

Inovace bakalářského studijního oboru Aplikovaná chemie

<http://aplchem.upol.cz>

CZ.1.07/2.2.00/15.0247

Tento projekt je spolufinancován
Evropským sociálním fondem a státním
rozpočtem České republiky.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



OKRESNÍ HOSPODÁŘSKÁ
KOMORA OLOMOUČ

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ



Internet a zdroje

Bezpečnost na Internetu

Základní typy útoků

1. network packet sniffers – neautorizovaný odposlech paketů
2. IP spoofing – paket, který obsahuje zfalšované informace (předstírá, že pochází odjinud, než doopravdy) – předvoj DoS útoku
3. útoky na hesla (Password Attacks) – trójský kůň, IP spoofing, dictionary program, sociální inženýrství atd.
4. útoky z cílem přenést citlivé interní informace z interních zdrojů k neautorizovaným externím zdrojům s cílem zneužití těchto informací
5. neautorizované vstupy do komunikačního kanálu, tzv. útoky "Man-in-the-Middle,,
6. útoky na síťové služby s cílem způsobit jejich nedostupnost, tzv. útoky DoS (Denial of Service) a DDoS (Distributed Denial of Service)



Sociální inženýrství

Způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace

- **Techniky sociálního inženýrství:**

- **Pretexting**

- využívání vymyšleného scénáře → skloubení lži s kouskem pravdivé informace získané dříve (datum narození, rodné číslo, jméno šéfa)

- **Phishing**

- internetový podvod (př. snaha získat přístup k bankovním účtům)

- **IVR (telefonní phishing)** → falešné hlasové automaty

- **Baiting** → trojské koně reálného světa (zanechání infikovaných médií: CD, Flash disků na „vhodném místě“)

Sociální inženýrství

Kevin David Mitnick (* 6. října 1963)

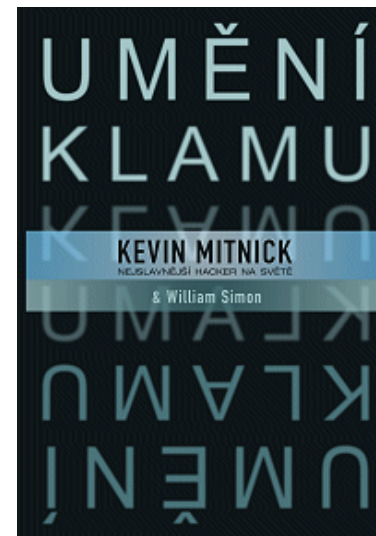
Využití sociálního inženýrství – **phreaking**

Protizákonné činy Kevina (prokázané):

- neoprávněné používání autobusového označovacího systému pro cestování zadarmo
- získání administrátorských práv na počítačích IBM na Computer Learning Center v LA
- nabourání se do systému DEC, nahlédnutí do VMS zdrojového kódu
- nabourání se do systémů firem Motorola, NEC, Nokia, Sun Microsystems a Fujitsu Siemens
- vyhýbání se FBI

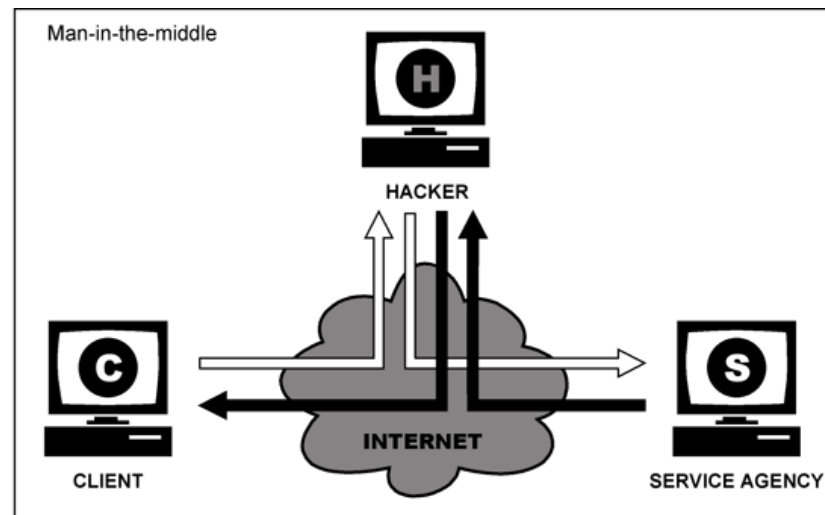
v 90. letech odsouzen (5 let)

V současnosti – bezpečnostní konzultant



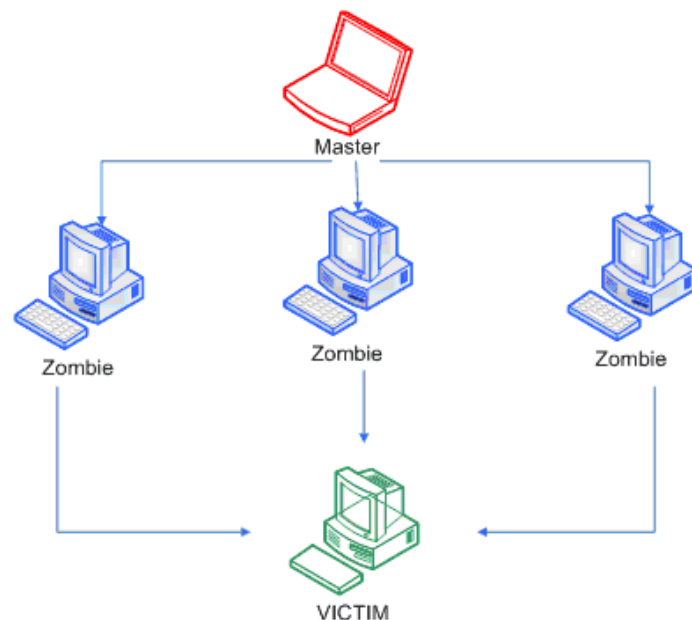
Útoky Man-in-the-Middle

- **Man in the middle** (člověk uprostřed) → odposlouchávání komunikace mezi účastníky tak, že se útočník stane aktivním prostředníkem
- **Řešení problému:**
 - vzájemnou výměnou veřejných klíčů jiným, bezpečným kanálem
 - ověřením získaných veřejných klíčů jiným bezpečným kanálem, nejlépe pomocí jejich otisku
 - ověřením klíčů pomocí elektronického podpisu pomocí certifikační autority nebo sítě důvěry
 - **Kvantová kryptografie** – propletenost a polarizace fotonů



Útoky DoS (1. část)

- **DoS (Denial of Service)** – technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a pádu nebo minimálně nefunkčnosti a nedostupnosti pro ostatní uživatele
- Projevy útoku:
 - zaplavení provozu na síti náhodnými daty které zabraňují protékání skutečných dat
 - Zabránění nebo přerušení konkrétnímu uživateli v přístupu ke službě
 - Narušení konfiguračního nastavení
 - Extrémnímu zatížení CPU cílového serveru
 - Pád samotného operačního systému



Útoky DoS (2. část)

Typy útoku

– ICMP floods

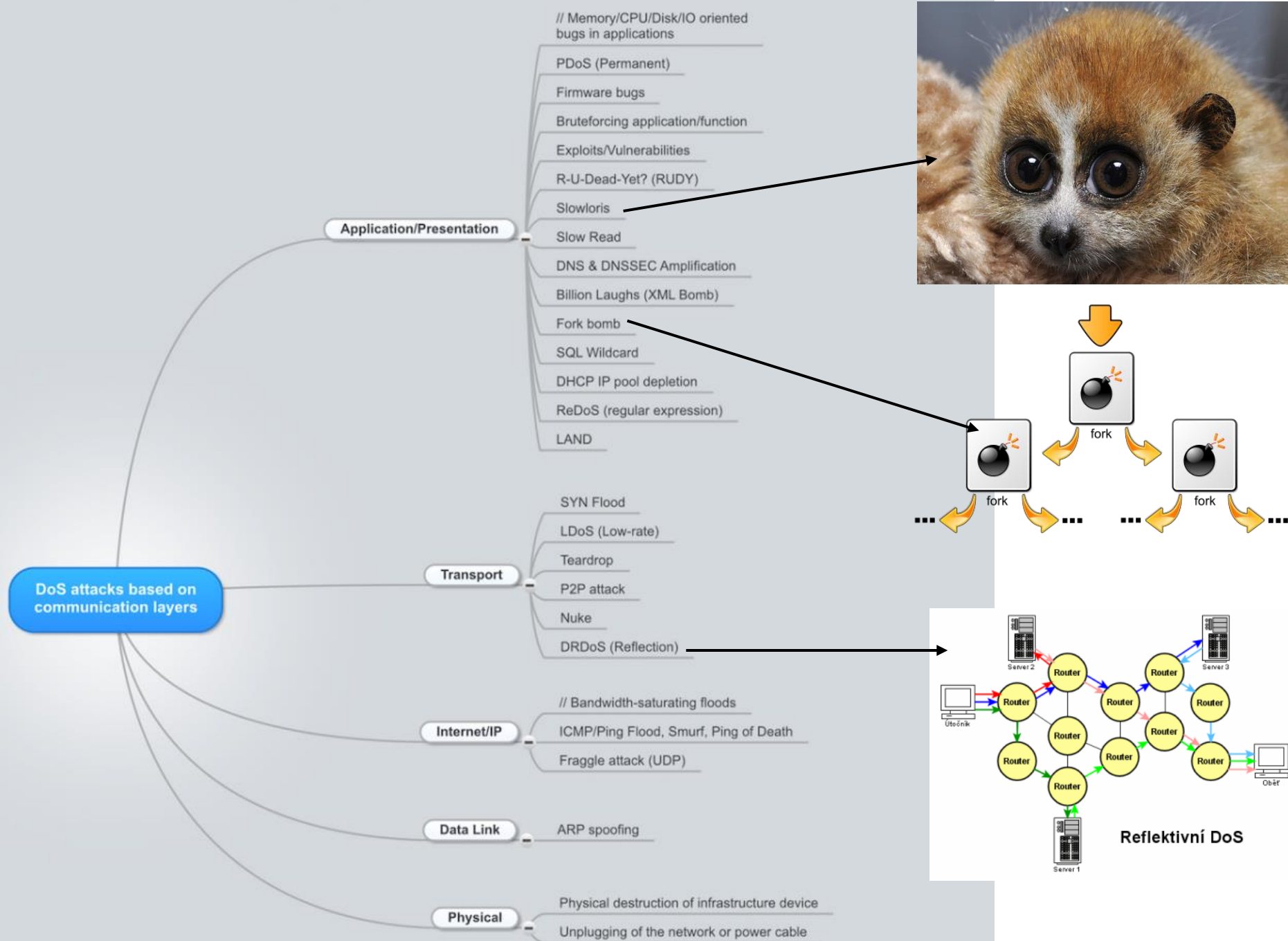
- **Smurf attack** – chyba v konfiguraci systému → rozeslání paketů všem počítačům zapojených v síti přes Broadcast adresu
- **Ping-flood** – zahlcení cílového počítače žádostmi o ping odezvu

– Teardrop útok

- zaslání IP fragmentu s překrývajícím se příliš velkým nákladem dat na cílový počítač

– Peer-to-peer útok – využití masivního zástupu lidí na P2P sítích (zneužití bugu v klientu DC)





http://www.digitalattackmap.com/

Digital Attack Map Top daily DDoS attacks worldwide

[Map](#) · [Gallery](#) · [Understanding DDoS](#) · [FAQ](#) · [About](#)

October 26

2015

Showing All Countries

Show Attacks



Large

Unusual

Combined

Large attacks on United States, Brazil, South Korea, + 10 others

Color Attacks By

Type

Source Port

Duration

Dest. Port

TCP Connection

Volumetric

Fragmentation

Application

Size (Bandwidth, in Gbps)



25

5

1

Shape (source + destination)



between two countries



internal

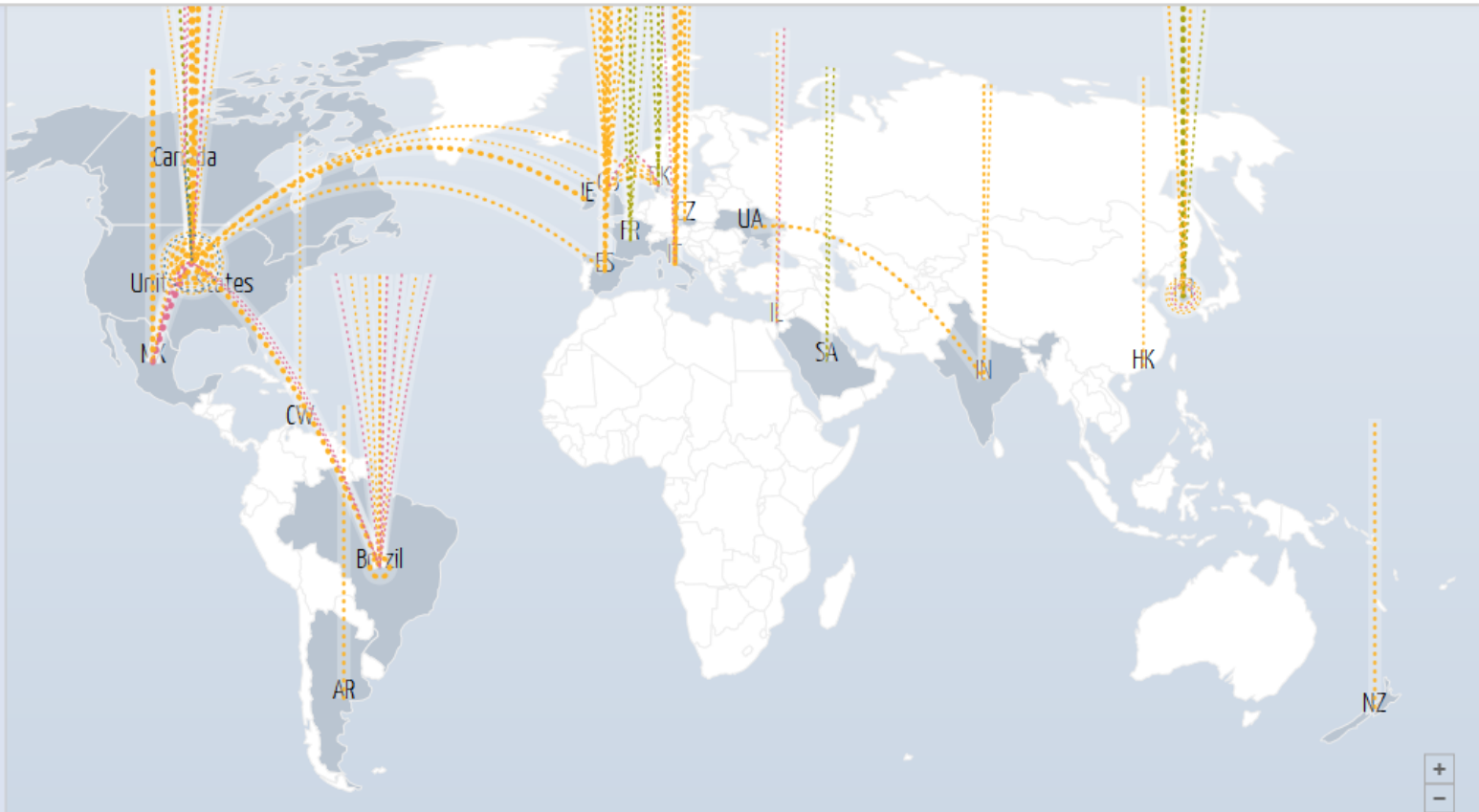


either source or dest. unknown

<Get Embed Code>

Map

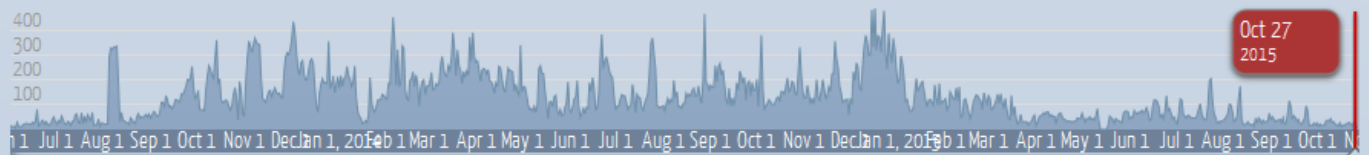
Table



Attack Bandwidth (All Countries), Gbps

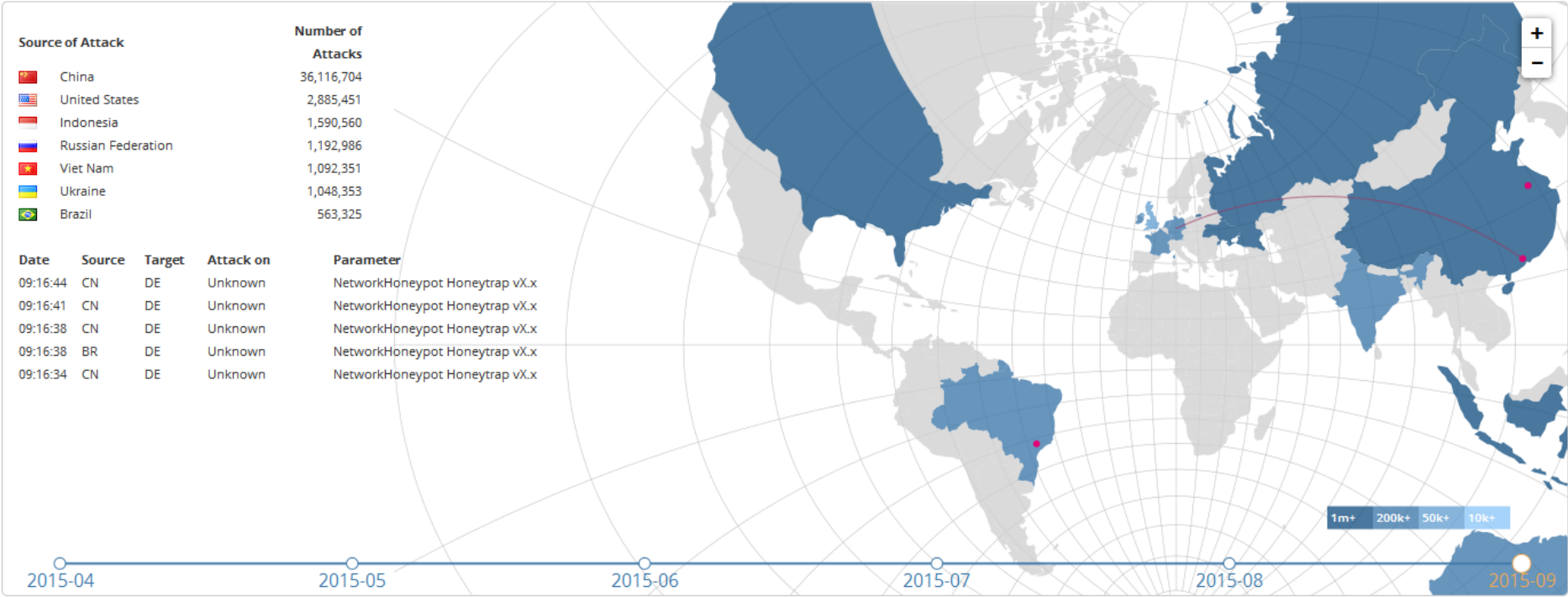
Dates are shown in GMT

Data shown represents the top ~2% of reported attacks

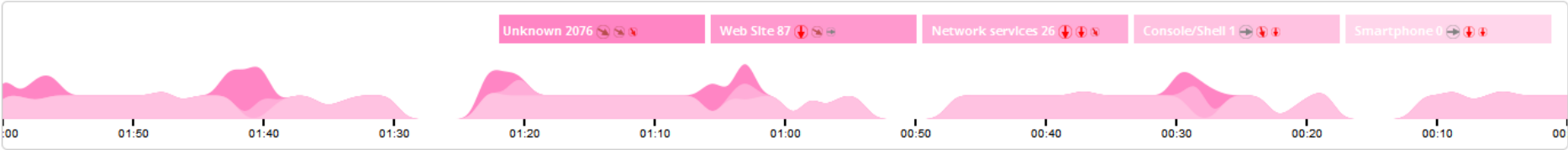


http://www.sicherheitstacho.eu/?lang=en

Overview of current cyber attacks on DTAG sensors (logged by 180 Sensors)



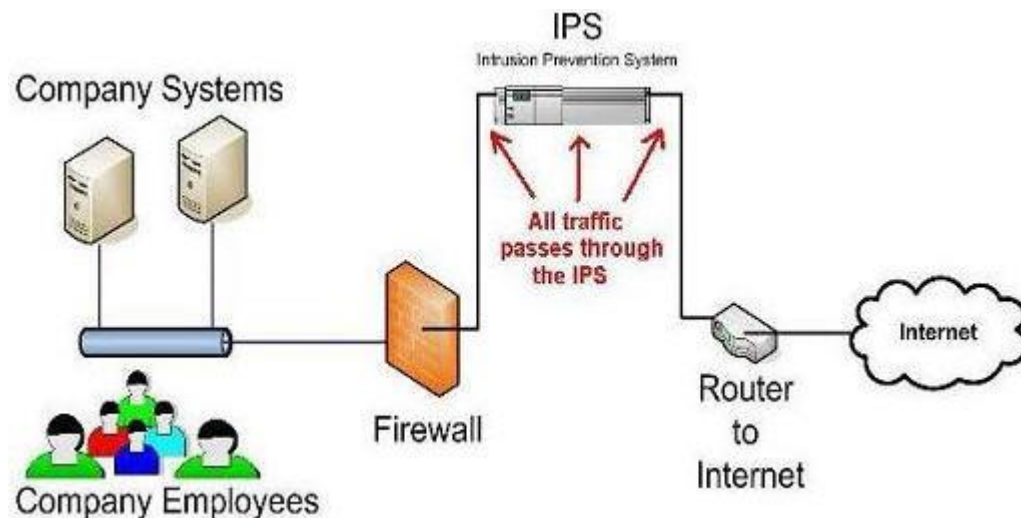
Trend Analyse



Útoky DoS (3. část)

Obrana

- **SYN Cookies**
 - **Modifikace protokolu TCP/IP** – k informacím na serveru se přistupuje až po ověření IP adresy
 - Běžná implementace v **OS Linux/Solaris**
- **Firewall**
- **Intrusion Prevention System** – útok musí mít stejný podpis jako útok, který se provedl dříve

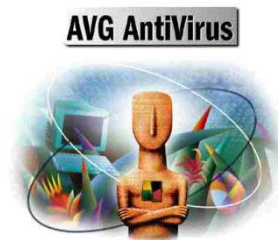


Právní odpovědnost za DOS/DDOS útoky:

[http://technet.idnes.cz/ddos-hrozba-cxk-
/sw_internet.aspx?c=A130308_124737_sw_internet_nyv](http://technet.idnes.cz/ddos-hrozba-cxk-/sw_internet.aspx?c=A130308_124737_sw_internet_nyv)

Jak se bránit?

1. **Používat aktuální antivir, antispyware, firewall**
2. **Pravidelně aktualizovat používaný operační systém a užívané programy (zejména prohlížeče a jejich pluginy. Flash, Java)**
3. **Používat bezpečné heslo**
4. **Kontrolovat u podezřelých stránek jejich skutečnou adresu v řádku prohlížeče**
5. **Neotvírat neznámé či podezřelé soubory, programy nebo přílohy poštovních zpráv**
6. **K citlivým službám se připojovat pouze z vlastního počítače a nikdy přes neznámou wifi nebo z internetové kavárny**



Jak se bránit? (2. část)

7. **U internetového bankovníctví se řádně odhlašovat ze služby**
8. K zabezpečení e-mailové komunikace používat vhodné programy jako PGP, GnuGP
9. Pamatovat že smazaná data nejsou na disku ve skutečnosti smazána, ale pouze označena k přepsání (Recuva)
10. **Pravidelně zálohovat důležitá data**
11. V sociálních sítích využívat co nejméně aplikací třetích stran (her, kvízů atp.)
12. **Uvažovat, které informace o sobě internetu poskytujete**



Viry/Antiviry

Virus = typ programu, který se dokáže sám šířit tím, že vytváří (někdy upravené) kopie sebe sama

Další info → Igiho stránka o virech: www.viry.cz

Typy virů:

Podle hostitele

- Spustitelné soubory (.exe, .com)
- Boot sektory (disky)
- MBR
- Dávkové soubory (.bat)
- Makra (Office)
- Skripty

Podle způsobu činnosti

Rezidentní/nerezidentní • stealth viry • makro viry



Antiviry – test (srpen 2015)

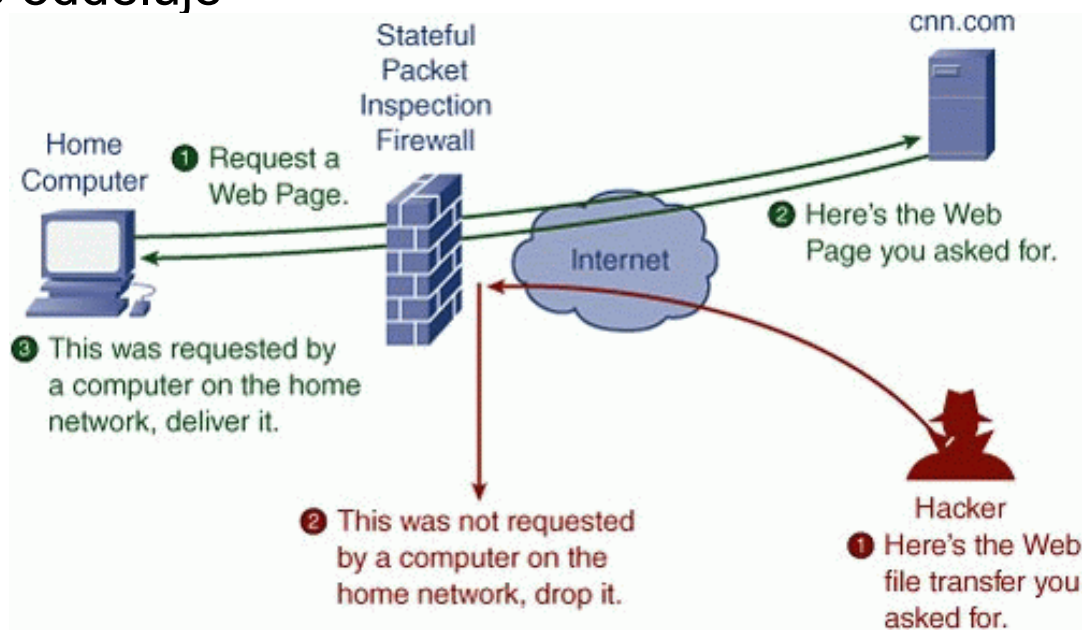
August 2015					
	Name		Protection	Performance	Usability
AhnLab	AhnLab V3 Internet Security 9.0				
avast!	Avast Free AntiVirus 2015				
AVG	AVG Internet Security 2015				
Avira	Avira Antivirus Pro 2015				
Bitdefender	Bitdefender Internet Security 2015				
BullGuard	BullGuard Internet Security 15.1				
COMODO	Comodo Internet Security Premium 8.2				
eset	ESET Smart Security 8.0				
F-Secure	F-Secure Internet Security 2015				
G DATA	G Data InternetSecurity 2015				
K7	K7 Computing Total Security 14.2 & 15.1				
Kaspersky	Kaspersky Lab Internet Security 2015 & 2016				
intel Security	McAfee Internet Security 2015				
eScan	MicroWorld eScan Internet Security Suite 14.0				
NORMAN	Norman Security Suite Pro 11.0				
Norton	Norton Norton Security 2015				
panda	Panda Security Free Antivirus 15.1				
360	Qihoo 360 360 AntiVirus (BD+QVM) 5.0				
Quick Heal	Quick Heal Total Security 16.0				
TREND MICRO	Trend Micro Internet Security 2015 & 2016				
Microsoft	Microsoft Security Essentials 4.8				

Firewall

- síťové zařízení/aplikace, sloužící k řízení a zabezpečení síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení
- **Zjednodušeně:** kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje

Rozdělení firewallů:

- **Paketové filtry**
- **Aplikační brány**
- **Stavové paketové filtry**
- Stavové paketové filtry s kontrolou známých protokolů a popř. kombinované s IDS



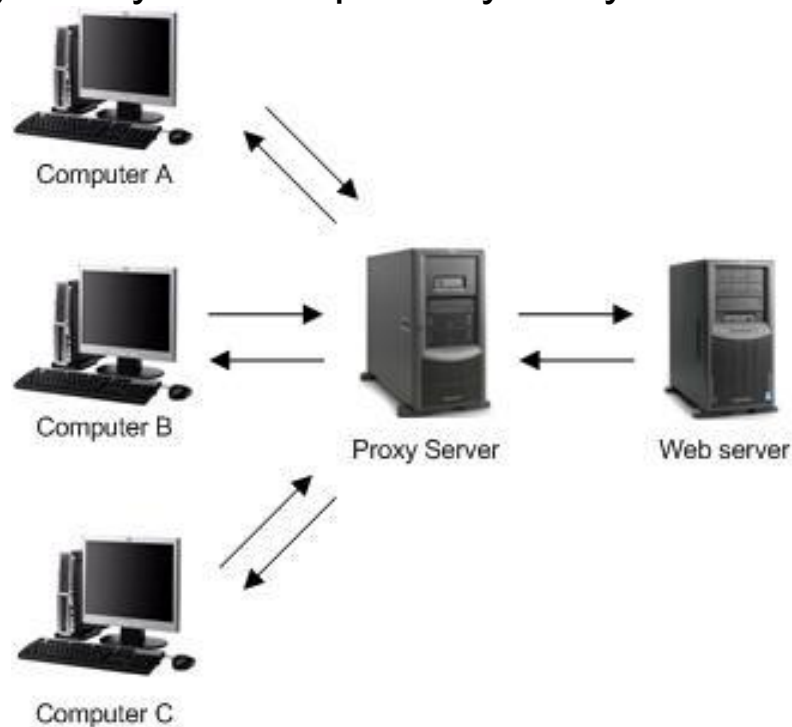
Firewall – podrobněji

Paketové filtry: Nejjednodušší a nejstarší forma firewallování

- pravidla přesně uvádějí, z jaké adresy a portu na jakou adresu a port může být doručen procházející paket
- **Výhoda:** vysoká rychlost zpracování (vysokorychlostní přenosy velkých množství dat)

Aplikační brány (Proxy firewall):

- **Průběh komunikace** → klient (iniciátor spojení) se připojí na aplikační bránu (proxy), ta příchozí spojení zpracuje a na základě požadavku klienta otevře nové spojení k serveru, kde klientem je aplikační brána. Data, která aplikační brána dostane od serveru, pak zase v původním spojení předá klientovi



Firewall – podrobněji 2

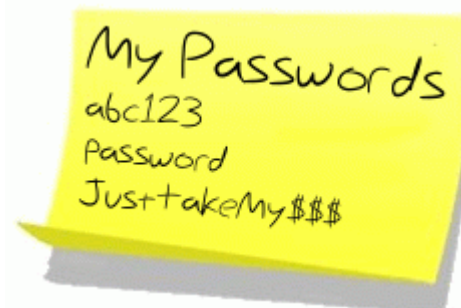
Stavové paketové filtry:

- kontrola jako u paketových filtrů + ukládání informací o povolených spojeních → usnadnění rozhodnutí zda pakety pustit nebo ne
- Výhody:
 - urychlení zpracování paketů již povolených spojení
 - nastavení směru navazování spojení → firewall sám povolí odpovědní pakety
 - Vysoká rychlost, relativně solidní úroveň zabezpečení (je horší než u Aplikační brány), jednoduchá konfigurace
- Příklady:
 - Komerční: Cisco PIX, Cisco IOS Firewall
 - Free: `iptables` v linuxovém jádře a `ipfw` v *BSD

Bezpečné heslo

- **Nevhodná volba hesla:**

- vlastní jméno či jméno někoho z rodiny, jméno psa, milenky apod.
- rodné číslo či datum narození
- č. domu, adresa, telefonní číslo...
- heslo, 1234...



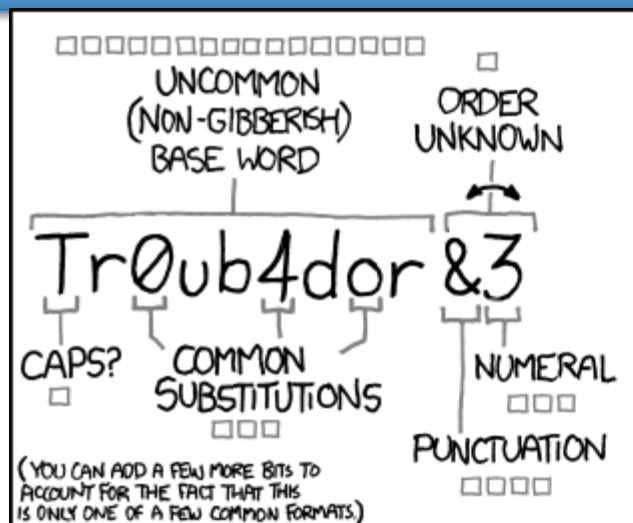
- **Délka hesla:** minimálně 8 znaků (nejlépe 14+)

- **Kvalita hesla:** kombinace písmen, čísel a znaků

- Heslo skládající se z 15 náhodných písmen a číslic je přibližně 33 tisíckrát bezpečnější než heslo tvořené 8 znaky z celé klávesnice

Délka hesla		4	5	6	7	8
		Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec
0-9	10 znaků	10 000 2 minuty	100 000 16 minut	1 000 000 3 hodiny	10 000 000 1 den	100 000 000 11 dní
a-z, 0-9	36 znaků	731 16 16 5 hodin	380 20 40 32 7 dní	2 x 10 ⁹ 8 měsíce	8 x 10 ¹⁰ 25 let	3 x 10 ¹² 900 let
a-z, A-Z, 0-9	62 znaků	14 776 336 2 dny	916 13 28 32 3 měsíce	5 x 10 ¹⁰ 18 let	4 x 10 ¹² 1000 let	2 x 10 ¹⁴ 70 000 let
a-z, A-Z, 0-9; ščáěě... ;@#\$%^*?!...	85 znaků	522 006 25 6 dní	44 370 53 12 1 rok	3 x 10 ¹¹ 120 let	3 x 10 ¹³ 10 000 let	3 x 10 ¹⁵ 800 000 let

Bezpečné heslo



~28 BITS OF ENTROPY

□□□□□□□□
□□□□□□□□
□□□□
□□□□

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

(PLAUSIBLE ATTACK ON A WEAK REMOTE
WEB SERVICE. YES, CRACKING A STOLEN
HASH IS FASTER, BUT IT'S NOT WHAT THE
AVERAGE USER SHOULD WORRY ABOUT.)

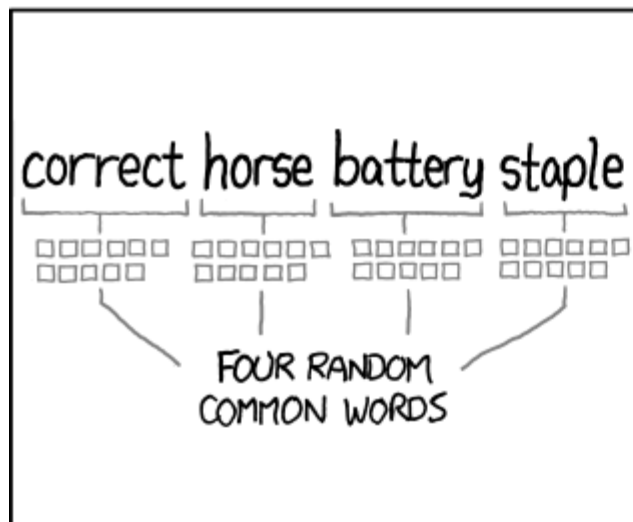
DIFFICULTY TO GUESS:
EASY

WAS IT TROMBONE? NO,
TROUBADOR. AND ONE OF
THE 0s WAS A ZERO?

AND THERE WAS
SOME SYMBOL...



DIFFICULTY TO REMEMBER:
HARD



~44 BITS OF ENTROPY

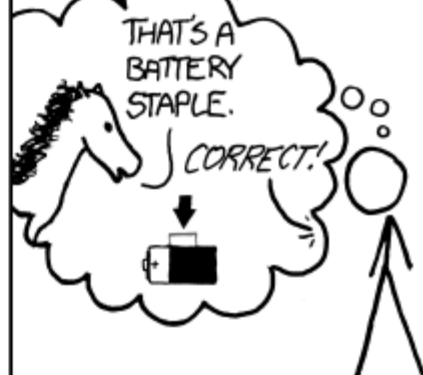
□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS:
HARD

THAT'S A
BATTERY
STAPLE.

CORRECT!



DIFFICULTY TO REMEMBER:
YOU'VE ALREADY
MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED
EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS
TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Historie šifrování

- První doložení šifrování zpráv – 480 př. n. l. v bitvě u Salemíny (Řecko-Perské války)

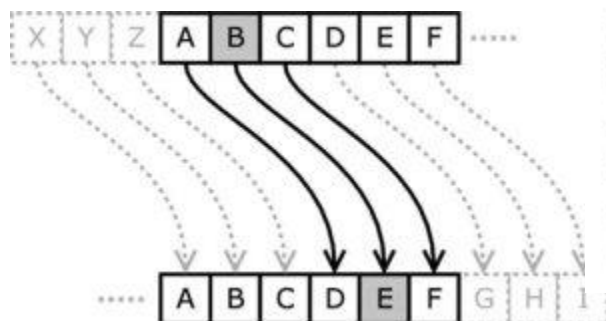
- Julius Caesar

Historické metody:

- **Substituční šifry** – Caesarova šifra, Vigenèrova
- **Aditivní šifry** – Vernamova šifra
- **Transpoziční šifry** – transpoziční mřížka



Caesarova šifra



Plaintext
Numeric Equivalent
+ Random Number
= Sum
= mod 26
Ciphertext

Vernamova šifra

V	E	R	N	A	M	C	I	P	H	E	R
21	4	17	13	0	12	2	8	15	7	4	17
76	48	16	82	44	3	58	11	60	5	48	88
97	52	33	95	44	15	60	19	75	12	52	105
19	0	7	17	18	15	8	19	23	12	0	1
t	a	h	r	s	p	i	t	x	m	a	b

Historie šifrování

Vigenèrova šifra

wikipedie
bagrbagrb

XIQZQEJZF

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Historie šifrování

Vernamova šifra (1917 Gilbert Vernam)

- jednorázová tabulková šifra
- posun každého znaku zprávy o náhodně zvolený počet míst v abecedě.

Vernamova šifra je v principu nerozluštitelná

Podmínky spolehlivosti:

1. Klíč je tak dlouhý jako přenášená zpráva
2. Klíč je dokonale náhodný
3. Klíč nelze použít opakovaně



One Time Pad or Vernam Cipher

Encryption									
S	H	E	I	S	L	A	Z	Y	
18	7	4	8	18	11	0	25	24	
2	3	1	4	5	13	7	6	2	
20	10	5	12	23	24	7	5	0	
U	K	F	M	X	Y	H	F	A	
Decryption									
U	K	F	M	X	Y	H	F	A	
20	10	5	12	23	24	7	5	0	
2	3	1	4	5	13	7	6	2	
18	7	4	8	18	11	0	25	24	
S	H	E	I	S	L	A	Z	Y	

Historie šifrování

Ukázka transpoziční šifry

T						F	M			O	W	A	S			G				
			H			Y	D					A		N	E	E		R		A
	R	E		P							X								T	I
						E	A		T			A							O	N
	O	R		T				H							G	X				

T	W	G	A	S	O
F	E	M	R	H	A
Y	A	D	N	E	E
X	R	E	T	P	I
E	A	A	O	T	N
X	O	R	H	T	G

Základy moderního šifrování

Symetrická kryptografie

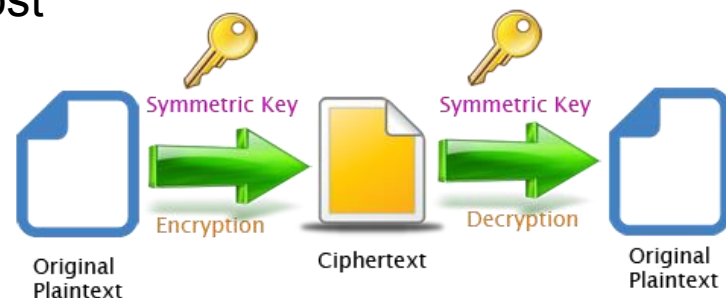
→ šifrovací algoritmus používá k šifrování i dešifrování jediný klíč

- Výhoda: nízká výpočetní náročnost
- Nevýhoda: nutnost sdílení tajného klíče

- **Rozdělení:**

- **Blokové šifry** → rozdělí otevřený text na bloky stejné velikosti a doplní vhodným způsobem poslední blok na stejnou velikost (AES, Blowfish, DES atd.)

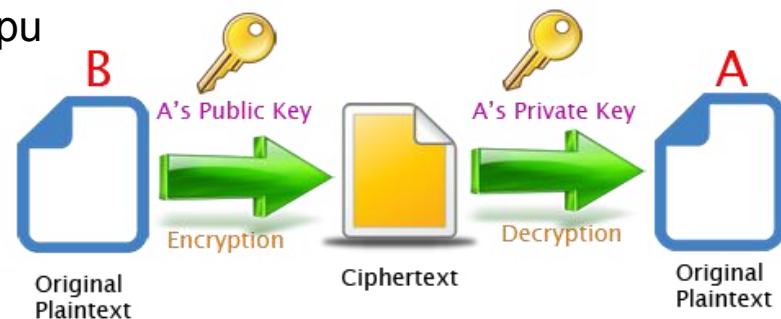
- **Proudové šifry** → zpracovávají otevřený text po jednotlivých bitech (FISH, RC4)



Základy moderního šifrování

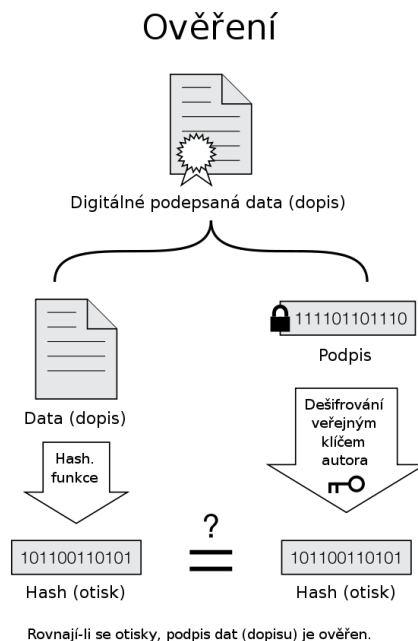
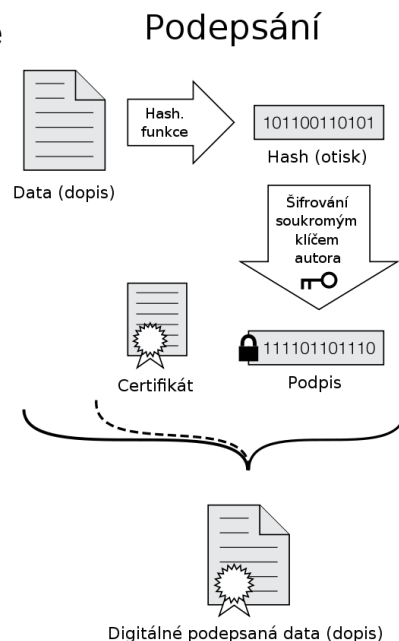
Asymetrická kryptografie

- pro šifrování a dešifrování používají odlišné klíče (využití i u elektronického (digitálního) podpisu)
- Nejběžnější verzí asymetrické kryptografie je využívání tzv. veřejného a soukromého klíče:
 - šifrovací klíč je veřejný, majitel klíče ho volně uveřejní
 - dešifrovací klíč je soukromý, majitel jej drží v tajnosti
- Mechanismy funkce
 - Asymetrická kryptografie je založena na tzv. jednocestných funkcích → operace, které lze snadno provést pouze v jednom směru
 - ze vstupu lze snadno spočítat výstup, z výstupu však je velmi obtížné nalézt vstup (např. násobení)
 - rozklad součinu na činitele (tzv. faktorizace) je velmi obtížný



Digitální podpis

- Elektronický podpis jsou elektronické identifikační údaje autora (odesílatele), které jsou připojené k elektronickému dokumentu
- Zaručený elektronický podpis dokumentu zajišťuje:**
 - autenticitu** – lze ověřit původnost (identitu subjektu, kterému patří elektronický podpis)
 - integritu** – lze prokázat, že po podepsání nedošlo k žádné změně, soubor není úmyslně či neúmyslně poškozen
 - nepopiratelnost** – autor nemůže tvrdit, že podepsaný elektronický dokument nevytvořil (např. nemůže se zříct vytvoření a odeslání výhružného dopisu)
 - může obsahovat **časové razítko**, které prokazuje datum a čas podepsání dokumentu



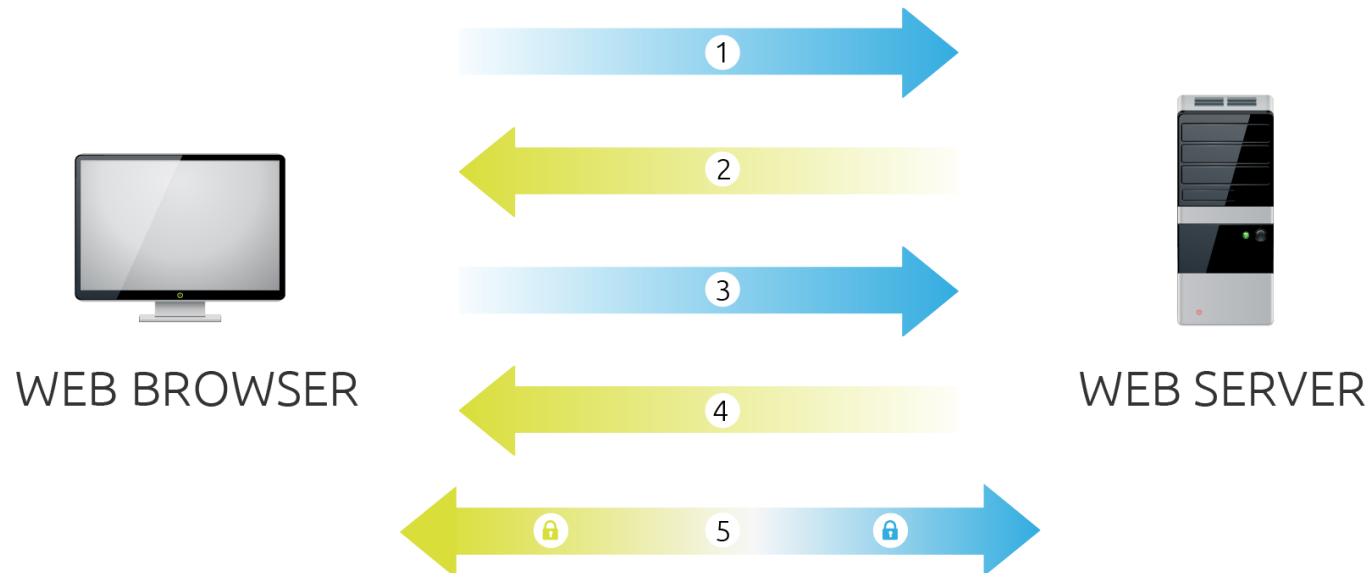
zaručený elektronický podpis – zákon č. 227/2000 Sb., o elektronickém podpisu

Certifikáty a jejich využití

- Využití při ověření veřejného klíče (viz asymetrické šifrování)
- Certifikát definuje vazbu uživatel—klíč a definuje délku trvání této vazby
- Certifikáty vydává certifikační autorita – certifikační servery,
 - např. Microsoft
 - U nás certifikační autorita (www.ca.cz) nebo CA Czechia (www.caczechia.cz)
- Certifikát musí obsahovat:
 - Identifikátor algoritmu certifikační služby
 - Jméno autority, která certifikát vydala
 - Dobu platnosti certifikátu
 - Informace o veřejném klíči



- **Browser** connects to a web server (website) secured with SSL (https). Browser requests that the server identify itself.
- **Server** sends a copy of its SSL Certificate, including the server's public key.
- **Browser** checks the certificate root against a list of trusted CAs and that the certificate is unexpired, unrevoked, and that its common name is valid for the website that it is connecting to. If the browser trusts the certificate, it creates, encrypts, and sends back a symmetric session key using the server's public key.
- **Server** decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.
- **Server** and **Browser** now encrypt all transmitted data with the session key.





HOW **SAFE** IS YOUR
COMPUTER?



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



OKRESNÍ HOSPODÁŘSKÁ
KOMORA OLOMOUČ

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

**Inovace bakalářského studijního
oboru Aplikovaná chemie**