VPN – Bezpečnostní souvislosti

Karel Miko, CISA (miko@dcit.cz)
DCIT, s.r.o (www.dcit.cz)

Bezpečnost VPN ≈ šifrování

- nejčastější technologie pro VPN – IPSec (příp. jeho proprietární variace)
- základem kvalitní šifra – obvykle 3DES / AES (DES v současnosti již není považován za dostatečný)
- význam autentizace
  - doporučujeme RSA – x.509 certifikáty
  - tzv.„pre-shared“ passwords nejsou obecně považovány za zcela vhodné
- existující standardy nabízí možnost velmi vysoké úrovně zajištění integrity a důvěrnosti přenášených dat (praxe může být různá)

DCIT

Obecně platí

- při korektním nastavení je VPN z hlediska použitých kryptografických prostředků prakticky „neprůstřelná“
- pokud někdo na VPN za útočí, zcela jistě se nebude pokoušet prolomit použitou šifru
- podstatně zranitelnější než samotná VPN jsou její koncové uzly
- VPN je od toho, aby zajistila bezpečný, spolehlivý komunikační kanál – nezkoumá, co je přenášeno

DCIT

VPN – AES vs. 3DES vs. DES

- AES (128/192/256 bit) – v současnosti doporučeno
- 3DES (112 bit) – v současnosti akceptovatelná šifra
- DES (56-bit) – není považován za dostatečnou šifru

Není to pouze o délce klíče

- způsob/náročnost výpočtu (3/DES náročnější)
- rychlost šifrování vs. dešifrování (a/symetričnost)
- odolnost vůči útokům hrubou silou (AES náročnější inicializace – komplikovanější brute-force)
- přesto je délka klíče významný faktor

DCIT

Velikost prostoru klíčů

• AES 256-bit	$1{,}1 * 10^{77}$	
• AES 192-bit	$6{,}2 * 10^{57}$	
• AES 128-bit	$3{,}4 * 10^{38}$	
• 3DES 112-bit	$5{,}2 * 10^{33}$	
• RC5 72-bit	$4{,}7 * 10^{21}$	2 roky - nerozluštěno
• DES 56-bit	$7{,}2 * 10^{16}$	rozluštěno za 22h

DCIT

Rozluštění šifry – reálné?

1999 – DES challenge

- velikost prostoru klíčů: **$7{,}2 * 10^{16}$**
- 56-bit DES **rozluštěn za 22h** skupinou **http://distributed.net**
- 100 tis. počítačů + Deepcrack - DES cracking machine
- špičkový výkon **250 miliard klíčů/s**

2002-? – RC5-72 challenge

- RC5 72-bitů (symetrická bloková šifra)
- velikost prostoru klíčů: **$4{,}7 * 10^{21}$**
- distributed.net: po 550 dnech **$5{,}2 * 10^{18}$** tj. 0,11 % prostoru klíčů
- aktuální průměr **160 miliard klíčů/s**
- současnou rychlostí - celý prostor za **980 let**
- při 40% ročním nárůstu (Moore) - celý prostor za **20 let**

DCIT

Rozluštění AES - hypoteticky

AES

- prostor klíčů **3,4 * 10^{38}** (128bit), **1,1 * 10^{77}** (256bit)
  - počet částic ve viditelné části vesmíru řádově 10^{80}
- RC5 vs. AES – řádově stejná výpočetní náročnost
- nechť máme výpočetní sílu **160 miliard klíčů/s** (DNet)
- konstantní rychlostí **100 trilionů = 10^{20} let** (128 bit !!)
  - stáří vesmíru je 15 miliard = 1,5 * 10^{10} let
  - stáří Země je 4,5 miliardy = 4,5 * 10^{9} let
- očekávaný nárůst výpočetní síly:
  - Mooreův zákon – roční nárůst 40%
  - Phil Zimmerman odhaduje – roční nárůst 60%
- při nárůstu 60% – **98 let** (128bit), **286 let** (256bit)

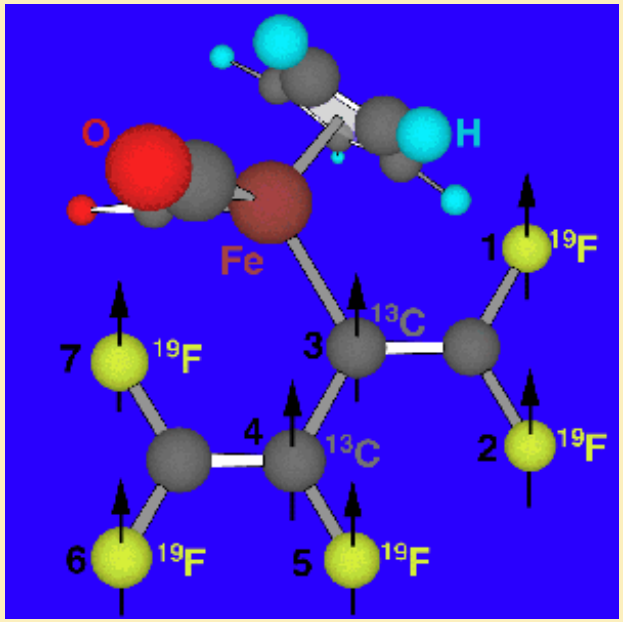
DCIT

Problematické oblasti

- spotřeba energie – existuje jisté termodynamické minimum energie na jednu operaci
- problém komunikační cesty (v distribuovaném prostředí) – za čas T oslovím max. **konst.*(c*T)^3** uzlů
- pokud by se výpočty účastnila hypoteticky veškerá energie hmoty – existuje limit **(2*mc^2)/(π*ħ)** = **5,4*10^{50}** elementárních operací za vteřinu na 1 kilogram hmoty
- počítač o teplotě T může na každém svém bitu provést za sekundu max. řádově **(k*T*ln 2)/ħ** operací (při teplotě 5,9*10^8 K je to cca 10^{19} operací/s/bit).
- problém vyzařování energie na každý „zahozený“ bit
- **Seth Lloyd: Ultimate physical limits to computation**

DCIT

Kvantové počítače – ohrožení?



- vysoce experimentální oblast
- 7-qbit počítač (IBM)
- $C_{11}H_5F_5O_2Fe$
  - pentafluorobutadienyl cyclopentadienyldicarbonyl-iron complex
- momentálně ohrožuje především asymetrické šifry – faktorizace v polynomiálním čase (Shorův algoritmus)
- IBM (7-qbit kvantový počítač) – faktorizace čísla 15
- jistý dopad i na symetrické šifry - Groverův algoritmus vyhledávání v nesetříděné databázi – O(sqrt N)

DCIT

Bezpečnostní úskalí – koncová zařízení

Zakončení VPN

- obvykle router (příp. firewall)

Obvyklé problémy

- aktualizace/patche – použité SW vybavení je poměrně komplikované (kryptografie), nelze vyloučit výskyt chyb
- **praxe:** neaktualizovaný SW – riziko DoS útoků, znepřístupnění či jiné negativní ovlivnění funkčnosti
- neodborným zásahem do nastavení lze jednoduše degradovat veškeré bezpečnostní vlastnosti VPN
- vysoké nároky na údržbu zařízení
  - kvalifikované lidské zdroje
  - znalosti (sledování aktuálního vývoje)

DCIT

Základní otázka: jak připojit VPN do vnitřní infrastruktury?

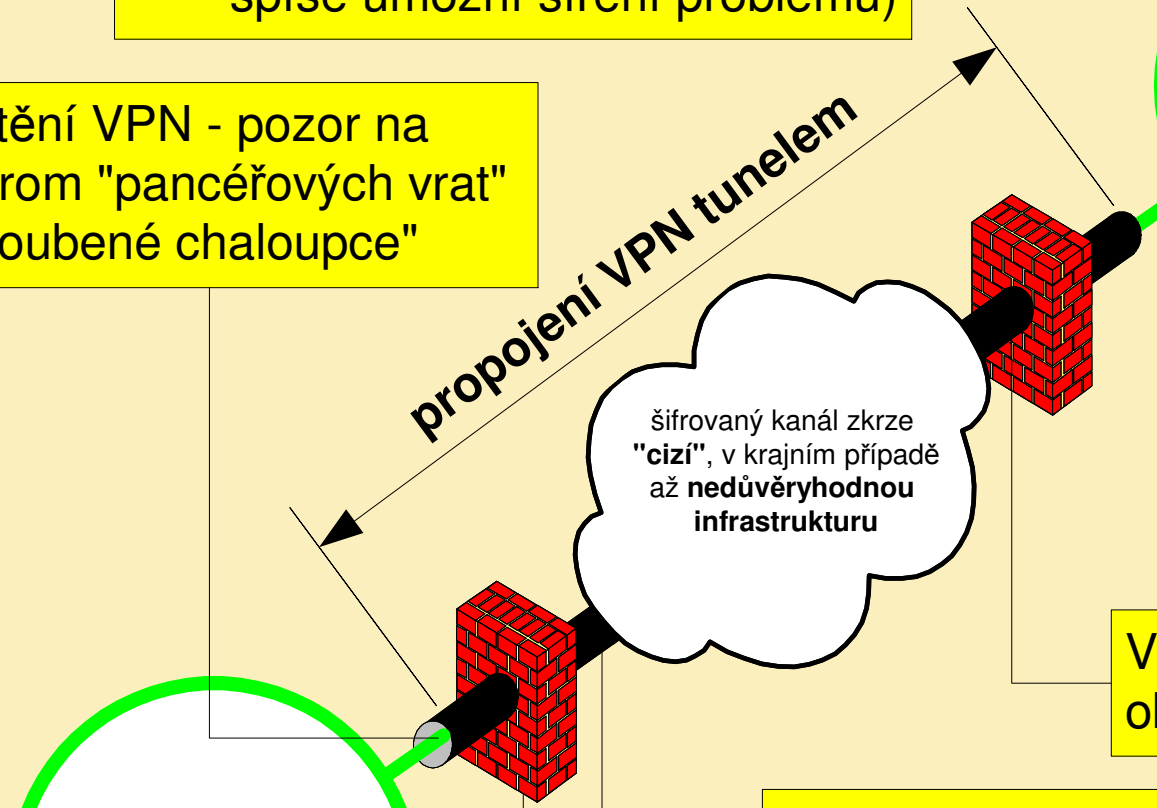
- vzdálený konec/konce VPN je vhodné vnímat do jisté míry jako vnější prostředí
- zakončení VPN přímo ve vnitřní LAN – ne zcela dobrá praxe (byť častá)
- **praxe:** šíření problémů mezi lokalitami skrze VPN
- ideální je připojení VPN do vnitřního prostředí přes prvek schopný řídit komunikaci probíhající přes VPN
  - firewall příp. router se základními funkcemi firewallu
  - opět zvýšené nároky na správu

DCIT

Bezpečnostní úskalí VPN – shrnutí

VPN Vás neochrání před vnitřním nepřítelem ve Vaší LAN (naopak spíše umožní šíření problému)

vyústění VPN - pozor na syndrom "pancéřových vrat" na "roubené chaloupce"



v bodě propojení s LAN nutno filtrovat provoz

VPN nekontroluje obsah komunikace

na šifrovaný VPN kanál hacker útočit nebude (riziko zanedbatelné)

zabezpečení koncového uzlu VPN je kruciální (riziko v případě úspěšného útoku vysoké)

DCIT

Zabezpečení VPN v běžném provozu

- všechna zmíněná úskalí bezpečnosti VPN jsou v praxi řešitelná
- příčiny významné části potenciálních problémů neleží v samotné VPN
- řešení vlastními silami vs. outsourcing

VPN a outsourcing

- v současnosti v podstatě již osvědčená kombinace
- nelze obecně prohlásit, že outsourcing je vždy tou nejlepší cestou / optimálním řešením – rozhodně **nejde jen o náklady**
- existují „pro“ i „proti“ – nutno vždy vyhodnotit případ od případu
- i při kompletním outsourcingu mohou vzniknout problémy s dopadem vně společnosti
  – tyto **problémy zůstanou vždycky „Vaše“**

DCIT

Nevýhody

- velká **závislost** na externím subjektu (velmi často výrazně asymetrický vztah: „velký“ zákazník vs. „malý“ dodavatel)
- byť **finanční úspory** bývají prezentovány jako výhoda, není tomu tak vždycky (přesto i finančně nákladnější outsourcing může být dobrou volbou)
- zvýšená **provozní rizika** – technologii nemáte „pod kontrolou“, „klíče“ od důležité části infrastruktury svěřujete „cizímu subjektu“
- praktická **vymahatelnost sankcí** v případě neplnění SLA bývá často sporná

DCIT

Výhody

- obecná „klišé“
  - ušetříte (možná – viz dále)
  - Váš podnik se může soustředit na „core business“
  - nižší počet zaměstnanců (lepší ukazatele produktivity)
- získáváte poměrně rychle know-how, které nemáte (příp. ani není vašim cílem jej mít)
- speciálně v případech, kdy vlastního specialistu nevyužijete na plný úvazek je outsourcing výhodný
- za jistých okolností přímé finanční úspory – pozor na nápadně levné nabídky

DCIT

Bezpečnost má širší kontext

- technická rovina
  - VPN, firewally, antiviry, IDS apod.
  - zabezpečení serverů, databází, aplikací, …
- procesně organizační rovina
  - řadu opatření nelze vynutit technickými prostředky
  - disciplína, firemní kultura
  - nepodceňovat formální aspekty – předpisy/dokumentace

Důvěřuj, ale prověřuj

- bezpečnostní audity - technické, organizační (ISO17799)
- penetrační testy (pronájem „hackera“)

DCIT

Děkuji za pozornost

Karel Miko, CISA
DCIT, s.r.o.
(miko@dcit.cz)

DCIT