Šifrování dat, kryptografie

Metody a využití

Šárka Vavrečková

Ústav informatiky, FPF SU Opava

sarka.vavreckova@fpf.slu.cz

Poslední aktualizace: 5. prosince 2013

Kryptografie a kryptoanalýza

Co to je

- kryptografie = disciplína věnující se ochraně dat před neoprávněným čtením
- kryptoanalýza = analýza šifrovacích algoritmů a šifrovaných dat

Kryptografie a kryptoanalýza

Je třeba rozlišit

- někdo chytrý vymyslí *algoritmus*
- *standard* popisuje funkčnost algoritmu, standard je *veřejný*
- konkrétní *nástroj* (například software) je implementací tohoto algoritmu
- jeden algoritmus může být implementován více různými nástroji

zranitelnost bývá spíše v nástrojích, ale může být i v algoritmu či standardu

Co potřebujeme k šifrování

- data, která chceme šifrovat (otevřený text)
- (dostupný) nástroj implementující šifrovací algoritmus
- „proměnnou“ součást šifrování (šifrovací klíč, heslo, token, apod.), *utajená součást*

kvalita šifrování závisí jak na nástroji, tak i na proměnné součásti (slabé heslo = slabé zabezpečení)

Co potřebujeme k šifrování

Při vysvětlování budeme značit

- A (Alice) – ten, kdo data odesílá
- B (Bob) – ten, kdo data přijímá

Rozlišíme

- otevřený text (data) = nezašifrovaná data
- šifrovaná data

Symetrické šifrování

- tentýž klíč slouží k šifrování i dešifrování
- postup:
  - Alice a Bob mají oba tentýž klíč (Alice ho poslala Bobovi)
  - Alice data zašifruje pomocí tohoto klíče, odešle
  - Bob přijme šifrovaná data a dešifruje je pomocí téhož klíče

Symetrické šifrování

- výhoda: rychlost šifrování i dešifrování
- nevýhoda: slabé místo = transport klíče
- typičtí zástupci: RC4, DES, 3DES, AES

Asymetrické šifrování

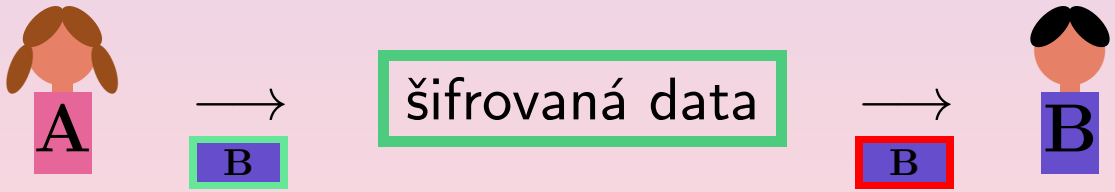
- algoritmus je založen na jednocestné funkci, tj. jeden klíč je pro šifrování a jiný pro dešifrování
- postup č. 1 (zajištění důvěrnosti dat):
  - Bob vygeneruje pár klíčů – soukromý a veřejný, veřejný pošle Alici
  - Alice data zašifruje veřejným klíčem Boba, odešle
  - Bob přijme šifrovaná data, dešifruje svým soukromým klíčem

  $\Rightarrow$ data může dešifrovat jen adresát (je zajištěna *důvěrnost*)

Asymetrické šifrování

- algoritmus je založen na jednocestné funkci, tj. jeden klíč je pro šifrování a jiný pro dešifrování
- postup č. 1 (zajištění důvěrnosti dat):
  - Bob vygeneruje pár klíčů – soukromý a veřejný, veřejný pošle Alici
  - Alice data zašifruje veřejným klíčem Boba, odešle
  - Bob přijme šifrovaná data, dešifruje svým soukromým klíčem

⇒ data může dešifrovat jen adresát (je zajištěna *důvěrnost*)



Asymetrické šifrování

- postup č. 2 (zajištění integrity a nepopiratelnosti dat):
  - Alice vygeneruje pár klíčů – soukromý a veřejný, veřejný pošle Bobovi
  - Alice data zašifruje svým soukromým klíčem, odešle
  - Bob přijme šifrovaná data, dešifruje veřejným klíčem Alice

  $\Rightarrow$ dešifrovat může kdokoliv, ale je zřejmé, že šifrovala Alice (digitální podpis)

Asymetrické šifrování

- postup č. 2 (zajištění integrity a nepopiratelnosti dat):
  - Alice vygeneruje pár klíčů – soukromý a veřejný, veřejný pošle Bobovi
  - Alice data zašifruje svým soukromým klíčem, odešle
  - Bob přijme šifrovaná data, dešifruje veřejným klíčem Alice

$\Rightarrow$ dešifrovat může kdokoliv, ale je zřejmé, že šifrovala Alice

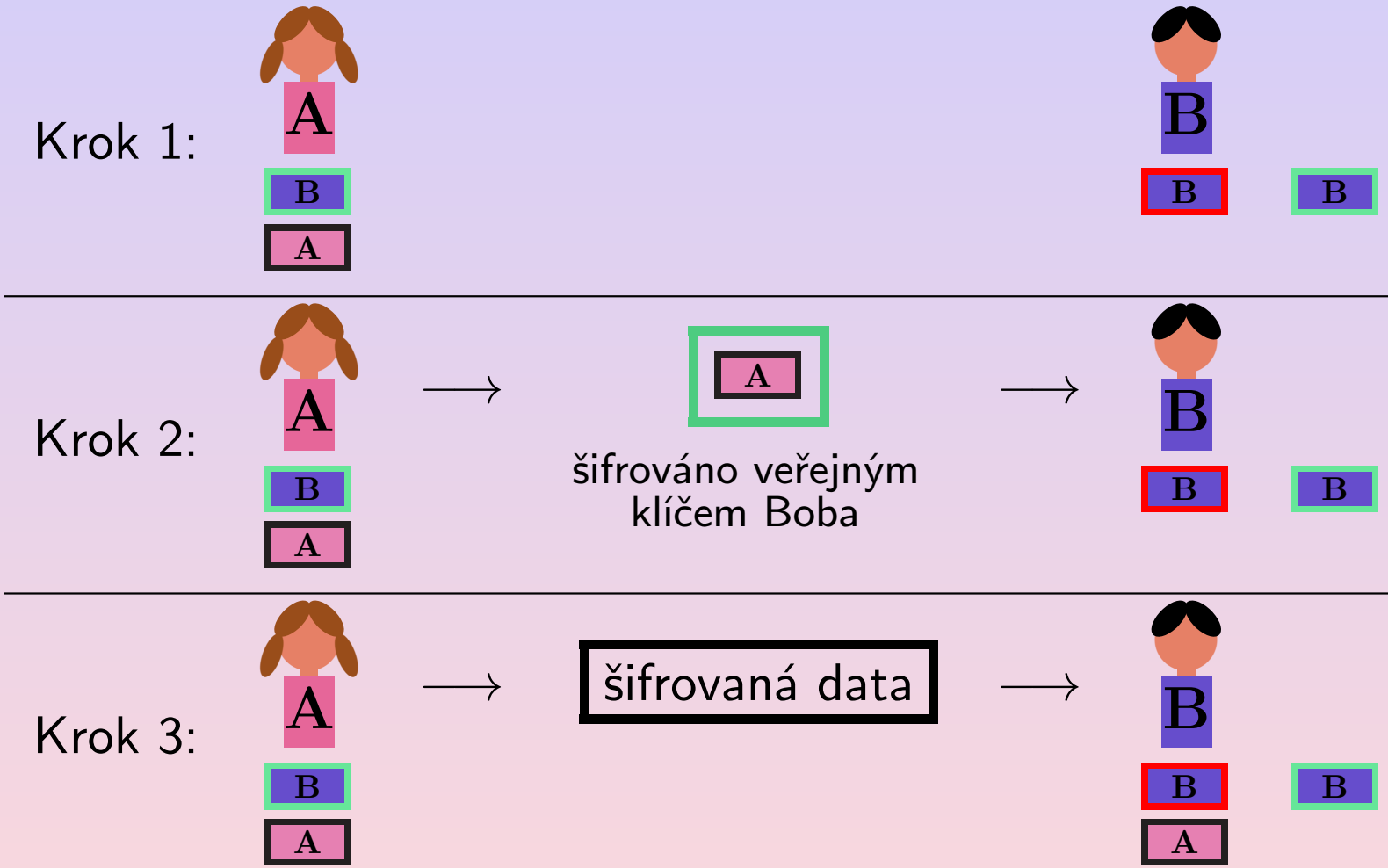
Asymetrické šifrování

- výhoda: veřejný klíč není problém jakkoliv zveřejnit
- nevýhoda: časově náročnější šifrování i dešifrování
- typičtí zástupci: RSA, DSA, PGP, používají se také certifikáty, digitální podpisy

Hybridní přístup

- kombinace symetrického a asymetrického šifrování
- postup:
  - Bob vygeneruje pár klíčů pro asymetrické šifrování – soukromý a veřejný, veřejný pošle Alici
  - Alice vygeneruje klíč pro symetrické šifrování, dále zašifruje
    - data (velký objem) symetrickým klíčem
    - symetrický klíč (malý objem) zašifruje veřejným klíčem Boba

    obojí pošle Bobovi
  - Bob svým soukromým klíčem dešifruje symetrický klíč od Alice, následně jím dešifruje data
- používá se hlavně pro delší relace (víc dat v obou směrech, symetrický klíč stačí bezpečně poslat jednou)


Krok 1:
A
B
A
B
B
B
Krok 2:
A
B
A
A
šifrováno veřejným klíčem Boba
B
B
B
Krok 3:
A
B
A
šifrovaná data
B
B
B
A

Jak funguje symetrická kryptografie

Symetrické algoritmy kombinují dva přístupy:

- substituce (nahrazování) – záměna jednotlivých znaků otevřeného textu za jiné znaky podle substituční tabulky
  - pevná substituční tabulka (nemění se, bez klíče) $\Rightarrow$ kódování
  - proměnlivá substituční tabulka (obsah závisí na použitém klíči) $\Rightarrow$ šifrování
- transpozice (přehazování) – změna pořadí znaků v otevřeném textu

Jak funguje asymetrická kryptografie

Asymetrická kryptografie je založena na matematice

- velmi složitý problém se dá vyřešit
  - v extrémně dlouhém čase, pokud nemáme „nápovědu“ (klíč)
  - v celkem krátkém čase, pokud máme k dispozici klíč
- obvykle jsou použity tyto problémy:
  - problém faktorizace součinu velkých prvočísel
  - problém výpočtu diskrétního logaritmu
  - problematika eliptických křivek

nejběžněji se využívá první problém (například v RSA)

Využití při autentizaci a řízení přístupu

Jak dokázat, že jsem to já:

- důkaz znalostí – znám něco, do jiný nezná (heslo, PIN apod.)
- důkaz vlastnictvím – mám něco, co jiný nemá (čipová karta, USB token)
- důkaz vlastností – biometrické informace

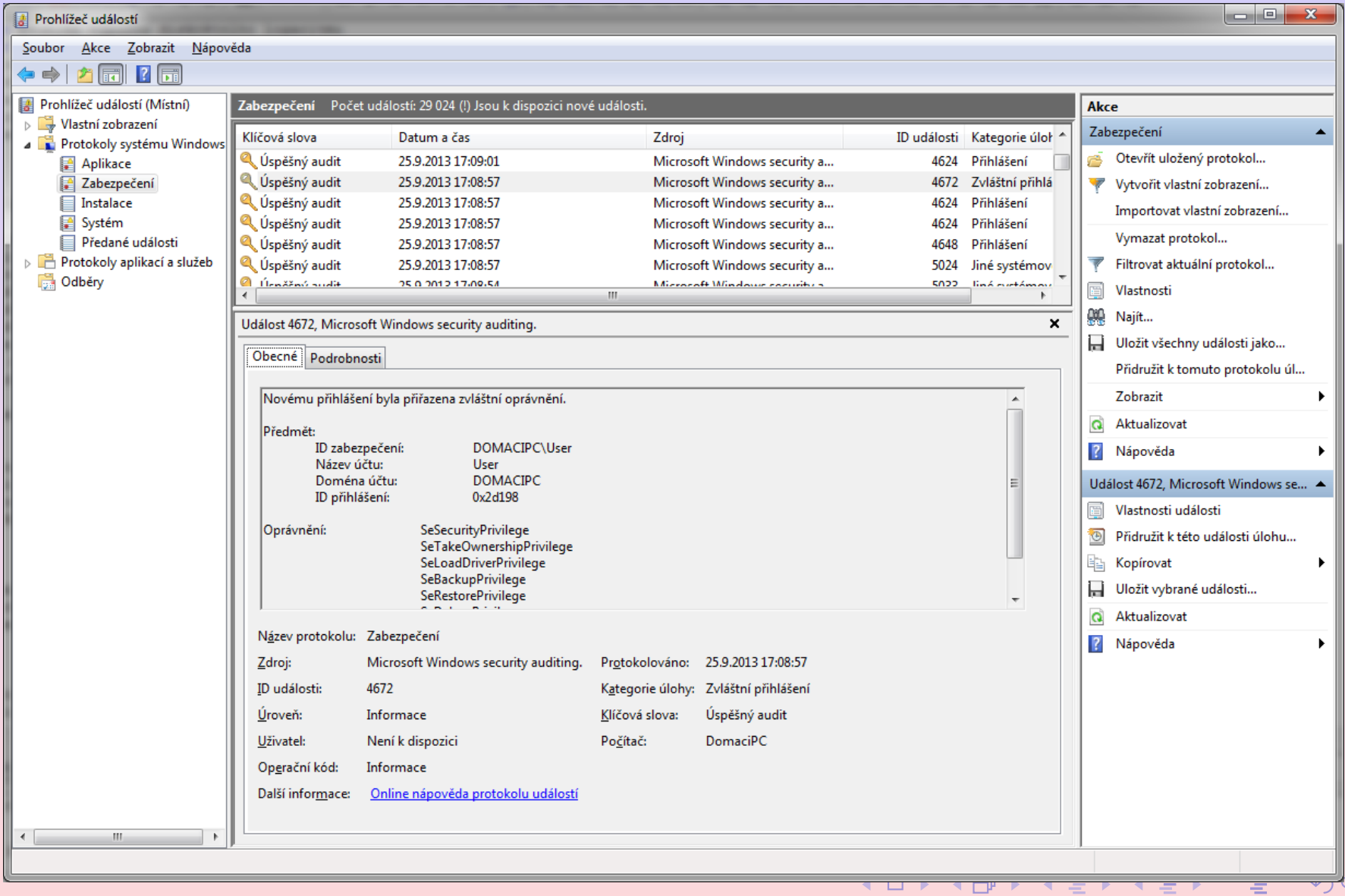
mohou se kombinovat

Auditní záznam ve Windows

Prohlížeč událostí

- Nástroje pro správu, také přes Ovládací panely
- najdeme Protokol zabezpečení

Auditní záznamy



Auditní záznam v Linuxu

Program Syslog (varianta syslog-ng)

- autentizační logy jsou většinou v souboru `/var/log/auth.log`
- zobrazíme například příkazem `tail /var/log/auth.log`
- ve větších distribucích je obvykle i nějaký nástroj s GUI
- důležité: u syslog-ng je možné agregovat logy z různých uzlů sítě pomocí LogWatch a automaticky vyhodnocovat pomocí SWatch

Hybridní síť (Windows + Linux)

NTSyslog

- proces běžící jako služba ve Windows
  http://ntsyslog.sourceforge.net/
- pracuje jako agent pro syslog, tj. dokáže posílat obsah logů (protokolů) ve Windows do síťového syslogu
- je vhodné vytvořit pro něj samostatný účet, kterému v Místních zásadách zabezpečení povolíme „Spravování protokolu auditu a bezpečnosti“

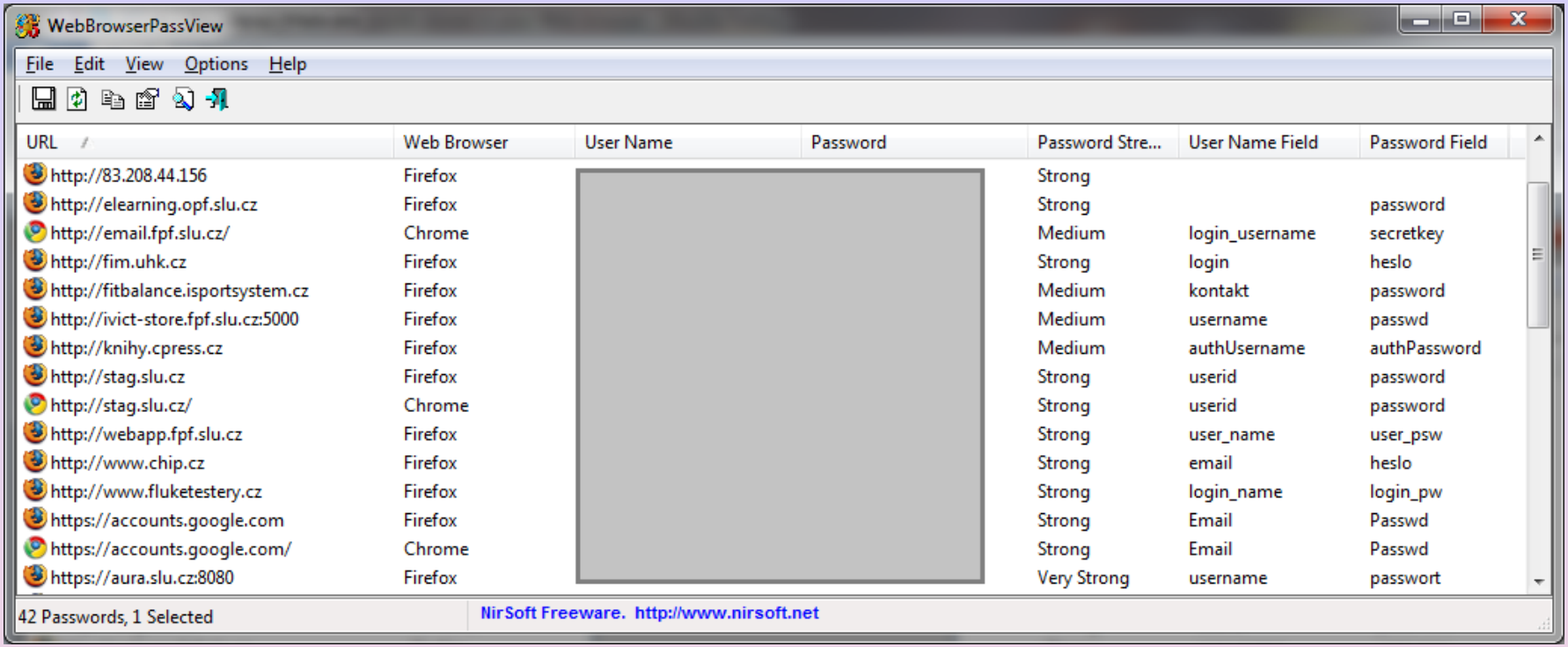
Hesla ve webovém prohlížeči (Windows)

Nirsoft WebBrowserPassView

- hodí se, pokud máme ve webovém prohlížeči uložena hesla, která si už nepamatujeme, ale potřebujeme je na jiném počítači
- vypíše všechna nalezená uložená hesla
- http://www.nirsoft.net/utils/web_browser_password.html

konkurenti: Asterisk Key, GrabWinText, MessenPass (také komunikační programy – Skype, ICQ, Miranda, atd.)

Hesla ve Windows



Hesla v e-mailovém klientovi

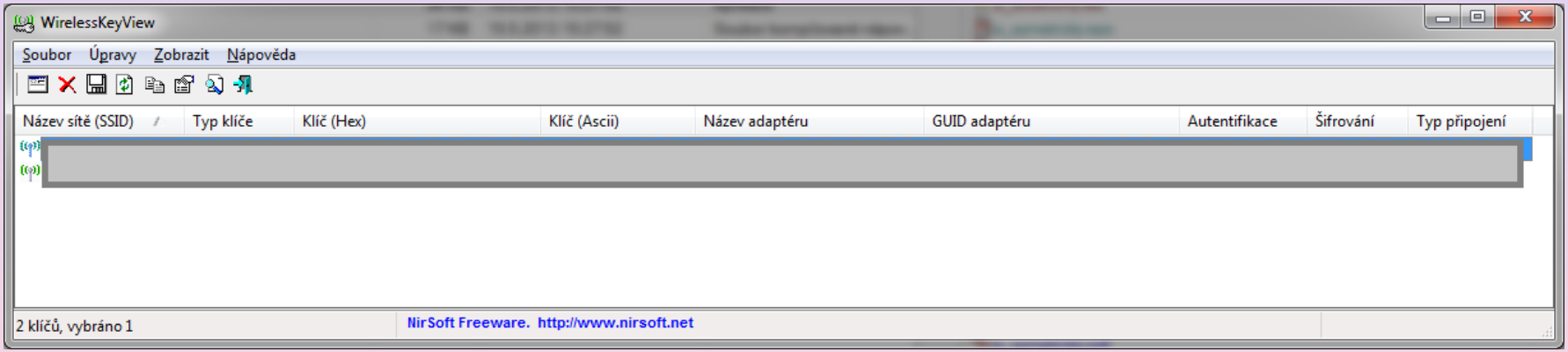
Nirsoft Mail PassView

- hledá přihlašovací údaje do e-mailových účtů

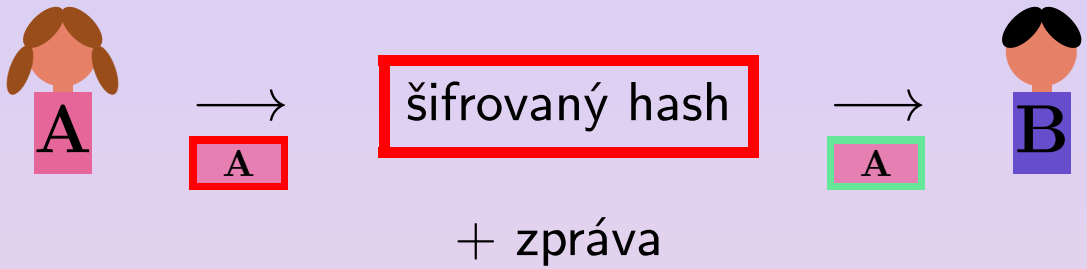
Přístupové údaje do Wi-fi sítí

WirelessKeyView

- zobrazí seznam sítí, do kterých máme na počítači přihlašovací údaje, včetně těchto údajů



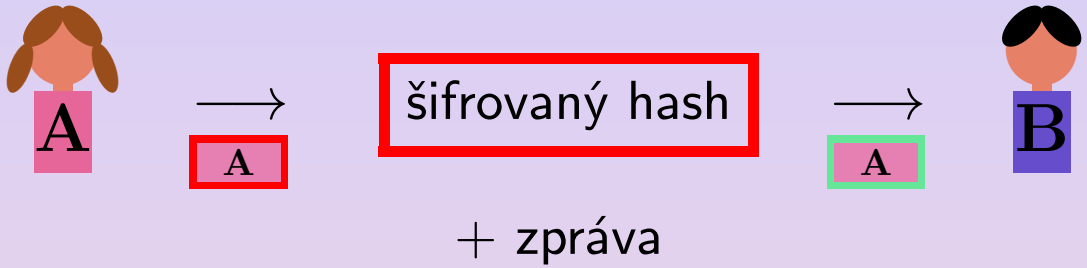
Postup vytvoření digitálního podpisu



Vlastnosti

- musí být jasné, kdo odesílá (tj. podepisuje)
- naopak přijmout (ověřit platnost podpisu) musí být schopen kdokoliv
- nebudeme šifrovat celou zprávu, protože by to bylo časově náročné

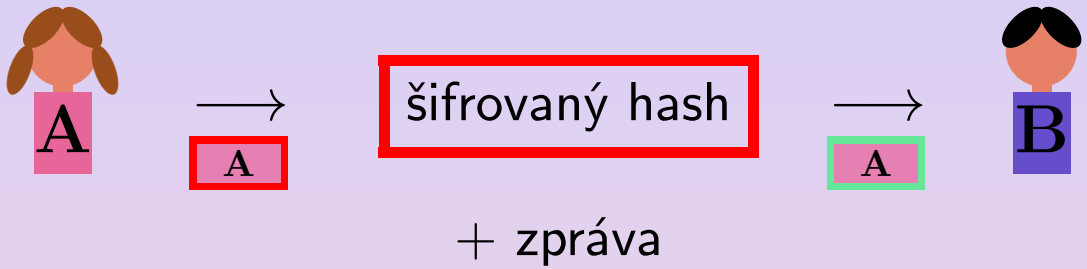
Postup vytvoření digitálního podpisu



Hash (digitální otisk, kontrolní součet)

- z celé (dlouhé) zprávy vypočítáme (krátký) hash
- hash jednoznačně identifikuje zprávu, ale přitom je prakticky nemožné z něj opětovně zprávu dešifrovat (jednoznačnost jen v jednom směru, náročnost)
- používané: MD5 (128b hash), SHA1 (160b hash), RIPEMD-160 (160b hash)

Postup vytvoření digitálního podpisu



Jak na to

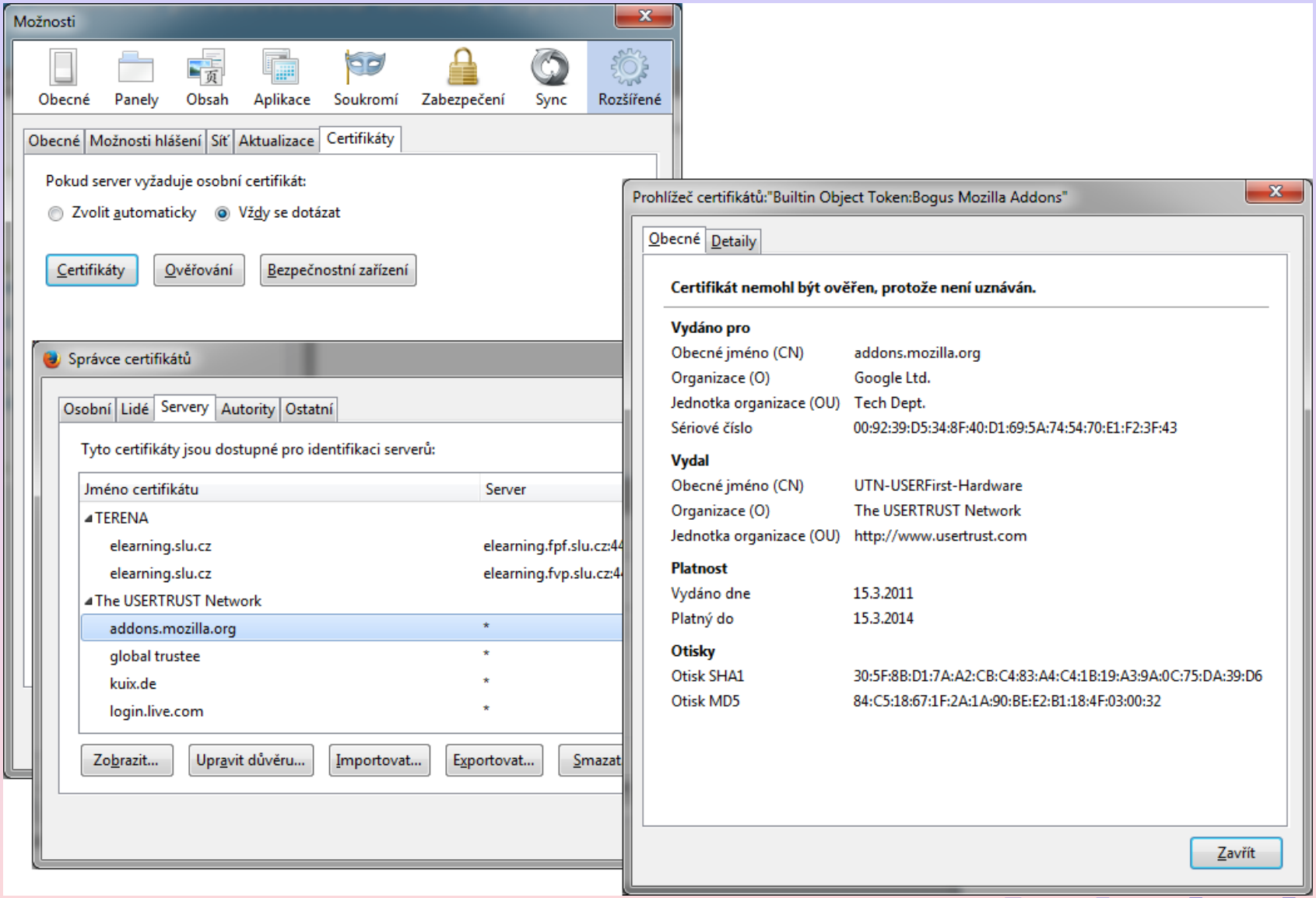
1. Alice vytvoří hash zprávy a zašifruje svým soukromým klíčem
2. Bob má veřejný klíč Alice, obdrží zprávu a její zašifrovaný hash
3. dešifruje hash – když to jde, odesílatel je Alice
4. ze zprávy vygeneruje taky hash – když souhlasí s tím od Alice, je zaručena integrita

Certifikát (elektronický podpis)

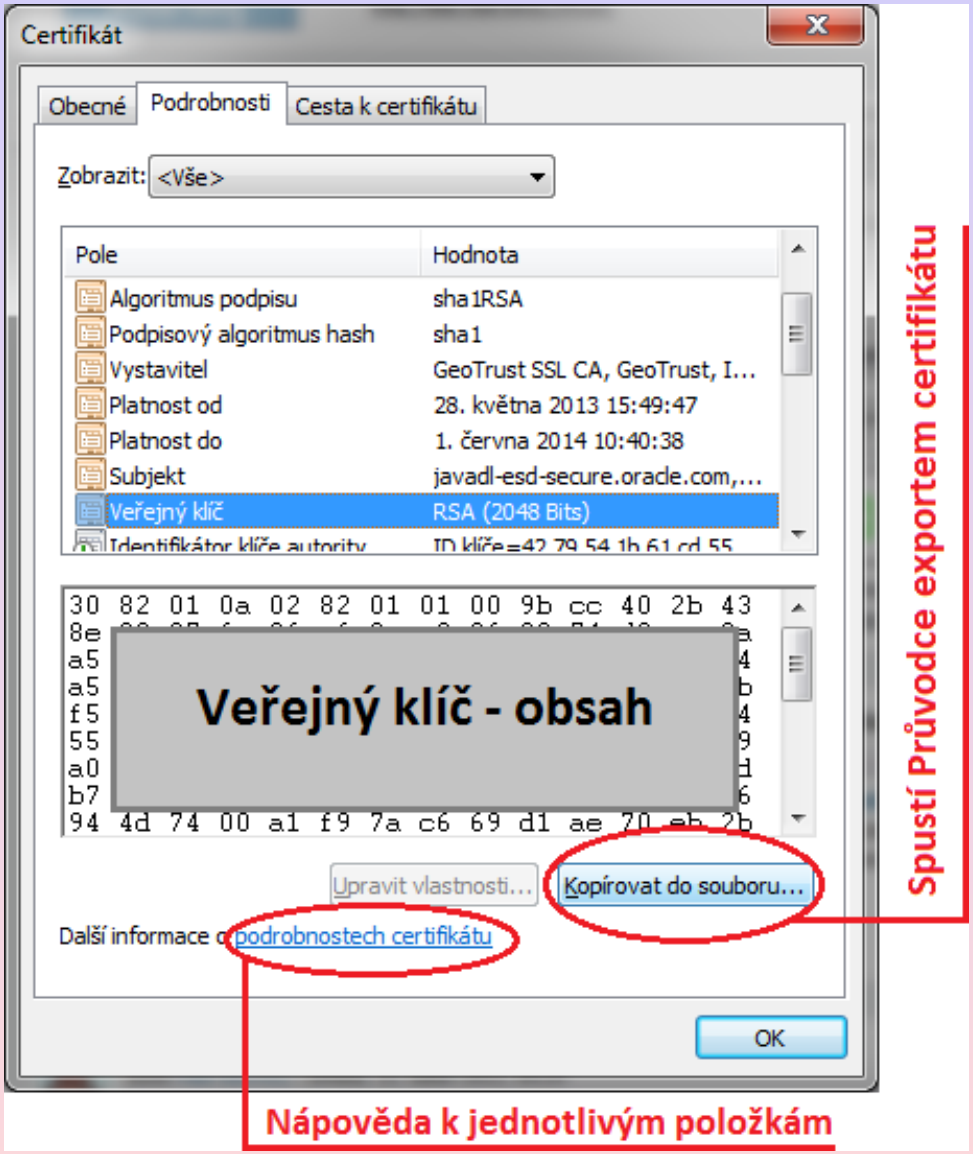
- problém: co když Bob dostane podvržený veřejný klíč, který ve skutečnosti není od Alice?
- certifikát = souhrn dat:
  - veřejný klíč ověřeného subjektu – vlastníka (například Alice)
  - identifikace vlastníka
  - identifikace certifikační autority
  - datum vydání a platnost certifikátu, použité algoritmy, atd.

  podepsán soukromým klíčem certifikační autority
- Bob musí důvěřovat této certifikační autoritě, její veřejný klíč musí být důvěryhodný
- musí být možné zkontrolovat seznam platných certifikátů a seznam odvolaných certifikátů

Certifikát


Možnosti
Obecné
Panely
Obsah
Aplikace
Soukromí
Zabezpečení
Sync
Rozšířené
Obecné
Možnosti hlášení
Síť
Aktualizace
Certifikáty
Pokud server vyžaduje osobní certifikát:
Zvolit automaticky
Vždy se dotázat
Certifikáty
Ověřování
Bezpečnostní zařízení
Správce certifikátů
Osobní
Lidé
Servery
Autority
Ostatní
Tyto certifikáty jsou dostupné pro identifikaci serverů:
Jméno certifikátu
Server
TERENA
elearning.slu.cz
elearning.fpf.slu.cz:44
elearning.slu.cz
elearning.fvp.slu.cz:4
The USERTRUST Network
addons.mozilla.org
*
global trustee
*
kuix.de
*
login.live.com
*
Zobrazit...
Upravit důvěru...
Importovat...
Exportovat...
Smazat
Prohlížeč certifikátů:"Builtin Object Token:Bogus Mozilla Addons"
Obecné
Detaily
Certifikát nemohl být ověřen, protože není uznáván.
Vydáno pro
Obecné jméno (CN) addons.mozilla.org
Organizace (O) Google Ltd.
Jednotka organizace (OU) Tech Dept.
Sériové číslo 00:92:39:D5:34:8F:40:D1:69:5A:74:54:70:E1:F2:3F:43
Vydal
Obecné jméno (CN) UTN-USERFirst-Hardware
Organizace (O) The USERTRUST Network
Jednotka organizace (OU) http://www.usertrust.com
Platnost
Vydáno dne 15.3.2011
Platný do 15.3.2014
Otisky
Otisk SHA1 30:5F:8B:D1:7A:A2:CB:C4:83:A4:C4:1B:19:A3:9A:0C:75:DA:39:D6
Otisk MD5 84:C5:18:67:1F:2A:1A:90:BE:E2:B1:18:4F:03:00:32
Zavřít

Certifikát


Certifikát
Obecné
Podrobnosti
Cesta k certifikátu
Zobrazit: <Vše>
Pole
Hodnota
Algoritmus podpisu
sha1RSA
Podpisový algoritmus hash
sha1
Vystavitel
GeoTrust SSL CA, GeoTrust, I...
Platnost od
28. května 2013 15:49:47
Platnost do
1. června 2014 10:40:38
Subjekt
javadl-esd-secure.oracle.com,...
Veřejný klíč
RSA (2048 Bits)
30 82 01 0a 02 82 01 01 00 9b cc 40 2b 43
Veřejný klíč - obsah
Upravit vlastnosti...
Kopírovat do souboru...
Další informace o podrobnostech certifikátu
OK
Spustí Průvodce exportem certifikátu
Nápověda k jednotlivým položkám

Třídy certifikátů

Třídy se liší mírou ověření žadatele o certifikát

- Class 1: pouze pro procvičování práce s certifikáty, certifikační autorita jen ověří, zda lze certifikát vytvořit
- Class 2: identita budoucího vlastníka certifikátu je ověřována třetí stranou (například může být zaslán notářsky ověřený formulář)
- Class 3: žadatel osobně navštíví certifikační autoritu, kde je stanoveným způsobem ověřena jeho identita
- Class 4: kromě osoby žadatele je ověřována oprávněnost žadatele k dané činnosti

Nejběžnější je Class 3.

Jak získat elektronický podpis v ČR

- certifikační autority jsou uspořádány do stromu, autorita podřízeného uzlu je garantována autoritou nadřízeného uzlu
- celou hierarchii označujeme PKI (Public Key Infrastructure)
- dva subjekty, které si potřebují v komunikaci důvěřovat, mohou mít různé certifikační autority, ale zřejmě bude ve stromu existovat nějaká společná nadřízená
- u nás: http://www.secustamp.eu/cs/jak-snadno-ziskat-elektronicky-podpis
- Další informace: http://crypto-world.info/pinkava/konference/cack.pdf http://www.lupa.cz/clanky/jak-jsem-si-poridil-elektronicky-podpis-ceske-posty/

Certifikační autority

- ne vždy můžeme důvěřovat každé certifikační autoritě (každý systém může být nabouratelný)
- můžeme si vytvořit taky vlastní certifikační autoritu (důvěryhodně ji můžeme používat třeba v rámci firmy)
- nástroj: OpenSSL

Další informace:

- http://www.linuxexpres.cz/praxe/bezpecny-web-s-https
- https://www.ca.cz/jak-to-funguje/navod/
- http://support.microsoft.com/kb/299875/cs

Jak probíhá komunikace ve Wi-fi

1. fáze autentizace, autorizace, přidružení do sítě (asociace)
2. komunikace
3. ukončení komunikace (de-asociace)

Autentizace – možnosti

WEP (Wired Equivalent Privacy)

- pouze základní stupeň bezpečnosti, možnosti (autentizace+přenos dat):
  1. otevřená síť
  2. symetrická RC4, 40bitový statický klíč + 24bitový proměnný inicializační vektor
  3. symetrická RC4, 104bitový statický klíč + 24bitový proměnný inicializační vektor
- inicializační vektor (IV) se mění pro každý paket, v praxi je však posílán jako součást nešifrovaného záhlaví paketu (!)

Autentizace – možnosti

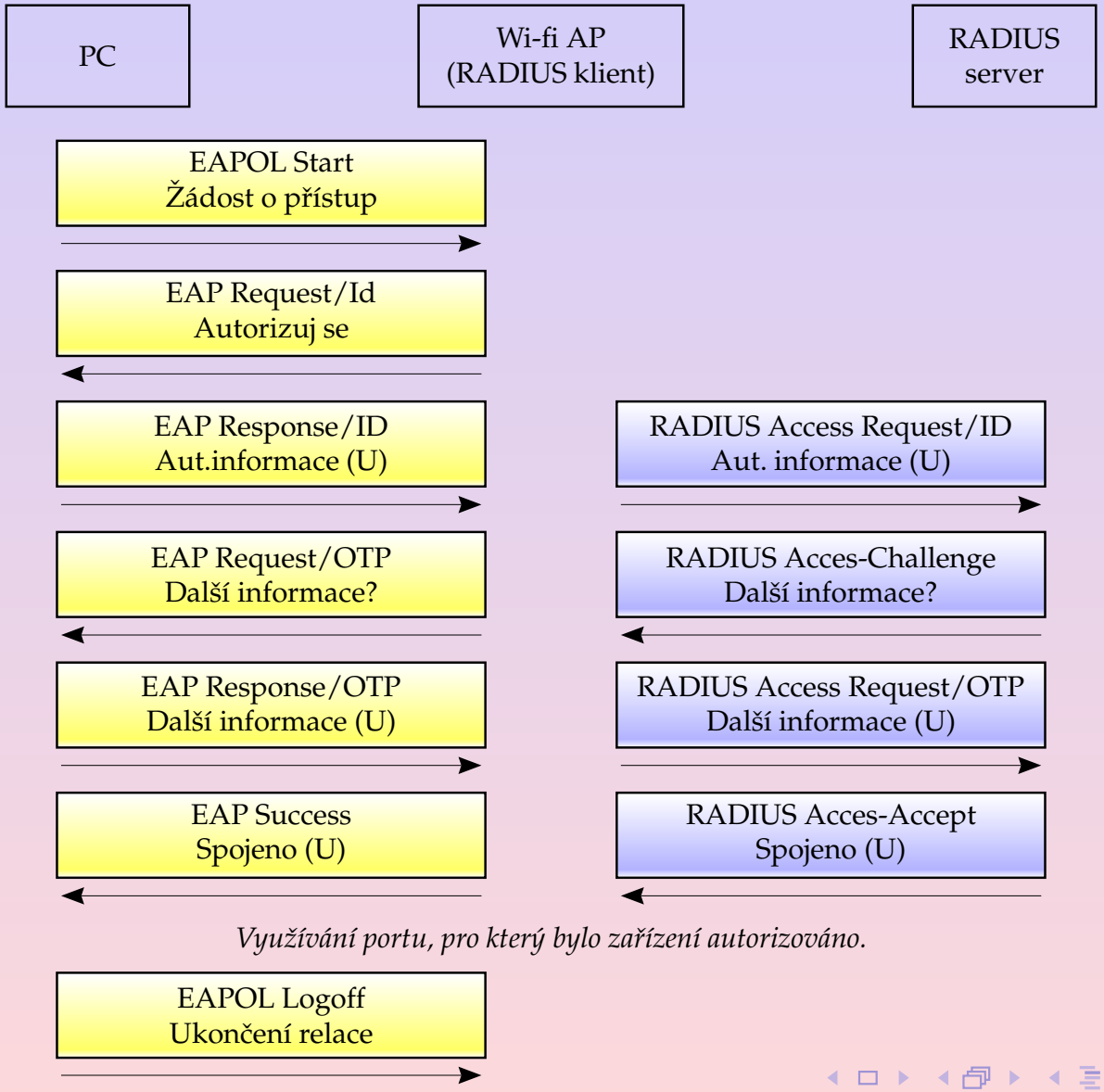
WEP (Wired Equivalent Privacy)

- autentizace probíhá takto:
  - stanice odešle žádost o připojení k AP
  - AP odpoví odesláním náhodné sekvence znaků (bez šifrování)
  - stanice tuto sekvenci zašifruje (RC4) a odešle AP
  - AP tuto sekvenci také zašifruje, srovná s tím, co dodala stanice
  - souhlasí $\Rightarrow$ stanice byla autentizována
- AirCrack prolomí WEP v maximálně několika minutách

Autentizace – možnosti

Využití autentizačního serveru

- účel: zabezpečení autentizační databáze a samotného procesu autentizace
- standard IEEE 802.1X, obvykle se používá RADIUS server
- RADIUS server je autentizátor
- RADIUS klient je obvykle AP


PC
Wi-fi AP
(RADIUS klient)
RADIUS
server
EAPOL Start
Žádost o přístup
EAP Request/Id
Autorizuj se
EAP Response/ID
Aut.informace (U)
RADIUS Access Request/ID
Aut. informace (U)
EAP Request/OTP
Další informace?
RADIUS Acces-Challenge
Další informace?
EAP Response/OTP
Další informace (U)
RADIUS Access Request/OTP
Další informace (U)
EAP Success
Spojeno (U)
RADIUS Acces-Accept
Spojeno (U)
Využívání portu, pro který bylo zařízení autorizováno.
EAPOL Logoff
Ukončení relace

Autentizace – možnosti

Čekání na nový standard

- velmi dlouhou dobu se chystal standard IEEE 802.11i (WPA2), který měl WEP nahradit
- problém: standard pořád nebyl hotov, navíc vyžadoval u hardwaru určité vlastnosti
- řešení: odlehčením vznikl WPA
  - dřív k dispozici
  - nevyžadoval změny na hardwaru, pouze aktualizaci firmwaru zařízení

Autentizace – možnosti

WPA (Wi-fi Protected Access)

- šifrování RC4, ale IV vektor je 48bitový
- navíc klíče nejsou statické, ale dynamické – zajišťuje protokol TKIP (pro každý paket je jiný celý klíč, nejen IV vektor)
- zajištění integrity zpráv: mechanismus MIC (Message Integrity Check) v protokolu TKIP
  - jde o obdobu digitálního podpisu paketu (64 bitů)
- varianty:
  - WPA-Enterprise (pro firmy) – v kombinaci s IEEE 802.1X
  - WPA-Personal (také WPA-PSK)
    - autentizace pomocí sdíleného klíče PSK (Pre-Shared Key), nepotřebujeme autentizační server
    - PSK je obvykle heslo o délce 8–63 ASCII znaků, jeho délka a složitost určují zabezpečení

Autentizace – možnosti

WPA2

- používá místo TKIP protokol CCMP s šifrováním AES (místo AES je možné použít starší RC4)
- varianty:
  - WPA2-Enterprise
  - WPA2-Personal (WPA2-PSK)

SSL (Secure Sockets Layer)

- podporuje oboustrannou autentizaci, ale často se autentizuje pouze klient
- zajišťuje šifrování a integritu dat, používá se asymetrické šifrování, případně certifikáty
- dynamické vytvoření klíčů během handshake:
  - klient pošle požadavek na spojení (adresa `https://...`)
  - server zašle klientovi certifikát svého veřejného klíče
  - klient vygeneruje náhodné číslo, zašifruje podle veřejného klíče serveru, pošle serveru (premaster secret)
  - server dešifruje svým soukromým klíčem, klient i server přidají k těmto datům další informace a vytvoří hlavní šifrovací klíč (master secret)

  autentizuje se především server (klient musí mít jistotu, s kým komunikuje)

TLS (Transport Layer Security)

- nástupce SSL, TLS v. 1.0 je velmi podobný SSL v. 3.0
- umožňuje oboustrannou autentizaci, ale většinou se používá jednostranná
- autentizace – asymetrická kryptografie
- komunikace – symetrická kryptografie (stejně jako u SSL)

Šifrování při správě serveru

SSH (Secure SHell) – vzdálená správa serverů

- šifrovaně *se mohou přenášet* přihlašovací údaje uživatele a následně celá komunikace (příkazy)
- autentizace:
  - asymetrické šifrování, na serveru musí být uložen veřejný klíč uživatele
  - zadání hesla, které se v otevřené formě přenáší k serveru
  - autentizace na základě IP adresy uživatele
  - externí mechanismus, např. GSSAPI využívající Kerberos (v komerční sféře)
- autentizace může být i obousměrná
- šifrování samotné komunikace: algoritmus je dohodnut během navazování spojení, často 3DES

SSH

- OpenSSH – pro unixové systémy (instaluje se na klienty i servery)
- PuTTY – pro Windows (jen pro klienty)

Přenos souborů

SFTP (Secure FTP)

- klient i server se navzájem autentizují, komunikace je šifrována (SSL, TLS)
- FTP podporováno v operačních systémech, s SFTP je to horší
- podpora v SSH, WinSCP, Filezilla, atd.

Přenos webových stránek

HTTPS

- protokol HTTP zabezpečený protokolem SSL
- signalizace: například ikona zámku u adresního řádku, protokol je `https://`

PGP (Pretty Good Privacy)

- program pro šifrování a podepisování pošty, ve formě plug-inů do mail klientů
- standard OpenPGP (RFC 2440)
- postup odeslání zprávy:
  - je vygenerován symetrický klíč (jiný pro každou novou zprávu)
  - zpráva je šifrována s tímto symetrickým klíčem
  - symetrický klíč je šifrován asymetricky a přidán k jím šifrované zprávě
- postup přijetí zprávy:
  - symetrický klíč je dešifrován (asymetricky)
  - dešifrovaný klíč použijeme k dešifrování zprávy