KOMUNIKAČNÉ A INFORMAČNÉ SIETE

BEZPEČNOSŤ

Ing. Michal Halás, PhD.
halas@ktl.elf.stuba.sk, B-514 , http://www.ktl.elf.stuba.sk/~halas

OBSAH

- Základné pojmy
- Aspekty bezpečnosti
- Šifrovanie
- Filtrácia
- VPN
- Spôsoby útokov
- Najznámejšie útoky

Bezpečnosť

- Bezpečnosť je proces a nie technické riešenie.
- Rieši množstvo aspektov, ktoré môžu viesť k nebezpečným situáciám:
  - neoprávnený prístup k citlivým dátam,
  - znemožnenie poskytovať služby,
  - . . .
- Vždy je pre užívateľov obmedzením, je potrebné nájsť vhodný kompromis.
- Zahŕňa sieťovú infraštruktúru aj aplikácie a OS koncových staníc.
- Infikované stanice môžu útočiť na sieťovú infraštruktúru.

Bezpečnosť

- Zahŕňa:
  - informovanosť užívateľov,
  - správu prístupových oprávnení,
  - sieťovú infraštruktúru,
  - aplikácie a OS koncových staníc,
  - . . .

Bezpečnosť

- všeobecne proces zabezpečenia komunikačných sietí a zariadení je rozdelený na:
  - prevencia
    - ochrana pred hrozbami
  - detekcia
    - odhalenie neoprávnených činností a slabých miest v systéme
  - náprava
    - odstránenie slabých miest v systéme

Základné pojmy

- Utajenie (confidentality) – útočník nerozumie získaným dátam.
- Autentizácia (authentication) – proces overenia identity komunikačnej strany, dôvera že komunikačná entita je tým, za koho sa vydáva.
- Autorizácia (autorization) – overenie oprávnenia entity využívať dané služby.
- Integrita (integrity) – dôvera, že dáta neboli pri prenose modifikované.
- Nepopierateľnosť (non-repudiation) – zdroj dát nemôže poprieť, že dané dáta odoslal.

Bezpečnosť

- Oblasti zabezpečenia:
  - fyzická bezpečnosť,
  - bezpečnosť operačných systémov,
  - bezpečnosť služieb a aplikácií,
  - bezpečnosť komunikačných sietí.
- Spôsoby zabezpečenia:
  - šifrovanie,
  - filtrácia komunikácie,
  - detekcia útokov.

Fyzická bezpečnosť

- Prístup k systému a jeho častiam by mal byť fyzicky obmedzený len pre užívateľov, ktorí nevyhnutne potrebujú na svoju prácu.
- V prípade, že je systém dostatočne fyzicky chránený a nie je možné sa k nemu pripojiť iným spôsobom, v podstate nie je potrebné riešiť žiadne ďalšie aspekty bezpečnosti.
- Jedná sa však o ideálny prípad, ktorý sa v praxi nevyskytuje.
- Je potrebné dostatočne chrániť prístup ku komunikačným serverom, sieťovej infraštruktúre a komunikačným prvkom siete.
- Fyzická bezpečnosť komunikačných liniek je kľúčovou pri riešení bezpečnosti v komunikačných sieťach. Špecifickým prípadom sú bezdrôtové siete, kde nie je možné zabezpečiť prenosové médium.

Bezpečnosť operačných systémov

- Každý komunikačný systém má svoj operačný systém, ktorý môže v sebe skrývať množstvo bezpečnostných dier.
- Je potrebné zabezpečiť operačný systém aj na strane serveru aj na strane klientov. Vo väčšine prípadov je totiž sieť vytvorená práve za účelom interakcie používateľov a serverov, a teda neoprávnené získanie kontroly nad používateľským zariadením, by mohlo znamenať získanie prostriedkov potrebných na získanie kontroly nad serverom.
- Výrobcovia operačných systémov pravidelne aktualizujú a zdokonaľujú dané produkty, je vhodné pracovať s aktuálnymi verziami.

Bezpečnosť služieb a aplikácií

- Samotná implementácia jednotlivých komunikačných funkcií na strane serveru alebo klienta je riešená ako samostatná aplikácia.
- Aplikácia, podobne ako operačný systém môže „vďaka“ nedokonalosti implementácie obsahovať viacero bezpečnostných dier, ktoré môže útočník využiť vo svoj prospech.
- Bežiaca aplikácia má zväčša právo zápisu na disk, prípadne možnosť priamo spustiť škodlivý kód.

Bezpečnosť služieb a aplikácií

- Je potrebné zabraňovať ich zneužitiu, prípadne samovoľnej inštalácií nechcených aplikácií.
- Napríklad tzv. „trójske kone“:
  - aplikácie, ktoré sa infiltrujú do operačného systému veľmi primitívnou cestou napríklad príloha e-mailu prípadne žiadosť o inštaláciu podporného balíka v internetovom prehliadači,
  - nainštalovaná aplikácia má prístup napríklad ku adresáru kontaktov mailového klienta a dokáže sa ďalej prenášať,
  - môže zabrániť behu iným aplikáciám napríklad formou obsadenia portu.

Bezpečnosť komunikačných sietí

- Z pohľadu komunikačných a informačných sietí je táto oblasť kľúčová.
- Veľmi často sú siete rozdelené na:
  - siete operátorov / internet,
  - lokálne siete spoločnosti / intranet,
- Riešenie zabezpečenia siete je veľmi závislé od spôsobu jej využívania, z toho dôvodu sa aj z pohľadu bezpečnosti oddeľujú vnútorné lokálne siete od vonkajších sietí.

Bezpečnosť komunikačných sietí

- Najčastejšie sa na rozhraní medzi sieťami filtruje prevádzka a na základe povolení je prepustená len povolená prevádzka.
- Filtráciu zabezpečuje:
  - Firewall,
  - Proxy server.
- Často sa rieši filtrácia prevádzky priamo aj na rozhraniach samotných komunikujúcich klientoch a serveroch.

Bezpečnosť komunikačných sietí

- Informovanosť o bezpečnostných aspektoch z pohľadu používateľov.
- Samotných používateľov v systéme predstavujú stanice alebo klienti.
- Je potrebné zabezpečiť niekoľko dôležitých krokov:
  - prístup do systému na základe autentifikácie,
  - autorizácia – teda rozvrhnutie politiky práv podľa reálnych požiadaviek,
  - informovanosť používateľov o dôležitosti zabezpečenia a prípadných nástrahách.

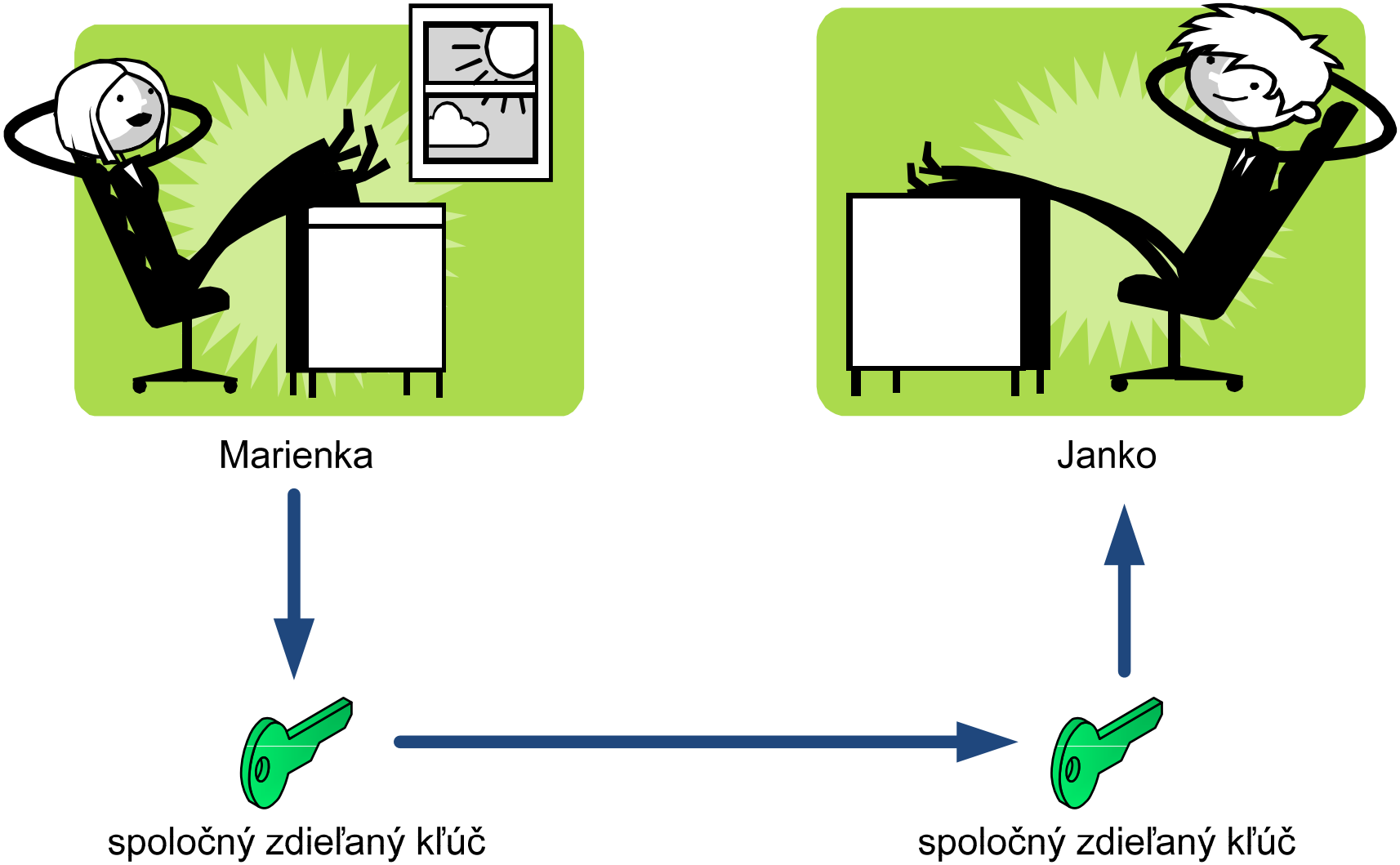
Šifrovanie

- Dáta sú pred prenosom kryptované takým spôsobom, aby ich nik okrem oprávneného príjemcu nebol schopný správne interpretovať
- Dve možnosti:
  - utajiť šifrovací algoritmus,
    - ak sa prezradí, je jeho implementácia nepoužiteľná,
  - využiť proces, ktorého vstupom sú okrem dát aj šifrovacie kľúče,
    - ak je dostatočne veľká množina možných kľúčov, môže byť samotný algoritmus známy.

Symetrické šifrovanie

- spoločný/zdieľaný kľuč,
- veľmi rýchle algoritmy, efektívna implementácia (SW aj HW),
- šifrovanie a dešifrovanie sa robí rovnakým kľúčom,
- problém s distribúciou kľúčov.
- Algoritmy: DES, 3DES, AES, ...
- Implementácia: WiFi, WinZIP, RAR, ...

Symetrické šifrovanie



Asymetrické šifrovanie

- Existuje vždy dvojica kľúčov:
  - verejný kľuč,
  - privátny kľuč,
- odosielateľ aj príjemca majú každý svoju vlastnú dvojicu kľúčov,
- oba kľúče sú vygenerované tak, aby dáta šifrované verejným kľúčom bolo možné rozšifrovať VŽDY LEN príslušným privátnym kľúčom,
- generovanie dvojíc kľúčov a hlavne potvrdenie ich platnosti vykonáva certifikačná autorita.

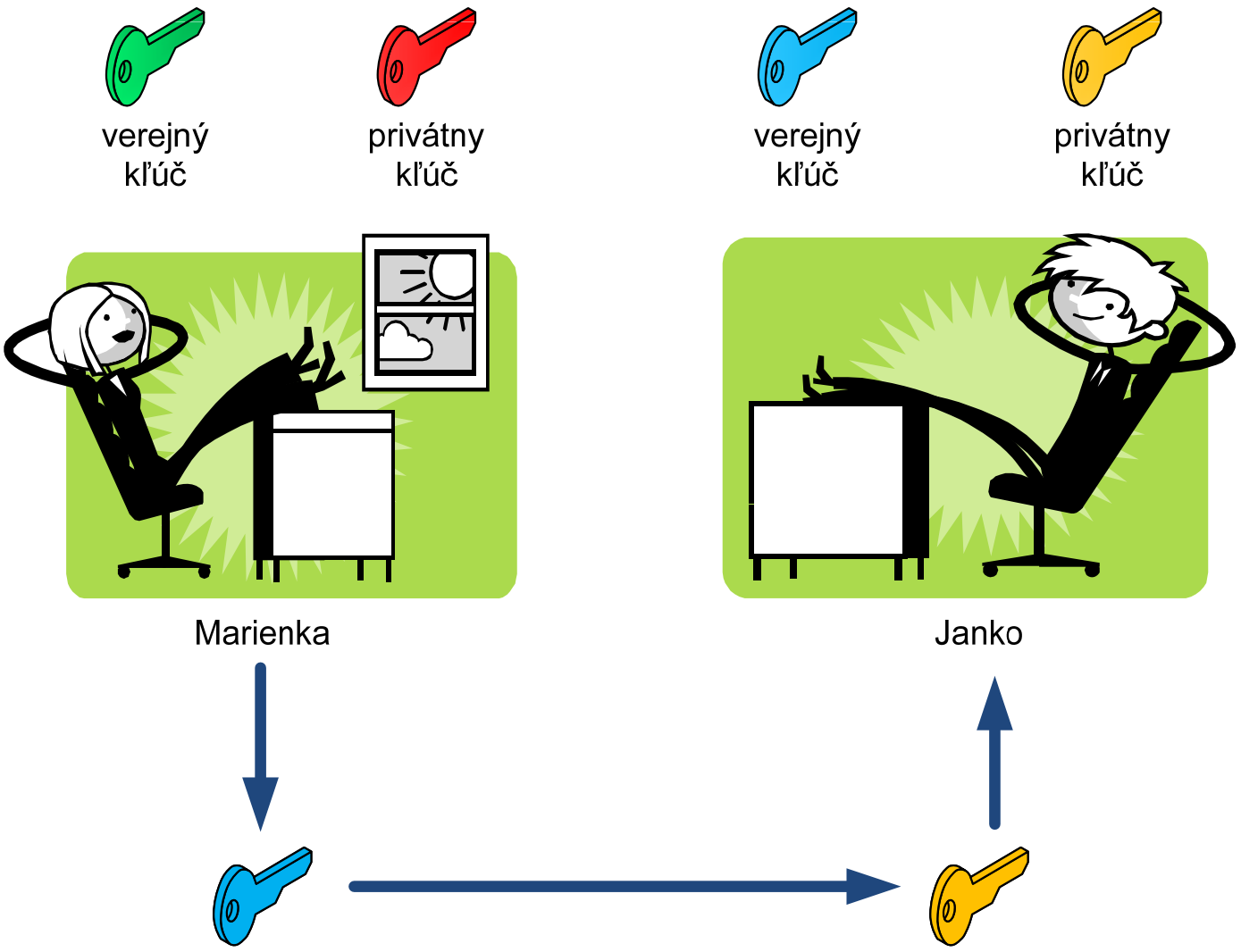
Asymetrické šifrovanie

- odosielateľ dáta šifruje verejným kľúčom príjemcu,
- príjemca dáta rozšifruje pomocou svojho privátneho kľúča,
- následne príjemca odpoveď zašifruje verejným kľúčom odosielateľa,
- odosielateľ prijatú odpoveď dešifruje svojim privátnym kľúčom.

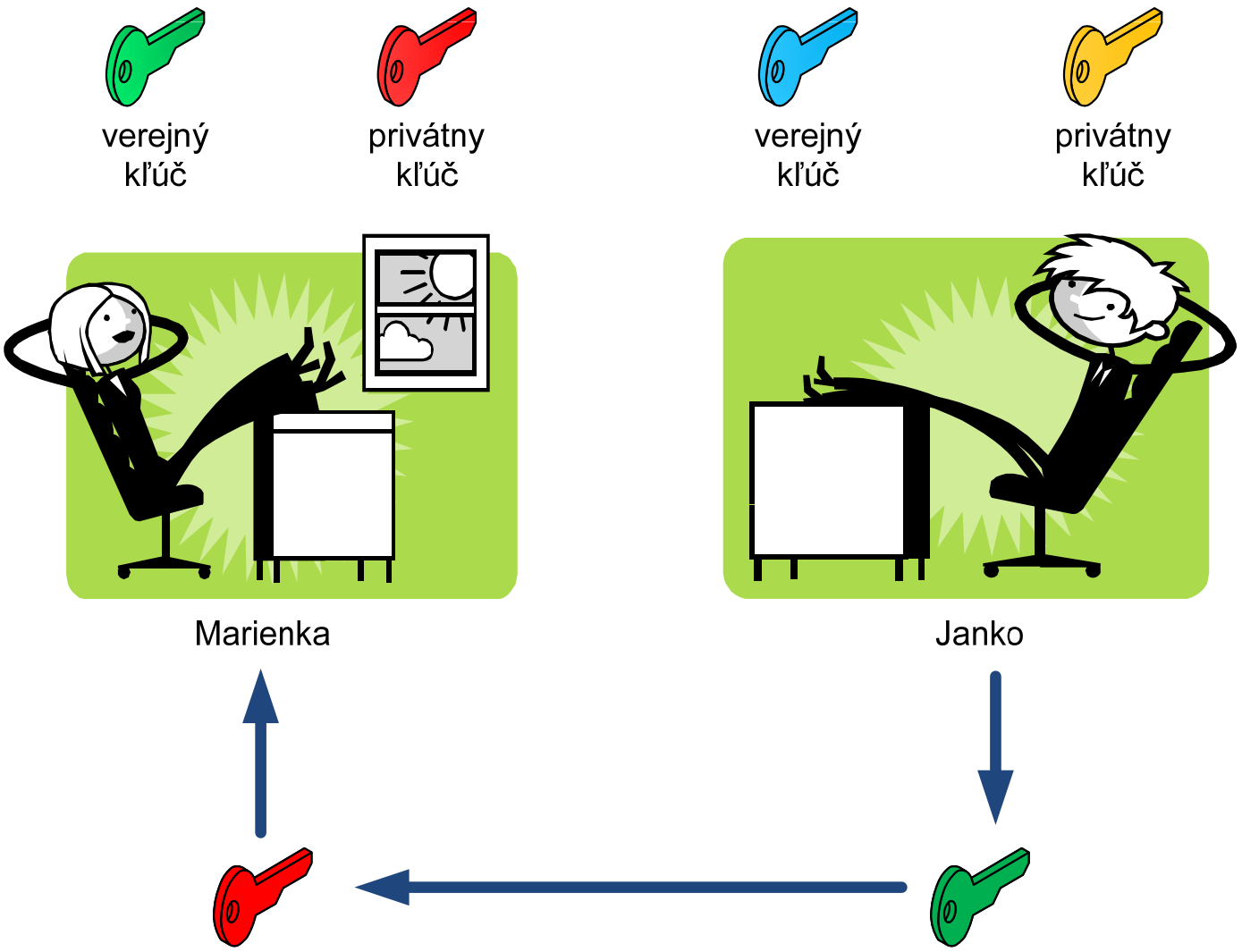
Asymetrické šifrovanie

- algoritmy sú omnoho náročnejšie ako pri symetrickom šifrovaní,
- využíva sa hlavne:
  - v digitálnych podpisoch a certifikátoch,
  - pre bezpečný prenos zdieľaného kľúča medzi komunikačnými uzlami.
- Algoritmy: Diffie-Hellman, RSA, …
- Implementácia: PGP, ZRTP, SSL, SSH, …

Asymetrické šifrovanie



Asymetrické šifrovanie



Možnosti šifrovania komunikácie

- Linková vrstva:
  - zabezpečenie bod-bod, neefektívne,
  - Layer 2 tunneling protocol (L2TP), point to point tunelling protocol (PPTP).
- Sieťová vrstva:
  - nezávislé na prenosovom médiu aj na použitých protokoloch vyšších vstiev,
  - IPSec.

Možnosti šifrovania komunikácie

- Relačná vrstva:
  - Secure Sockets Layer (SSL) a Transport Layer Security (TLS),
    - využíva protokol TCP,
  - Secure Realtime Transport Protocol (SRTP),
    - rozšírenie profilu pre RTP.
- Prezentačná a aplikačná vrstva:
  - šifrovacie algoritmy DES, AES, ...,
  - šifrovanie rieši osobitne každá aplikácia,
  - napr. S/MIME Secure Multipurpose Internet Mail Extensions , rozšírenie pôvodného MIME.

Filtrácia komunikácie

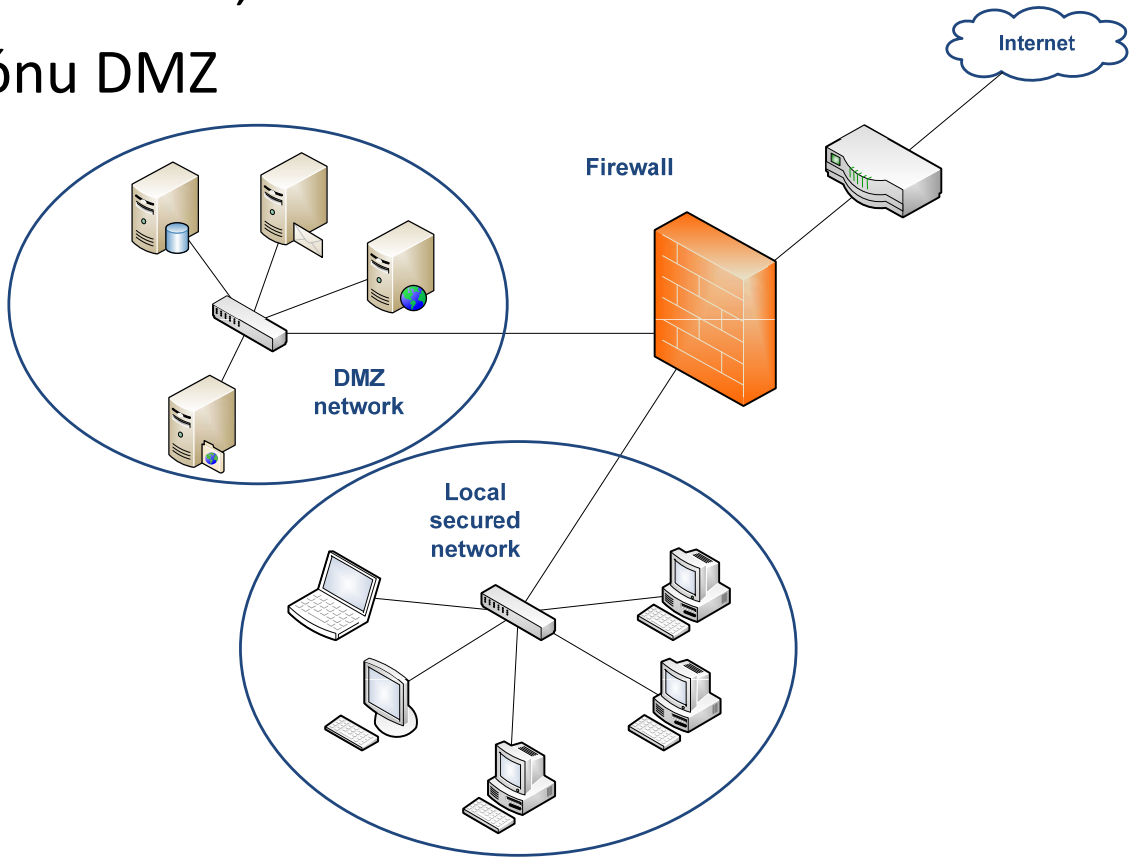
- Bezstavová (paketové filtre):
  - na základe identifikácie dát v pakete sa rozhodne o povolení alebo zamietnutí prenosu paketu,
  - problém s analýzou dát na 4. a vyšších vrstvách.
- Stavová (transparentná alebo ako proxy server):
  - na základe rekonštrukcie dátových tokov sa robí filtrácia,
  - potrebné uchovávať stavové informácie pre každý tok,
  - obmedzené možnosti škálovateľnosti.

Firewall

- Sieťové zariadenie, ktoré slúži na riadenie a zabezpečenie sieťovej prevádzky medzi sieťami s rôznou úrovňou dôveryhodnosti a zabezpečenia.
- Monitoruje prevádzku prechádzajúcu medzi sieťami a na základe pravidiel tzv. ACL rozhoduje, ktorý typ prevádzky povolí, a ktorý nie.
- ACL – Access Control Lists:
  - pravidlá aplikované na jednotlivé sieťové rozhrania, pomocou ktorých sa filtruje prevádzka,
  - môžu byť aplikované na 2., 3., 4. vrstve,
  - vždy je potrebné osobitne povoliť oba smery komunikácie → reflexívne ACL.

Firewall

- Rozdeľuje komunikačné oblasti na:
  - vnútornú – chránenú sieť,
  - vonkajšiu – nebezpečnú sieť,
  - demilitarizovanú zónu DMZ – nezabezpečenú vnútornú sieť.



Firewall

- Povôdne boli pravidlá definované na základe zdrojovej, cieľovej IP adresy, zdrojového, cieľového portu a transportného protokol,
  - bezstavové firewally.
- Moderné firewally pracujú so stavom spojenia
  - stavové firewally,
- hlbšou analýzou a znalosťou aplikačných protokolov , prípadne kombinované s mechanizmami IDS (Intrusion Detection System).

Firewall

- Firewally sa delia do nasledovných skupín:
  - paketové filtre,
  - aplikačné brány,
  - stavové paketové filtre,
  - stavové paketové filtre s kontrolou známych protokolov, prípadne kombinované s IDS.

VPN

- Virtuálne privátne siete:
  - umožňujú budovať privátne siete s použitím zdieľanej infraštruktúry siete,
  - poskytujú rovnakú úroveň konfigurovateľnosti a bezpečnosti ako pri použití vlastnej infraštruktúry,
  - virtuálne komunikačné spojenie medzi jednotlivými bodmi VPN je tvorené tunelmi, cez ktoré sú prenášané dáta,
  - na zabezpečenie prevádzky sa využívajú šifrovacie metódy a autentizácia komunikujúcich uzlov.

IPsec

- Protokol sieťovej vrstvy
- podpora bezpečnostných služieb v IP
- vytvára tunel medzi dvoma komunikujúcimi zariadeniami
- prevádzka prenášaná tunelom je transparentne šifrovaná, nezávisle od použitých protokolov vyšších vrstiev
- využíva algoritmy 3DES a AES

SSL/TLS

- Bezpečnostné protokoly relačnej vrstvy
- poskytujú šifrovaný prenos pre protokolu aplikačnej vrstvy, ako transportný protokol je využitý TCP
- primárne určený na zabezpečenie konkrétnych aplikačných tokov
- neskôr implementácie ako napr. OpenVPN umožnili vybudovanie tunelov šifrovaných pomocou TLS
- principiálne má TLS lepšie vlastnosti pri prechode cez NAT a Firewall ako IPsec.

Detekcia a prevencia útokov

- Intrusion Detection Systems a Intrusion Prevention Systems:
  - systém monitorujúci prevádzku v sieti,
  - rozpoznáva podozrivé vzory komunikácie,
  - pracuje na rôznych vrstvách,
  - klasifikuje nebezpečenstvo, informuje správcu, prípadne, inteligentne reaguje na vzniknutú situáciu:
    - zablokovaním komunikácie,
    - prekonfigurovaním firewallu.

Spôsoby realizácie útokov

- Man in the middle.
- Eavesdropping.
- Denial of Services.
- Zneužitie nedokonalosti návrhu protokolov.
- Zneužitie slabých miest v systéme.
- . . .

Eavesdropping

- pasívne odpočúvanie komunikácie na spoločnom zdieľanom médiu
- sieťová karta v promiskuitnom móde
- útočník nevstupuje do komunikácie, len ju zachytáva

Man in the middle

- aktívne odpočúvanie prevádzky medzi dvoma koncovými zariadeniami
- útočník presmerováva prevádzku cez seba tak, že komunikujúce uzly si myslia že komunikujú priamo medzi sebou
- útočník je schopný zachytiť všetky správy, ktoré si komunikujúce strany medzi sebou vymieňajú

Denial of Services

- DoS, alebo Distribuovaný DoS DDoS
- technika zameraná na znemožnenie poskytovania služieb, vďaka zahlteniu systému veľkým množstvom falošných požiadaviek
- server danej služby sa snaží vyhovieť všetkým požiadavkám, čo vedie k situácii, že vyčerpá všetky svoje dostupné kapacity a nie je schopný reagovať na „oprávnené“ požiadavky

Zneužitie nedokonalosti návrhu protokolov

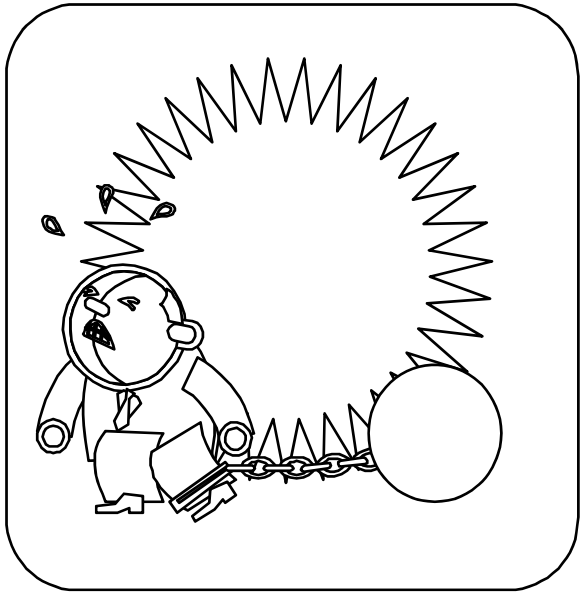
- využitie nedokonalosti v návrhu jednotlivých komunikačných protokolov
- množstvo protokolov sa vo svojich prvotných verziách nezaoberalo problematikou bezpečnosti
- existuje množstvo zdokumentovaných slabín jednotlivých protokolov, ktorých vhodné využitie útočníkom, môže viesť na narušeniu bezpečnosti komunikácie, prípadne celého komunikačného systému

Zneužitie slabých miest v systéme

- kuzly majú svoj operačný systém a viacero aplikácií, ktoré realizujú príslušné komunikačné funkcie,
- implementácia týchto aplikácií a operačných systémov obsahuje množstvo bezpečnostných dier,
- ich využitím môže útočník získať prístup k citlivým informáciám (prípadne ich môže aj zmeniť) alebo destabilizovať systém do takej miery, že nie je schopný poskytovať dané služby,
- je potrebné využívať aktuálne verzie produktov a pravidelne inštalovať bezpečnostné „záplaty“.

Reálne útoky na sieťovú infraštruktúru

- ARP spoofing,
- DHCP spoofing,
- MAC flooding,
- Port stealing,
- DNS spoofing,



- jedná sa o útoky Man in the middle a Eavesdropping,
- podstatou je sledovanie prevádzky medzi dvoma komunikujúcimi uzlami.

ARP Spoofing

- ARP Spoofing resp. ARP Cache poisoning,
- využíva slabinu ARP protokolu, ktorý vo svojom návrhu neimplementuje žiaden mechanizmus overenia totožnosti klienta,
- pri odoslaní prvého paketu IP musí odosielateľ zistiť MAC adresu cieľového uzlu,
- získanú dvojicu IP adresa → MAC adresa si kvôli zvýšeniu výkonu uchováva vo svojej vyrovnávacej pamäti, tzv. ARP cache.

ARP Spoofing

- útok spočíva v presvedčení odosielateľa, že IP adrese príjemcu zodpovedá MAC adresa útočníka a zároveň presvedčenie príjemcu, že IP adrese odosielateľa zodpovedá MAC adresa útočníka,
- toto je možné vykonať napríklad pomocou modifikovaného pingu, kde je uvedená falošná MAC adresa,
- falošné ARP pakety je potrebné zasielať v pravidelných intervalov (20 sec), aby sa udržiavali aktuálne informácie v ARP cache.

DHCP Spoofing

- využíva nedokonalosť DHCP protokolu, ktorý umožňuje aby bolo v sieti súčasne viacero DHCP serverov,
- klient pri inicializácii posiela DHCP Discover, na ktorý server odpovedá DHCP Offer, platí pravidlo, že ak príde viacero DHCP Offer, klient komunikuje so serverom, ktorý mu odpovedal skôr,
- je potrebné zabezpečiť, aby falošný DHCP server odpovedal rýchlejšie ako riadny DHCP server.

DHCP Spoofing

- v prípade, že klient získa nastavenia od riadneho DHCP serveru, je potrebné vyčkať, kým vyprší „lease time“ a klient si bude musieť aktualizovať svoj záznam,
- klient posiela DHCP request, priamo na IP adresu DHCP serveru, takže je potrebné zabezpečiť, aby mu riadny DHCP server nebol schopný prideliť žiaden záznam,
- je potrebné DHCP server zahltiť požiadavkami, tak aby si vyčerpal všetky dostupné voľné IP adresy, následne nebude schopný odpovedať na žiadne požiadavky.

DHCP Spoofing

- Riadny DHCP server nebude schopný odpovedať na DHCP request a bude sa musieť spustiť znova celý proces DHCP discovery.
- Falošný DHCP server najčastejšie v modifikovaných záznamoch posiela ako „gateway“ adresu svoju IP adresu, vďaka čomu presmeruje všetku odchádzajúcu prevádzku z klienta do internetu cez seba.
- Nie je však schopný presmerovať opačný smer komunikácie internet → klient.

MAC Flooding

- Využíva slabinu smerovačov v prípade preplnenia internej tabuľky MAC adries.
- V prípade, že na switch dorazí paket ktorého cieľovú MAC adresu nemá v CAM pamäti, switch ju prepošle na všetky porty okrem portu odkiaľ paket prijal,
- ak prijme paket, ktorého zdrojovú MAC adresu ešte nemá v pamäti, zapíše si do CAM dvojicu MAC adresa → port a následne dáta preposiela už len na konkrétny port

MAC Flooding

- CAM tabuľka MAC adries má obmedzenú veľkosť, preto dochádza k jej pravidelnému premazávaniu
- podstatou útoku je zaplniť CAM tabuľku switchu nezmyselnými údajmi, najčastejšie umelo generovanými paketmi s náhodne zvolenými zdrojovými MAC adresami
- ak dôjde k zaplneniu pamäte (tisíce/stotisíce záznamov), switch sa prepne do režimu fail open a začne preposielať všetky pakety ako HUB.
- takýmto spôsobom je útočník schopný odpočúvať prevádzku v sieti.

Port Stealing

- Útok zameraný na presvedčení switchu, že adresát sa nachádza na porte ku ktorému je pripojený útočník.
- Modifikáciu CAM tabuľky switchu sa dá dosiahnuť odosielaním paketu, kde cieľová MAC adresa bude adresa útočníka a zdrojová adresa bude adresa príjemcu.
- Switch po prijatí takéhoto paketu si aktualizuje svoju CAM tabuľku a MAC adrese príjemcu priradí port útočníka.

Port Stealing

- útočník je schopný prijať dáta, je potrebné zabezpečiť, aby sa dáta následne predoslali adresátovi,
- pred tým, je však potrebné „opraviť“ záznam v CAM tabuľke, napríklad vyslaním korektného ARP Request na adresáta.

DNS Spoofing

- využíva slabinu DNS protokolu, ktorý neoveruje identitu zdroja DNS záznamu,
- útočník sa snaží podvrhnúť modifikovanú DNS správu, ktorá je odpoveďou na žiadosť o preklad doménového mena,
- pri žiadosti o preklad doménového mena klientom, je potrebné, aby modifikovaná správa prišla skôr od útočníka ako od riadneho DNS serveru.

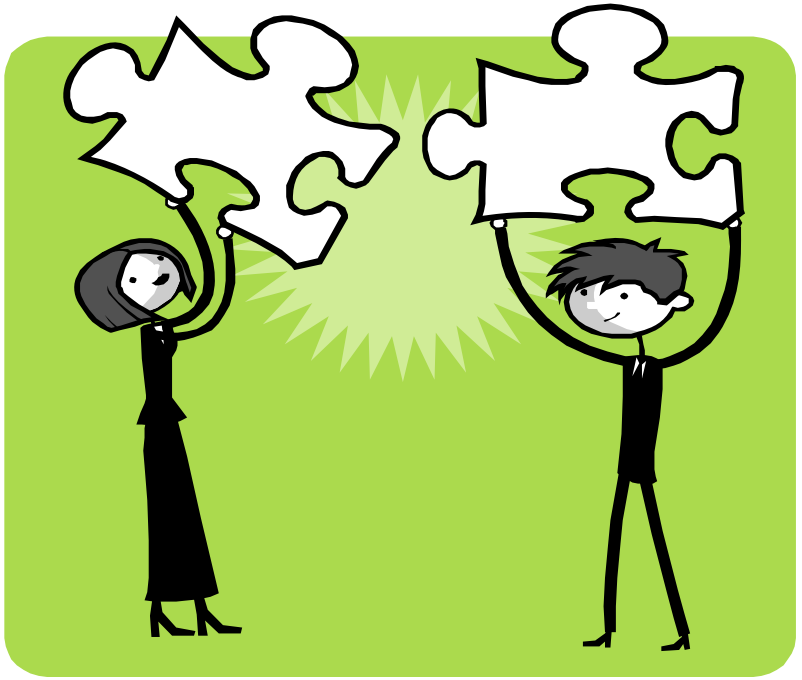
DNS Spoofing

- klient si po obdržaní odpovede o preklade doménového mena uloží vo svojej vyrovnávacej pamäti IP adresu útočníka a ďalej ju používa po dobu platnosti DNS záznamu,
- na rozdiel od predošlých útokov, DNS spoofing umožňuje presmerovať prevádzku aj mimo lokálnu sieť,
- podobným spôsobom je možné modifikovať záznamy aj na lokálnom DNS serveri, ktorý ich následne „v dobrej viere“ poskytuje jednotlivým klientom.

Ako sa brániť

- Firewall,
- Heslá,
- Autentifikácia, autorizácia,
- Šifrovanie,
- Detekcia útokov,
- Prevencia pred útokmi

. . .



KOMUNIKAČNÉ A INFORMAČNÉ SIETE

BEZPEČNOSŤ

Ing. Michal Halás, PhD.
halas@ktl.elf.stuba.sk, B-514 , http://www.ktl.elf.stuba.sk/~halas