Bezpečnosť IT infraštruktúry

Virtuálne súkromné siete (VPN)

RNDr. Jaroslav Janáček, PhD.
KI FMFI UK

Motivácia

- fyzické súkromné siete
  - je možné použiť prostriedky fyzickej bezpečnosti na ochranu pred externým útočníkom
  - dobre použiteľné len pre rozsahom malé siete v chránenom prostredí
  - náročné pre geograficky rozľahlé siete
    - napr. prepojenie vzdialených pobočiek
  - málo flexibilné
    - viazané na existenciu bezpečných fyzických liniek

Motivácia

- Nestačí riešiť bezpečnosť na vyšších vrstvách (transportná, aplikačná)?
  - nie vždy je to možné – vyžaduje si to súčinnosť aplikácií
  - často je vhodných viac „línií obrany“
    - sotfvér obsahuje chyby, ktoré je často možné zneužiť
    - pravdepodobnosť súčasného nastatia viac javov je často nižšia ako pravdepodobnosť jednotlivých javov

Úloha VPN

- vytvorenie bezpečného komunikačného kanála
  - ochrana dôvernosti a integrity prenášaných údajov a autentifikácia koncových bodov
- na sieťovej alebo linkovej vrstve
- transparentne pre vyššie vrstvy
  - bez potreby súčinnosti s aplikáciami

Realizácia VPN

- kryptografické prostriedky
  - šifrovanie
  - HMAC
  - autentifikácia
  - manažment kľúčov
    - PKI
    - statický preshared secret

Scenáre VPN

- bezpečné prepojenie niekoľkých fyzických súkromných sietí cez verejnú sieť
  - napr. prepojenie geograficky vzdialených pobočiek
- bezpečné pripojenie vzdialeného počítača cez verejnú sieť do chránenej siete
  - napr. pripojenie počítača doma alebo „na cestách“ do chránenej siete (napr. firemnej)

Negatíva VPN

- VPN vytvárajú „dieru“ do chránenej siete
  - vzdialený počítač pripojený cez VPN sa zvyčajne posudzuje rovnako ako počítač priamo v chránenej sieti,
  - ale zároveň má (môže mať) spojenia s vonkajším svetom, ktoré nie sú pod kontrolou správcu chránenej siete.
- Používanie VPN preto treba aj organizačne ošetriť.

Konkrétne riešenia

- IPsec
  - pôvodne povinná, neskôr voliteľná súčasť IPv6, voliteľné v IPv4
  - protokoly AH, ESP, ISAKMP/IKE, IKEv2
  - rôzne implementácie na mnohých platformách
    - nie vždy celkom kompatibilné
- OpenVPN
  - open-source produkt
  - manažment kľúčov založený na SSL/TLS
  - Linux, Windows, Mac OS X, Solaris, ...BSD, ...

IPsec

- kryptografická ochrana dôvernosti a/alebo integrity a autentifikácia koncových bodov na sieťovej vrstve
- operácie sú riadené politikou (SPD = Security Policy Database)
  - prepustiť paket bez zmeny
  - zahodiť paket
  - aplikovať IPsec transformáciu

Security Policy Database (SPD)

- pre spracúvaný paket sa nájde záznam v SPD
  - adresa zdroja a cieľa
  - protokol transportnej vrstvy, čísla portov
- záznam určí spôsob transformácie
  - IPsec mód
  - IPsec protokol
  - v tunelovom móde adresy koncov tunela

Security Association (SA)

- SA predstavuje jednosmerný komunikačný kanál, ktorý poskytuje konkrétne bezpečnostné služby pre ochranu prenášaných údajov
  - SPI (Security Parameters Index)
    - identifikuje SA u prijímateľa
  - mód
  - protokol
  - kryptografické algoritmy
  - kryptografické kľúče

Transportný vs. tunelový mód

- transportný mód
  - IPsec hlavička (AH, ESP) sa vkladá medzi IP hlavičku a hlavičku transportnej vrstvy
  - bezpečnosť priamo medzi koncovými počítačmi
- tunelový mód
  - pôvodný IP paket sa celý „zabalí“ do nového paketu
  - pribudne nová IP hlavička a IPsec hlavička
  - nový IP paket môže mať iné adresy zdroja a cieľa – adresy koncov tunela
  - typické použitie pre VPN medzi sieťami

Protokol AH (51)

- ochrana integrity
  - nemenných častí IP hlavičky pred AH
  - údajov transportnej vrstvy a vyššie
    - v tunelovom móde celého vnútorného IP paketu
- ochrana proti replay-attack-u
  - 32 (alebo 64) bitové sekvenčné číslo
- položky AH
  - next header, payload length, SPI, seq #, ICV

Protokol ESP (50)

- ochrana dôvernosti a/alebo integrity
  - údajov transportnej vrstvy a vyššie
    - v tunelovom móde celého pôvodného IP paketu
- ochrana proti replay-attack-u
- položky ESP hlavičky
  - SPI, seq #
  - dáta, padding, padding length, next header
  - ICV

AH vs. ESP

- oba umožňujú ochranu integrity
  - AH pokrýva aj nemenné časti IP hlavičky
  - ESP nepokrýva IP hlavičku
- interakcia s NAT
  - AH nie je možné použiť, ak je na ceste NAT
  - ESP je možné **čiastočne** použiť
    - problém je s rozlíšením rôznych ESP tokov
    - riešenie – enkapsulácia do UDP

Manažment SA a kľúčov

- ručne
- ISAKMP/IKE
  - ISAKMP – protokol na manažment SA a framework pre manažment kľúčov
  - IKE – protokol na manažment kľúčov
  - 2 fázy
    - 1. fáza – vytvorenie ISAKMP SA – obojsmerného bezpečného komunikačného kanála
    - 2. fáza – vytváranie párov SA pre AH/ESP
  - autentifikácia pomocou PKI alebo pre-shared secret

Manažment SA a kľúčov

- IKEv2
  - snaha o odstránenie niektorých nedostatkov ISAKMP/IKE
  - funkčne podobný (2 fázy)
  - nekompatibilný
  - autentifikácia
    - PKI
    - pre-shared secret
    - EAP

Podpora IPsec

- ISAKMP/IKE
  - Windows 2000/XP/Vista
  - Windows Server 2008/2008
  - Linux, OpenBSD, ...
- IKEv2
  - Windows 7
  - Windows Server 2008 R2
  - Linux, OpenBSD, ...

OpenVPN

- ochrana dôvernosti aj integrity a autentifikácia koncov
- ochrana proti replay-attack-u
- UDP alebo TCP
  - bezproblémové prechody cez NAT
- vytvára IP alebo L2 tunel
  - tun/tap sieťový interface

OpenVPN – manažment kľúčov

- statické kľúče
- SSL/TLS
  - autentifikácia servera
    - pomocou PKI
  - autentifikácia klienta
    - pomocou PKI
    - meno + heslo

IPsec vs. OpenVPN

- IPsec
  - transportný mód
  - povinné v IPv6
  - implementované priamo v mnohých OS
- OpenVPN
  - jednoduchšie protokoly na manažment kľúčov
  - bezproblémové prechody NAT-om, firewall-mi
  - tunel viditeľný ako virtuálny sieťový interface
  - jednotná implementácia – 100% kompatibilita
  - umožňuje aj L2 tunel