,
- **IKE1 a IKE2** - Internet Key Exchange (sada autentizačních schémat včetně certifikátů),
- **Kerberos** - Kerberized Internet Negotiation of Keys (KINK).

# Protokol IPsec - implementace Strongswan

- **Strongswan** je **open source IPsec knihovna** (Linux 2.6, 3.x, 4.x kernels, OS X, iOS, Android a Windows)
- Podpora IKEv1 a IKEv2 pro ustanovení klíčů (včetně X.509 certifikátů, OCSP, CA managementu, podpory EAP-TLS, smartkaret a TPM přes opensc tool).
- NAT-Traversal funkce přes zapouzdření UDP a port floating k překonání bran s NAT.
- Podpora IPv4 i IPv6.
- Implementace state-of-the-art kryptografie (např. AES-GCM, 25519 elliptic curve DH group (RFC 8031) a Ed25519).

Existují i další knihovny **Libreswan**, **Openswan**,...



# Protokol IPsec - implementace Strongswan

Konfigurace pomocí upravy konf. souborů, ukázka ipsec.conf:

# /etc/ipsec.conf - strongSwan IPsec configuration file

config setup

conn %default

ikelifetime=60m

keylife=20m

rekeymargin=3m

keyingtries=1

**keyexchange=ikev2**

**ike=aes256gcm128-aesxcbc-x25519!**

**esp=aes256gcm128-x25519!**

conn rw

left=192.168.0.1

leftcert=moonCert.pem

leftid=@moon.strongswan.org

leftsubnet=10.1.0.0/16

leftfirewall=yes

right=%any

auto=add

# Zabezpečení transportní vrstvy

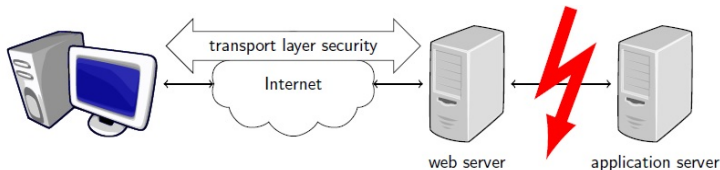
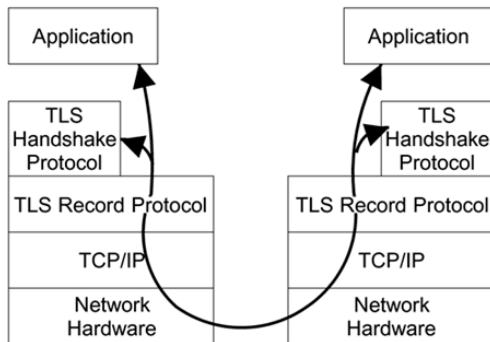


Figure : 4L bezpečnost [1]

- Komunikace v síti mezi servery a klienty v rámci TCP/UDP přenosu,
- např. TLS v1.3 (dříve SSL)
- šifrování protokolu TCP/UDP po data v datagramech,
- část cesty nemusí být šifrována (např. mezi web server/proxy a aplikačním/DB servery).

# TLS protokol



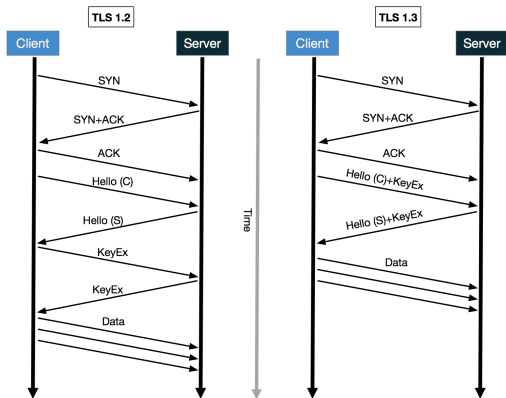
- Transparentní pro aplikační vrstvu,
- TLS se chová jako bezpečné TCP,
- protokoly nad TCP jako např. HTTP, SMTP lze zabezpečit (HTTPS, SMTPS atd.).

# TLS protokol - součásti

Součásti TLS protokolu:

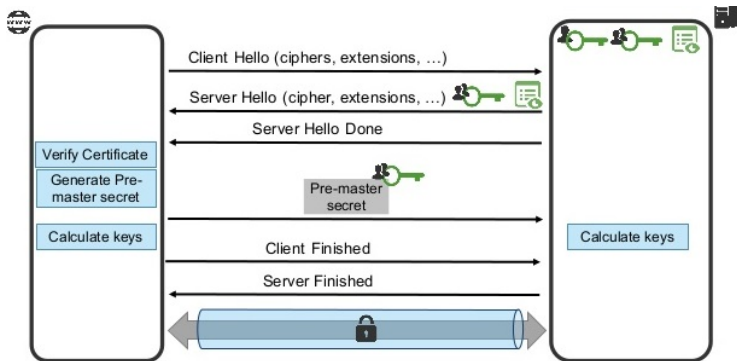
- **Handshake Protokol** - inicializace spoje, autentizace stran (klient/server) a ustanovení klíče.
- **Record Protokol** - datový přenos šifrovaných dat a MAC autentizace.
- **Alert Protokol** - slouží k notifikaci chyb a varování.

# TLS protokol - verze



- SSL 1.0 n/a, SSL 2.0 1995, SSL 3.0 1996, TLS 1.0 1999, TLS 1.1 2006, TLS 1.2 2008, TLS 1.3 2017.

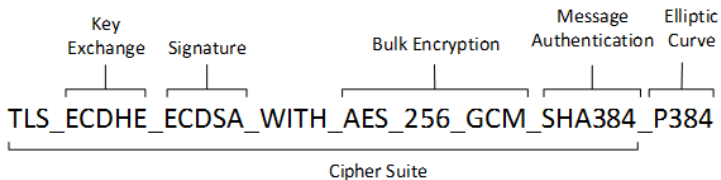
# TLS - ustanovení klíče a autentizace



- Liší se dle verzí autentizace a kryptobalíčků.
- Klient volitelně posílá certifikát - oboustranná autentizace.

# TLS - použitá kryptografie

Syntaxe CipherSuites:



# TLS - použitá kryptografie

## Which SSL/TLS Cipher Suites to use?

[illegible]

## NULL and EXPORT



## Which SSL/TLS Cipher Suites to use?

### Bez DES a RC4 šifrování

# TLS - použitá kryptografie

## Which SSL/TLS Cipher Suites to use?

TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256

TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
TLS\_DHE\_DSS\_WITH\_AES\_256\_GCM\_SHA384

TLS\_DH\_DSS\_WITH\_AES\_128\_GCM\_SHA256

TLS\_ECDH\_RSA\_WITH\_AES\_128\_GCM\_SHA256

TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_ECDH\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_DH\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_DH\_DSS\_WITH\_AES\_256\_GCM\_SHA384  
TLS\_DH\_RSA\_WITH\_AES\_128\_GCM\_SHA256

TLS\_DHE\_DSS\_WITH\_AES\_128\_GCM\_SHA256

TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

TLSECDHE-RSA-WITH-AES-256-GCM-SHA384

TLS ECDH ECDHE WITH AES 256 GCM SHA384

TLS ECDHE RSA WITH AES 128 GCM SHA256

Use ephemeral key exchange!

# TLS - použitá kryptografie

## Which SSL/TLS Cipher Suites to use?

TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256

TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
TLS\_DHE\_DSS\_WITH\_AES\_256\_GCM\_SHA384

TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_DHE\_DSS\_WITH\_AES\_128\_GCM\_SHA256

TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

## DSS and ECDSA

# TLS - ideální kryptografický balíček

- Ustanovení klíče s dočasnými klíči: např. ECDHE nebo DHE. (raději ne PSK, DH a ECDH).
- Bezpečný podpis, např. RSA, ale DSS a ECDSA lze použít (pozor na slabé RNG).
- Bezpečné šifrování a mód, např. autentizované šifrování AES-GCM (Nechceme RC4, DES, TDES!).
- Bezpečnou hash funkci, např. SHA-256, SHA-384 (MD5 nechceme!).

Př. bezpečný krypto balíček:

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

Př. málo bezpečný krypto balíček:

TLS\_RSA\_WITH\_**RC4**\_128\_**MD5**

Otestovat klienta: <https://www.howssmyssl.com/>

# Knihovna OpenSSL

- Open source SW knihovna pro protokoly TLS a SSL.
- Kryptografické funkce a utility (generátory, šifry, hashe, PKC).
- Prog. jazyk C/Assembler, první verze 0.9.1 (1998), poslední verze 1.1.1 (2017) podporuje TLS 1.3 a SHA-3.
- OpenSSL jako základ pro mnoho kryptografických implementací a VPN aplikací.
- Dříve problémy s buggy a zranitelnosti (např. Heartbleed, Key Recovery Attack on Diffie Hellman small subgroups).

# Datagram Transport Layer Security (DTLS)

- Zabezpečení pro nestavové datagramové protokoly (např. UDP).
- DTLS poskytuje šifrování, autentizaci a integritu (jako TLS).
- Secure Real-time Transport Protocol (SRTP)- DTLS-SRT.
- Stream Control Transmission Protocol (SCTP) encapsulation.

# Podpora TLS a DTLS v SW knihovnách

	<b>TLS 1.0</b> <b>RFC 2246</b>	<b>TLS 1.1</b> <b>RFC 4346</b>	<b>TLS 1.2</b> <b>RFC 5246</b>	<b>TLS 1.3</b> <b>RFC 8446</b>	<b>DTLS 1.0</b> <b>RFC 4347</b>	<b>DTLS 1.2</b> <b>RFC 6347</b>
wolfSSL	Ano	Ano	Ano	Ano	Ano	Ano
BoringSSL	Ano	Ano	Ano	Draft 23	Ano	Ano
GnuTLS	Ano	Ano	Ano	Draft 26	Ano	Ano
MatrixSSL	Ano	Ano	Ano	Ano	Ano	Ano
OpenSSL	Ano	Ano	Ano	Ano	Ano	Ano
rustls	Ne	Ne	Ano	Draft 22	Ne	Ne

Table : Podpora TLS a DTLS

## 4L bezpečnost - nedostatky

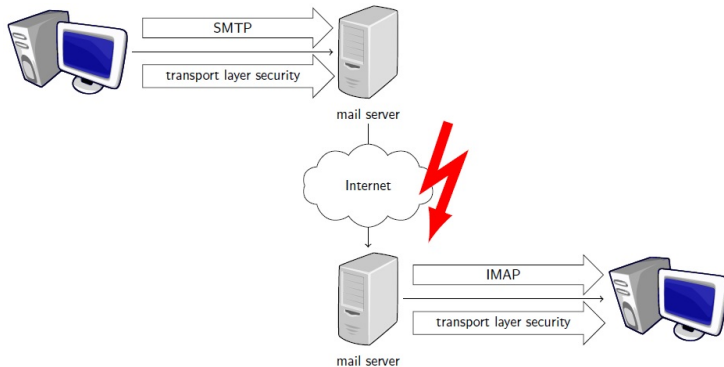


Figure : 4L bezpečnost - nedostatky u přenosu el.pošty [1]

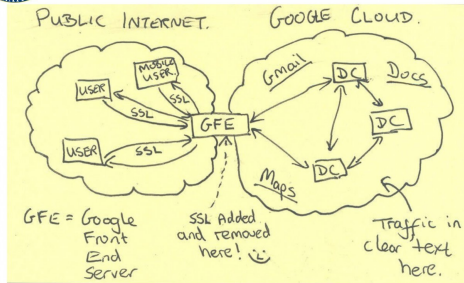


## 4L bezpečnost - nedostatky

TOP SECRET//SI//NOFORN



### Current Efforts - Google



TOP SECRET//SI//NOFORN

Figure : Google - nedostatky [1]

# Zabezpečení aplikační vrstvy

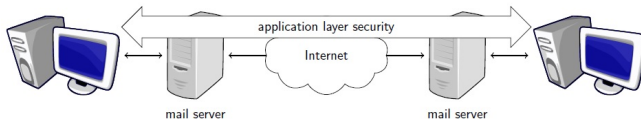
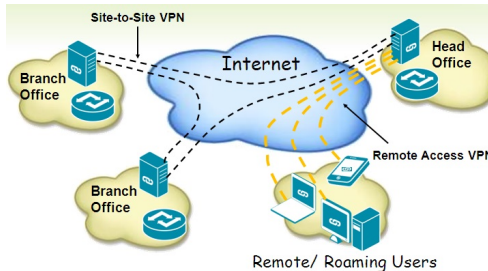


Figure : 7L bezpečnost [1]

- Komunikace v síti mezi aplikacemi/uživateli,
- často proprietární, kryptografie přímo v aplikaci, VPN implementace,
- např. šifrování emailu v rámci aplikace, šifrování zpráv v IM (WhatsApp),
- celá cesta musí být šifrována bod-bod,
- SSH - Secure Shell, klient (WinSCP, Putty) - server (TCP port 22), SFTP/SCP protokoly, krypto RSA/AES/MAC...

# Virtual Private Networks



## Typy VPN:

- **site-to-site** - propojení dvou sítí jedné instituce - více spojení,
- **vzdálený přístup** (klient - server) - many-to-one.

Šifrování/autentičnost dat pomocí IPsec, TLS, proprietární, HW zařízení jako VPN brány.

# Virtual Private Networks - implementace

## openVPN:

- projekt od 2001, nyní verze 2.5 (říjen 2020)
- multi-platformní, utilizace SSL/TLS, založen na OpenSSL knihovně,
- spoje bod-bod, síť -síť,
- NAT traversal,
- GitHub: <https://github.com/OpenVPN/openvpn>

## SoftEther VPN:

- multi-platformní, aplikace klient, server, bridge, GUI,
- podpora SSL VPN, L2TP/IPsec, OpenVPN, Microsoft Secure Socket Tunneling Protocol včetně možnosti paralelní spojení pro zvýšení propustnosti 1 - 32 kanálů pro uživatele,
- NAT traversal, VPN přes ICMP a DNS (pro omezené sítě).
- WWW: <https://www.softether.org/>

# Útoky v sítích

# Útoky v sítích - obecné typy

- Útok **na přenos**: odposlech dat, útok mužem uprostřed, útok opakovaním zpráv, padělání zpráv,...  
např: ARP spoofing, Routing útoky, SSL Strip útok.
- Útok **na koncové prvky**: Počítačový škodlivý software (malware) - viry, kryptoviry, ransomware, rootkity a trojské koně - šíření nebo škody na konkrétním uzlu i mezi uzly (např. počítačové červy - worms).
- Útoky **na síť**: Nepovolené průniky do sítě a služeb pomocí bezpečnostních chyb, zranitelností a mezer v zabezpečení.
- Útoky odepření služeb (DoS, DDoS).
- Útok zneužívající fyz.osoby (**sociální inženýrství**, phishing).

# Útoky v sítích - obecné metody obrany

- Bezpečná **konfigurace síťových prvků**.
- **Nasazení aktivních prvků**: firewallů, IDS / IPS, honeypotů a sond provozu.
- **Sestavení** a dodržování **pravidel** v síti.
- **Zabezpečení koncových prvků** vhodným software (update, patch, antiviry, anti-spyware, osobní firewally, atd.).
- **Nasazení** kryptografických ochran a **protokolů** (autentizace, šifrování, kontrola integrity dat, VPN, IPsec, TLS...).
- **Testování** obecných **zranitelností**.
- Celkový **audit** bezpečnosti sítě a síťových služeb.
- **Školení uživatelů a dohled**.

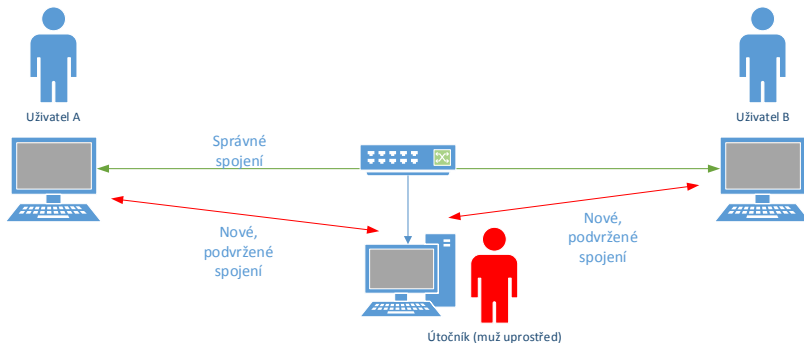
# Síťové útoky

- Útoky v síti **Internet** (SSL strip na proxy serveru) nebo **Intranet** (lokální SSLstrip, ARP spoofing) na přenášené data (komunikaci) nebo na konkrétní síťové služby.
- Útoky se většinou dělí na **pasivní** (např. pouhý odposlech) a **aktivní** (modifikace dat, podpisů - složitější na realizaci).
- Aktivní útočník může např. odposlouchávat nešifrovaný přenos dat, modifikovat přenášená data (např. Man in the Middle attacks), znovu zasílat zprávy (Replay attacks), padělat data, nepovolaně přistupovat ke službám přes síťové připojení, útok na odepření služeb atd.
- Obecná ochrana: nasazení kryptografických prostředků, nasazení bezpečnostních síťových prvků (filtrace útoků a nepovoleného provozu, ...).

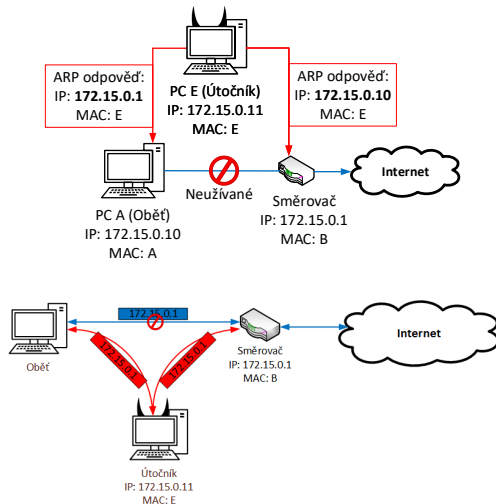


# Síťové útoky - MitM

Odposlech, útok mužem uprostřed (Man in the Middle attack).

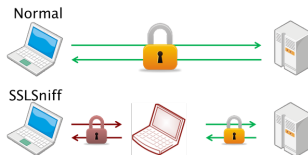



# Síťové útoky - MitM pomocí ARP poisoning



# Síťové útoky - MitM pomocí podvrhnutí certifikátu - SSL Sniff

Přeposlání zašifrované zprávy přes útočníka, dvojí SSL pomocí falešného certifikátu (podobný název certifikátu jako pravý).





**Toto připojení není důvěryhodné**

Přistáváte na Firefox o zabezpečené připojení k serveru **elcamino.aster.cz**, ale nebe ověřit, že tomu tak skutečně je.

Pokud je požadováno zabezpečené připojení, měl by server předložit důvěryhodnou identifikaci a tím prokázat, že se připojujete na správné místo. Nicméně, identita tohoto serveru nemohla být ověřena.

**Co mám teď dělat?**

Pokud se k tomuto serveru obvykle připojujete bez problému, může tato chyba znamenat, že se za tento server někdo snaží vydávat, a neměli byste pokračovat.

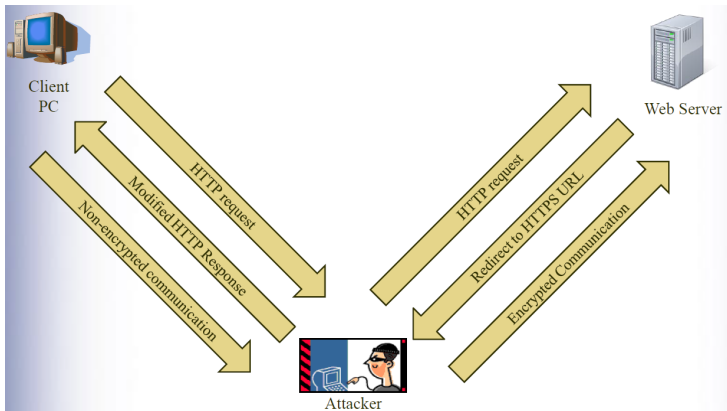
[Rychle odejít pryč!](#)

- **Technické detaily**
- **Vím, o co se jedná**

Mitigace: neignorovat bezpečnostní upozornění, ověřit pravost certifikátu!

# Síťové útoky - SSL Strip

Změna hlavičky z https na http (druh MitM).



# Netechnické útoky v sítích

# Netechnické útoky v sítích - motivace

- Často se jedná o snadnou a rychlou formu útoků.
- Využívá se oklamání uživatelů (tzv. bugs in the human hardware).
- Psychologická manipulace.
- Dokáží překonat i lepší technické zabezpečení.

# Útoky v sítích - netechnické typy I.

- **Sociální inženýrství** - jedná se o psychickou manipulaci s lidmi za účelem zisku informací, přístupu ke službě nebo provedení podvodu - (Kevin David Mitnick).
- **Phishing** - kontaktování velkého počtu lidí pro získání citlivých informací pro škodlivé účely.
- **Spear Phishing** - kontaktování konkrétních lidí, kontaktní zpráva navíc může obsahovat malware.
- **Baiting** - tzv. reálný trojský kůň. Jedná se o zanechání malwaru na médiu, které oběť má objevit a použít. Na médiu často je návnada pro jeho použití. Např. nadpis: Výplaty oddělení za čtvrtletí.

## Útoky v sítích - netechnické typy II.

- **Quid pro quo** - (něco za něco) útočník náhodně volá do firmy, kdy se vydává za technickou podporu, která volá zpět na určitý problém. Oběť, pokud v minulosti něco žádala, se pak může nachytat a prozradit citlivé údaje (login, hesla, atd.).
- **Tailgating** - průnik do chráněných prostor s pomocí legitimního uživatele, tzv. podržení dveří u vstupu hlídaného čipovou kartou.
- **Insider threats** - hrozby od vnitřního uživatele (nespokojený zaměstnanec, neproškolený zaměstnanec), který útočí zevnitř.
- **Neautorizovaný fyzický přístup** - fyzický přístup útočníka do chráněných prostor, nebo k uživatelské stanici, serveru či síťovému zařízení.



# Tailgating

Neoprávněný přístup do chráněných prostor pomocí jiného legitimního uživatele.



# Phishing

- Útok využívá **sociálního inženýrství**.
- Pokus o získání citlivých informací jako je uživatelské jméno, heslo, detaily platební karty, osobní data atd. pro škodlivé účely.
- **Vektory útoku** mohou být: emaily, sociální sítě, webové portály, instant messaging, atd.
- Data, která se často sbírají, slouží k přístupu do e-bankovníctví, web.portálů, sociálních sítí, IT služby atd.
- **Obrana:** legislativa, školení uživatelů, veřejná informovanost, technické opatření (blokování emailů, zpráv od podezřelých zdrojů, posílení autentizace).
- Obrana z pohledu uživatele: neposkytovat data neověřeným stranám, sledovat aktuality, používat více hesel a loginů (na každou službu jiný).

# Phishing - typy I.

- Obecný **Phishing** - získání dat (login, heslo, data kreditní karty) od uživatelů za pomoci vydávání (tzv. masquerading) za důvěryhodnou entitu prostřednictvím elektronické komunikace.
- **Spear phishing** - phishing **přímo cílený** na konkrétní skupinu uživatelů či firmu.

## Phishing - typy II.

- **Clone phishing** - výroba, update nových phishing zpráv z legitimních původních zpráv. Nová zpráva se znovu přepošle, ale se spoofovaným - jiným odkazem, nebo jinou přílohou, což navede oběť na škodlivé stránky nebo spustí škodlivou přílohu.
- **Whaling** (velrybářský) - phishing cílený na vlivné představitele firem a organizací. Obsah zprávy či stránek (odkazu) je padělán jako stížnost od jiné firmy nebo jako předvolání od vyšší autority (kontrolní úřady, finanční úřady). Manažer může z důvodu obav naletět falešné vyšší autoritě.

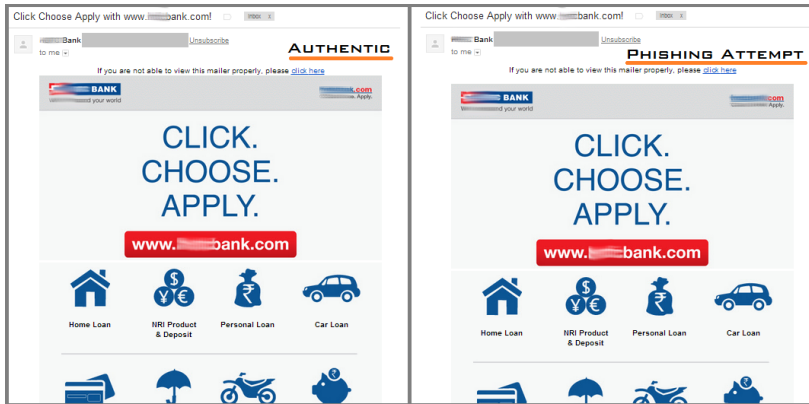
# Phishing - techniky útočníka I.

- **Manipulace odkazů (linků)** - technika podvodu, kdy odkaz (link) ve zprávě vypadá jako původní link na organizaci, ale ve skutečnosti je cílen na podvodnou stránku. Využívají se **modifikované URL** nebo subdomény. Např.  
`http://www.yourbank.example.com/`, což navede oběť na stránky example, kde název "yourbank" je jen sekce. Dalším trikem je zobrazení textu odkazu mezi <A> tagy. Text popisuje důvěrné cíle, ale odkáže na stránky phisherů. Jinou metodou je Internationalized Domain Names (IDN) spoofing.
- **Vyhnutí filtrům (Filter evasion)** - využití obrázků místo textu znesnadňuje detekci útoků. Proto vznikly filtry s OCR (Optical Character Recognition) pro filtraci závadných obrázků s falešnými odkazy atd. **IWR (Intelligent Word Recognition)** detekují i pootočený text, kurzívu atd.

## Phishing - techniky útočníka II.

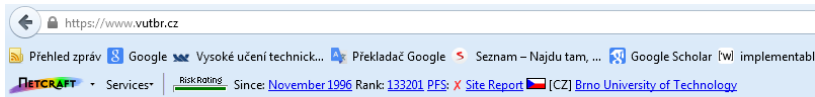
- **Padělání web.stránek** - stránky se jeví jako validní (originál). Útočník jen musí dostat oběť na stránky.
- **Skryté přesměrování (covert redirect)** - přesměrování legitimních odkazů na stránky phisherů. Využívá se chyb jako např.: **XSS zranitelnosti, login pop-up** na postižené doméně. Útočník využije legitimních stránek, ale kompromituje např. okno login pop-up dialogu.
- **Vishing (voice phishing)** - pomocí telefonu, VoIP může útočník zjistit např. PIN, heslo k bankovníctví atd. Falešné ale relativně důvěryhodné call-ID způsobuje větší důvěru u obětí.
- **Zlé dvojče (Evil twins)** - útočník vytvoří falešnou bezdrátovou síť se stejným SSID např. v hotelu, kavárně apod. za účelem zisku dat, přenášných v této síti.

# Phishing - ukázka padělané stránky



# Antiphishing - Netcraft

- Služby proti podvodům a phishing útokům.
- Toolbar pro prohlížeče Firefox, Chrome a Opera.



VYSOKÉ UČENÍ  
TECHNICKÉ  
V BRNĚ

NAVUT.CZ





# Antiphishing - PhishTank

- Web bojující proti phishingu.
- Poskytuje open API pro developery a výzkumníky.

The screenshot shows the PhishTank website. At the top, a navigation bar includes links for Home, Add A Phish, Verify A Phish, Phish Search, Stats, FAQ, Developers, Mailing Lists, and My Account. The main content area features a 'Join the fight against phishing' section with links to Submit, Track, Verify, and Develop. Below this is a form to report a phishing site. To the right, there are two informational boxes: 'What is phishing?' and 'What is PhishTank?'. At the bottom, a 'Recent Submissions' table lists various URLs and the users who reported them.

PhishTank is operated by [OpenDNS](#), a free service that makes your Internet safer, faster, and smarter. [Get started today!](#)

**PhishTank**® Out of the Net, into the Tank.

username   [Sign In](#)  
[Register](#) | [Forgot Password](#)

[Home](#) [Add A Phish](#) [Verify A Phish](#) [Phish Search](#) [Stats](#) [FAQ](#) [Developers](#) [Mailing Lists](#) [My Account](#)

## Join the fight against phishing

[Submit](#) suspected phishes. [Track](#) the status of your submissions.  
[Verify](#) other users' submissions. [Develop](#) software with our free API.

**Found a phishing site?** Get started now — see if it's in the Tank:

[Is it a phish?](#)

### Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
<a href="#">3383436</a>	<a href="http://www.chsbk.be/f6a0839ad2c7d545583a0385bfc61b...">http://www.chsbk.be/f6a0839ad2c7d545583a0385bfc61b...</a>	<a href="#">knack</a>
<a href="#">3383435</a>	<a href="http://www.chsbk.be/">http://www.chsbk.be/</a>	<a href="#">knack</a>
<a href="#">3383434</a>	<a href="http://cajam.se/femman/index.htm">http://cajam.se/femman/index.htm</a>	<a href="#">sine</a>
<a href="#">3383433</a>	<a href="http://https.identifiant.changement.statut.ebaypal...">http://https.identifiant.changement.statut.ebaypal...</a>	<a href="#">PhishReporter</a>
<a href="#">3383432</a>	<a href="http://sadsadasdas9856014083defwewrewwer.arhansig...">http://sadsadasdas9856014083defwewrewwer.arhansig...</a>	<a href="#">GovCERTCH</a>

### What is phishing?

Phishing is a fraudulent attempt, usually made through email, to steal your personal information.

[Learn more...](#)

### What is PhishTank?

PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.

[Read the FAQ...](#)

# Metody obrany u netechnických útoků

Mitigace útoků sociálního inženýrství:

- Autentizace - přísně a úzce definovat působnost uživatelů v síti a ve službách (mitigace útoků sociálního inženýrství).
- Bezpečnost web. aplikací, antiviry, anti-spyware, blokování spamů.
- **Školení uživatelů (Cyber hygiene)** - školení, osvěta a testování znalostí/reakcí (**nejdůležitější**).
- Monitoring sítě a provozu.

Access Control System (ACS) - přístup do log. i fyz. prostor, více faktorová. Např. detekce obličeje uživatele + čipová karta (mitigace tailgatingu).

**Děkuji za pozornost!**  
**Dotazy ?**

[malina@feec.vutbr.cz](mailto:malina@feec.vutbr.cz)

# Reference I



Peter Schwabe

*Encrypting Network Communication (Presentation)*

<https://cryptojedi.org/peter/teaching/network-security-2017.shtml>, 2017.



Harris, Shon.

*CISSP exam guide.*

Logical Security, 2007.



Christopher Elisan

*Advanced Malware Analysis.*

McGraw-Hill Education, 2015.



Christopher Hadnagy

*Social Engineering : The Art of Human Hacking*

Wiley, 2011.