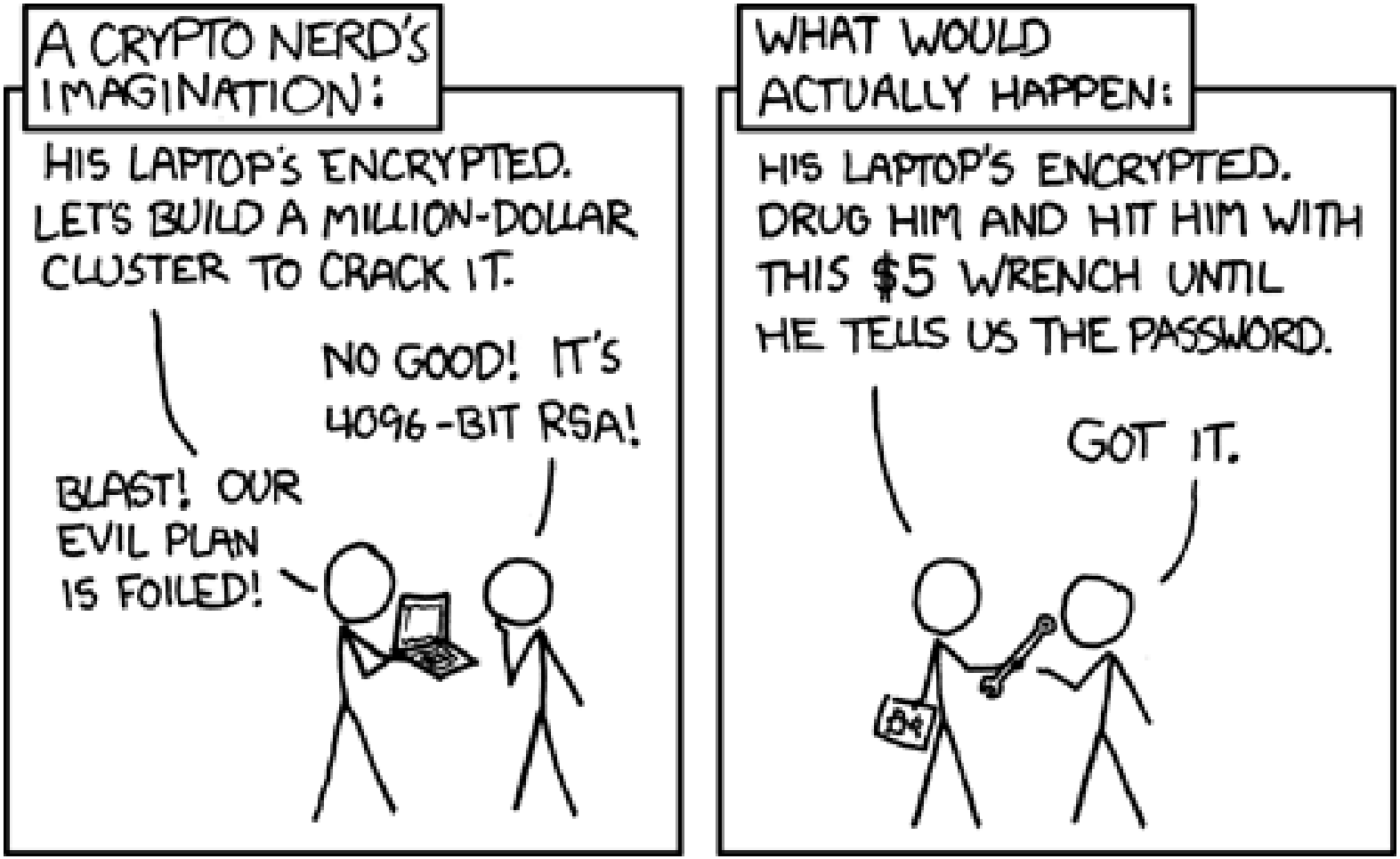
Be Safe!

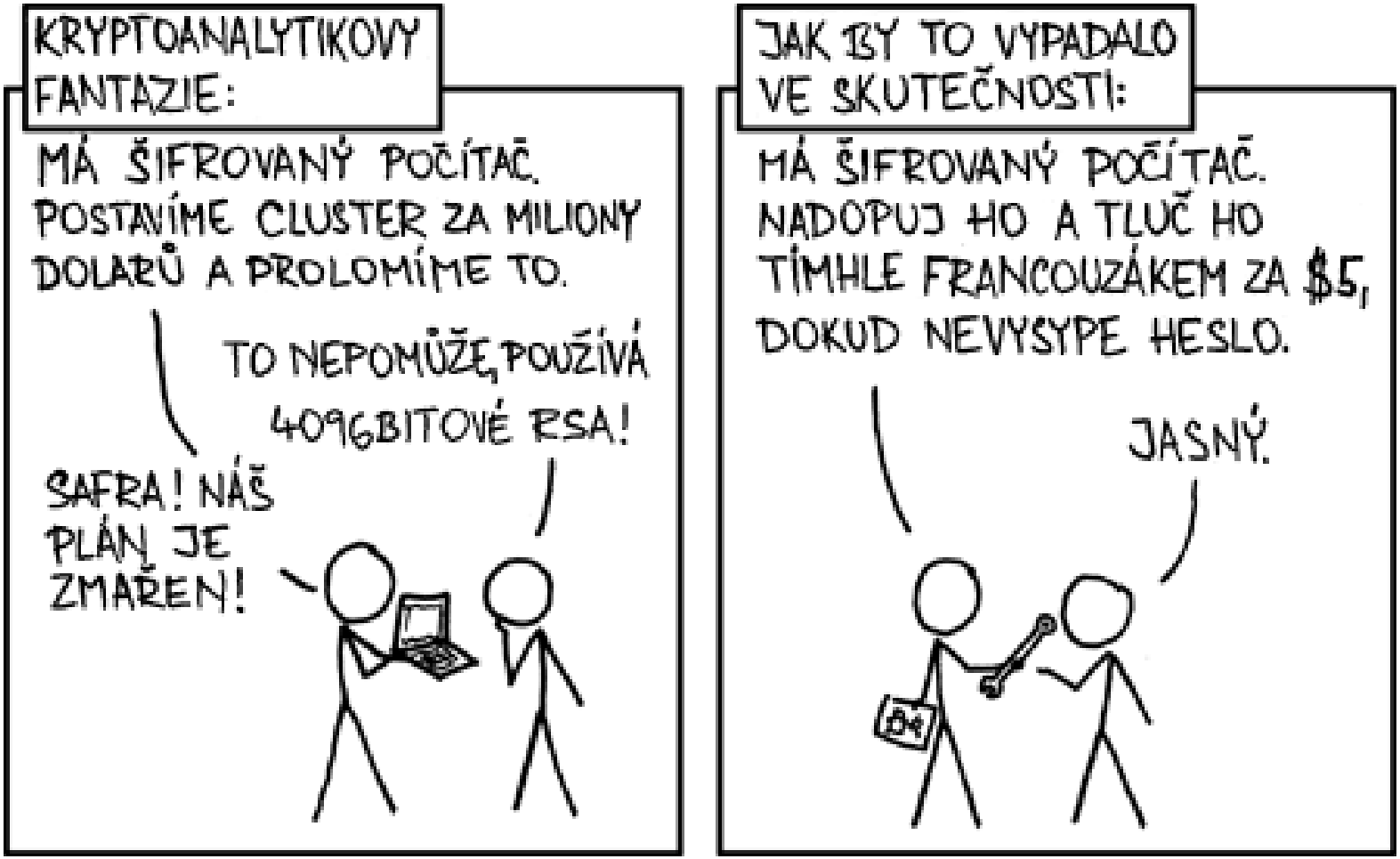
Radim Roška

Installfest 2010
Silicon Hill

6.4. 2009



zdroj:xkcd.com



zdroj:abclinuxu.cz

Obsah

Co je to bezpečnost?

- bezpečná komunikace/přenos dat
- bezpečné uložení dat
- celistvost dat (ochrana před neoprávněnou manipulací..)

Outline

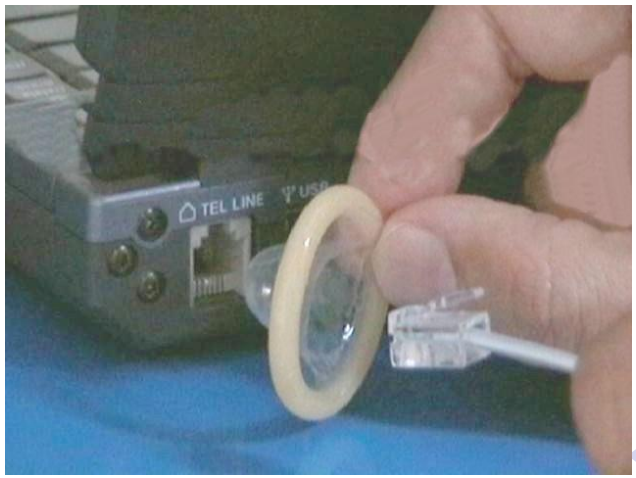
Malware = malicious software

- software, jehož účelem je nabourat cizí počítač
- neboli sw co je nepřátelský, otravný,..atd (záměrně:)
- viry, červy, trojské koně, rootkity, spyware
- v USA v zákonech označovány jako “computer contaminant”
- cíl:
  - získat citlivé údaje
  - začlenit PC do botnetu - ty pak rozesílají spam, provádí DOS útoky, fast flux DNS technika

Botnet

Viry

- program, který se sám množí a rozšiřuje (většinou emaily)
- většinou jsou součástí legitimního programu -> infikovaný program - hostitel
- vyžaduje nějakou uživatelskou akci (neklikat bez rozmyslu)
- prakticky win-only
- můžou být destruktivní, často jen prudící...
- způsob ochrany: antivirové programy (existují i pro Linux - SMTP servery)



Červi - fuj

stejně jako viry se rozšiřují, ale

- rychleji - nevyžadují uživatelskou akci
- jsou to samostatné programy
- mohou napadnout jakýkoliv děravý počítač (chyby v programech)
- => nejúčinější zbraň

Červi - fuj fuj

- nakažené PC scanují počítače v Internetu a snaží se najít děravého kolegu => scanování = podezřelá činnost

Ochrana:

- PRAVIDELNÉ AKTUALIZACE
- neklikat bez rozmyslu
- mít spuštěné jen ty nejnutnější síťové služby *netstat -putnal*

Trojské koně

- Kdo s tím přišel? :)
- trojan je součástí zdánlivě užitečně fungujícího sw
- pro fungovaní vyžaduje uživatelskou akci
- neplecha: zařazení pc do botnetu, krádež hesel, instalace malwaru, backdoor, . . .

Pozn. pro přednášejícího - ukaž příklad ls.

Trojské koně

- nakažení:
  - stažený sw - nedůvěryhodný zdroj (p2p), kompromitovaný zdroj (význam hashu u aplikací na netu?:)
  - emaily, web
  - díra v aplikaci -> červ nainstaluje trojana
- obrana:
  - např. AIDE - databáze hashů souborů (?)
  - antivirové programy
  - prevence při instalaci

Rootkity, spyware

- rootkit - maskuje přítomnost malware
- spyware - odesílá bez vědomí uživatele informace
  - adware - obtěžující reklama
  - hijacker - mění homepage
  - dialer - přesměrování linky
  - keystroke logger

Outline

Lidé

- faktor #1 LENOST
- zloděj - krádeže notebooků, mobilů s citlivými daty
- sociální sítě (velmi vhodné pro phishing)

Phishing (sociální inženýrství)

- chytání bezstarostných uživatelů
- cíl : získat z rybiček přístupové údaje, informace o platební kartě, ...
- medium : email, instant-messaging, oblíbené webové služby/stránky

Phishing - příklad

From: Paypal.co.uk [Alerts@Paypal.co.uk] Sent:
To: Elinor Mills
Cc:
Subject: Paypal Account Notification.

PayPal

Dec 2009

Dear users of PayPal services,

Privacy. Prevention. Protection. PayPal

Due to upcoming changes in our Service Agreement in December 2009, you will need to submit additional details on your PayPal account. Starting in 2010 all PayPal accounts will come with complete detailed information! Identity protection matters. And PayPal works day and night to help keep your identity safe.

Identity protection matters. Get Verified!

According to the new changes in our Service Agreement, any unverified account will be deleted from the system in 72 hours after receiving this notice.

Your Account

Tips to Protect Your Account NEW!
PayPal's world class fraud investigators share 5 important

Identity Protection Highlights

New spoof tutorial
Learn how to spot and avoid fraudulent "spoof" emails and websites with PayPal's handy 5-step spoof tutorial.

Phishing - příklad

-----Original Message-----
From: Facebook [mailto:notificationzj4oo4ta4c9@newparamejnetco.com]
Sent: Friday, November 06, 2009 2:52 PM
To: undisclosed-recipients
Subject: Caroline sent you a message on Facebook...

Caroline sent you a message.

(no subject)

Hello, have we met ever before??

Thanks,
The Facebook Team

To reply to this message, follow the link below:
http://facebook.montadalitihad.com/html-h1.htm

Phishing - ochrana

- zkontroluj odchozí adresu, podívej se na hlavičku
- je to https?!!, zkontroluj certifikát
- tyto vadné emaily/stránky často plné chyb
- v emailu nikdy nikdo legitimně nechce citlivé údaje
- mysli kam klikáš
- ignoruj přílohy od neznámých lidí
- používej vhodný webový prohlížeč (čti nepoužívej IE)

Outline

Zranitelnost různých OS

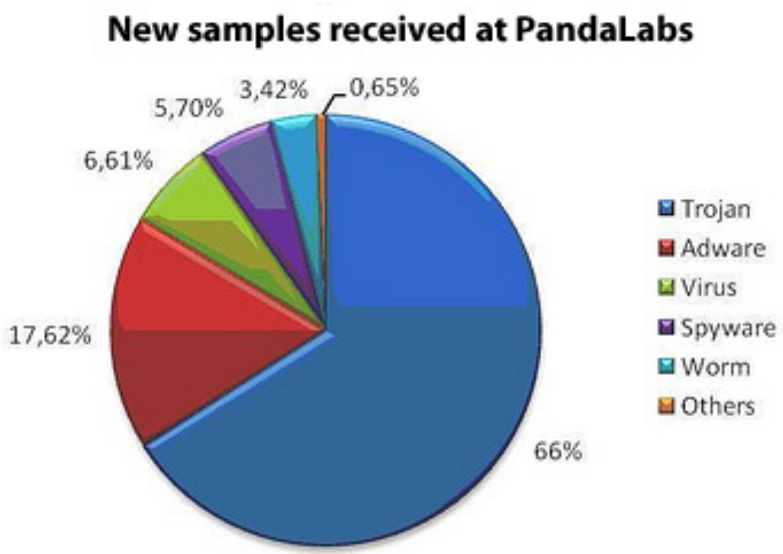
- všichni se musí mít na pozoru! - sociální inženýrství neni OS related:)
- Windows* OS jsou zranitelnější vůči malware než třeba Linux, protože
  - repozitaře v Linuxu
  - nové(stažené soubory) nejsou implicitně spustitelné
  - fungující access control mechanismus v Linuxu
  - navíc Linux z hlediska počtu uživatelů nezajímavý
  - . . . :)
- neaktualizovaný sw je pozvánka pro červy

Další

- wireless - WEP,. . .
- neznámé prostředí -> nedůvěřujte zabezpečení sítě
- spousta pokročilých útoků v sítí - arp poisoning, dns poisoning,. . .

Statistiky

- v průměru aktivováno 312 000 zombie denně(přes 20% v Brazílii)!
- téměř všech 98% emailů je nevyžádaných (81% lékárenské produkty:)
- v roce 2009 bylo vytvořeno 25 milionů nových druhů malware
- rozložení malware



zdroj:net-security.org

Outline

Kryptografie

- wiki: “Kryptografie neboli šifrování je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí.”
- šifra je kryptografický algoritmus, který převádí prostý text na šifrovaný text
- kryptografický systém = vstupní zpráva, tajný klíč, šifrovací algoritmus, zašifrovaná zpráva

Kryptoanalýza

- Luštění zašifrovaných zpráv - bez znalosti klíče
- šifra je výpočetně bezpečná, pokud ji není možné zlomit v rozumném čase a nebo levněji než je cena zašifrované informace
- základ - brute force ;)
  - 128 bitový klíč => 3.4 x 10^{38} různých klíčů=> milion decrypt operací/ms => 5.4 x 10^{18} let

Základní rozdělení šifer

- substituční = nahrazení každého znaku jiným podle nějakého pravidla
- transpoziční = změna pořadí znaků

Substituční šifry

- Caesarova - velmi jednoduchá šifra, klíčem je pevný počet pozic, o které se písmena vstupní zprávy posunou
  - klíč = 5; NSXYFQQKJXYGQF = ?
    úkol: jak zní zpráva?
- Vigenerova - postavena na vigenerově tabulce
- Vernamova - anglicky též one time pad
  - klíč je dokonale náhodný, stejně dlouhý jako text a použije se jen jednou => nepraktická
  - NEPROLOMITELNÁ šifra => používala se za studené války (Moskva-Washington)

Jak zlomit substituční šifru?

Útok na tyto šifry přes frekvenční analýzu písmen(ahoj -> a=25%,b=25%,..)
Platí pro delší texty a je třeba znát jazyk:).

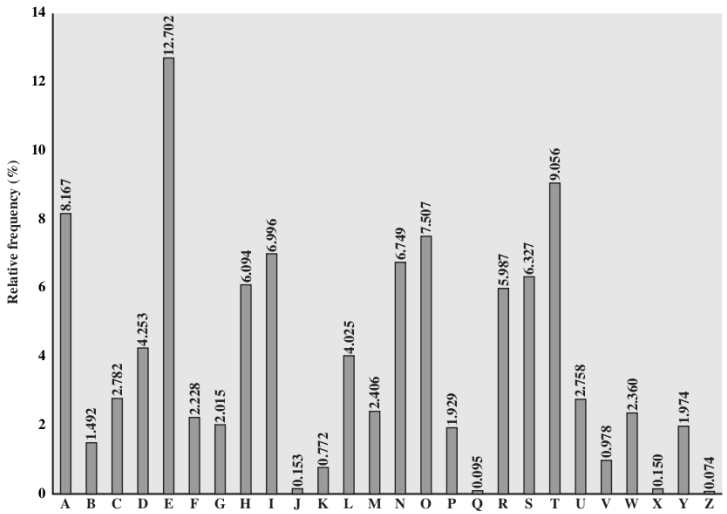


Figure 2.5 Relative Frequency of Letters in English Text

Transpoziční šifry

- sloupcová šifra - klíč = délkou určuje počet sloupců a abecední pořadí určuje pořadí pro daný sloupec

```
heslo                                   heslo
21534                                   21534

dnesn                                    n
idenj   =>  ndfdiesnjnjneae   =>         d
efajn                                    f
```

- Rail Fence šifra - klíč = počet řádků
  úkol: jak se dešifruje?

```
i   t   l   s
 n   a   f   t   =>  itlsnaftsle
  s   l   e
```

Další vývoj kryptografie

- Po základních substitučních a transpozičních šifrách lidé přišli s algoritmy, které šifrují vícenásobně. Např. kombinace substituční a transpoziční šifry.
- Používání strojů - 2 světová válka - Enigma
- Zásadní změna s příchodem počítačů. . .

Další základní rozdělení šifer:)

- blokové = šifruje se po blocích - třeba po 128 bitech
  - DES, AES
- řetězové = šifrují po jednom bitu/bytu/znaku (e.g. one time pad)
  - RC4

Nejklíčovější rozdělení z pohledu využití:

- symetrické = šifruje/dešifruje se jedním klíčem - musí znát POUZE odesilatel a příjemce, problém s distribucí klíče
  - DES, AES
- asymetrické = jsou 2 klíče - soukromý a veřejný
  - RSA, DSA

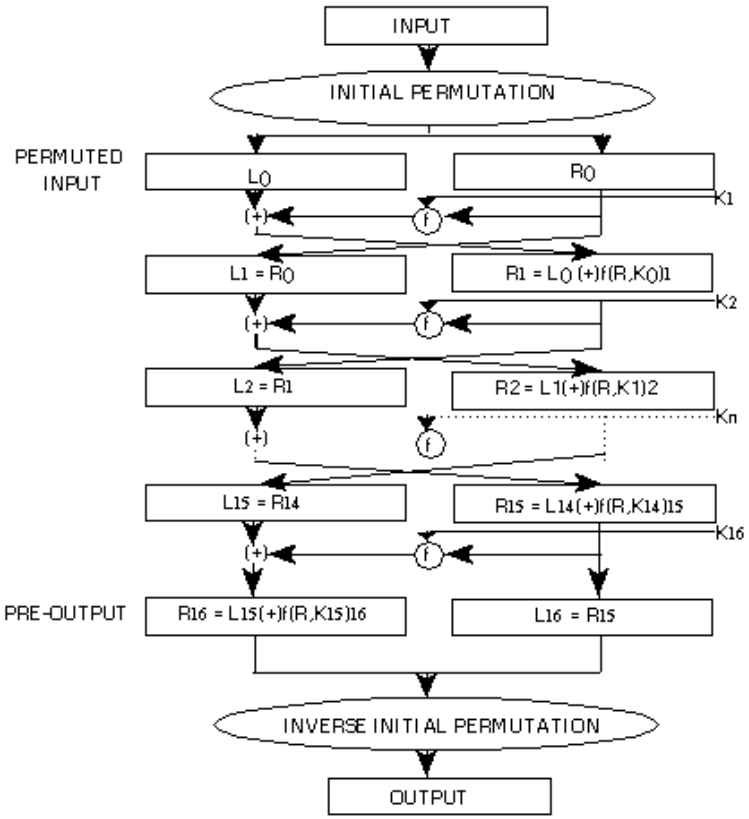
Porovnání a/symetrických šifer

- symetrické
  - + krátší klíče (dnes doporučeno alespoň 128bitů), rychlejší,
  - - klíč musí být bezpečně přenesen příjemci, odesilatel není jednoznačně identifikován
- asymetrické (též public-key šifra)
  - + schéma public/private key odstraňuje problém s distribucí klíče(veřejného), jednoznačná identifikace
  - - výrazně delší klíč (doporučeno min. 2048bitů), výrazně pomalejší)(100x-1000x pomalejší)

Outline

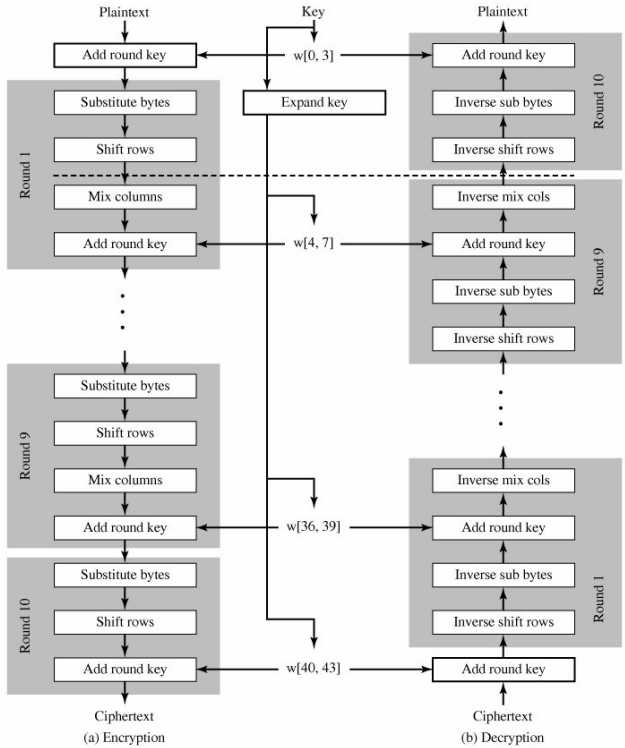
DES - Data Encryption Standard

- 1974 - by IBM & NSA; 56-bit klíč
- upgrade => 3DES enc(k3,(dec(k2,enc(k1,msg))))



AES - Advanced Encryption Standard

V roce 2000 vybrána jako náhrada za DES. Klíč má 128 bitů.



výborná animace: http://www.cs.bc.edu/ straubin/cs381-05/blockciphers/rijndael_ingles2004.swf

RSA

Princip: rozložit(faktorizovat) velké číslo na součin prvočísel je velmi těžké (více na wiki;)
(Velké číslo = je doporučeno používat 2048bitů velké klíče)

Klíč je ve skutečnosti pár klíčů - soukromý a veřejný. Pro zašifrování se použije jeden z nich, pro dešifrování druhý.

RSA je vhodné jak pro šifrování tak pro podpis.

Outline

Hash = “otisk dat”

účel - detekce změn ve zprávě

hash = hash_funkce (zpráva)

Algoritmy - SHA, MD5, Whirlpool

note: ukázka avalanche efektu

MAC = Message Authentication Code

MAC se někdy označuje jako kryptografický hash
účel - detekce změn + ověření odesilatele (nedokonalé)
mac = mac_funkce(tajný klíč, zpráva)

Outline

Princip digitálního podpisu

účel: ověření odesilatele, integrita dat

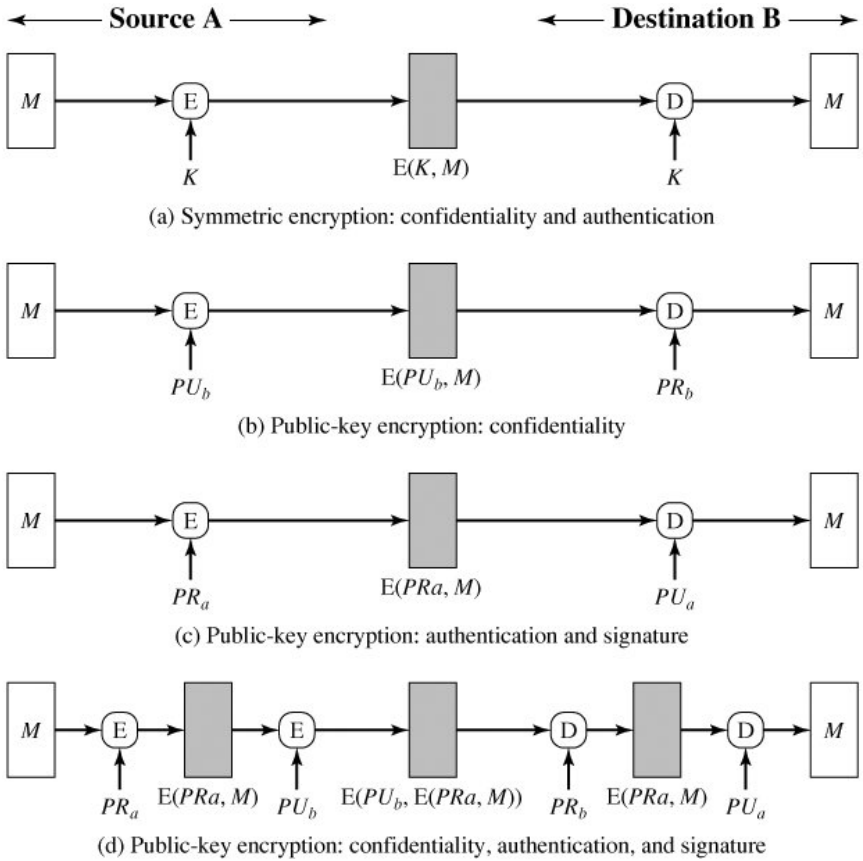
1. uživatel má vygenerovanou dvojici: soukromý a veřejný klíč
2. zašifruje hash zprávy svým soukromým klíčem = podpis
3. připojí výsledek ke zprávě
4. příjemce dešifruje přilepený podpis => hash
5. spočítá hash zprávy
6. porovná obě hashe

Princip digitálního podpisu

účel: ověření odesilatele, integrita dat

1. uživatel má vygenerovanou dvojici: soukromý a veřejný klíč
2. zašifruje hash zprávy svým soukromým klíčem = podpis
3. připojí výsledek ke zprávě
4. příjemce dešifruje přilepený podpis => hash
5. spočítá hash zprávy
6. porovná obě hashe

Různé aplikace šifer



(a) Symmetric encryption: confidentiality and authentication

(b) Public-key encryption: confidentiality

(c) Public-key encryption: authentication and signature

(d) Public-key encryption: confidentiality, authentication, and signature

Certifikát

- Certifikát potvrzuje vlastníka podpisu.
- (Optional)Certifikáty následují doporučení X.509.
- Certifikační autorita(CA) - důvěryhodný orgán, který musí podepsat certifikát.
- stromová hierarchie CA(kořenové jsou v prohlížečích. . .) - umožňuje jednoduchou správu => podřízené CA mohou podepisovat certifikáty uživatelů a přitom jsou stále důvěryhodné

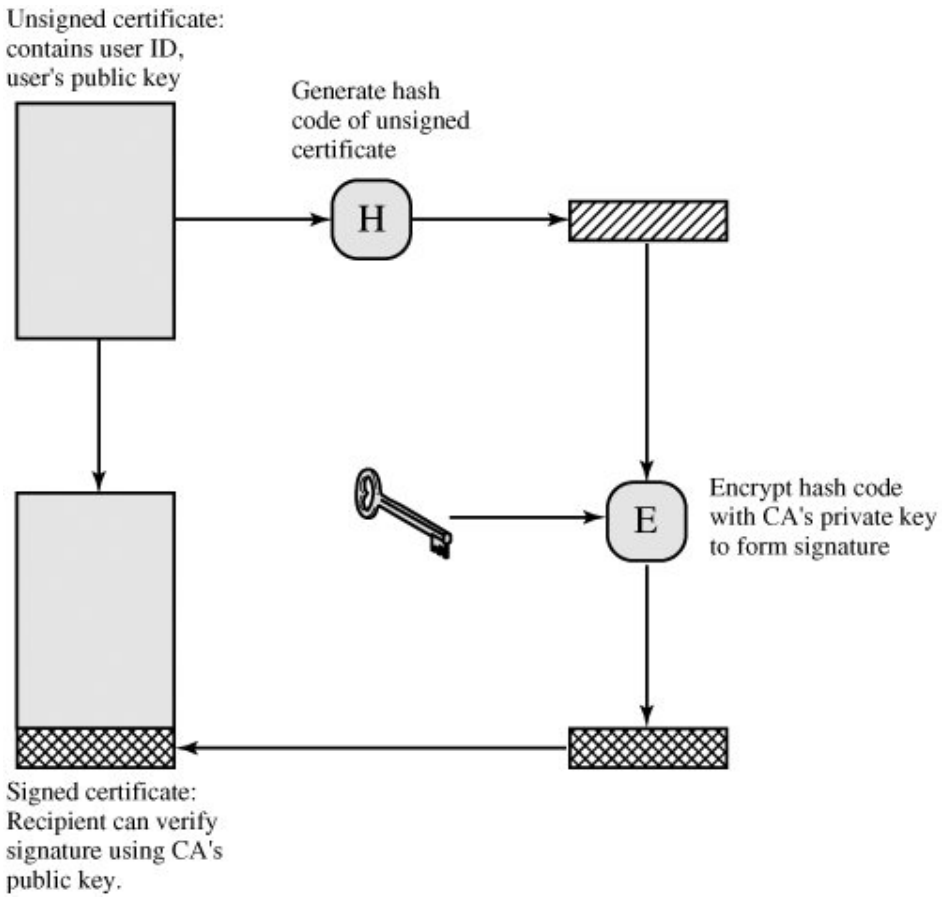
ukázat browser certs

Certifikát

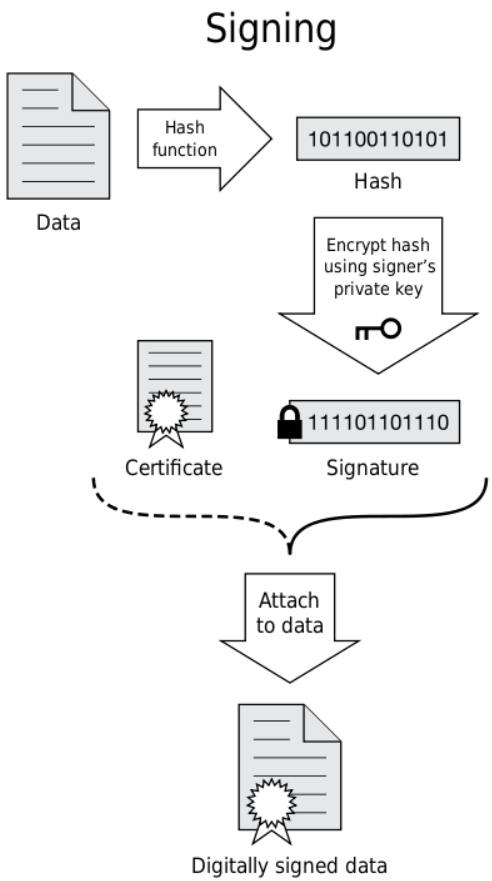
Použití:

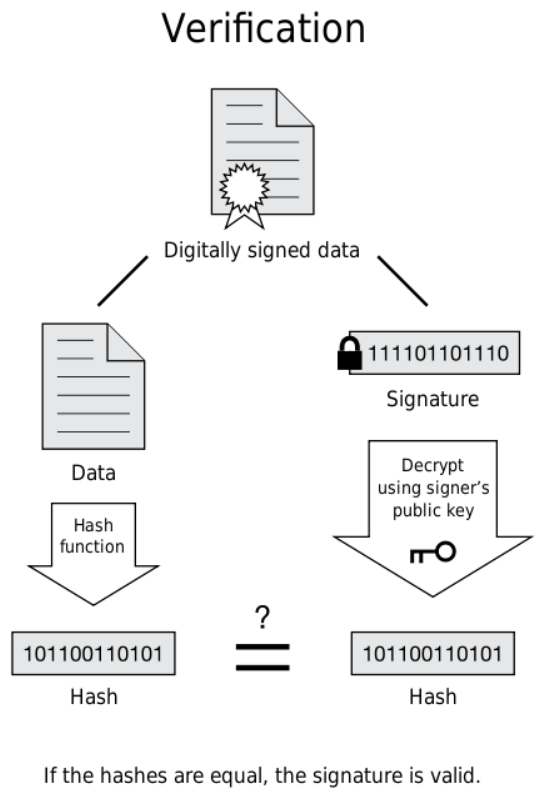
- elektronický podpis
- SSL, TLS - https a další protokoly

Certifikát


Unsigned certificate: contains user ID, user's public key
Generate hash code of unsigned certificate
H
E
Encrypt hash code with CA's private key to form signature
Signed certificate: Recipient can verify signature using CA's public key.

Podpis s certifikátem





Outline

S/MIME = Secure/Multipurpose Internet Mail Extension

Účel: ověření odesilatele, celistvost zprávy, autentizace.
Uživatel musí mít certifikát. Podepíše zprávu. S/MIME definuje, jak se podpis přiloží k emailu. Podpora ve většině emailových klientů.(ukázka v thunderbirdovi)

- Certifikát vystavuje řada institucí - Česká pošta - úředně platný elektronický podpis (190kč na rok)
- Alternativa - velmi jednoduché a účel splní:

  http://www.comodo.com/home/internet-security/free-email-certificate.php

GPG (PGP)

Nevyužívá CA hierarchii. Místo toho tzv. Web of Trust = každý si vytvoří svůj pár klíčů, pro ověřování si uživatelé musí nejprve vyměnit veřejné klíče.

- GPG poskytuje sadu nástrojů a umožňuje kromě podpisu emailu a s právy klíčů šifrovat(ukázka), podepisovat soubory,. . .
- Integrace do emailových klientů.

Outline

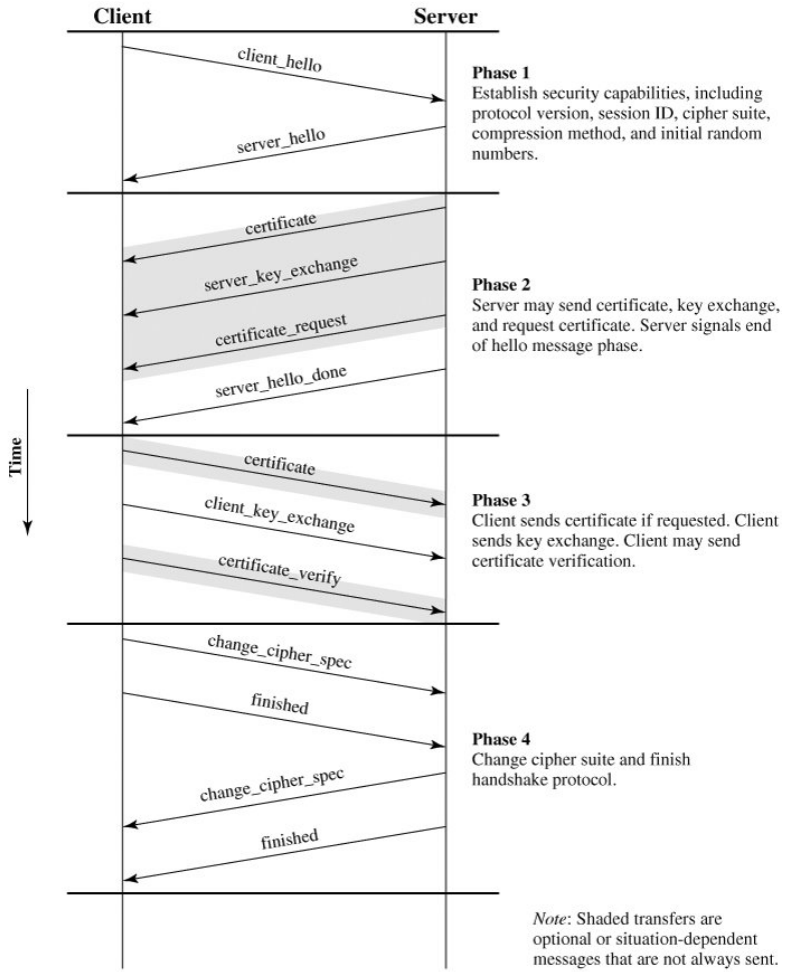
Kontext

TLS(Transport Layer Security) a jeho předchůdce SSL (Secure Sockets Layer) jsou kryptografické protokoly. Šifrují síťová spojení end-to-end (na 4. - transportní vrstvě).

Poskytuje autentizaci koncových bodů komunikace a soukromí přenášených dat.

Použití: web browsing(HTTPS!), email,instant messaging, voice-over-IP (VoIP)...

Navázání spojení



Outline

SSH = secure shell

Nejpoužívanější implementace OpenSSH by OpenBSD.

- umožňuje bezpečnou komunikaci mezi 2 počítači.
- používá asymetrickou šifru pro autentizaci vzdáleného počítače, případně i pro autentizaci uživatele.
- transparentně šifruje přenášená data (pomocí symetrické šifry)
- port ? :)

Schopnosti SSH

- login ke vzdálenému PC
- scp
- tunelování portů
- forwardování X aplikací
- sshfs
- ...

Rekapitulace

1. Identifikace hrozeb
2. Úvod do kryptografie
3. Kryptografie v praxi

Desatero

1. bezpečná hesla a často je měnit (apg)
2. ignorujte neznámé přílohy
3. vyvarujte se pochybným stránkám
4. aktualizujte pravidelně sw!
5. citlivé operace neprovádějte na neznámých místech a z cizích PC
6. instalujte aplikace z oficiálních repozitářů
7. pokud 6 nelze tak kontrolujte autorem vystavený hash
8. nepoužívat nezabezpečené protokoly(pop,ftp,imap,telnet,...)
9. ...?

Security workshop

Budeme si hrát, žádná teorie. . .

1. projdeme si možnosti gpg nástroje
2. pomocí openssl si vygenerujeme certifikát. . .
3. každý si vygenerujeme emailový certifikát
4. budeme si hrát s sshckem
5. můžeme si vysvětlit podrobněji věci probrané v této přednášce
6. . . . ? :)

Q/A

?

Zdroje

- wikipedia
- Cryptography and Network Security Principles and Practices, William Stallings
- net-security.org