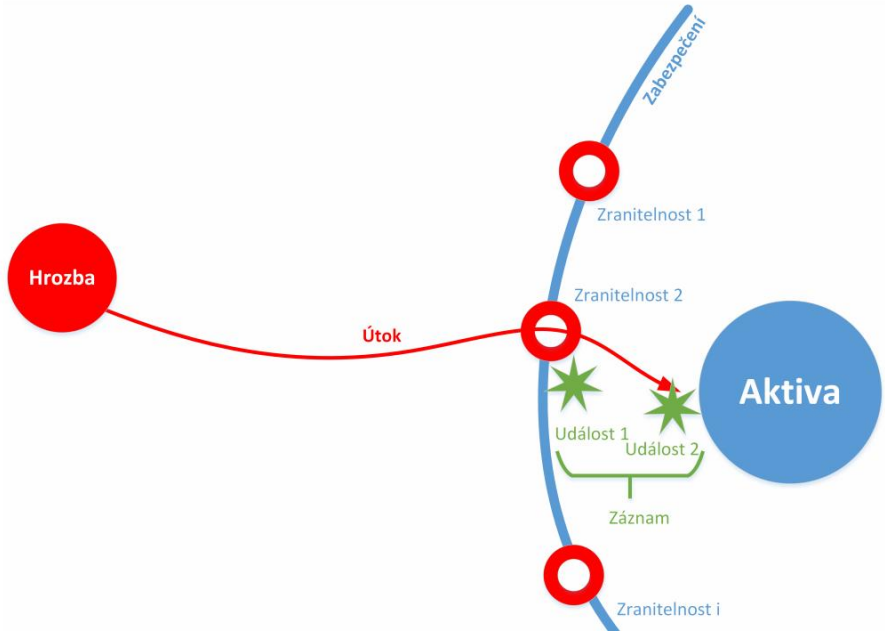
1. Úvod do bezpečnosti

1.1 Základní pojmy

- *Aktiva*: cokoliv, co je majitelem považováno za cenné
- *Hrozba*: možnost ztráty aktiv, popsána:
  - nositelem hrozby (konkurenční firma)
  - objektem hrozby (zákaznická db)
  - mechanismem hrozby (krádež db, kopírování dat)
- *Ochrana*: opatření snižující četnost nebo velikost ztrát aktiv
  různý charakter (administrativní, organizační, personální, technické opatření)
- *Bezpečnost*: stav, kdy ztráta aktiv nepřekračuje stanovenou míru
  nemůže být absolutní (nelze ochránit před všemi hrozbami)
- *Zabezpečení*: ucelený systém ochran – komplexní, systematická a efektivní
- *Slabina*: zranitelné místo
- *Riziko*: pravděpodobnost využití zranitelného místa
- *Incident*: jakákoliv realizace hrozby
- *Průnik*: dopad
  pokud při incidentu došlo ke ztrátě aktiv, rozsah škod, důsledek útoku



- *Počítačová síť*: technické prostředky realizující spojení, výměnu informací mezi PC a umožňují uživatelům komunikaci
- *Bezpečnost sítě*: neustálý proces (není to stav), kterým má být dosaženo uspokojivého zabezpečení sítě a toto zabezpečení udrženo
  - k zajištění užíváme *bezpečnostní služby:*
    - *autentizace* – oveření identity
    - *řízení přístupu* – autorizace
    - *důvěrnost* přenášených dat
    - *integrita*
    - *nepopiratelnost* – ochrana proti odmítnutí původu
  - užití kryptografických mechanismů a zařízení k zajištění těchto služeb
- *Role*: *legitimní* – Alice, Bob (od Rona Rivesta, 1978)
  útočníci – Eve, Mallory, Oscar, Trudy (eavesdropper, adversary, opponent)

1.2 Síťové útoky

- dlouhou dobu ignorována, nepředpokládalo se masivní propojení pc – Internet
- současnou motivací je malware – ekonomické ztráty
- mají nejednotné dělení (aktivní/pasivní útoky, aktivní/pasivní útočník, sw/hw útoky)
- *vnitřní útoky* (škody způsobené nedbalostí, útok z řad zaměstnanců)
- *vnější útoky* (náhodný či promyšlený útok zvenku)
- *pasivní útočník* (základní prostředky, odposlech komunikace, hádání údajů)
  - *odposlech dat* (zachycení a přečtení dat na kom. lince)
  - *analýza provozu komunikace* (pro šifrovanou komunikaci, četnost dat, interval vysílání a přijímání, potvrzovací zprávy, hlavičky)
  - *útok na slabou autentizaci* (bruteforce)
  - *social engineering* (využití neznalosti uživatelů)
  - *skenování* (nalezení dostupných systémů a služeb pomocí ICMP echo, sken portů TCP, UDP, získání seznamu *aktivních serverů a služeb*)
- *aktivní útočník* (pokročilé prostředky výpočetní, komunikační, sofistikované útoky)
  - *modifikace dat* (zachycení přenášených dat, cílená modifikace k vyvolání chyby či nesprávné odezvy)
  - *útok opakováním – replay attack* (zaznamenání komunikaci a znovuposlání)
  - *MITM* (spoofing, ARP, DHCP, SSL, atd.)
  - *DoS* (útok na dostupnost služeb, vyřazení z činnosti pomocí vyčerpání komunikační, výpočetní, paměťové kapacity, chyby v implementaci TCP/IP – SynFlood, Ping of Death, atd.)
    - *DDoS* (účast velkého množství počítačů)
    - ochrana využitím *IPS – Intrusion Prevention Systems* a FW
  - *útoky postranním kanálem* (na dosud bezpečné kryptografické algoritmy, např. AES, RSA, typicky na čipových kartách, mikro kontrolerech, telefonech, cílí na implementaci algoritmu)

2. Konfigurace přepínačů a směrovačů

2.1 Bezpečná konfigurace přepínače

- přepínač (switch), 2. vrstva modelu ISO/OSI
- zabezpečení LAN
- L3 přepínače pracují i se 3. vrstvou
- *útoky uvnitř sítě:*
  - *MAC address spoofing* (neautorizovaný příjem cizích zpráv změnou zdrojové adresy MAC na přepínači)
  - *ARP poisoning* (úprava ARP cache – MITM útok)
  - *Rogue DHCP server/spoofing* (útočník řídí falešný DHCP server a rychleji odpoví na request klientům, podvrhne svou bránu – MITM, DNS nebo přiřadí neroutovatelnou IP – DoS)
  - *DHCP starvation* (útočník zaplaví DHCP server velkým počtem DHCP requests a snaží se vyčerpat pool IP adres)
  - *STP manipulation* (Spanning Tree Protocol, útočník se nastaví jako root bridge)
  - *MAC address table overflow* (či *address flooding attack*, záplava falešnými zprávami o MAC adresách – vyčerpání tabulky MAC adres na přepínači a ten degraduje na HUB)

    - *LAN storm* (přepínače posílají broadcast všemi porty – degradace LAN záplavou paketů, vytížení CPU – DoS)
    - *VLAN útoky*
        - *VLAN hopping* (spoofing DTP zpráv, d*ouble-Tagging VLAN* (vnoření extra hlavičky do dat)
- *postup bezpečné konfigurace:*
    - zabezpečení fyzického přístupu k prvku
    - nastavení bezpečného lokálního přístupu (uživatelé a privilegia)
    - nastavení bezpečného vzdáleného přístupu (SSH klíče RSA 2048b, HTTPS)
    - vypnutí nepotřebných služeb a portů
    - zapnutí dalších bezpečnostních funkcí (DHCP snooping, port security)
    - zajištění záloh konfigurace
    - kontrola konfigurace, testování, ověrování
- *konfigurace Cisco přepínače:*
    - *metody obrany:*
        - *dynamic ARP inspection*
        - *port security* (omezení počtu MAC adres na port)
            - `switchport mode access, switchport port-security, switchport port-security maximum value`
        - *DHCP snooping* (omezení rogue DHCP a DHCP starvation)
        - *PortFast* (`spanning-tree portfast default`)
        - *Root guard* (posiluje umístění root bridge pomocí limitace portů)
        - *BPDU guard* (blokuje BPDU tam, kde by neměl chodit – měl by chodit jen od SW, ne od PC na access portech, `spanning-tree portfast bpduguard default`)
        - *Storm Control* (proti LAN storm, `storm-control`)
        - *zmírnění LAN hoppingu* (vypnutí trunkingu na portech, nepoužívat VLAN1 pro vše)
        - *Private VLAN funkce – PVLAN Edge* (izolace portů v rámci VLAN, provoz přeposílán jen přes L3 assety)
        - *SPAN – Switched Port Analyzer* (zrcadlení provozu pro sondy IPS)
- *shrnutí:*
    - bezpečný přístup ke konfiguraci (SSH)
    - port security
    - uživatelské porty na non-trunking `switchport mode access`
    - PortFast na non-trunking porty
    - BPDU guard na non-trunking porty
    - Root guard na STP root porty
    - manuálně nastavit trunk porty a zakázat DTP na nich
    - konfigurace DHCP snoopingu
    - užití CDP (Cisco Discovery protocol) jen pokud je to nutné
    - nadefinovat vlastní VLAN
    - zakázat nepoužívané porty a přiřadit nepoužívané VLAN
    - PVLAN Edge
    - Vyšší verze SNMP (3) a autentizace u VTP
    - zapezpečit ARP/MAC/IP (DAI, IP Source Guard)

2.2 Bezpečná konfigurace směrovače

- směrovač (router), 3. vrstva ISO/OSI
- *hraniční směrovač (edge router)*
  - mezi vnitřní sítí a nedůvěryhodnou sítí (vnější)
  - paketová filtrace
  - nutnost *fyzické bezpečnosti* (uložení, UPS – uninterruptible power suply, bezpečnost OS – aktualizace, patche, záloha conf, bezpečná konfigurace – *router hardening* – bezpečná administrace, zakázání neužívaných portů, služeb, logování)
  - zabezpečení sítě pomocí funkcí směrovače a filtrování provozu
- *útoky na směrovače:*
  - *průnik do nastavení* (defaultní hesla)
  - *routing table poisoning* (změna routovací tabulky pomocí spoofingu routing protokolů)
  - *hit-and-run attack* (škodlivé pakety na směrovač v náhodných intervalech)
  - *DoS/DDoS attack* (zaplavením pakety a vytížení CPU/RAM, logické útoky – *Xmas*)
  - *Packet mistreating attack* (implementace škodlivého kódu a špatné zpracování paketů, tvoření smyček, DoS)
- *postup bezpečné konfigurace:*
  - zabezpečení směrovače (router hardening, fyz. bezpečnost, aktualizace, patch)
    - *router hardening:*
      - zabezpečit administrativní přístup
      - zobrazit upozornění
      - konfigurovat SSH
      - konfigurovat privilegia uživatelů
      - vypnutí neužitých rozhraní
      - zrušení nepotřebných služeb
      - zákaz skenů (blok ICMP), vypnout CDP u hraničních směrovačů
      - definovat paketovou filtraci (ACL)
        - standardní a rozšířené u Cisco
        - iptables Mikrotik
      - bezpečnostní funkce a protokoly (AAA, IPS, VPN)
      - bezpečný management sítě (restrikce SNMP – v3 s autentizací a šifrováním)
      - monitorovat, logovat, kontrolovat logy (syslog)
      - zálohovat, testovat, skenovat odolnost vůči pentestům
  - zabezpečit směrovačem síť (ACL, NAT, bezpečné směrování)
  - konfigurovat další bezp. funkce (modul firewall, VPN brána, podpora AAA, IPS, monitoring, load balancing)
- zabezpečení administrativního přístupu:
  - lokální přístup (konzole, bezp. hesla, chránit i privilegované režimy)
  - vzdálený přístup (SSH, 2048b RSA)
  - autentizace pomocí AAA serverů (TACACS+, RADIUS)
- *autentizační protokoly*
  - *PAP – Password Authentication Protocol* (slabé, pouze sdílené heslo)
  - *CHAP – Challenge–Handshake Authentication Protocol* (ochrana proti replay, náhodná výzva, sdílené heslo)
  - *EAP – Extensible Authentication Protocol* (autentizační framework, různé verze)

- zabezpečení přístupu pro protokoly a ostatní zařízení:

- EAP autentizace pro servery a služby (device-to-device)
- CHAP/EAP pro přenos Point-to-Point Protocol PP
- autentizace routovacích protokolů (MD5 otisk při sdíleném heslu OSPF, RIPv2)
- autentizace SNMP v3 a NTP v3

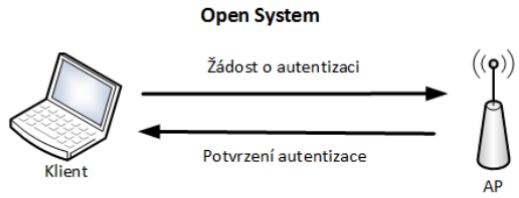
- *konfigurace Cisco směrovače:*
  - jednoduché směrovače mají automatizované procedury, které samy nastaví věci:
    - *AutoSecure* (`auto secure`)
      - nastavení základní úrovně zabezpečení (vypnutí globálních služeb, služeb na rozhraních, service password-encryption, logování, banner, login heslo)
      - CLI
    - *One-step Lockdown*
      - GUI, Security Device Manager
      - NEdělá na rozdíl od AutoSecure:
        - nevypne NTP
        - nekonfiguruje TCP přerušení
        - nekonfiguruje AAA
        - nekonfiguruje ACL antispoofing na vnějších rozhraních
        - nekonfiguruje SPD hodnoty
        - nepodporuje konfiguraci SNMP v3
  - AAA:
    - metody autentizace:
      - none
      - s heslem (line local)
      - Kerberos 5 (krb5)
      - Radius (group radius)
      - Tacacs+ (group tacacs+)
    - autorizace a accounting pomocí serveru (trackování, logování, shromažďování dat)
  - ACL:
    - zmírňují síťové útoky, kontrola provozu v síti
    - *standardní ACL* (co nejblíže cílovému uzlu, založeno jen na zdrojových adresách)
    - *rozšířené ACL* (co nejblíže ke zdroji, který je filtrován)
  - VPN:
    - site-to-site VPN
    - remote-access VPN
    - metody:
      - *Cisco IOS SSL VPN* (spojení přes prohlížeč a nativní SSL modul)
      - *Generic Routing Encapsulation* (GRE, zapouzdřuje spojení přes IP, podpora více protokolů, vhodné pro site-to-site VPN)
      - *Internet Protocol Security* (IPsec, tunelující protokol nad IP, šifrování dat a autentizace stran)
- *bezpečnost na Mikrotik směrovačích:*
  - MikroTik RouterOS, přístup přes *GUI – Winbox*, SSH, Telnet, atd.
  - funkce: FW, VPN brána, routing, proxy, bridge, hotspot, syslog, trafficmonitor server
  - *konfigurace:*
    - změna přístupových údajů na admina
    - *omezení přístupu podle IP adresy*, atd.
    - FW: založen na *linux iptables* (input, output, forward, accept/reject/drop)

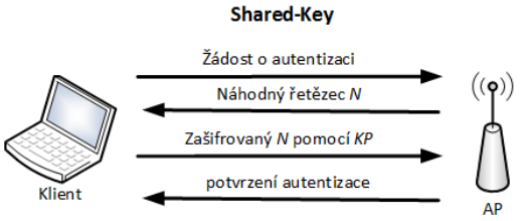
3. Bezpečná konfigurace bezdrátových sítí

- signál přenášen volným prostorem, pomocí elektromagnetického vlnění nejčastěji
- podle dosahu (WPAN, WLAN, WMAN, WWAN)
- nejrozšířenější WLAN technologie *IEEE 802.11 WiFi*
  - řada rozšíření normy, nové funkcionality
    - zvýšení přenosové rychlosti (802.11a, 802.11b)
    - nová frekvenční pásma (802.11n)
    - komplexní zabezpečení *IEEE 802.11i*
- *motivace zabezpečení bezdr. sítí:*
  - možnost odposlechnutí kýmkoliv v rozsahu (nelze omezit přístup k médiu), nutná *implementace bezpečnostních mechanismů*
    - *autentičnost* (authentication), ověření autora zprávy
    - *důvěrnost* (confidentiality), utajení informace před neoprávněnými uživateli
    - *integrita dat* (integrity), rozpoznání modifikace při přenosu
    - *nepopiratelnost* (non-repuditation), odesílatel nemůže popřít, že danou zprávu odeslal

3.1 Zabezpečení

- *skrytí SSID:*
  - mylně označováno za zabezpečení, přináší správci obtíže a ne bezpečnost
- *MAC filtr:*
  - filtrování MAC adres klientů
  - vytvoření seznamu povolených MAC adres na AP
  - jednoduše se dá obejít
  - nevýhody pro správce při výměně koncových stanic
- *WEP (Wired Equivalent Privacy)*:
  - již využívá implementace kryptografických algoritmů, což je správná cesta
  - první volitelný způsob zabezpečení
  - snadno *prolomitelný*:
    - nevhodná implementace šifrovacího algoritmu
    - chybějící management klíčů
    - předvídatelnost obsahu
  - dva typy *autentizace:*
    - *open system* (2-way handshake, je autentizován uživatel, který odeslal požadavek na autentizaci se správně vyplněným SSID)
    - *shared-key* (4-way handshake, účastník odešle požadavek na autentizaci, AP v odpovědi pošle náhodně vygenerovaný řetězec, účastník zašifruje sdíleným WEP klíčem, AP dešifruje a porovná řetězec)



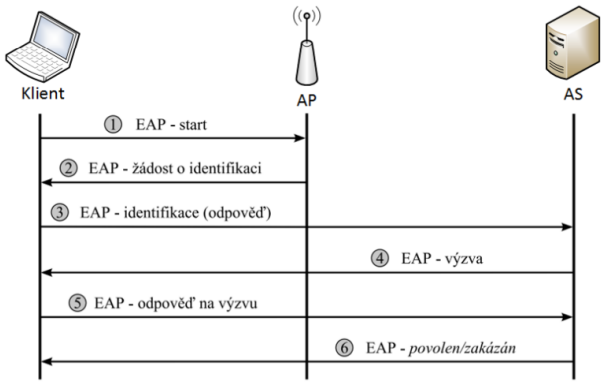


  - *slabiny autentizace:*
    - jednostranná (jen strana uživatele)
    - autentizováno zařízení, ne uživatel
    - možnost *zachycení výzvy a odpovědi během autentizace*, určení tajného klíče K pomocí kryptoanalýzy
  - *důvěrnost:*
    - *proudová šifra RC4* klíčem KP = IV || K
    - *IV* (24b) pro každý paket generován
    - norma 802.11 definovala *WEP klíč délky 64b s efektivní délkou 40* (24b IV)
    - *RC4* navrhl *Ron Rivest* z RSA Laboratories
      - jednoduchá struktura, implementace v SW i HW
      - základní požadavek nabezpečnost:
        - *IV plus klíč nesmí být stejné pro dvě zprávy*
        - WEP nespecifikuje *změnu IV*, délka 24b – 2^{24}, porušení bezpečnosti RC4
      - klíče jsou zadávány staticky
  - *integrita dat*
    - ICV (integrity check value)
    - *CRC-32*
    - *data nejsou chráněna proti úmyslné modifikaci – útočník změní data a přepočítá CRC*
    - pouze detekce chyb vzniklých při přenosu či zpracování
  - *shrnutí slabin WEP:*
    - nekompletní implementace kryptografických technik
    - statické klíče, vkládají se ručně, není mechanismus distribuce klíčů
    - efektivní délka klíče 40b je *zcela nedostatečná*
    - jednostranná autentizace
    - zachycení výzvy a odpovědi *možnost získat klíč*
    - není specifikováno, jak se generuje IV – opakování IV, útok
    - zajištění integrity pouze pomocí CRC
- *WPA (WiFi Protected Access)*
  - Mezikrok mezi WEP a doporučením 802.11i
  - r. 2002 byly publikovány vybrané části
  - řeší největší problémy WEP při zachování kompatibility

- *vlastnosti:*
  - *autentizace* pomocí IEEE 802.1x nebo PSK (Pre-Shared Key)
  - *důvěrnost* pomocí TKIP (Temporal Key Integrity Protocol)
  - *integrita* pomocí MIC (Message Integrity Code)
  - *kompatibilita* se stávajícími zařízeními – upgrade firmware
  - *pracovní režimy:* firemní vs osobní řesení

Režim	Wi-Fi Protected Access – WPA	
	Autentizace	**Šifrování**
Enterprise Mode (firemní mód)	802.1x / EAP	TKIP / MIC
Personal Mode (osobní mód)	PSK	TKIP / MIC

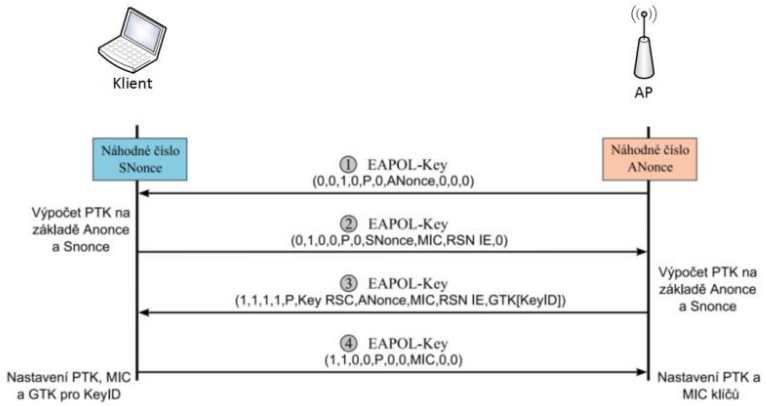
- hierarchie a distribuce klíčů:
  - využívá kolekce klíčů
  - *základem* je výstup *úspěsné autentizace*, získání hlavního klíče *PMK* (*Pairwise Master Key*), závisí na metodě autentizace, nikdy se nepoužije k šifrování
    - 802.1x – PMK z autentizačního serveru z MK
    - PSK – PSK = PMK
  - další klíče jsou *derivovány z hlavního PMK*
    - *KCK* (Key Confirmation Key) – pro MIC během 4-way handshake (4WH)
    - *KEK* (Key Encryption Key) – zajištění důvěrnosti (šifrování) během 4WH
    - *TK* (Temporary Key) – šifrování dat (TKIP, CCMP)
    - *TMK* (Temporary MIC Key) – k autentizaci dat, pouze u algoritmu Michael s TKIP
  - *autentizace 802.1x:*
    - autentizace na portech
    - bezpečnostní rámec pro autentizaci v metalických LAN
    - při autentizaci *AP zprostředkovává spojení mezi uživatelem a autentizačním serverem AS* (Radius nebo Kerberos)
    - tři entity – žadatel, autentizátor, autentizační server
    - jádro je tvořeno protokolem EAP



1. žadateli je umožněna komunikace přes EAP, zbytek blokován, startovací rámec
2. autentizátor pošle žadateli rámec s žádostí na indentifikaci
3. rámec s identif. údaji
4. na základě údajů vyšle AS výzvu
5. žadatel odpoví
6. AS ověří správnost, AP přenastaví řízený port na povolen/odepřen

u EAP-TLS je v poslední zprávě předán MK, MK = hash(PMS, Snonce, ASNonce)

- *autentizace PSK:*
  - v AP a stanicích je 256b klíč, v dalších fázích má funkci *PMK*
  - *PSK* se nezadává přímo, ale místo něj se *zadá heslo* – passphrase – 8-64 zn.
  - *passphrase se převede na PSK/PMK pomocí hashovací funkce PBKDF2* (Password-Based Key Derivation Function)
  - *4 way handshake*



1. AP vygeneruje náhodné číslo *ANonce,* otevřeně odesláno uživateli
2. uživatel generuje náhodné *SNonce*, vypočítá PSK-PTK, odvodí dočasné klíče, s využitím KCK posílá AP zprávu obsahující SNonce a MIC otevřeně,
   AP přijme zprávu, pomocí SNonce vypočítá PTK s dočasnými klíči, vypočte MIC a ověří shodu (autentizace uživatele, passphrase)
3. AP zašle klientovi zprávu s GTK, zašifrované pomocí KEK, uživatel ověří MIC (autentizace AP)
4. závěrečná zpráva od uživatele k AP potvrzuje dokončení 4WH

- *TKIP:*
  - protokol navržen k *řešení známých nedostatků WEP*
  - *proudová šifra RC4* (zpětně kompatibilní)
  - *MIC* nahradí CRC
  - *generování IV* – nedefinovaný způsob
  - *mixování klíče* pro každý paket, statické klíče
  - *distribuce a správa klíčů*, příme použití klíče
  - *integrita dat pomocí MIC:*
    - jednocestná hashovací funkce *Michael*
    - kompromis mezi *bezpečností a náročností* (bitové posuny, XOR)
    - výstupem 64b kontrolní součet MIC
  - *generování a užití IV:*
    - délka 48b
    - IV jako sekvenční čítač, eliminace možnosti příjmu rámce s jinou než očekávanou hodnotou
  - *mixování klíčů:*
    - každý paket jiný klíč
    - pomocí nelineární substituce S-box

    - slabiny:
        - použití PSK lze vypočíst ze znalosti *passphrase*
        - po odchycení 4WH hádání passphrase a kontrola symetrickým podpisem
            - odchycení nonce, hádání hesla PSK -> PMK -> PTK
            - ověření MIC druhé zprávy
            - jestli najde shodu -> nalezen PTK
        - přenos důležitých hodnot v opentextu – obě nonce
        - *KRACK přenastavení klíčů*, replay attack, znovu resetování nonce
- *WPA2 (802.11i):*
    - komplexní zajištění informační bezpečnosti pro bezdrátové sítě (IEEE 802.11b/g/a/h/n)
    - *navazuje na WPA*
    - *jiný šifrovací algoritmus* – RC4 nahrazen standardem *AES*
    - MIC vypuštěn, integrita zajištěna režimem *CCMP* (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)
    - hierarchie a distribuce klíčů:
        - stejná jako u WPA
        - *kratší délka PTK* (Pairwise Temporal Key) – KCK (128b) KEK (128 b) TK (128b)
        - *dva režimy:*
            - *personal*
            - *enterprise*
        - *PSK nebo 801.x (EAP)*

Režim	Wi-Fi Protected Access 2 – WPA2	
	Autentizace	**Šifrování**
Enterprise Mode (firemní mód)	802.1x / EAP	CCMP – AES
Personal Mode (osobní mód)	PSK	CCMP – AES

    - *slabiny:*
        - *stejná problematika hesla jako u WPA*
        - útok na chybně zvolené heslo
        - problém podpory WPS:
            - je ve většině nových routerů ve firmware
            - cílem je zjednodušit nastavení zabezpečení bezdr. sítě
            - 8 místné číslo – PIN – náchylný na bruteforce, router odpoví, která půlka byla správně – snížení počtu kombinací, poslední číslo je kontrolní součet předchozích sedmi
            - celkově tedy max 11k pokusů, řád hodin
        - díky jádru AES nejsou známé útoky

	Metoda zabezpečení bezdrátové sítě WLAN				
	WEP	**WPA (PSK)**	**WPA**	**WPA2 (PSK)**	**WPA2**
Autentizace	nulová	PSK	802.1x (PEAP)	PSK	802.1x (PEAP)
Šifrování	WEP (RC4)	TKIP (RC4)	TKIP (RC4)	CCMP (AES)	CCMP (AES)
Podnikové sítě	nevhodné	nevhodné	velmi dobrá úroveň	nevhodné	nejlepší úroveň
Domácí a malé sítě	nevhodné	velmi vhodné	nevhodné (AS)	nejvhodnější (silné heslo)	nevhodné (AS)

3.2 Testování bezpečnosti

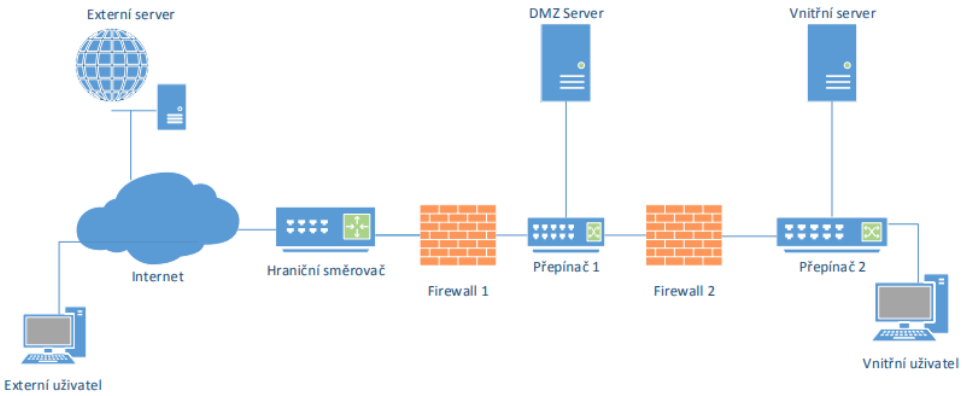
- *WEP, útoky užívají slabinu IV:*
  - aktivní (generování provozu obs. IV – ARP dotaz, aireplay-ng, Chopchop attack, Caffe Latte attack)
  - pasivní (odposlech komunikace, airodump-ng)
- *WPA, útoky užívající slabé heslo:*
  - bruteforce (airodump-ng, aircrack-ng)
  - dictionary attack
  - rainbow tables, GPU (hashcat) – zrychlení výpočtu hashování PBKDF2 (WPA2 sůl v podobě SSID – předpočteno pro nejvíce používané SSID)
  - *WPS zranitelnost*
- *WPA, zmatení uživatele* (social engineering)
  - naslouchání provozu a vytvoření falešného AP
  - vyzrazení hesla
- *celkové testování*
  - wifite
  - fluxion

4. Firewally a aplikační filtry

4.1 Firewally

- *síťový bezpečnostní systém* (zařízení, program), *monitoruje a kontroluje* síťový *provoz* na základě *definovaných pravidel*
- *omezení* příchozího a odchozího provozu pomocí *filtračních pravidel*
- pojmy:
  - *DMZ* (demilitarizovaná zóna)
    - část sítě na perimetru mezi vnější a vnitřní sítí
    - bezpečnější umístění serverů a služeb poskytovaných do Internetu
    - pro FW rozhraní se *stupněm důvěrnosti* mezi vnitřní a vnější sítí
  - *honeypot*
    - falešná návnada
    - systém nebo SW na serveru vypadá zranitelně a má přitahovat útoky
    - součástí IDS často
- historie FW:
  - *paketové filtry (IP a porty)*: 3. a 4. vrstva ISO/OSI
    - zkoumají IP adresu, hlavičku, porty
    - využití acl
    - rychlost, jednoduchost, nízká cena
    - nižší úroveň zabezpečení, nechrání proti spoofu, ...
  - *stavové paketové filtry, stavová inspekce (stateful packet inspection):* 3. a 4. vrstva
    - jako paketový fw, ale rozhoduje se ještě podle stavu (nové spojení, existující)
    - *ukládá info o stavu jednotlivých spojení do paměti*, např. povolit jen odpovědi, atd.
    - *ukládá info o socketech (src IP, dest IP, src port, dest port, TCP/UDP)*
    - rychlost, jednoduchost, vyšší bezpečnost než paketový fw
    - nižší zabezpečení než aplikační filtry, nechrání proti některým útokům a je náchylný na DDoS

    - *aplikační brány/proxy firewally:* 3., 4. a 7. vrstva
        - *aplikační firewall*
            - *Next Generation FW (NGFW) s deep packet inspection*
            - vyšší bezpečnost, prevence proti červům, trojanům, mitigace DDoS
            - vyšší zpoždění, výpočetní náročnost, periodický update a revize, složitost může způsobit vznik chyby či zranitelnosti
        - *virtuální firewall*
            - provoz mezi virtuálními stroji
        - *osobní firewall*
            - *v OS na 2. až 7. vrstvě*
            - součástí OS + IPS/IDS
        - *proxy server*
            - *prostředník* v komunikaci, sám vystupuje jako klient
    - *moderní fw (fw + deep packet inspection na aplikační vrstvě)*
    - rozšíření dnešních fw – IPS, integrace uživatelských entit (ID s IP a MAC), WAF
- *load balancing* – vyvážení zátěže provozu (kombinace fw, stavový F1 a aplikační F2)



- *konfigurace firewallu:*
    - přímá/vzdálená přes CLI/WebUI
    - *WebUI = dashboard = GUI*
    - SSH či HTTPS přístupy, jiné zakázat
- *pracovní režimy:*
    - *směrovací režim* (pracuje jako směrovač, propojuje rozhraní podsítě a pakety jsou směrovány podle pravidel a NAT)
    - *transparentní režim* (bridging mode, pracuje jako přepínač, pouze kontroluje bezpečnostní pravidla)
    - *tap režim* (pouze monitoring provozu pomocí mirroringu)
    - *virtual wire režim* (monitoring provozu přímo na spojení + pravidla)
- *základní funkce:*
    - filtrace a zabezpečení komunikace
        - uplatnění pravidel na IP adresy, protokol, typ provozu, uživatele, zóna původu a cíle (*trusted, untrusted, DMZ*), seznam *zhora dolů* podle priorit¨
        - *akce*: povolit/allow/accept, zakázat/reject a poslat ICMP, zahodit/deny/drop bez ICMP a další
        - *metody* pokročilé detekce a filtrace:
            - znalost *signatur útoku* (databáze příznaků)
            - *behaviorální analýza a AI*

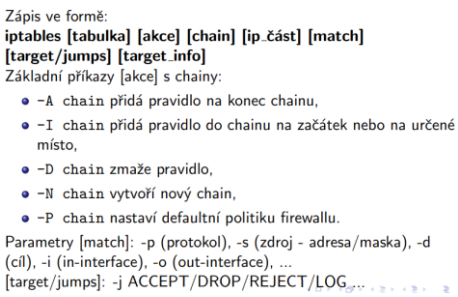
    - logování událostí a paketů
    - překlad adres (NAT, PAT), šifrovaná spojení (VPN), IDS, autentizace a autorizace, správa šířky pásma, atd.
    - *NGFW funkce* (detekce malware, ochrana proti útokům na L3–L7, signatury, behaviorální analýza, sledování prahů, strojové učení, DDoS ochrana)
- *port knocking:*
    - otevření přístupu/služby z externího nedůvěryhodného uzlu do sítě chráněné FW
    - port služby se otevře po zaslání správné *sekvence o připojení na skupinu předem specifikovaných portů*
    - sekvenci hlídá *démon*, vyhodnocuje se i *pasivní autentizace* (hash tagy zabraňují replay útokům)
    - *předcházení exploitů na permanentně otevřených portech*
- *strategie konfigurace:*
    - mít přehled zařízení a služeb v síti
    - pravidla: zakázat vše a pomolit málo, horší donastavování, vyšší bezpečnost
      povolit vše a zakázat málo, jednodušší nastavování, nižší bezpečnost
    - pravidelné testování konfigurace a FW
    - aktualizovat, sledovat aktuální hrozby

4.2 Hardwarové firewally

- samostatná síťová zařízení, umístění v racku
- stavové a paketové, aplikační
- různý počet rozhraní
- *bezpečnostní zařízení* pro ochranu sítí
    - monitoring, detekce IPS/IDS a AV modulů, filtrace, proti škodlivému kódu a kyberútokům – behaviorální analýza, strojové učení
    - VPN brány, AAA servery
- *CISCO fw:*
    - součástí přepínačů a směrovačů jsou *ACL moduly*
        - starší: PIX (Private Internet Exchange)
        - novější: ASA (Adaptive Security Appliance)
- *Check Point fw*
- *Juniper fw*
- *Palo Alto fw:*
    - *NGFW* – ochrana koncových prvků (traps – sledování procesů Cyber Kill Chain a ochrana proti útokům), automatická cloud ochrana (*Wildfire* proti malware a zerodays, Autofocus korelace bezpečnostních služeb, db a údajů o útocích v rámci cloudu a upozorňování na útoky v síti)
- *Hillstone fw*
- *FortiGate (Fortinet)*
- *Mikrotik*
- *Dell SonicWall*
- *Barracuda*
- *ZyWALL (ZyXel)*
- *WatchGuard*

4.3 Softwarové firewally

- *firewally bežící na OS Win, Linux, MAC, na platformách chytrých zařízení*
- větší ochrana aplikační vrstvy
- *Windows fw:*
  - Win10: *Windows Filtering Platform (WFP)*
    - pracuje se stackem TCP/IP
    - prohledává vnitřní strukturu paketů a klasifikuje a filtruje provoz
    - public/private/domain profily
- *UNIX a Linux fw:*
  - *IPFilter* – stavový fw a NAT balíček
  - *PF* – stavový paketový filtr, součást všech hlavních programů
  - *NetFilter/iptables* – součástí Linux Kernel
  - *Nftables* – následník iptables
  - *ipfirewall* – IP paketový filtr (Mac OS X)
- *sw fw pro nasazení do sítě*:
  - běžící na klasickém HW a mající aspoň dvě rozhraní
  - iptables jako core
    - kolekce tabulek obsahujících chains, což jsou sady rules
    - princip:
      - chains: INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING
      - tabulky: filter, nat, mangle


Zápis ve formě:
iptables [tabulka] [akce] [chain] [ip_část] [match]
[target/jumps] [target_info]
Základní příkazy [akce] s chainy:
- `-A chain` přidá pravidlo na konec chainu,
- `-I chain` přidá pravidlo do chainu na začátek nebo na určené místo,
- `-D chain` zmaže pravidlo,
- `-N chain` vytvoří nový chain,
- `-P chain` nastaví defaultní politiku firewallu.

Parametry [match]: -p (protokol), -s (zdroj - adresa/maska), -d (cíl), -i (in-interface), -o (out-interface), ...
[target/jumps]: -j ACCEPT/DROP/REJECT/LOG,...

- virtuální fw:
  - běžně dostupný HW využívají
  - *Vyatta:* virt. stav. fw a router pro IPv6, cli nebo web conf, Debian, i VMware
  - *pfSense:* open source fw/router, na pc nebo virtuální stroj
- *aplikační filtry:*
  - 7. vrstva
  - *často součástí mnoha fw, ale mohou fungovat i samostatně*
  - náročné na výpočetní výkon
  - větší zpoždění
  - mitigace a blokace malware
  - dělení:
    - filtry pro sítě (WAF)
      - *monitorují provoz*
      - *web služby a aplikace*
    - filtry pro hosty
      - monitorují u aplikací vstupní, výstupní a systémová volání
      - *ochrana aplikacím*

        - filtrování podle ID procesu
        - náročnější na výkon
        - Mandatory Access Control, Sandboxing, ...
- *speciální filtry a fw:*
    - *webové filtry*: kontrola aktivity uživatelů v síti podle přístupu na webové stránky (*shoda dle URL)*
    - *distribuované firewally:* separované části fyzicky rozmístěny v různých místech sítě
    - *cloud-based WAF*

5. Penetrační testování

5.1 Základní pojmy

- *penetrační test:* *posouzení úrovně bezpečnosti* metodou *pokusu o průnik*
  technická forma, zkušenosti, inteligence, při nalezení zranitelnosti je *napravena*
  nutnost povolení majitele systému
- *zranitelnost:* slabé místo systému
- *exploit:* využití zranitelnosti, exploit nese payload
- *payload:* náklad, umožní kontrolu nad systémem (*Metasploit – Meterpreter*)
- *vulnerability assessment:* není penetrační test samotný, pouze odhaluje zranitelnosti, čistě mechanická a strojová záležitost nesoucí false-positives
  neobnáší demonstraci nalezených slabin
- *bezpečnostní audit:* zhodnocení stavu vůči normě
- nutno balancovat šířku a hloubku testů
- testováno musí být vše, u čeho hrozí *riziko nežádoucího průniku*
- dělení:
    - obecně:
        - externí testy: vnější hrozby, útok crackera z internetu
        - interní testy: z vnitřní strany, potenciální útočník, co získal přístup do vnitřní sítě či neloajální zaměstnanec
    - podle znalostí o systému:
        - *black-box testy:*
            - jsou známy pouze vstupy a výstupy systému, není známa vnitřní struktura
        - *white-box testy:*
            - jsou k dispozici všechny možné informace o systému
            - topologie, zařízení, údaje, zdrojové kódy atd.
        - *grey-box testy:*
            - kombinace above
    - podle způsobu provedení:
        - *manuální* (testy na míru pro specifické podmínky, nutné mít rozsáhlé znalosti)
        - *automatizované* (nelze jimi otestovat úplně všechno)
        - *semiautomatizované* (kombinují výhody obou způsobů above)
    - podle cíle:
        - *síťová infrastruktura*
        - *WWW aplikace*
        - *mobilní zařízení*
- *metologie testování:*
    - *plánování:* počáteční fáze, časový plán a sestavení týmu, stanovení detailních cílů

- *sběr informací:* co nejvíce info o cílové síti/systému, rozsahy IP, otevřené porty, služby
  - nmap, zenmap
- *odhalování zranitelností:* síťové služby, porovnání verzí s db zraniteností, chybné konfigurace, specializované nástroje
  - Nessus
  - Security Focus
  - ExploitDB
  - OpenVas
- *zneužití chyb (exploitace):* využití nalezených zranitelností, už existuje řada exploitů možnost otevření nové služby či cesty, postup začne od začátku
  - Metasploit Framework
    - výběr a konfig exploitu
    - kontrola zranitelnosti cíle
    - kontrola a konfig payloadu
    - volba šifrovací techniky (obcházení IPS)
    - execution
  - Armitage
  - Rapid7
- *report*: předání výsledků penetračních testů
  nalezené zranitelnosti včetně řešení
  výsledky min. do 6 měsíců (jinak ztratí vypovídací hodnotu)
  zaslat šifrovaně, psát neutrálně

- *metodiky*:
  - *Open Source Security Testing Methodology Manual*
  - *NIST 800-115*
  - *OWASP* (dokumentace, iso, návody)

6. Útoky DDoS, testování bezpečnosti a výkonnosti sítě

6.1 DoS a DDoS

- *DoS*: odepření dostupnosti služby
- *DDoS*: DoS od více uzlů, vyšší intenzita
- *DDoS botnet*: kompromitované uzly zapojeny do sítě – botnetu
  zisk uzlů pomocí distribuce malware, trojan (Zeus botnet, Mirai)
  DDoSaaS (as a service, na objednávku)
  - *principy a vlastnosti*:
    - vytvoření (infikace) – zombie pc
    - bot se připojí ke kontrolnímu serveru (C&C server, botmaster)
    - komunikace klient server
    - DNS, IRC, IM nebo HTTP/HTTPS
    - dále i bitcoin mining, spam
- dělení:
  - *záplavové/volumetrické (flooding attacks)*
    - vytížení komunikační, paměťové, výpočetní kapacity
    - *TCP flood, UDP flood, HTTP flood, ICMP flood*
    - *ARP flood:*
      - falešné dotazy ARP

    - *reset flood:*
        - pakety s falešnou src IP, příznak RST – resetuje spojení
        - skutečná komunikace je neoprávněně ukončena
    - *syn flood:*
        - otevření několika polootevřených spojení a čekání na potvrzující zprávu, která od útočníka nepřijde
    - *HTTP flood:*
        - ze zombie klientů, zaslání legitimních požadavků http GET nebo POST – jsou náročnější
    - *UDP flood:*
        - velký počet IP paketů s UDP datagramy
    - *PingSweep:*
        - ICMP echo s podvrženou src IP
    - *Smurf:*
        - ICMP se spoofovanou adresou oběti zaslány na broadcast
- *logické útoky (logical attacks)*
    - útok na slabinu v programu/protokolu/OS
    - protokolové
    - aplikační
    - *ping of death, land attack, Slowloris, R-U-Dead-Yet (RUDY), Apache Range Header attack*
    - *Teardrop:*
        - fragmenty paketů přesahující falešně nastavený offset jsou zasílány cíli
        - cíl nezvládne sestavit paket nazpět a spadne
    - *Land:*
        - TCP-SYN jsou podvrženy, stejná src i dest IP, nekonečná smyčka
    - *Ping of death:*
        - Ping o velikosti vyšší než 65 535 B
    - *Regular expression Dos (ReDoS):*
        - Zatížení procesu zpracování výrazů (dlouhé divné username a heslo)
    - *RandomUnreachableHost*:
        - poslání ICMP host unreachable na náhodné IP adresy, přerušení některých spojení v síti
    - *UnreachableHost:*
        - ukončení legitimních spojení pomocí ICMP host unreachable
    - *Slowloris:*
        - generuje a opakovaně posílá částečné http požadavky, ale neukončí je
        - cíl otevírá další a další spojení
    - *XMasTree*:
        - generování paketů, kde jsou příznaky FIN, URG, PSH v TCP hlavičce a jsou náročné na zpracování
- *DoS využívající traffic amplification by reflecting:*
    - útočník využívá legitimní servery v síti, zašle jim dotaz se zdrojovou adresou oběti a požaduje odpověď
    - odpovědi jsou v řádu kB, dotazy malé v B
    - faktor amplifikace 28 až 10k

- *motivace:*
  - poškodit společnosti
  - vydírání
  - protesty
  - demonstrace síly
  - zakrytí hlavního útoku
- *detekce:*
  - *signatur* (znalost útoku, sestavení příznaku/signatury)
  - *anomálií* (v síťovém provozu – překročení prahu pro hustotu provozu)
  - *heuristická/prahová detekce*
- *mitigace:*
  - použití fw, IDS, honeypoty
  - redundantní linky, servery
  - black a white list
  - *Tarpit akce (netfilter, mikrotik)*
    - udržet příchozí podezřelé spojení v open state ale snížit TCP window na 0 a neumožnit tím přenos dat
  - *filtry a DDoS pračky*
    - *rate limiting* na routerech
    - *podle reputace zdroje/geolokace/služby*
    - *pračky:*
      - jednoduchá pravidla, čištění provozu, prahy pro IP adresy

6.2 Testování sítí

- testování *výkonnosti* odhalí bottlenecky, špatné konfigurace a limity sítě
- *zátěžové testování* – mimo provoz díky saturování sítě
- *testování emulované sítě* – přenesení konfigurace a test virtuální sítě
- *stress test (zátěžový test)*
- *vulnerability test*
- *blackbox test*
- *whitebox test*
- *pentest*

6.3 Testování výkonnosti a odolnost proti DDoS

- testují se *sítě* a *síťové prvky*
- zjištění *limitů* a *bottlenecků*
- *generování zátěže* (HW a SW testery)
- *analýza provozu* (monitoring chování segmentů, sondy provozu)
- *metodologie:*
  - *definice testování* (specifikace)
  - *příprava testování* (zvolení doby, zálohování služeb a aplikací, nastavení testeru)
  - *realizace testování* (monitorování testování, opakování)
  - *vyhodnocení testování* (dokumentace)
- *typy testů zátěžového testování:*
  - *výkonnostní test (performance test)* – definovaná zátěž a změření chování
  - *test hraniční zátěže (load/stress test)* – nalezení limitu, kdy aplikace překročí požadavky

    - *test odolnosti (soak test)* – dlouhodobé testy, nedostatky aplikace při nepřetržitém provozu
    - *test selhání (failover test)* – oveření chování systému v případě selhání a nahrazení záložním systémem, zotavení
    - *test části infrastruktury (targeted infrastructure test)* – zaměřený na konkrétní úroveň architektury řešení, zjištění nejslabšího místa
    - *test objemu dat (volume test)* – chování aplikace při nárůstu objemu dat
- *hardwarové zátěžové testy*:
    - zařízení s více síťovými rozhraními
    - emulace síťových klientů a serverů
        - Spirent Avalanche
- *softwarové zátěžové testy:*
    - SW aplikace umožnují nastavovat a generovat data
    - levné a snadné na konfiguraci
        - jMeter
        - trafgen
        - *Low Orbit Ion Cannon (LOIC)* – open source
        - *hping3*
- potřebná výbava:
    - zátěžový tester (HW, SW, který umí generovat DDoS)
    - emulátor provozu a DDoS útoků
- zhodnocení:
    - *zjištění limitů zařízení, sítí, služeb*
    - *ověření správnosti konfigurace a propustnosti sítě, služeb, zařízení*

7. Systémy IDS a IPS

7.1 Základní pojmy

- *průnik (intrusion):* realizace útoku, při které došlo ke ztrátě aktiv
  škodlivé i neškodlivé průniky
- *detekce průniku:* proces monitorování událostí a analýza (alarm při pokusech, incidentech)
- *IDS (detection):* sw nebo hw řešení, automatizace procesu detekce průniku
- *IPS (prevention):* všechny funkce IDS a zároveň ještě dokáže blokovat nežádoucí incidenty
  vylepšená verze IPS, které je zastaralé
- *cíl IDS/IPS:*
    - vyhlášení alarmu, potlačení útoku, jen pokud jde o skutečný incident
    - vyvážit nastavení false-positives vs funkčnost

7.2 Logy

- *logování* (záznamová data, logovací zpráva, log je soubor záznamů popisující konkrétní události, které nastaly ve sledovaném systému)
    - *informační* (popisují stavy, události)
    - *ladící* (při vývoji)
    - *varovné* (chybějící funkce, součást systému)
    - *chybové* (chyby ohrožující funkčnost systému)
    - *pohotovostní* (označující události spojení s bezpečností)

- *formát logu:*
  - textový
  - binární
- obsah logu:
  - kdo (jaké prvky)
  - kde (lokální – text/db, vzdálené, kombinace)
  - jaké události (chyby při autentizaci, chyby systému, detekované anomálie)
  - co log obsahuje (čas, zdroj, uživatel, událost; závažnost, návratová hodnota, nesmí být klíče a hesla)
  - minimální příklad:
    - časové razítko
    - zdroj
    - vlastní data
- *agregace logů:*
  - *logovací server* (malé podniky)
  - *centrální sběrné místo a logovací server* (redundance a šifrování)
  - *centrální sběrné místo, logovací server a externí úložiště* (bezpečnější decentralizované)
- *ochrana logů:*
  - *uložení:*
    - monitoring volného místa, detekce změn, záloha read only, řízení přístupu, nastavení zpráv, rotace logů
  - *přenos:*
    - zajištění důvěrnosti a autentičnosti dat
- *cíle analýzy logů:*
  - *detekce známých událostí*
  - *detekce neznámých událostí* (pomocí detekce anomálií)
  - techniky analýz:
    - *ruční jednoduchá*
    - *automatická*
      - *agregace* (stahování záznamů na jedno místo)
      - *filtrace* (analýza raw dat a rozhodnutí, která data jsou potřebná)
      - *normalizace* (záznamy na společný formát, kategorizace)
      - *korelace* (nejkritičtější a nejvíce problematický blok)
        - *na základě pravidel* – detekce signatur (nepříznivé známé události)
          - pravidla v programovacím jazyce
          - SIEM, doprogramovat korelace
          - vkládání ručně
          - problém neschopnosti definice důležitých událostí a korelací
        - *na základě modelu* – detekce anomálií (nepříznivé neznámé eventy)
          - *frekvenční model* (výskyt za daný okamžik)
          - *referenční model* (odchylky od normálu)
          - *model strojového učení*
            - *klasifikace dat do tříd*
            - *regrese*
            - *shlukování dat s podobnými vlastnostmi*
            - *algoritmus k-nejbližších sousedů*
      - *reportování*

- *IDS/IPS umístěné na síti:*
  - odchytávání paketů (packet sniffing) a analýza, jsou inline jako firewally, promiskuitní if
  - komplexní zařízení/sw řešení/cloudové řešení
- *IDS/IPS umístěné na hostiteli:*
  - softwarový agent na monitorovaném zařízení
  - kontrola vstupních/výstupních paketů, logování souborového systému, webu, přihlašování, systému
  - často na *kritické systémy* nasazováno
- jedna komponenta vs vícevrstvá architektura (3 vrstvy, manažer, agent, senzor)
- *SNORT:*
  - opensource IDS/IPS
  - packet detector, preprocesor, detection engine, logging and alerting systém, output modules
- *Suricata*:
  - nejužívanější, aktualizace signatur
  - rychlejší než Snort – paralelní zpracování dat
  - jsou na ní založeny komerční zařízení

8. Analýza škodlivého provozu

- cílem analýzy je poskytnutí informací k:
  - *vytvoření důkazního materiálu*
  - *obraně proti stejnému incidentu v budoucnu*
- *malware:*
  - *vir* (šíření v rámci výpočetní jednotky)
  - *červ* (šíření mezi výpočetními jednotkami, přes síť)
  - *trojan* (tváří se jako užitečný, nese škodlivý payload)
  - *rootkit* (zakryje stopy malware v napadeném prostředí)
  - *spyware* (shromažďuje informace o uživateli bez jeho vědomí)
  - *ransomware* (šifrování souborů, blokace služby, vymáhání výkupného)
    - *Locky* (.doc, makra, .locky, RSA 2048, AES 128)
- *další incidenty:*
  - *DoS*
  - *minery*
  - *malvertising* (prostřednictvím real time bidding)
- *analýza:*
  - *statická* (pochopit strukturu programu bez spuštění)
    - sken antiviry
    - podle otisku – obfuskační techniky – komprimační, šifrovací
    - *PEiD*
      - freeware nástroj, základ statické analýzy, GUI, sken adresářů a souborů
      - výsledkem je detekce .exe, kompilátorů a nástrojů pro šifrování
    - *GT2*
      - CLI, detekuje COM/různé EXE *modifikátory, kompilátory podle binárního podpisu*
    - Dependency Walker, HexDive (extraktor řetězců), strings (řetězce z binárního souboru), DIE (identifikace vzorku), pestudio (informace pro dekompilování a debugování), IDA (dekompilace), debugging (x32dbg)

    - *dynamická* (spuštění programu v sandboxu – kontrolovaném prostředí)
        - *bezpečné prostředí* = odpojené od sítě, virtualizace a spuštění
        - rozlišit mezi normálními změnami a změnami způsobenými škodlivým kódem
        - dělení nástrojů:
            - *hook-based* (do API funkcí, zaznamenání změn), největší škála možností
            - *difference-based* (instalační monitory, obraz systému a registrů) - Regshot
            - *notification-based* (oznámení systému při určité události – vytvoření složky, smazání souboru)
- *metody detekce změn systému:*
    - *sledování API funkcí*
    - *logování neúspěšných událostí*
    - *logování dočasných souborů*
    - *rozlišování mezi typy modifikací*
    - *ukázka změn v reálném čase*
    - *zobrazení procesů které způsobily změny*
    - *zobrazení změn v časové ose*
- *Process Monitor:*
    - zachycení *Windows API funkcí*
    - hybrid mezi *hook-based* a *notification-based*
    - *event tracing pro Windows*
    - *filtrování*

9. Bezpečnostní protokoly a útoky v sítích

9.1 IPsec protokol

- účel a princip:
    - end-to-end bezpečnost
    - šifrování a autentizace na úrovni síťové vrstvy = zabezpečení síťové vrstvy
- součásti:
    - *authentication header protocol (AH)*
        - *integrita a autentičnost IP paketů* (MAC funkce)
        - *sekvenční číslo*, ochrana proti replay attacks
    - *encapsulating security payloads protocol (ESP)*
        - *důvěrnost dat pomocí šifrování*
        - autentizace pouze ESP částí a dat, ne IP hlavičky
    - *security association (SA)*
        - formálně popisuje spojení mezi dvěma stranami a parametry použité pro zabezpečení
        - aktivní spojení v db SAD
        - SA management a pravidla jsou uložena v SPD
        - SA parametry v SAD – sekvenční čísla, AH informace, ESP informace, životnost SA, IPsec protokol mód, max velikost paketu, security parameter index (SPI, 32b)
- módy:
    - *transportní mód:* ochrana payloadu paketu, IP není šifrovaná, mezi hosty
    - *tunelující mód:* ochrana celého paketu (IP hlavička a data), paket se stane payloadem v novém paketu s novou hlavičkou, mezi hosty, bránami (překlad IP)

- ustanovení klíče:
  - *PSK*
  - *IKE1 a IKE2*
    - Internet Key Exchange (sada autentizačních schémat včetně certifikátů)
    - implementace pomocí knihoven Strongswan, Libreswan, Openswan
  - *Kerberos*

9.2 TLS protokol

- chová se jako bezpečné TCP, lze zabezpečit protokoly nad TCP
- zabezpečení transportní vrstvy
- součásti:
  - *handshake protocol* (inicializace, autentizace stran, ustanovení klíče)
  - *record protocol* (datový přenos šifrovaných data MAC autentizace)
  - *alert protocol* (notifikace chyb a varování)
- ideální ciphersuite:
  - *ustanovení klíče s dočasnými klíči* (ECDHE, DHE)
  - *bezpečný podpis* (RSA, DSS, ECDSA)
  - *bezpečné šifrování a mód* (AES-GCM)
  - *bezpečná hashovací funkce* (SHA-256, 384)

9.3 Virtual Private Networks

- musí být šifrováno point to point
- šifrování/autentičnost pomocí IPsec, TLS, proprietární, HW zařízení jako VPN brány
- typy:
  - *site-to-site* (Intranet VPN), propojení dvou sítí jedné instituce, více spojení
  - *vzdálený přístup* (klient-server), many to one

9.4 Útoky v sítích

- typy:
  - *na přenos* (odposlech dat, MITM, replay, ARP spoof, routing útoky, SSL strip)
  - *na koncové prvky* (pomocí malware)
  - *na síť* (nepovolené průniky do sítě)
  - *odepření služeb* (DoS, DDoS)
  - *zneužití fyz. osob* (social engineering, phishing)
- metody obrany:
  - bezpečná konfigurace
  - aktivní prvky
  - sestavení a dodržování pravidel
  - zabezpečení koncových prvků
  - nasazení správné kryptografie, obran a protokolů
  - testování obecných zranitelností
  - celkový audit
  - školení uživatelů a dohled
- *netechnické útoky*:
  - využití oklamání uživatele
  - psychologická manipulace

- dokážou překonat i lepší technická zabezpečení
- typy:
  - *social engineering*
    - *phishing* (pokus o zisk citlivých údajů maskováním se za legitimní entitu)
      - vektory útoku: maily, sociální sítě, web portály, IM
      - techniky: manipulace URL, vyhnutí filtru (obrázek místo textu), padělání web stránek, skryté přesměrování, vishing (voice phishing), zlé dvojče (evil twin – falešné AP)
      - *spear phishing* (konkrétní lidi, konkrétní zpráva)
      - *clone phishing* (výroba phishing zpráv z legitimních zpráv)
      - *whaling* (cílené na starší vlivné představitele firem a organizací, předvolání od vyšší autority – finančák, jiná firma aj.)
  - *baiting* (reálný trojský kůň, zanechání malware na médiu, flashka před budovou)
  - *quid pro quo* (volání do firmy a vydávání se za technickou podporu)
  - *tailgating* (průnik do chráněných prostor s pomocí legitimního uživatele, podržení dveří například)
  - *insider threats* (hrozby od vnitřního uživatele)
  - *neautorizovaný fyzický přístup* (fyz. přístup útočníka do chráněných prostor k stanici, serveru, síťovému rozhraní)
- *metody obrany:*
  - autentizace
  - bezpečnost, antispyware, školení, monitoring, antiviry