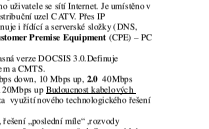
****Současné trendy v oblasti komunikačních technologií
Vývoj v oblasti ICT směřuje k cíli zajistit přenos informace
v reálném čase, se stálým přístupem uživatele k přenosovému systému, se zajištěnou spolehlivostí, se zajištěnou
bezpečností, s minimálními provozními náklady, s maximálním využitím infrastruktury
Pojmy **Lokální počítačová síť (LAN)** – v rámci organizace (koncová zařízení uživatelů – „desktop", host, server ...),
Rozlehlá (tranzitní) síť (WAN) – přenosy mezi LAN, **Přístupová síť** - přístup koncového uživatele (poslední metr)
nebo podnikové sítě (poslední míle), **Distribuční síť** – distribuce dat do agregačního uzlu (ISP), **Páteřní síť** (propojení
přístupových sítí přes agregační uzly) – např. pro přístup k poskytovateli služby – řeší provozovatel tranzitní sítě,
Přenosová infrastruktura – přenosová zařízení (zesilovače, přepínače, směrovače, rozbočovače, multiplexory ...)
Topologie – sběrnice, kruh, strom, dvoubodová, s plně nebo částečně propojenými uzly, **Techniky přenosu** –
přepínání paketů, přepínání spojů (okruhů), vytváření virtuálních spojů, **Techniky pro zvýšení využití spojů** – TDM,
FDM,WDM, DWDM, CDMA, ODFM
Sdílení přenosového spoje Časový multiplexing (TDMA), Synchronní, Asynchronní – statistický, Kódový multiplexing
(CDMA), Frekvenční multiplexing (FDMA), Kombinace (např. TDMA a FDMA), WDM – přenosy po optických
kabelech, OFDM (Ortogonální multiplex s kmitočtovým dělením v rozprostřeném spektru) – vysoká odolnost proti
interferencím
Typy komunikačních kanálů podle směru, přenosu (simplex , full duplex , half duplex)
Typy přenosů (využití podle příjemce zprávy, **unicast** – jeden příjemce, **multicast** – specifikovaná skupina příjemců,
anycast – „nejvýhodnější" příjemce ze specifikované skupiny, **broadcast** – „všesměrový" přenos, **Qos** - Přenosy s
rozšířením kvality služby
****Techniky pro hezdrátové přenosy
Spread Spectrum techniky zajištění odolnost signálů proti odposlechu, zvyšují kapacitu signálu – kapacitu
přenosového kanálu, snižují interference – zvýšení kvality signálu
DSSS poskytuje vyšší přenosovou kapacitu než FHSS, velká citlivost na vnější prostředí (odrazy), vhodná pro řešení
PMP (Point-to-Multipoint) na krátké vzdálenosti, na delší PP (Point-to-Point), typické použití vnitřní WLAN
pojítka mezi budovami, **FHSS** velmi odolná proti rušení (od jiných radiových zařízení, umožní pokrytí větších
geografických oblastí, **OFDM** Technologie rozprostřeného spektra (SS), Nosné jsou rozmístěny ve spektru úplně
oddělené ve velmi přesných pásmech, Demodulátory jsou nastaveny na tyto frekvence, takže nedochází k interferencím.
Výhoda je vysoká spektrální účinnost a nízké zkreslení. Používá se typicky v bezdrátových a kabelových přenosech,
WLAN, konfigurace Point-to-Point, Point-to-Multipoint (IEEE 802.11a, pásmo 5.8 GHz), Technologie ADSL
Bezdrátové sítě 3 frekvenční pásma: **radio frekvence** v rozsahu přibližně od 30 MHz do 1 GHz, **mikrovlnné frekvence**
v rozsahu přibližně od 2 do 40 GHz, **Široké pásmo** – cca 20 – 50 GHz, **Úzké pásmo** - ISM Band – 2,4 GHz až 2,485
GHz (IEEE 802.11b)
Technika „rozprostřeného spektra" (Spread Spectrum) OFDM, infračervené frekvence (IR) - v rozsahu frekvencí
vyšších než mikrovlnných a nižších než z oblasti viditelných frekvencí
Mikrovlnné frekvence pro bezdrátové připojení **2,4 GHz, 5,8 GHz** – vhodné pro datové přenosy, generální licence
ČTÚ, spojení „point-to-multipoint", nezaručená kapacita (nižší spolehlivost), použití v WLAN, ISM band, **3,5 GHz** –
pásmo pro FWA (Fixed Wireless Access) MMDS, přenosy dat a hlasu v nižší kapacitě, nutnost individuálního
povolení ČTÚ pro každou základnovou stanici, spolehlivé přenosy do 2 Mbps, spojení „point-to-multipoint",
vhodnépro připojení menších firem do Internetu prostřednictvím ISP vlastnícího licenci na toto pásmo. **26 GHz** –
pásmo FWA LMDS, nutnost povolení ČTÚ pro základnové stanice, garantovaný vysokorychlostní přenos hlasový a
datový, rychlost přenosu, do 8 Mbps, spojení „point-to-multipoint", vhodné pro větší podnikové sítě **40,5 – 43,5 GHZ**
– nutnost povolení ČTÚ, univerzální pásmo MWS, pro komerční provoz (datové a multimediální služby – např.
připojení k Internetu, kabelová televize, telefon), spojení „point-to-multipoint", nebo „multipoint-to-multipoint".
Bezdrátové optické sítě **Signály z IR** pásma – neviditelné, neprostupují hmotnými překážkami, kvalita přenosu
částečně ovlivněna počasím, vzdálenost přenosu až 4 km. Řeší problém zavedení optických kabelů do určité lokality
(bezdrátové WAN připojky)Technologie **FSO** (Free-space Optic) – širokopásmová (100 Mbps, 155Mbps – *OC3*, 622
Mbps – *OC12* a cca 2 Gbps – *OC48*) komunikace na přímou viditelnost LOS (Line-of-sight) Technologie **IrDA**
(Infrared Data Association) – velmi krátké vzdálenosti – využití v sítích PAN nebo LAN(IrLAN)
Bezdrátová pojítka
Bezdrátové optické sítě (**WON**) – náležejí do technologické skupiny širokopásmových bezdrátových technologií
BWA,spojení „point-to-point" (PP) nebo „point-to- multipoint" (PMP)
topologie point-to-point, stromová (FSO-hub), plně propojená, kruhová
Funkcí mezilehlého zařízení zajišťuje **FSO transceiver,** vzájemné navázání veřejné přímé viditelnosti, spojení full-
duplex, obsahuje laserový vysílač a čočku pro vysílání signálu, detektor přijímaného signálu, použitelnost poslední
míle, propojení objektů v areálu, záložní spoj
****Bezdrátové sítě **Výhody** snadná realizace, připojení a odpojení, infrastruktura bez kabelů – nižší pořizovací
náklady, možnost přenositelnosti bezdrátových zařízení, prokazatelná úspora pracovního času uživatelů
Specifické problémy **nevýhody** bezpečnost (možnost odposlechu), roaming (u mobilních sítí), náchylnost na rušení,
podpora multimediálních přenosů (vysoká přenosová kapacita, garance QoS)
Bezdrátové sítě: Bezdrátové lokální sítě **WLAN,** Bezdrátové přístupové sítě, Bezdrátové širokopásmové přístupové sítě,
Mikrovlnná bezdrátová pojítka, Celulární mobilní sítě (datové služby), Satelitní sítě, Bezdrátové osobní sítě (bezdrátová
připojení periférií k počítačům), Bezdrátové optické spoje

Standard IEEE 802.11a pracovní pásmo 5 GHz - problém v Evropě – pásmo určeno ETSI pro satelitní vysílání
dosah 170 m, rychlost přenosu deklarovaná 54 Mbps, reálná 30 – 36 Mbps při použití techniky OFDM,Použití – DAB,
DVB, bezdrátové přenosy
Standard IEEE 802.11b (Wi-Fi) Pracovní pásmo 2,4 GHz (bezlicenční ISM), Dosah 100 m, rychlost přenosu
deklarovaná do 11 Mbps, reálná 5 – 6 Mbps při použití techniky DSSS s modulací CCK, Nejrozšířenější technologie
WLAN současnosti (podle údajů přes 90% sítí), vývoj probíhá v rámci činnosti Wi-Fi Alliance
Standard IEEE 802.11g Nový standard z r. 2003, Pracovní pásmo 2,4 GHz – zpětná kompatibilita s IEEE 802.11b
Dosah 150 m, rychlost přenosu deklarovaná do 54 Mbps, reálná 12 Mbps při použití techniky OFDM pro rychlosti 6, 9,
... 48, 54 Mbps nebo DSSS-CCK pro rychlosti 1, 2, 5,5, 11 Mbps(volitelné)
IEEE 802.11e - Wi-Fi s rozšířením podpory QoSWMM (Wi-Fi Multi-Media)
Standard ETSI – HIPERLAN 1/2 současná verze HiperLAN 2 (z 2003) používá pásmo 5,15 – 5,35 GHz, použití
pouze uvnitř budov, dosah 80 m, rychlost přenosu deklarovaná 54 Mbps, reálná 31 Mbps při použití techniky OFDM,
podpora QoS, vysoká bezpečnost přenosu, problém s uplatněním na trhu
Bezdrátové sítě Komponenty **WLAN** sítě, přístupová zařízení AP, bezdrátové stanice STA, oblast pokrytí jedním AP
(buňka) – BSA – základní sada služeb (BSS), propojení buněk distribučním systémem – ESA – rozšířený soubor
služeb ESS (roaming ...), konfigurace point-to-point (ad hoc) – nezávislá WLAN bez AP
Problém bezpečnosti vašich IEEE 802.11 SSID (Service Set Identifier) – AP vysílá SSID broadcastem – nutné
konfigurační potíže, otevřená síť bez ověřování autentizace – při vytváření asociace – použití autentizaci se sdíleným
(tajným) klíčem WEP, při vytváření asociace filtrace podle MAC adres, autentizace uživatele podle EAP, používat *ssh*
Specifikace **WEP** používá šifrování symetrických algoritmem RC4 s délkou klíče 40 b (default) až 104 b a
inicializační vektor 24 b., 40 bitový řetězec lze vrelálně dobře prolomit
Vývoj a normalizace WLAN,průmyslová aliance *WLANA*, průmyslová aliance *Wi-Fi Alliance*
WPAN Standard IEEE 802.15.1-3 (Bluetooth") pro sítě WPAN komunikace mezi bezdrátovými elektronickými
zařízeními výpočetního systému (tiskárny, myši ...), mezi počítači (laptop) pásmo 2,45 GHz – 3 výkonové třídy, dosah
deklarovaný 100 m (pro třídu 1) osvědčená použitelnost 10 – 20 m (třída 2), přenosová rychlost současné verze 3 je 11,
22, 33 a 44 Mbps při použití techniky FHSS, čip Bluetooth obsahuje vysokofrekvenční modul pro vysílání a příjem a
řadič, Komunikace zařízení master – slave, vytváření komunikujících skupin – „piconet", možnost vzájemných
propojení přes Bluetooth bridge, 24-bitový identifikátor třídy (pro jakou službu je zařízení určeno), Bluetooth profily
(24, další se dokončují) – definice možných aplikací (přehrávání audio/video, headset pro mobily, přenosy souborů do
tiskárny, přenosy dat z lékařských aparatur (,.....), Wi-Fi vs. Bluetooth (Ethernet – USB), Vývoj a normalizace
Bluetooth – průmyslové sdružení Bluetooth Special Interest Group
Standard IEEE 802.15.4 („Zigbee") pro sítě WPAN Technologie jednoduší a levnější než Bluetooth - cíl: velmi
nízká spotřeba energie (ale nižší přenosové rychlosti), HW – jednoduchý mikroprocesor, Pokrývá PHY – modulace
DSSS, pásma 2,4 GHz **Využití** - řízení průmyslových systémů, lékařská zařízení, bezpečnostní a požární systémy,
automatizované systémy v budovách a domácnostech (osvětlení, klimatizace...)
Bezdrátové sítě **– FWA** Fixed Wireless Access (FWA) – technologie pro pevné připojení uživatele ho WAN (jedno z
řešení „poslední míle"), úzkopásmové (3,5 GHz) – systémy **MMDS** (Multichannel Multipoint Distribution Systems)
pro domácnosti a malé podniky, přenosové rychlosti max. 2 Mbps, dosah 30 – 50 km, širokopásmové (26 GHz) -
systémy **LMDS** (Local Multipoint Distribution Systems) pro střední až velké podniky, přenosové rychlosti 30Mbps
(garantované 8 Mbps), dosah do 5 km, **Způsob propojení** point-to-point, point-to-multipoint (PMP), Přenosy
datové, hlasové, video, multimediální, **Šíření signálu** na přímou viditelnost LOS (Line-of-Sight), bez přímé viditelnosti
NOS (Non-Line-of-Sight) - technika OFDM
WiMax - Wireless Metropolitan Area Networks FWA ,druhé generace" – specifikace **IEEE 802.16** z r. 2001 – původně
pásmo 10 – 66 GHz LOS, Šíření signálu na přímou viditelnost – LOS Systém MWS, pásmo 40,5 – 43,5 GHz, propojení
k základné PMP, Integrované přenosy zejména pro domácnosti, malé kanceláře,malé a střední podniky, Rychlost na
fyzické vrstvě 120 Mbps, reálná rychlost – několik desítek Mbps, reálná rychlost – stovky kbps, Technologie
RADSL-přizpůsobuje šířku pásma kvalitě služby, 7Mpbs, 1,5Mbps, **UADSL**- asymetrická ver., pomalejší, bez splíteru
u klienta, až 5,5km, 1,5Mbps, 386 kpbs, **VDSL**-maximální dosah 1,5km, 13-52Mbps, 1,2-2Mbps
ADSL zařízení **DSLAM**- centrální uzel, ke kterému se přes DSL připojují jednotlivé koncová ADSL zařízení. DSLAM
bývá napojen na páteřní síť. **Splitter** - Zařízení které na datové DSL lince vydělí definované frekvenční pásmo. To je

poté využito jako standardní telefonní linka nebo pro ISDN. Díky tomu je možné na jednom připojeném vedení mít
současně ADSL a ISDN či klasický telefon. **ADSL modem** - modulo/demodulace datového toku nízké nosné
frekvence (analogového signálu). **ADSLswitch/router** – stejná funkce jako modem, možnost připojení více PC (sítě),
konfigurovatelný (jako FW), podpora protokolů a služeb (např. TCP/IP, ARP, IPCP, CHAP, ICMP, DHCP)



CATV, CATV: Cable TV systems. Moderní uspořádání kabel nebo HFC Zařízení:
CMTS: Zařízení pro propojení koncového uživatele se sítí Internet. Je umístěno v
„headend" CATV **Headend:** centrální distribuční uzel CATV. Přes IP
switch/router je připojen k Internet. Zahrnuje i řídící a serverské složky (DNS,
DHCP, mail server, Web hosting …), **Customer Premise Equipment** (CPE) – PC
a modem
DOCSIS: - průmyslový standard. Specifikuje CATV TV systém. Definuje
technické specifikace pro kabelový modem a CMTS.
Struktura specifikace **DOCSIS 1.0** 38Mbps down, 10 Mbps up, **2.0** 160Mbps down, 30Mbps up, **3.0** 160Mbps down, 120Mbps up Budoucnost kabelových
přenosů UWB – Cable technologie, Dvojnásobek přenosové rychlosti CATV za využití nového technologického řešení
a téměř mezních přenosových kapacit koaxiálního kabelu
****Technologie PLC – datové přenosy po vodičích v elektrické rozvodné síti, řešení „poslední míle" ,rozvody
domácích sítí, **Přístupová síť** - využívá distribuční elektrickou síť, začíná v transformátoru ze středního na nízké
napětí, umožňuje připojení zákazníka přes access point **Princip** – elektrické vedení je transformováno do komunikační
sítě prostřednictvím superponovaného nízko výkonového datového signálu do výkonové vlny. Aby byla možná
koexistence, jsou frekvenční pásma značně vzdálená: Výkonová vlna - 50 Hz (v Evropě), Datový signál - od 3 do 148,5
kHz pro PLC narrowband aplikace, od 1 do 30 MHz pro PLC broadband aplikace,, PLC fórum
Vlastnosti PLC - přenosová rychlost 14 – 20 Mbps, elektrický vodič je sdílené médium, je třeba řešit problém
násobného přístupu – deterministická metoda, kromě přístupu k Internetu může PLC řešit monitorování a ovládání el.
spotřebičů v reálném čase, dálkové snímání stavů elektroměrů, zabezpečení objektů, alarmy apod.
Ethernet v první míli má předpoklady k zajištění „poslední míle" do objektů s rozvody UTP a se zásuvkami RJ45
EFM (Ethernet in the First Mile) – IEEE **802.3ah**, Spojení mezi POP (Point of Presence) a přístupovým bodem propojí
páteřní síť (*Core Layer*) s uživatelem (*Home Network*), **Topologie** point-to-point, Point-to-multipoint
Ethernet v první míli Standard IEEE 802.3ah specifikuje 3 přístupové topologie a fyzické vrstvy, **EFM** Copper
(**EFMC**) přes UTP Cat3 (minimálně) do vzdálenosti 750 m – rychlost min. 10 Mbps – topologie point-to-point,
využívá „local loop"umožňuje současný přenos hlasu (IP telefonie), video a širokopásmový přístup do Internetu,
vhodné použít pro sítě v hotelech, nemocnicích, školách…
EFM Fiber – (**EFMF**) po optickém vodiči single mode do vzdálenosti nejméně 10 km – rychlost 100/1000 Mbps –
topologie point-to- point,full-duplex připojení optickým vodičem single-mode do vzdálenosti 10 km, přenosová
rychlost 1000 Mbps, ISP zajistí propojení uživatele (domácnost, kancelář, SOHO apod.) přes ONU EFM PON (Passive
Optical Network) – (**EFMP**) po optickém vodiči do vzdálenosti 20 km – rychlost 1000 Mbps, topologie point-to-
multipoint s použitím pasivního optického splíteru, sdílení přenosové kapacity optického vodiče 16 – 32 uživatelů přes
pasivní optický splíter
Kritické faktory EFM požadavek na QoS a šířku pásma – Ethernet byl původně určen k datovým přenosům vývoj
technologie EFM se zaměřuje na zajištění služeb, přenosy třídy digitální video, MPEG 2 a 4, DVD, přenosy třídy
digitální hlas (VoIP), datové přenosy – vysokorychlostní přístup k Internetu (transparentní připojení LAN)
podpora VPN (pro vzdálený přístup k databázím, pro e-commerce…)
****Úvod do **BIS** Informace = hodnota= chránit před: Před neoprávněným přístupem, Před zcizením, zfalšováním a
zneužitím, Před vyzrazením, Před zablokováním přístupu oprávněným subjektům, Informace je chráněna v rámci
informační bezpečnostní politiky (**BP**) organizace, jejímž je majetkem
IS zajišťují informaciím přípravu ke zpracování (vstup do IS), zpracování a vyhodnocování, přenosy a uchovávání,
prezentaci, výstupní informace
Složky IS **IT** (HW tj. počítače, servery, tiskárny, SW tj. operační systémy, programové vybavení..) **lidé**, **data**
Základní fáze řešení bezpečnosti IS Určení základních cílů a strategie BP, Provedení analýzy rizik, Ustavení celkové
bezpečnostní politiky (CPB), Vypracování prováděcích směrnic, bezpečnostních norem, Implementace bezpečnostního
systému, Provádění monitoringu a auditu
Funkce informačního bezpečnostního systému - dosažení bezpečnostních cílů stanovených v bezpečnostní politice
(řízení bezpečnostních rizik), **Analýza rizik (AR)** je klíčovým krokem ve výstavbě informačního bezpečnostního
systému, odpovídá: Co nastane, když nebudou informace chráněny?, Jak může být bezpečnost informací porušena?,
Bezpečnostní cíl, Zranitelné místo, Hrozba, Riziko, Útok, Dopad, Jaká je pravděpodobnost, že to nastane?
Základní bezpečnostní cíle zachování důvěrnosti informace, zachování integrity informace, zachování dostupnosti
informace, zachování autenticky (spolehlivosti) informace, zajištění prokazatelnosti původu informace, zajištění
prokazatelnosti převzetí informace Cíl informační bezpečnostní politiky – informace má zajištěnou ochranu v kontextu
základních bezpečnostních cílů na stanovené úrovni
Zranitelné místo – vlastnost IS může být v **HW,** SW, v provozním prostředí, v lidech
Cíl AR: odhalení zranitelných míst, určení přijatelné míry rizik vyplývajících z existence zranitelných míst
určení způsobu, jak riziko na přijatelné úrovni udržet, **Hrozba** – možnost využití zranitelné místa, **Riziko** –
pravděpodobnost využití zranitelného místa (pravděpodobnost uskutečnění hrozby), **Útok** – úmyslné (subjektivní útok)

nebo neúmyslné (objektivní útok) využití zranitelného místa. Základní typy útoků: přerušení, odposlech, změna,
padělání - zfalšování
Dopad – důsledek útoku vyjádřený v určité hodnotě (zpravidla finanční)
Další termíny: **Objekt IS** – pasivní entita IS, obsahuje nebo přijímá informace, používají ji autorizované subjekty,
Subjekt IS – aktivní entita IS autorizovaná k manipulaci s informací v rámci určité ho objektu, **Bezpečnostní funkce** –
opatření k dosažení bezpečnostního cíle, **Bezpečnostní mechanismus** – prostředek nebo nástroj k dosažení
bezpečnostního cíle
Typy bezpečnostních funkcí (**BF**) – bezpečnostních protiopatření, **podle času** : preventivní BF – vytvářejí preventivní
bezpečnostní subsystémy, detekční BF – *IDS*, opravné BF – zálohy, kontrolní BF – monitoring, auditní systémy,
zastrašovací BF – podniková ustanovení, zákonná opatření **podle způsobu implementace:** fyzické BF – zámky,
trezory, může ….. hardwarové BF – identifikační karty, archivní média, softwarové BF – SW řízení přístupu, aplikace
pro digitální podpisování, administrativní BF – směrnice, předpisy
Postup při provádění analýzy rizik: Identifikace a ocenění aktiv: Nalezení zranitelných míst, Odhad rizik, Stanovení
nepřijatelných a přijatelných rizik, Stanovení očekávaných ročních ztrát, Identifikace použitelných bezpečnostních
opatření na snížení rizik na přijatelnou míru, Odhad ročních úspor po zavedení bezpečnostních opatření do IS
Systémová bezpečnostní politika (**SBP**) – vychází z celkové bezpečnostní politiky, zahrnuje technickou složku (popis
technických řešení a postupů) a administrativní složku (směrnice a předpisy; zřízení pravomocí a zodpovědnosti atd.).
Součástí SBP je „Plán obnovy" a „Havarijní plán", Monitoring a audit – průběžné a následné sledování účinnosti
informačního bezpečnostního systému
Typy bezpečnostních mechanismů podle doby uplatnění preventivní, detekční, následné Typy bezpečnostních
mechanismů podle funkce pro zajištění oprávněného přístupu do IS, pro detekci narušení IS, pro zajištění obnovy a
kontinuity provozu IS, pro zajištění integrity IS, pro zajištění důvěrnosti informace, pro zajištění neodmítatelnosti
odpovědnosti
Implementace bezpečnostních mechanismů: kryptografické systémy, firewally, systémy IDS, AAA technologie,
monitorovací a auditní systémy, digitální podpis, biometrické systémy, čipové karty
Systémy pro detekci průniku - **IDS** (Intrusion Detection Systems) mechanismy preventivní a detekční, Cílem IDS je
detekce průniku nebo pokusu o průnik a generace odezvy na průnik, IDS může zabezpečit **cíle** dostupnost, integritu,
důvěrnost, **Princip činnosti IDS**: sběr informací z různých částí IS, analýza informací o výskytu příznaků
bezpečnostních problémů, Analogie s fyzickými bezpečnostními mechanismy detekce průniku - kamerami.
IDS SW často vyžaduje dedikovaný výpočetní systém - značné nároky na výpočetní výkon – na IDS navazuje modul
protiopatření **Obecná struktura IDS**: sensor - generátor událostí (agent, čidlo) poskytuje informace o vzniku určité
události, analyzátor - logický modul, který informace o událostech zpracovává a vyhodnocuje, manager - správní
komponenta, generátor odezvy - reakce na detekci (oznámení) událostí, ukládací mechanismus - archivace reportů nebo
jejich částí
BIS -IDS další bezpečnostní nástroje: systémy pro analýzu (hodnocení) zranitelnosti - ověřují odolnost na známé útoky,
generují "snímky" bezpečnostních stavů systému v určitém čase pro možnost zjištění problémů v důsledku lidských
chyb nebo pro potřeby auditu, systémy pro kontrolu integrity souborů - používají kryptografické kontrolní sumy pro
kontrolu kritických datových objektů. ***Integrity checkers*** mohou preventivně ochránit systém před útokem (příprava
útočníka často spočívá v předběžné modifikaci určitých systémových souborů).
Typy IDS podle oblasti, ve které se provádějí sběr informací a analýza : IDS orientované na hostitelský systém (**HIDS**)
- sbírají informace na určitém samostatném výpočetním systému. Využívají systémové záznamy generované jádrem a
dalšími systémovými zdroji, Monitorují probíhající procesy v kontextu a aktivitami uživatelů a změnami v souborovém
systému. Výhoda: mohou monitorovat data i v případě, že jejich přenosy jsou šifrované, nejsou ovlivňované
přepínanými sítěmi, mohou odhalit útoky, které není možno odhalit síťovým IDS. Nevýhoda: pro každý systém je
nutné nastavit vlastní konfiguraci - složitá administrace, IDS může být napadený v rámci útoku na hostitelský systém,
IDS může být vyřazen z činnosti útokem DoS, IDS představuje pro monitorovaný systém značnou zátěž.
Aplikačně orientované IDS (**ApIDS**) - speciální podmnožina host-based IDS, zaměřená na určený typ aplikace.
Umožňuje sledovat postupy uživatelů, Zaznamenává pokusy a překročení autorizovaných práv atd.
IDS orientované na určitý objekt/atributy objektu (object-based IDS) - monitorování souborů a jejich změn.
Provádí se zpravidla v režimu intervalovém. Na základě zpráv lze např. stanovit, zda se má obnova systému provádět ze
zálohy nebo originálu.
Síťové orientované IDS (network-based IDS - **NIDS**) - zpracovávání informací získaných ze síťových rozhraní v
promiskuitním režimu. Agent může být implementován v HW síťových produktech. Síťový IDS na bázi HW může
pracovat v režimu "stealth" (útočník o jeho existenci nevíš), HW síťové IDS komunikují s managerem přes jiné síťové
rozhraní, než které sledují. Většinou pracují v reálné čase na principu "analýzy signatur", protože lze sestavit poměrně
značné přesné vzory TCP sekvencí a protokolových dialogů.
Chyby IDS Nepravé pozitivní chyby – nesprávná klasifikace legitimních akcí, Nepravé negativní chyby – nesprávná
klasifikace nelegitimních akcí
BIS -IDS Typy IDS podle způsobu provedení analýzy: Detekce na základě statistické analýzy (statistické anomálie) -
hodnocení statistiky významných vlastností. **Nevýhoda** mohou vzniknout mnoha falešných poplachů z důvodu
nepředvídatelného chování uživatelů (i sítí), potřeba dlouhého zkušebního provozu než je nasnímáždělno dostatečné
množství podkladů pro stanovení normálu, Detekce podle srovnávání se vzory (Signature Analysis) - vzory odpovídají
událostem nebo sledům událostí typickým pro známé útoky nebo narušení systému.**Riziko:** pokud poměrně

jednoduchého maskování škodlivé aktivity nabo oklamání sensoru (např. postupnou změnou uživatelského chování, tzv.
"slow attacks")
Implementace IDS Na dedikovaných počítačích, Na firewallech, **SW produkty volně šířitelné**: TripWire, AIDE, Snort
BIS – **Kryptografické systémy** – nejpoužívanější bezpečnostní mechanismy současnosti
Kryptografické algoritmy **symetrické** – DES (Data Encryption Standard), IDEA (International Data Encryption
Algorithm), RC2 a RC4 (Rivest Cipher), Kryptografické algoritmy **asymetrické** – RSA (Rivest Shamir Adleman)
DSS (Digital Signature Standard), EC (Eliptic Curve)
Hash funkce Vstupní data libovolné délky jsou transformována do výstupních dat pevné délky (128, 160, 256, 512 bitů)
Jednocestná funkce s klíčem nebo bez klíče Nejrozšířenější hash algoritmy MAC (Message Authentication Code) -
jednocestná funkce s klíčem (heslem) - výstup algoritmu přiložený ke zprávě ověřuje její autenticitu (heslo) a integritu
(hash) MD 5 (Message Digest 5) - autor Ronald Rivest. Výstup 128 b., vstupní bloky 512 b. SHA-1 (Secure Hash
Algorithm) *FIPS PUB180* - výstup 160 b., vstupní bloky 512 b. Srovnání funkcionality MD5 a SHA-1: MD5 má
neomezenou délku vstupní zprávy (SHA-1 má limit 2^64-1 bitů) a výpočetní asi dvakrát rychlejší než SHA-1.
BIS – **E-podpis** Složky zajišťující digitální podpis, asymetrické kryptografické systémy, hash funkce , správa veřejných
klíčů – PKI (Public Key Infrastructure), certifikát veřejného klíče – certifikační autorita (CA), Digitální podpis
zabezpečuje: integritu podepsané zprávy, autentičnost podepsané zprávy. Obsah certifikátu: jméno vlastníka certifikátu
sériové číslo certifikátu, doba platnosti certifikátu, kopie veřejného klíče vlastníka certifikátu, jméno CA, digitální
podpis CA, Správa veřejných klíčů – systém PKI
Digitální podpis prostředke m pro bezpečné ověřování elektronických podpisů.
Akreditovaní poskytovatelé certifikačních služeb v ČR První certificiní autorita, a.s., **PostSignum QCA** (Česká pošta,
s. p.) eIdentity, a.s. **Typy certifikátů** testovací, komerční, kvalifikované, Časové razítko – elektronický důkaz o
existenci určitého dokumentu v určitém čase
Technologie **AAA** Autentizace, Autorizace, Účtovatelnost , Omezení rizika : neoprávněných přístupů do podnikové sítě,
překročení přidělených oprávnění, Sběr informací k účtování Autentizace (ověření totožnosti) – preventivní
bezpečnostní funkce – řízené povolení k přihlášení, připojení, **Metody autentizace**: Uživatelské jméno a heslo, statické
(velmi slabá autentizace), s omezenou dobou platnosti, Jednorázová hesla (one-time passwords) – např. metoda S/Key
(silná autentizace), Identifikační tokeny – např. smartcards (velmi silná autentizace), Biometrické prostředky
Implementace autentizace - protokoly PAP a CHAP – součást specifikace PPP
PAP (Password Authentication Protocol) – dvoucestná autentizace – „slabé" (přenáší se nezašifrované heslo). Request
(autentizační data) – response (potvrzení/odmítnutí).
CHAP (Challenge Handshake Authentication Protocol) – třícestná autentizace (výzva – odpověď – přijetí/zamítnutí),
ověřování periodické v průběhu relace.
Princip **OTP** (One-time password) - vytváří řadu hesel $f(s), f(f(s)), f(f(f(s))), \ldots$ poslední se uloží na serveru
s – tajná přístupová fráze (initial seed), f – jednosměrná šifra (hash function), uživatel pro autentizaci používá postupně
hesla ze seznamu v obráceném pořadí, server si spočítá algoritmem hash hodnotu ze zaslaného hesla a porovnává ji s
hodnotou, kterou má uloženou v minulé relace atd. až do vyčerpání seznamu
Autorizace - omezení uživatelských přístupů k službám, Na základě provedené autentizace zjistí přístupový server
autorizační informace z příslušné databáze
Účtovatelnost – sledování přístupu k síťovým prostředkům – vytváření záznamů do příslušné databáze - Obdoba *syslog*
Podpora mechanizmu AAA – databáze zabezpečení – pro lokální autentizaci, autorizaci a
účtovatelnost. Pro malé sítě dostačující. Vzdálená databáze zabezpečení – podpora centralizovaného systému AAA –
přístupová zařízení (servery, routery, switche) získají informace ze společné databáze. Pro střední a velké sítě.
Protokol **TACACS** – fy. CISCO – aplikační protokol sady TCP/IP (Transportní protokoly TCP/UDP port 49 a 65 pro
databázové služby), Implementace - server (aplikace pro platformu UNIX, Windows NT typu démon + databáze),
klient běží na přístupových serverech, směrovačích, přepínačích. Komunikace: klient (request) – server (response),
Procesy: autentizace, autorizace, účtování
Charakteristika protokolu TACACS+ Formát paketů – záhlaví + data, 3 typy paketů: pole „packet type", Pakety
TACACS+ se přenášejí zašifrované , Autentizace prostřednictvím mechanismů PAP a CHAP, Podpora zpětného volání
(reverze účtování)
Protokol **RADIUS** - aplikační protokol sady TCP/IP (Transportní protokoly TCP/UDP port 1812 a 1813 pro účetní
služby), Procesy: autentizace a autorizace (port 1812) a účtování (port 1813), Autentizace: klient – přístupový server
(OTP, PAP, CHAP), Autorizace: RADIUS server – přístupový server (na výzvu na princ pu sdíleného tajemství)
Charakteristika protokolu RADIUS Formát paketů – záhlaví + data (atributy) typ, délka, hodnota, 4 typy paketů:
Autentizace PAP a CHAP, Šifruje se pouze hesla uživatelů, Podpora zpětného volání
Čipové karty autentizační (kryptografické),autenticity odesílatele zprávy, integrity zprávy, důvěrnosti zprávy,
neodmítatelnosti odpovědnosti odesílatele zprávy, **Smart cards (čipové karty)** - kryptografické tokeny
Smart card (SC) – pokračovatel vývojové řady identifikačních karet používaných v přístupových a I&A systémech
Typy SC kontaktní, bezkontaktní, hybridní, **Využití SC** bezkontaktní – v přístupových zabezpečovacích systémech,
kontaktní – v systémech autentizačních, pro vytvoření elektronického podpisu, pro šifrování dat, Kryptografický token,
Čipová karta, USB token, Technická charakteristika SC,RAM - operační paměť – asi 1 kB, ROM – pevná paměť – asi
16 kB, EEPROM – pracovní paměť (úložiště kryptografických dat) – asi 24 kB , procesor – 8bit – 5MHz, ryptografický
koprocesor, operační systém – je uložen v ROM Funkční charakteristika SC autentizace uživatele – znalost PIN –
ochrana před zneužitím privátního klíče (v EEPROM) – po následném nesprávném zadání je karta blokována

identifikační data – privátní a veřejný klíč + certifikát, kryptografické algoritmy RSA, DES, generátor náhodného čísla
RNG, hash algoritmy (SHA-1, MD5), přenosové rozhraní – protokoly T=0 (znakové orientovaný), T=1 (blokově
orientovaný) Další fyzické podoby tokenů USB token – výhoda : nemusí se pořizovat čtecí zařízení – nevýhoda: nelze
použít pro další aplikace (např. jako identifikační vrcholovou kartu), má větší životnost než SC „Klíče", „pouzdra";
„knoflíky" – proprietární řešení využívá specifická čtecí zařízení Další kryptografické produkty – kryptografické
akcelerátory – zásadní zrychlení kryptografických procesů – zvýšení bezpečnosti procesů