1. Definujte a vysvětlete základní pojmy (aktiva, hrozba, ochrana, bezpečnost, zranitelnost, riziko, incident a dopad).

* Aktiva = cokoliv cenné (data, služby ,software, hardware)
* Hrozba = možnost ztráty aktiv
* Ochrana = opatření ke snížení četnosti nebo velikosti ztrát.
* Bezpečnost = stav, kdy ztráty aktiv nepřekračují určitou míru.
* Zranitelnost = místo bez dostatečné ochrany
* Riziko = využitelnost zranitelného místa
* Incident = realizace hrozby
* Dopad = důsledek útoku, rozsah škod

1. Problematika logování, hlavní cíle a rozdělení (definice logu, základní kategorie, formát, obsah logu, struktura záznamu, ochrana logů).

Záznamová data, logovací zpráva nebo jen log je soubor záznamů reprezentující popis konkrétní události, která nastala ve sledovaném systému.

* Informační: pouze popisující stavy, události
* Ladící: použivané při vývoji
* Varovné: označující chybějící funkci, součást systému
* Chybové: označují chyby ohrožující funkčnost systému
* Pohotovostní: často označující události spojené s bezpečností.

**Formát**: testový, binární

Obsah logu: Kdo, kde (lokální, vzdálené)

Jaké události (chyby autentizace, chyby systému, anomálie)

Co (Čas, zdroj, uživatel, událost, závaźnost)

**Struktura záznamu**: Časové razítko, zdroj, vlastní data

**Ochrana logů**: záloha, šifrování, centrální logovací server. Soubory je nutné chránit jak při ukládání, tak přenosu.

**Ukládání**: detekce změn logovacího souboru, záloha s read-only přístupem, pokročilé řízení přístupu.

**Přenos**: Dbát na zajištění důvěrnosti a autentičnosti dat, obvykle pomocí nechanismů kryptografie.

**Cíle analýzy logů** se mohou lišit v závislosti na potřebách konkrétního systému.

**Lze definovat 2 cíle logů:**

* **Detekce známých nepřiznivých událostí, které se již staly.**
* **Detekce neznámých nepříznivých událostí, které zatím nikdy nebyly realizovány.**

1. Bezpečná konfigurace přepínače a směrovače (základní postupy konfigurace, bezpečnostní funkce, útoky, Port Security, port Fast, hardening).

L1 ISO/OSI= rozbočovač (hub), opakovač (repeater)

L2 ISO/OSI = most (bridge), přepináč (switch)

L3 ISO/OSI = smérovač (router), přepinač (switch), brána (gateway)

L4-L7 ISO/OSI = IPS sonda, IDS sonda, VPN brána, anti-DDOS,stavový FW….

**Bezpečná konfigurace přepínače**

Pracuje na 2.vrstvě ISO/OSI, přeposíla data uvnitř sítě již po odfiltrování provozu firewalem/ hraničním směrovačem. (L3 přepínače pracuji i se 3 vrstvou).

**Možné útoky uvnitř sítě:**

* MAC adres spoofing (Neautorizovaný příjem cizích dat zpráv pomocí změny zdrojové adresy MAC na přepínači).
* ARP poisoning (úprava cache ARP na dvou portech vede k útoku (MitM), kdy je komunikace vedena přes útočníka)
* Rogue DHCP Server/Spoofing (Útočník řídí falešný DHCP server a odpoví rychleji na DHCP request klientům (může podvrhnout bránu)).
* DHCP starvation ( zaplavení DHCP requestu na server – snaha o vyčerpání IP adres, které lze přiřadit)
* LAN storm útoky – přeposílání

**Konfigurace:**

* **Zabezpečení fyzického a lokálního přístupu k přepínači.**
* **Nastavení bezpečného vzdáleného přístupu** (SSH, RSA 2048b)
* **Vypnutí nepotřebných služeb a portů.**
* **Zapnutí bezpečnostních funkcí** (dhcp snooping,port security)
* **Záloh konfigurací**, testování, ověřování

**Port security** = omezení počtu MAC adres na port, ochrana před MAC útoky

**PortFast** = nastaví port na forwarding state ihned po zapojení, je vhodné jen při připojení stanic a serverů.

BPDU Guard – chrání síť před zasláním BPDU zpráv na porty, kde by neměli chodit. BPDU zprávy jsou zprávy generované spaning tree protokolem.

RootGuard – Zabraňuje nahrazení root bridge spofovanou zprávou od útočníka. Nastavit na všechny root porty pro STP

**Bezpečná konfigurace směrovače:**

Pracuje na 3.vsrtvě ISO/OSI, síťové zařízení pro přeposílání dat a jejich směrování mezi sítěmi.

Můžou být: Směrovače v síti, hraniční směrovače, s paketovou filtrací a bezpečnostními funkcemi.

**Hraniční směrovač:**

* Poslední směrovač mezi vnitřní a nedůvěryhodnou sítí (vnější).
* Většinou s paketovou filtrací pro zajištění bezpečnostních pravidel.
* Zajistit fyzickou bezpečnost, bezpečnost OS směrovače (aktualizace, patche, záloha conf) a bezpečnou konfiguraci směrovače tzv. **router hardening** (bezpečná administrace, zakázat nepouživané porty a rozhraní, nepotřebné služby a logovat události).

**Útoky na směrovač:**

* Pokus o průnik do nastavení na směrovači (zneužití default hesel).
* Routing table poisoning – vyvolání nežádoucí změny ve směrovací tabulce pomocí spoofování routovacích protokolů.
* Hit and Run – posíla škodlivé pakety do směrovače v náhodných intervalech.
* DOS/DDOS – zaplavení množstvím paketů a vytížení CPU/RAM, logické útoky (Xmax attack atd)

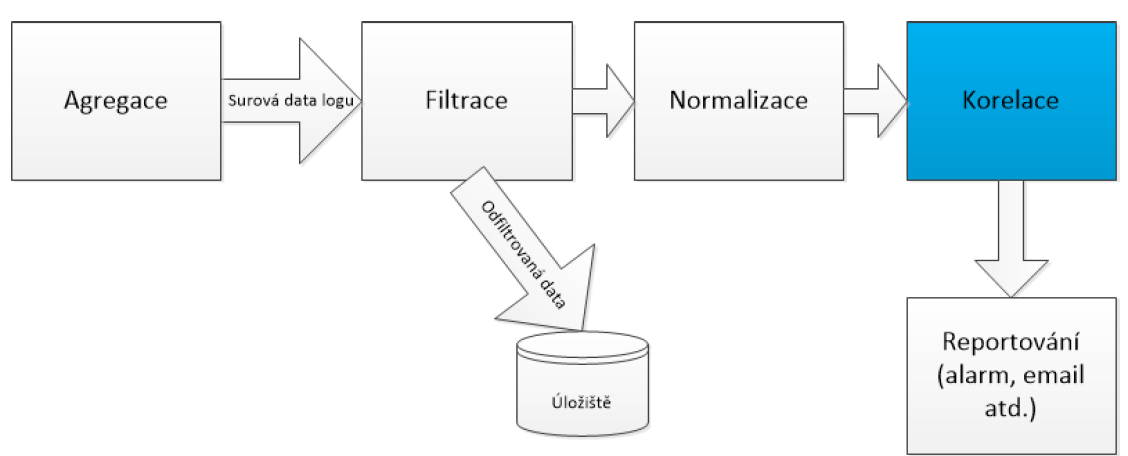
**Základní body postupu pro bezpečnou konfiguraci:**

1. **Zabezpečit směrovač** (router hardening, fyzická bezpečnost, aktualizace, patch)
2. **Zabezpečit směrovačem síť** (nastavit ACL, konfigurace NAT, bezpečné směrování)
3. **Podpůrné bezpečnostní funkce podporující bezpečnost sítě** (Modul firewall, brána VPN, podpora AAA, IPS, monitoring¨)

* **Zabezpečit přístup** (změnit heslo)
* **Zobrazit upozornění** (notifikace pro neautorizované uživatele)
* **Konfigurace SSH**
* Konfigurace privliegii
* Vypnutí nepoužitých rozhraní
* Zákaz skenů (blokace CICMP)
* Definovat Acess Control List a ustanovit odchozí a příchozí politiku filtrování adres
* Zapnout bezpečnostní funkce (IPS, VPN)
* Monitorovat, Logovat a kontrolovat bezpečnostní logy

**Nastavení autentizace device-to-device pro servery a služby** (EAP)

1. Definice operací nutných k aplikaci automatické analýzy logů (blokové schéma včetně popisu funkce jednotlivých bloků). Jakým způsobem je realizován blok korelace při detekci známých a neznámých událostí.



* Agregace – Proces stahování záznamů na jedno centrální místo.
* Filtrace – analýza surových dat v logu a rozhodnutí, která data jsou potřebná
* Normalizace – úprava záznamů na společný formát (společná databáze, nad kterou bude probíhat anaýza).
* Korelace – spojení několika podobných nebo naprosto rozdílných událostí ve znalost o nějaké větší probíhající události, o které chceme být informování z pohledu bezpečnosti.

Představuje nejvíce problematický blok.

**detekce signatur**

Na základě pravidel: detekce signatur (nepříznivé známé události). Tato korelace muze být realizována vytvořením pravidla v nějakém programovacím jazyku.

Pravidla se vkládají ručně, dodatečné náklady.

**detekce anomálií** (nepřiznivé neznámé události).

Na základě modelu:

* Frekvenční model – počítá výskyt definovaného jevu za pevně definovaný časový okamžik.
* Referenční model – vytvoření referenčního modelu „normálního“ chování a sledování povolených odchylek. Při běhu systému jsou sbírány data a porovnány s modelem. **Při odchýlení od normálního provozu je vyvolána akce.**

Na vytvoření modelu je potřeba mnoho vzorových dat a „experta“ který dokáže rozlišit co je normální a co je škodlivé chování.

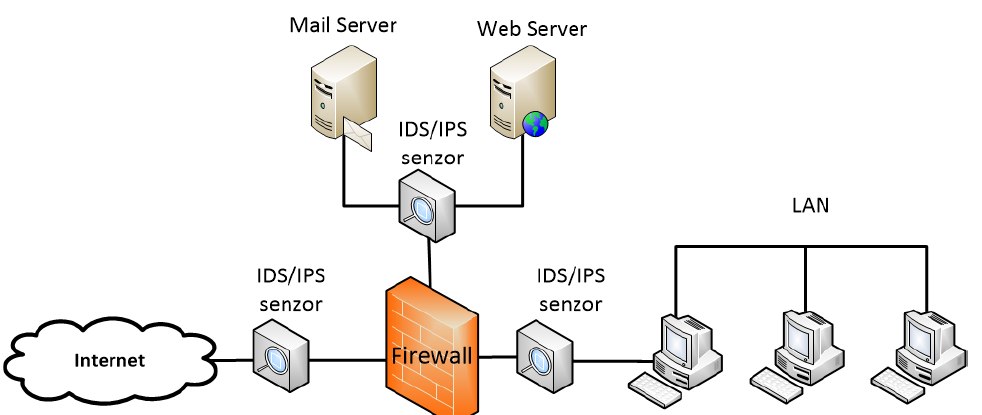
* Model Strojového učení – model je vytvořen a porovnáván s využitím algoritmů strojového učení. **Základní princip**: Definování zajímavých událostí k různým vzorům útoku. Čím více zajímavých vlastností a vzorů, tím lepe bude model klasifikovat neznámé útoky.

1. Detekce nepříznivých událostí na základě signatur a anomálií, systémy IDS/IPS (vzájemný vztah, efektivita a ladění, umístění, základní architektura, zástupci, referenční model).

Tyto systémy realizují odchytávaní paketů a následnou analýzu k detekci a potlačení podezřelé aktivity.

Typicky jsou nasazeny jako „inline“ jako síťové firewally (2 porty (vstup/výstup)).

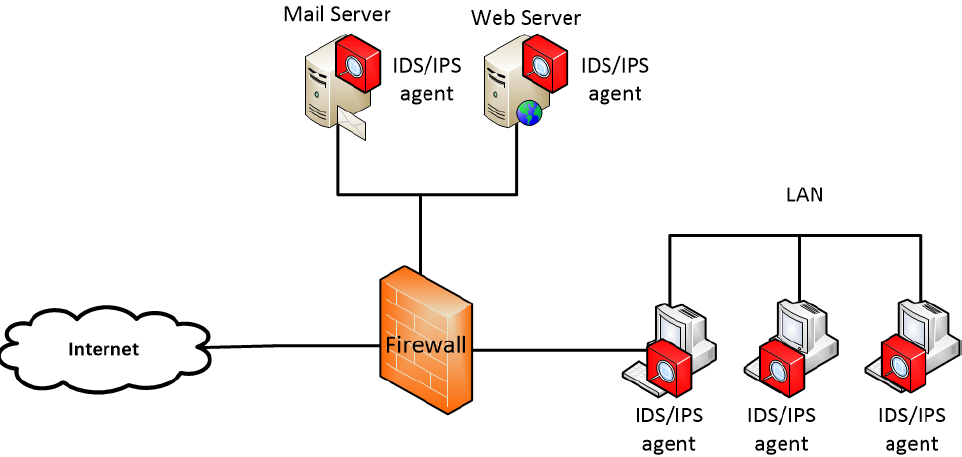
Umístění je rozhodující pro správnou funkci, často mezi komponenty síťové infrastruktury.



**Popisuje umístění na síti.**

IDS/IPS jsou k dispozici ve 3 variantách:

* **Komplexní zařízení:** Speciální HW včetně SW k efektivnímu odchytávaní a analýze provozu. (F5 Network).
* **Softwarová:** SW instalovaný na server, který je umístěn v sítí a monitoruje provoz (Snort,Suricata).
* **Cloudová:** Dostupné jako služba od IPS poskytovatelů (Radware,F5,McAfee).

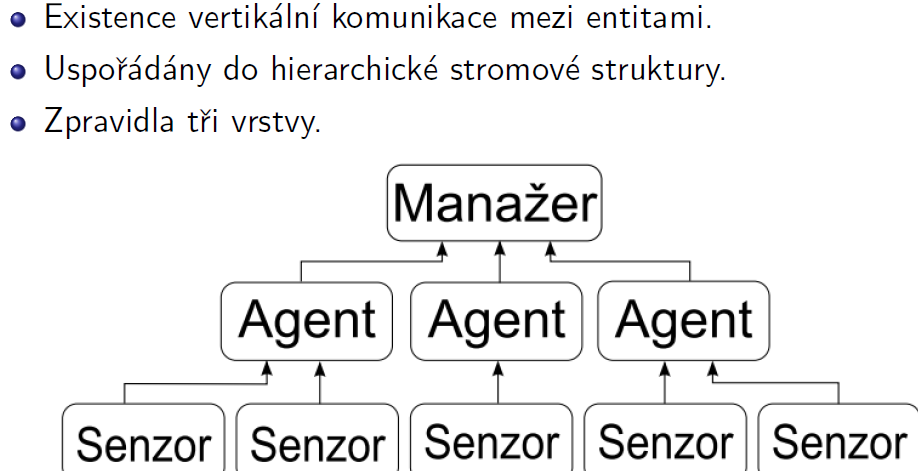
****

**IDS/IPS na hostitely**

Jednovrstvá architektura:

* IDS a IPS je tvořen pouze jednou komponentou. Obstarává všechny potřebné funkce

**Vícevrstvý architektura:**

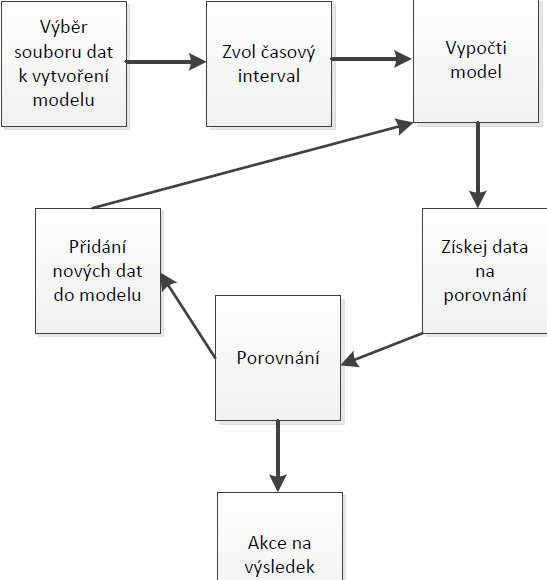


Senzory = monitorování provozu a data pŕedávají k zpracování agentům.

Agenti analyzuji konkrétní protokol, služby.

Manažer analyzuje hlášení a realizuje definovaná opatření (info admina, uprava pravidla FW, uloží incident v Databázi).

Referenční model pro detekci anomálií.

****

IDS – Instrusion detection systém: SW řešení nebo HW řešení, které automatizuje proces detekce průniků.

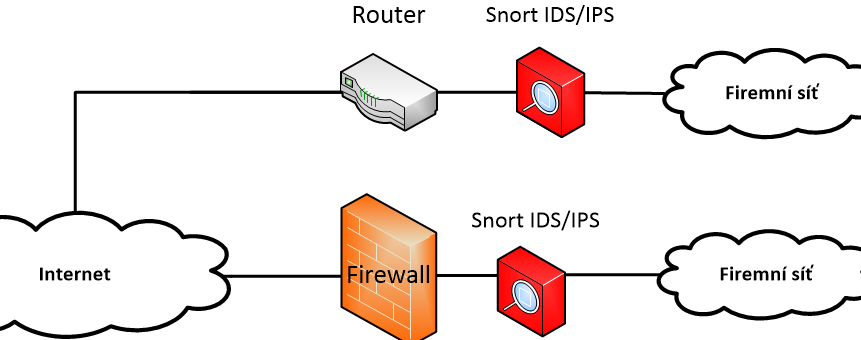
IPS – má všechny funkce IDS a navíc dokáže blokovat možné nežádoucí incidenty (konfigurací firewallu).

IPS je vylepšená IDS (umožňuje i preventivní opatření). Efektivita a ladění je důležitou součásti při nasazení IDS,IPS.

Detekce průniku = proces monitorování událostí v systému nebo síti a jeho následná analýza k detekci možných průniků.

**Přiklady: SNORT, SURICATA (použivanější).**

* Používá jazyk popisující pravidla, detekci anomálií, signatur a analýzu protokolu.



Packet Detector- Ukládá pakety z různých typů síťových rozhraní, připravuje pakety na zpracování. Preprocesot – příprava dat pro detekování, sleduje anomálie v hlavičkách paketů. Detection engine – Aplikuje pravidla na pakety. Output Modules – zpracovávájí aletry a logy do výsledného výstupu. Loggin and Alerting systems – Logování popřípadě vyvolání alertu.

1. Dělení penetračních testů (dle znalosti, způsobu realizace a cíle), metodologie testování (pět kroků testování). Penetrační testování webových aplikací (OWASP, průzkum prostředí, mapování aplikace, testování vstupů, závěreční report).

Penetrační testování = posouzení bezpečnosti metodou pokusu o průnik do testovaného systému. Pomocí slabých míst v síti a následně využití slabiny. Jedná se o technickou formu posouzení bezpečnosti. Je mít vždy souhlas majitele systému.

Exploit: program, jehož cílem je zneužití zranitelnosti a realizovat přístup do systému.

Payload: Program, který umožní kontrolu.

**Dle znalosti:**

* Black Box – Z pohledu útočníka, jsou známy pouze jeho vstupy a potencionální výstupy. Neznáme vnitřní strukturu systému.
* White-Box-Testy – Z pohledu uživatele. K dispozici jsou všechny možné znalosti o systému. (topologie sítě, přítomná zařízení, různé přístupové údaje).
* Grey-Box-testy – Kombinace předchozích dvou typů testů. Tester má pouze základní znalosti o systému, které se snaží maximálně využít.

**Podle způsobu provedení:**

* Manuální testy – tester vykonává manuálně. Umožňuje vytvořit test na míru pro specifické podmínky.

Nevýhody: potřeba rozsáhle znalosti testované oblasti, dovednost vytvořit testovací proceduru, časová náročnost.

* Automatizované testy – nástroje pro automatické testování vytváří profesionálové v oboru a tester potřebuje pouze znát jak pracovat s takovým nástrojem a porozumět výsledkům.
* Semiautomatizované. testy – kombinace předchozích.

**Dle cíle:**

* Síťové infrastruktury (bezdrát), webových aplikací, mobilních aplikací.

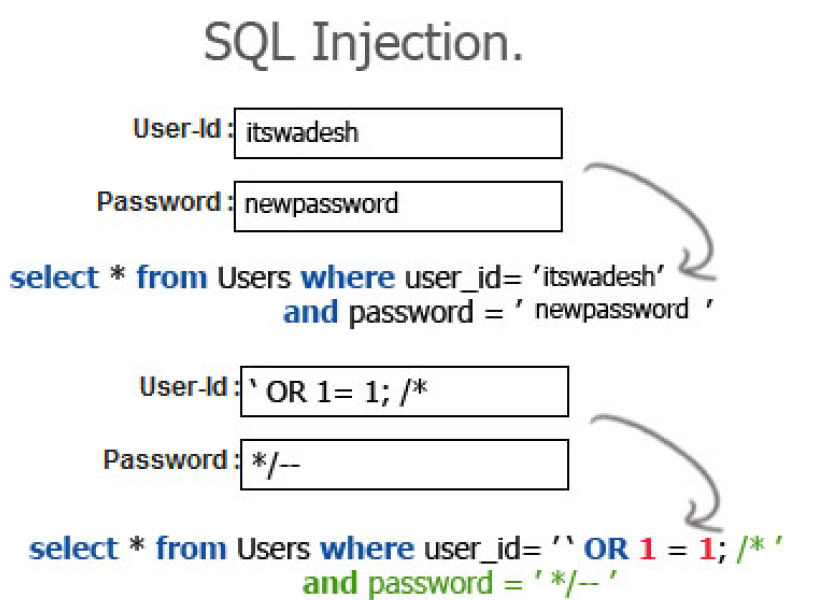
**5 kroků testování:**

1. Plánování – Určují se detailní cíle a časový plán. Vymezení prioritních cílů
2. Sběr informací – Cílem je zjistit co nejvíce informací o cílové síti. Údaje jako jsou rozsahy IP adres, otevřené porty, síťové služby.
3. Odhalování – za otevřenými porty se skrývají nějaké síťové služby, které běží na OS. Představuji aplikace, které mohou představovat zranitelnost. Porovnají se verze síťových služeb a OS s databází známých zranitelností.
4. Zneužití chyb – Využívání nalezených zranitelností. (Metasploit)
5. Report – Předání výsledků penetračních testů. Cílem je prezentovat zadavateli závěrečnou zprávu, která povede ke zlepšení bezpečnosti (nalezené zranitelnosti včetně jejich řešení).

**OWASP:**

* Celosvětová nezisková organizace zaměřená na zlepšování bezpečnosti softwaru.
* Cílem je, aby jednotlivci popřípadě organizace měli neomezený přístup k informacím o bezpečnostních hrozbách.

**SQL injection:** Je vložení SQL dotazu (select).jestli je SQL injection úspěšné (dotaz vyhodnocen za korektní), můžeme např číst a editovat data z databáze. Obvykle dochází k tomuto útoku při přihlašování do web aplikací.

****

1. (D)DoS útoky (princip, rozdělení, popis základních útoků, SYN Flood, HTTP Flood, DNS reflection, Ping of Death, Slowloris). Zátěžové testování (typy testů, nejznámější nástroje).

* DoS (Denial of Service) – snaha útočníka o to, aby vybraná služba byla uvedena do nefunkčního stavu. Uživatelé dále tuto službu nemohou využívat.
* DDoS (Distributed Denial of Service) – DoS útok, který je realizován od více uzlů, které s hlavním útočníkem spolupracují a napadají cílový uzel v určitém čase s určitou intenzitou útoku.

Bootnety = kompromitované uzly. (ty, které se podílí na útoku jsou označeny jako zombies a tvoří síť bootnet).

**Rozdělení (D)DoS:**

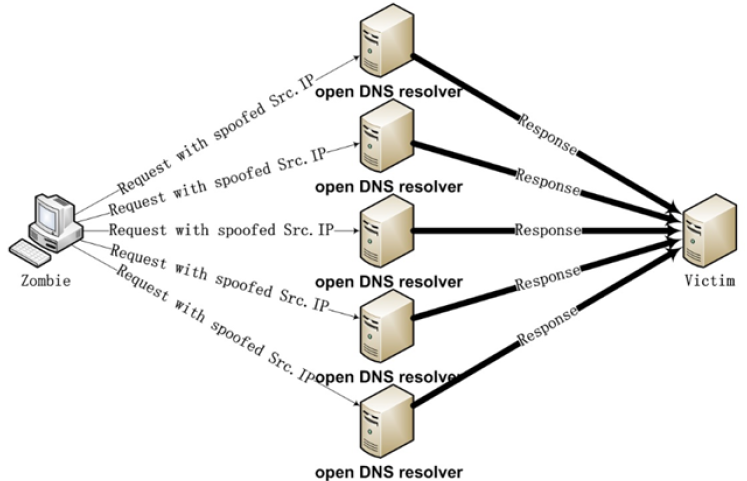
* **Záplavové útoky =** Vytížení komunikační / paměťové/ výpoćetní kapacity cíle útoku. (TCP flood, UDP flood, http flood, ICMP flood.)
* **Logické útoky =** Útoky na logickou slabinu v programu, protokolu, OS. Lze dále dělit na **protokolové útoky a aplikační** útoky. (Ping of death, Land attack, SlowLoris).

**Záplavové útoky:**

* **ARP flood** – Oběť je zahlcena velkým počtem falešných dotazů ARP, které vyčerpají výpočetní nebo paměťové zdroje cílového uzlu.
* **Reset Flood** – Záplava paketů, které mají falešné zdrojové IP adresy, porty a aktivní příznak RST, který resetuje spojení. Skutečná komunikace je neoprávněně ukončena.
* **Syn Flood** – Útok otevírá několik polootevřených spojení a čeká na potvrzovací zprávu, která však od podvržených adres nepřichází a tím odchází postupem času ke snížení dostupnosti až po úplné zahlcení služby u cílové oběti.
* **http flood** – útok vedený z několika zombie klientů, na cílový webový server posílají legitimní ale procesně náročné žádosti HTTP GET nebo POST.

**Logické útoky:**

* **Útok land**: Pakety TCP-SYN jsou podvrženy tak, že mají cílovou IP adresu a port identickou jako zdrojovou. **Nekonečná smyčka** při jejich zasílaní zpět.
* **Ping of Death** – Škodlivý ping dotaz. Ping o velikosti **vyšší než 65 535 bajtů** může způsobit pád cílového systému.
* **SlowLoris**- nástroj generuje a opakovaně posílá částečné **HTTP požadavky,** ale nikdy nekončí celý požadavek (nekompletní GET request) Cíl postupně otevírá více a více spojení až vyčerpá jejich povolený počet.

D

**DNS**

**REFLECTION**

**Zátěžové testování:**

Preventivní testování odhalí zranitelnosti a umožní jejich odstranění dříve, než je zneužije útočník. Testování výkonnosti sítě a síťových zařízení odhalí také úzká hrdla sítě, špatnou konfiguraci a limity sítě.

**Testovat lze:**

* PC sítě jako celek
* Síťové zařízení (servery, routery, firewally)
* Koncové stanice (PC,Ntb, smartphone)
* Aplikace, webové služby a OS

**Zátěžové testování** je vhodné realizovat mimo provoz. **Testování emulované sítě** (přenesení konfigurace, virtualizace, emulované prostředí).

Obsahuje tyto kroky:

Definice testování (specifikace sítě a požadavků) > příprava testování (nastavení sítě na testování) > realizace testování > vyhodnocení testování.

**Typy testu:**

* **Výkonnostní test:** zatížení systému definovanou zátěží pro změření jeho chování. Např pro testování před a po updatu sítě.
* **Test hraniční zátěže:** Zatížení systému narůstajícím počtem paralelních procesů. Účelem je najít limit, při kterém aplikace překročí akceptovatelné požadavky.
* **Test odolnosti:** Dlouhodobé testy, které odhalují nedostatky v aplikaci při jejím nepřetržitém provozu.
* **Test selhání:** možné ověřit chování systému v případě jeho selhání a nahrazení záložním systémem. Také je možné ověřit rychlost jeho zotavení.
* **Test objemu dat:** Tímto typem testů dochází k ověřování chování aplikace při zvyšujícím se objemu dat.

**Nástroje:**

* Avalanche – generování provozu do 40 Gb/s (HW tester)
* Apache jMeter – postavený na javě k zátěžovému testování serverů.
* Ow Orbit Cannon (LOIC) Open Source / C#, .. SW tester

1. Netechnické typy útoků, sociální inženýrství, phising (používané techniky), útoky MitM (ARP spoofing, DNS spoofing, SSL strip, SSL sniff).

Sociální inženýrství = psychická manipulace s lidmi za účelem zisku informací, přistup ke službě nebo provedení podvodu.

**Phishing** - kontaktování velkého počtu lidí pro zisk citlivých informací pro škodlivé účely.

Spear Phishing – kontaktování konkrétních lidí, kontaktní zpráva navíc může obsahovat malware.

Clone phishing - Výroba, aktualizace nových phishing zpráv z legitimních původních zpráv.

Whaling – Phishing cíleny na starší nebo vlivné.

Baiting - Zanechání malwaru na médiu, které ma oběť objevit a použít.

Obrana proti phishingu je pomocí školení uživatelů, technické opatření ( blokování emailů od podezřelých zdrojů).

**Phishing techniky útočníka.**

* **Manipulace odkazů –** link ve zprávě vypadá jako původní link na organizaci,, ale je cílen na podvodnou stránku. Využívají se modifikované URl.
* **Vyhnutí filtrům –** využití obrázků místo textu znesnadňuje detekci útoků. Proto vznikly OCR (Optical Character Recognition) pro filtraci závadných obrázků s falešnými odkazy atd..

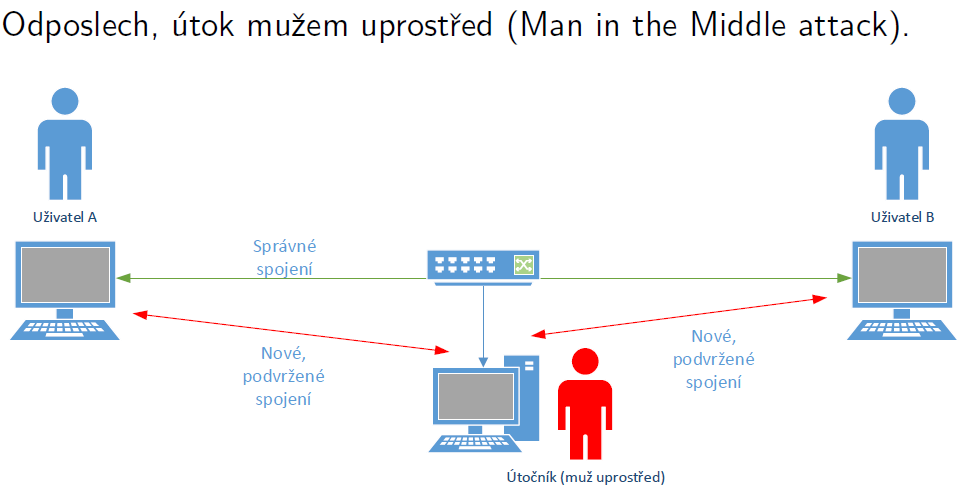
**Útok MitM =** Máme 2 strany, které spolu komunikují. MitM je princip útoku, kdy třetí strana odposlouchává probíhající komunikaci a může buď data podvrhnout nebo komunikace probíhá přímo skrz třetí stranu.

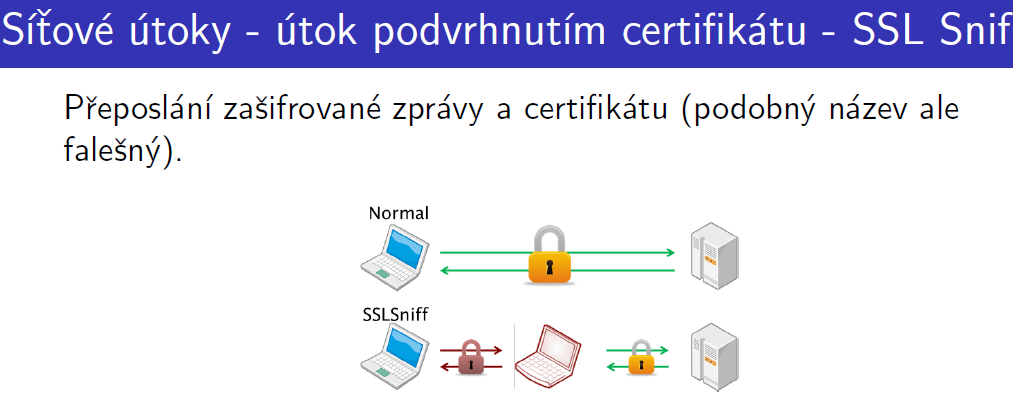
ARP spoofing = Neautorizovaný příjem cizích dat pomocí nelegitimní změny zdrojové MAC adresy na přepínači.

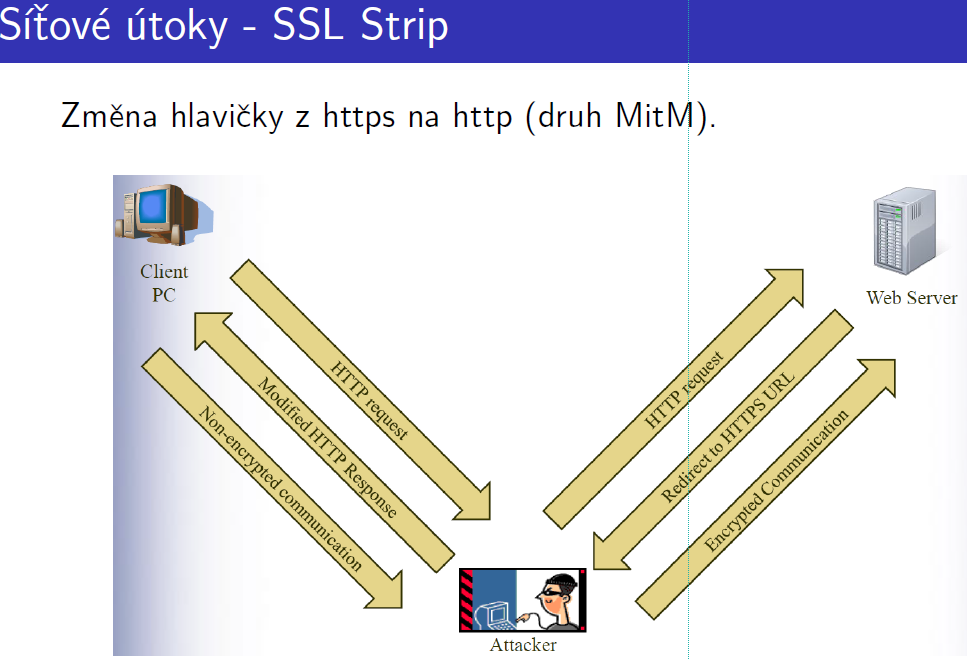
DNS spoofing = Podstrčení falešné IP adresy doménového jména.

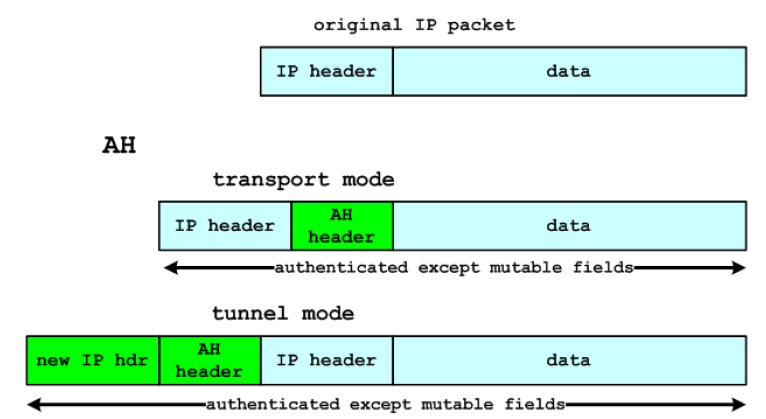
SSL Strip = změna hlavičky z HTTPS na http (součást MitM).

SSL Snif = útok MitM, zachytávaní SSL







1. Protokoly IPsec a TLS (princip, umístění TCP/IP, průběh komunikace, autentizace, utajení a integrita dat).

**IPsec -** síťová vrstva (podle TCP/IP, 3.),

- při komunikaci mezi zařízeními s IP adresou

- šifrování po IP adresu (data v paketech, celé pakety)

- poskytuje end-to-end bezpečnost,

- šifrování a autentizace dat a stran

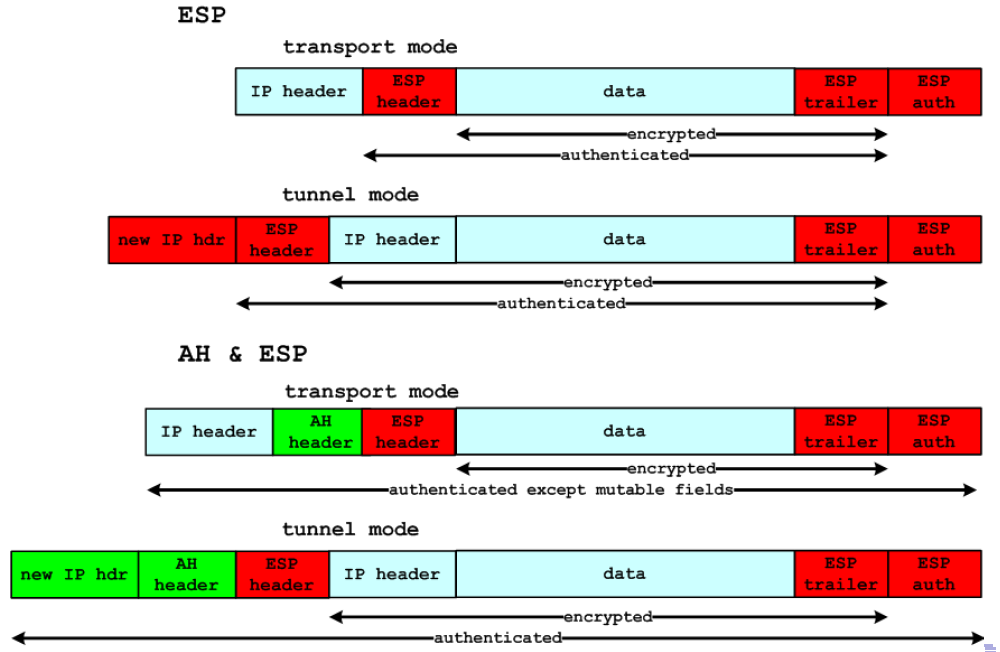
- lze tak tunelovat TCP i UDP datagramy

**Skládá se z více částí:**

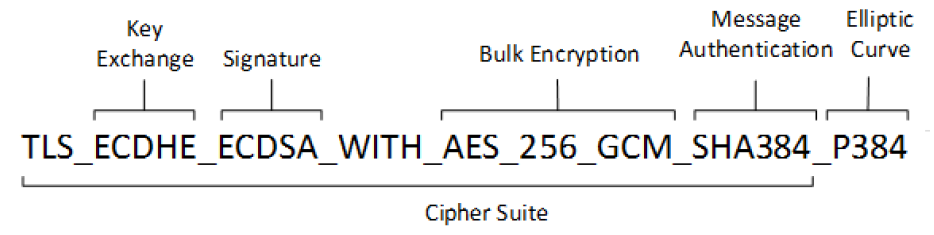
* **Authentication header (AH)** protokol – Autentizace
  + Poskytuje integritu a autentičnost IP paketů, ochrana proti replay (sekvenční čísla…)
  + Údaje v AH hlavičce, autentizační tag (ICV)
* **Encapsulating Security Payloads (ESP)** protokol
  + Důvěrnost dat pomocí šifrování
  + ESP hlavička, šifrovaná data, případně přídavná ochrana + AH hlavička
  + Poskytuje základní autentizaci pouze ESP části
* **Security Association (SA)** – popis spojení IPsecu
  + popis spojení mezi stranami, včetně parametrů zabezpečení
  + aktivní spojení uložené v databázi (SAD)
  + SA management a bezp. pravidla jsou uložena v SPD – Security policy Database
  + Popis obsahuje (idnex, sekvenční čísla, algoritmus autentizace a šifrování a jejich klíče, životnost klíčů, mód, max velikost paketu)

**Více módů:**

* **Transportní** (ochrana dat v paketu, IP hlavička nešifrovaná, použití mezi hosty)
* **Tunelující** (ochrana celého paketu, paket se stane daty nového paketu s jinou IP hlavičkou, použití mezi hosty a bránami)

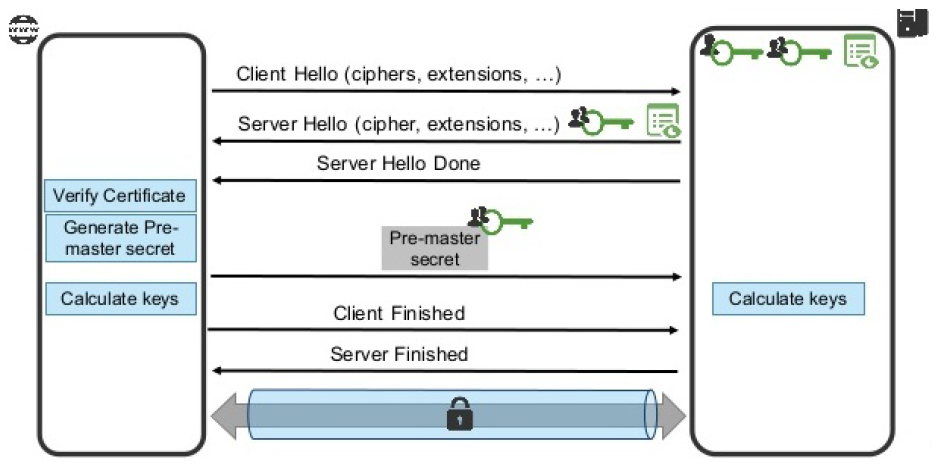
Ustanovení klíče, IPsec využívá symetrické algoritmy  
- Použití PSK (pre-shared key), IKE1 a IKE2 (Internet Key Exchange), Kerberos

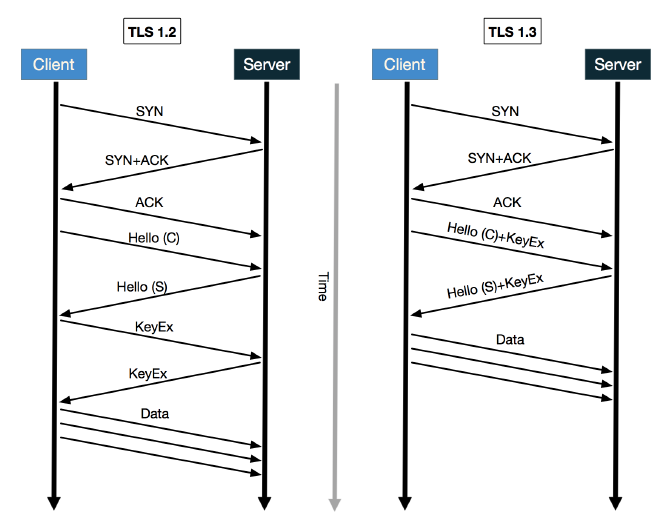
**TLS** - transportní vrstva (podle TCP/IP, 4.)

- komunikace v síti mezi servery a klienty v rámci TCP/UDP, šifrování po data v datagramech, část cesty nemusí být šifrována (mezi web serverem a proxy nebo DB serverem)

**Součásti**:

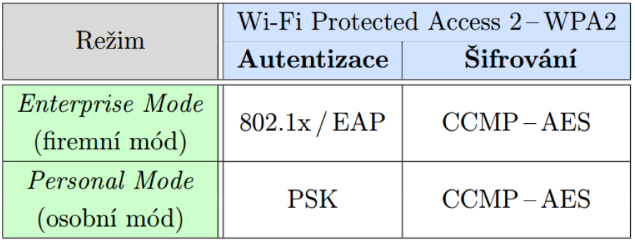
* **Handshake** protokol – inicializace spoje, autentizace stran a ustanovení klíče
* **Record** protokol – datový přenos šifrovaných dat a MAC autentizace
* **Alert** protokol – slouží k notifikaci chyb a varování

Klíče jsou ustanoveny pomocí dočasných klíčů (ECDHE, DHE), podpis RSA, ECDSA, šifrování AES-GCM, bezpečný hash SHA-256, SHA-384



1. Zabezpečení 802.11 (WPA2, používaná kryptografická primitiva, klíčové hospodářství, popis 4Way Handshake, testování bezpečnosti).

**WEP** – Wired Equivalent Privacy, nevhodná implementace šifrovacího algoritmu, chybějící management klíčů, předvídatelnost obsahu.  
Autentizace 2 typů – autentizován zasláním správně vyplněného SSID. Shared-key, 4 cestný, zašifrování výzvy sdíleným klíčem

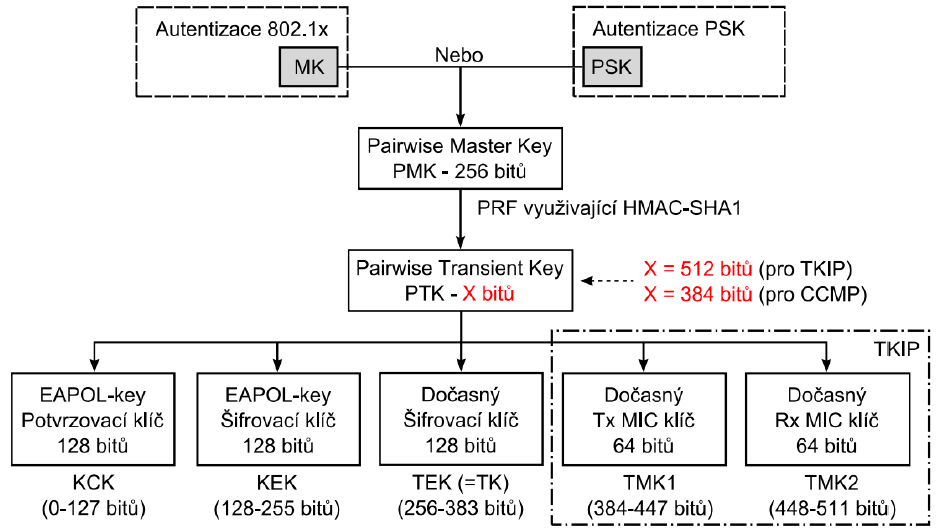
**WPA2** – WiFi Protected Access

- autentizace pomocí PSK nebo IEEE 802.1x (pro firemní sítě, autentizace AP učivatelem a auth serverm – RADIUS, Kerberos, žadatel/autentizátor/autentizační server = 3 entity. Využíván protokol EAP – Extensible Authentication Protocol)

- důvěrnost pomocí šifrovací algoritmus AES, integrita dat pomocí MIC (message integrity code), WPA2 MIC nahrazen CCMP

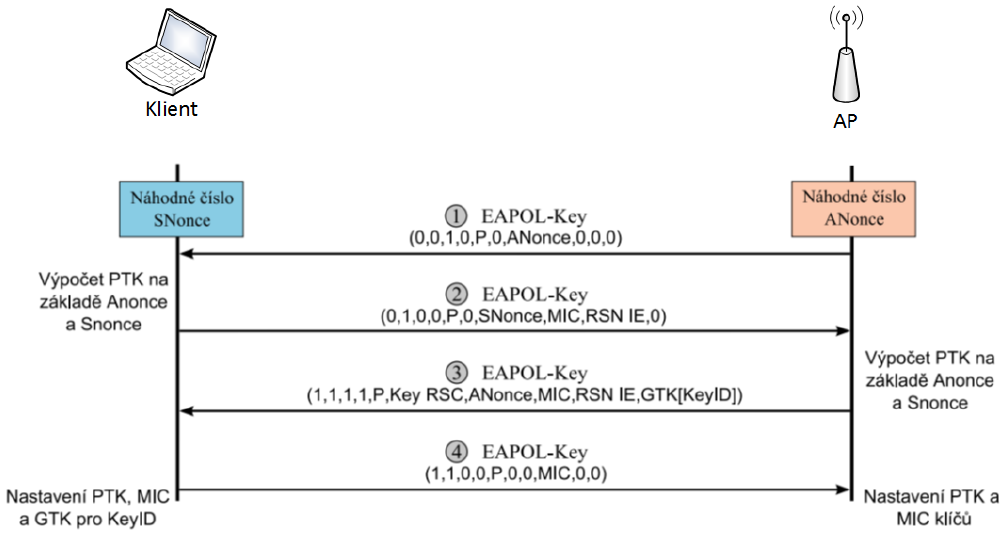
Využívá více klíčů (kolekce klíčů):

* Základem je výstup úspěšné autentizace, získání hlavního klíče PMK (Pairwise Master Key)
* Získání PMK je závislé na metodě autentizace, u firemního je získán z autentizačního serveru. U osobního platí PSK = PMK
* Další klíče jsou derivovány od PMK pomocí hash funkce. Samotný PMK se nikdy nepoužije ke kontrole integrity nebo šifrování
* Z PMK se generuje PTK (Pairwise Transient Key)
  + KCK 128b (Key Confirmation Key), pro autentizační MIC během 4-WH
  + KEK 128b (Key Encryption Key), zajištění důvěrnosti (šifrování) během 4-WH
  + TK 128b (Temporary Key), používán k šifrování dat (používané TKIP a CCMP)
  + TMK (Temporary MIC Key), k autentizaci dat. Pouze s algoritmem Michael s TKIP
* PMK/PSK se v osobním módu nezadává přímo. Zadává se pouze heslo, které je výpočtem převedeno na 256-bitový klíč. Funkce Password-Based Key Derivation Function



TKIP (asi jen u WPA, je v tom bordel) – mixování klíčů, každý paket je šifrován jiným klíčem

**4-Way Handshake:** (MIC u WPA2 nahrazen CCMP-CounterMode with Cipher Block Chaining Messege Authentication Code Protocol)

1. AP generuje náhodné Anonce, které je zasláno k žadateli (otevřeně)
2. Uživatel generuje náhodné SNonce, výpočet PSK-PTK, odvození dočasných klíčů. S využitím KCK posílá k AP zprávu s SNonce a MIC (otevřeně). AP vypočte z SNonce PTK a dočasné klíče a MIC a ověří shodu (Autentizace uživatele, passphrase)
3. AP zasílá klientovi zprávu s GTK zašifrované pomocí KEK, uživatel ověří MIC (autentizace AP)
4. Závěrečná zpráva od uživatele k AP, potvrzuje 4-WH

Problematika hesla. Útok na chybě zvolené heslo, problematika WPS

**Testování bezpečnosti**

