

Pavel Dvořák

Gymnázium Velké Meziříčí

**Zabezpečení zařízení při připojení k síti**

Registrační číslo projektu: CZ.1.07/1.5.00/34.0948

Datum: 17. 11. 2013

Jazyk: čeština

Cílová skupina: studenti vyššího gymnázia, 15–16 let

Druh učebního materiálu: výklad + testové otázky

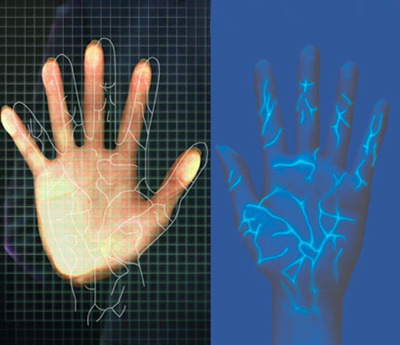
Očekávaný výstup: student se seznámí se zabezpečením zařízení připojených k datové síti

Anotace: výklad + testové otázky

# Přístup k prostředkům sítě (popř. informacím) je většinou zabezpečen pomocí   základních prvků:

1. **Něco znám** – např. heslo, pin
2. **Něco mám** (vlastním) – např. přístupovou karta, token, klíčenka
3. **Něco jsem** – využití biometrických údajů dané osoby – např. otisk prstů, sken ruky, sken krevního řečiště ruky, sken obličeje, rohovka oka, duhovka oka, sítnice oka, dynamika podpisu, hlas, …, chůze, …





# 

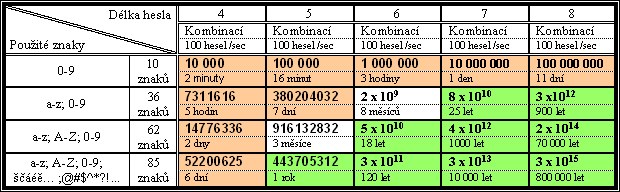
# Výsledek obrázku pro biometrie hlasu

# Heslo

* obecný prostředek k autentizaci uživatele (nemusí to být obecně pouze člověk)
* uživatel je pokládán za oprávněného, pokud prokáže znalost hesla
* heslo je použitelné pouze tehdy, není-li ostatním uživatelům známé. Oprávněný uživatel musí držet heslo v tajnosti.
* uživatel je obvykle odlišen od ostatních uživatelů uživatelským jménem (login)

## Bezpečné heslo

* takové, které není snadno zjistitelné, uhodnutelné nebo jinak snadno zneužitelné
* hesla slouží pro ochranu přístupu k nejrůznějším systémům a informacím, do kterých by se neměl dostat nikdo nepovolaný
* **nebezpečné** je používat taková hesla, která lze uhádnout s použitím hrubé síly – například použít všechna slova z připraveného slovníku
* heslo by mělo být dlouhé a mělo by se skládat z „náhodné“ skupiny znaků. Je dobré si tuto „náhodnou“ skupinu znaků nějakým *mnemotechnickým způsobem* označit. Například „12345ctJcts?“ – „Jedna dvě tři čtyři pět, cos to Janku cos to sněd?“.
* Známé hlášky, obměny jednoduchých slov, data narození, jména přítelkyň, manželek, dětí, psů aj. jsou pro hesla *zcela nevhodná*. Pomocí slovníkového útoku, nebo informovaného útočníka, lze taková hesla snadno odhalit.
* Tabulka – délka hesla, počet možných znaků a délka „hacknutí“ hesla



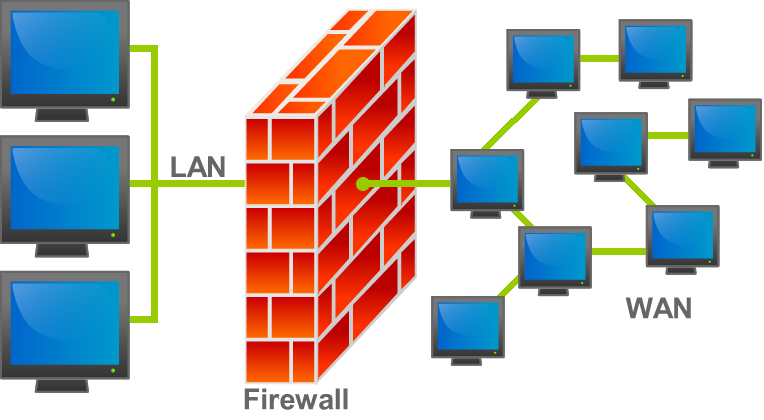
Volné dílo, [cit. 2013/11/17], SroubekJirka, <http://cs.wikipedia.org/wiki/Soubor:Kvalita_hesla.jpg>

# Proxy server

* prostředník mezi internetem a lokální počítačovou sítí
* všechny počítače v lokální síti využívají proxy server pro přístup k internetu
* jednotlivý počítač požádá o dané informace proxy server, proxy server data stáhne z internetu a poskytne dané stanici
* k internetu je tedy připojen přímo pouze jeden počítač (proxy server), lze tedy nastavovat a sledovat různé parametry:
  + omezení zobrazování některých stránek (porno, soc. sítě, warez, …)
  + omezení stahování velikostně objemných souborů (mp3, videa, …)
  + omezení přístupu jen pro dané počítače, osoby
  + auditing přístupu do internetu – kdo, kdy, co stahoval a jaké stránky navštívil
  + rychlejší načítání obsahu internetu z cache paměti proxy serveru (platí jen pro často navštěvovaný obsah)

# Firewall

* jedná se o HW nebo SW nástroj, který vytváří bezpečnostní zeď mezi internetem a lokální sítí (lokálním počítačem)
* komunikace mezi internetem a počítačem probíhá na určitých portech (označovaných čísly, např. port 80 – komunikace pomocí www stránek)
* dané porty jsou hlídány (před heckery a neoprávněným přístupem) a v případě potřeby blokovány



Creative Commons, BY, [2013-11-17], Bpedrozo, <http://cs.wikipedia.org/wiki/Soubor:Firewall.png>

# Antivirový systém

* jedná se o počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného škodlivého software (malware). K zajištění této úlohy se používají dvě odlišné techniky:
  + prohlížení souborů na lokálním disku, které má za cíl nalézt sekvenci odpovídající definici některého počítačového viru v databázi
  + detekcí podezřelé aktivity nějakého počítačového programu, který může značit infekci. Tato technika zahrnuje analýzu zachytávaných dat, sledování aktivit na jednotlivých portech či jiné techniky.
* úspěšnost závisí na schopnostech antivirového programu a aktuálnosti databáze počítačových virů
* aktuální virové databáze se dnes nejčastěji stahují z Internetu.

## Metody kontroly

### Virové slovníky/databáze

Při kontrole souboru antivirový program zjišťuje, zda se nějaká jeho část neshoduje s některým ze známých virů, které má zapsány v databázi. Pokud je nalezena shoda, má program tyto možnosti:

* pokusit se opravit/vyléčit soubor odstraněním viru ze souboru (pokud je to technicky možné)
* umístit soubor do karantény (virus se dále nemůže šířit, protože ho nelze dále používat)
* smazat infikovaný soubor (i s virem)

K dosažení trvalého úspěchu ve středním a dlouhém období vyžaduje virová databáze pravidelné aktualizace.

Antivirový program fungující na platformě databáze virů kontrolují soubory v momentě, kdy je operační systém počítače vytvoří, otevře, zavře nebo je zasílá/přijímá emailem.

Ačkoli lze při kontrole za pomoci virových databází virus spolehlivě zničit, tvůrci virů se vždy snaží být o krok napřed v psaní virových softwarů pomocí "oligomorfních", "polymorfních" a stále častěji "metamorfních" virů, které šifrují část sami sebe nebo jinak upravují vlastní kód jako metodu zamaskování před rozpoznáním virovými databázemi. Dalo by se říci, že jde o jakési dynamické mutace klasických virů, které není vždy jednoduché rozpoznat.

### Nebezpečné chování

Metoda zjištění nebezpečného chování se oproti virovým databázím nesnaží najít známé viry, namísto toho sleduje chování všech programů. Pokud se takový program pokusí zapsat data do spustitelného programu, antivirus například označí toto nebezpečné chování a upozorní uživatele, který je vyzván k výběru dalšího postupu.

Výhodu má tento postup zjištění nových virů v tom, že ačkoli je virus zcela nový, neznámý ve virových databázích, může ho snadno odhalit. Nicméně i tato metoda má své nevýhody. Stává se, že antivirový program hlásí spoustu falešných "nálezů" viru. To může mít za výsledek, že uživatel postupem času přestane vnímat ta "pravá" varování. Z tohoto důvodu tento postup stále více moderních antivirových programů využívá méně a méně.

### Další metody

Určité antivirové programy používají další typy **heuristických analýz**. Například se může pokusit napodobit začátek kódu každého nového spustitelného souboru tak, že ho systém vyvolá ještě před přenosem do tohoto souboru. Pokud se program chová tak, že použije "samo-modifikační" kód nebo se jeví jako virus (pokud například začne hledat další spustitelné soubory), můžeme předpokládat, že virus nakazil další spustitelné soubory. Nicméně i tato metoda může hlásit falešné pozitivní nálezy.

Další metoda detekce virů se týká užití tzv. **sandboxu**. Sandbox, neboli pískoviště, napodobuje systém a spouští .exe soubory v jakési simulaci. Po ukončení programu software analyzuje sandbox, aby zjistil nějaké změny, ty mohou ukázat právě přítomnost virů. Tato metoda může taky selhat a to pokud jsou viry nedeterministické a výsledek nastane za různých akcí nebo akce nenastanou při běhu – to způsobí, že je nemožné detekovat virus pouze z jednoho spuštění.

Existují také antiviry, které varují uživatele před viry na základě toho, jakého typu soubor je.

Perspektivní metoda, která si obvykle poradí s malware, je tzv. "**whitelisting**". Spíše než vyhledávání jen známého zákeřného softwaru tato technika předchází spouštění všech kódů kromě těch, které byly již dříve označeny jako důvěryhodný administrátorem (uživatelem). Navíc aplikace v počítači, které jsou označeny jako malware, mají automaticky zakázáno spouštění, jakmile nejsou na "whitelist", tedy seznamu povolených programů. Dnes již existuje velké množství aplikací vytvořených velkými organizacemi, které jsou široce používané a "whitelist" je tedy tvořen především administrátory, kteří software rozpoznávají.

## Antivirové programy

* Microsoft Security Essentials – bezplatný antivirus i pro menší podniky
* Avira antivirus – antivirus německé produkce, i FREE verze ke stažení
* ClamAV – antivirový program šířený pod licencí GNU GPL
* AVG – antivirový systém od české firmy AVG Technologies (dříve Grisoft)
* Norton AntiVirus – produkt firmy Symantec pro domácí uživatele
* Symantec EndPoint Security – antivirové a bezpečnostní řešení pro korporátní sféru
* ESET NOD32 Antivirus – slovenský komerční antivirový program, který byl magazínem Virus Bulletin již mnohokrát oceněn jako nejlepší antivir
* McAfee Antivirus – klasický antivirový produkt
* Kaspersky Antivirus – výrobek ruské společnosti Kaspersky Labs
* BitDefender – kvalitní antivirový produkt rumunské společnosti SoftWin
* avast! – český antivirový program od firmy ALWIL Software. Pro domácí nekomerční použití freeware.
* Dr.Web – ruský antivirus
* TrustPort Antivirus – český produkt vyznačující se kvalitní detekcí díky kombinaci více antivirových jader
* eScan – kvalitní antivirový produkt z Indie
* Sophos antivirus
* Norman antivirus
* F-Secure antivirus
* eTrust antivirus

# Antispamový systém

Ochranný systém poštovního serveru (popř. poštovního klienta) před nevyžádanou poštou. Podrobněji u tématu **Bezpečnost služby e-mail**.

# Kontrolní otázky

* 1. Popiš funkci firewallu.
  2. Popiš základní využití proxy serveru.
  3. Jak funguje metoda antivirové kontroly pomocí databáze virů?
  4. Vyjmenuj alespoň 5 příkladů antivirového systému.
  5. K čemu slouží antivirový program?
  6. K čemu slouží antispamový program?
  7. Co je to bezpečné heslo? Uveď příklad.