1. Hrozby, slabá místa, aktiva, škodlivý software (malware).

Zranitelná místa (vulnerabilities) jsou slabiny v informačním systému, která mohou být využita pro provedení bezpečnostního incidentu (útoku). **Hrozby (threats)** jsou okolnosti, které mají potenciál způsobit bezpečnostní incident. **Aktiva (assets)** jsou složky IS, které mají hodnotu (ludia, procedury, data, software, hardware). **Opatření (measures)** redukují pravděpodobnost vzniku bezpečnostního incidentu. **Riziko** je zranitelné místo zkombinované s bezpečnostní hrozbou.

Detailněji je **zranitelné místo** chyba nebo slabina v návrhu, implementaci nebo provozu systému, která může být využita pro narušení bezpečnosti systému. **Kategorie zranitelných míst podle vzniku**:

- při návrhu (chyba architektury);
- při implementaci (např. chyba ve zdrojovém kódu);
- při provozu (např. nedodržení metodologií).

Detailněji je **hrozba** je taková vlastnost prostředí, která může způsobit narušení bezpečnosti, pokud dostane příležitost. **Hrozby lze kategorizovat** následovně:

- **neúmyslné** (živelné události, poruchy zařízení, selhání osob);
- **úmyslné** (algoritmické), kdy:
    - cílem NEJSOU data (krádež HW, úmyslné poškození nebo zničení);
    - cílem JSOU data (neoprávněná manipulace s daty, krádež SW;
    - škodlivé programy (viry, červy, logické bomby, trójské koně)

Malware - Škodlivý software“– Software, který je v počítačovém systému a provádí neautorizované činnosti, zpravidla bez vědomí nebo souhlasu uživatele. Jsou to například Viry, Trojské koně, Červi, Logické bomby, Žertovné programy

- **Virus** - “…program který vytváří kopie sama sebe tak, aby ‘infikoval’ části operačního systému nebo aplikačních programů.” Provadi replikace medzi soubory, z disku na disk. Podmienky jeho sirenia su: siroka populacia pocitacov s rovnakym OS, dalej neexistencia systemu pristupovych prav a rozvinuta vymena programov v spustitelnom tvare. Virus typicky vyzaduje hostitelsky program, ktory musi byt spusteny. Moze robit destruktivnu cinnost. Existuju *boot sector viry, suborovy infektor, makroviry, skriptovacie viry a multiparitne* ktore su kombinaciou predoslych.
- **Červ** - Samostatný program. Nepotřebuje hostitelský program. Replikuje se ze systému na systém. Infikuje systémy, ne soubory. Typicky se šíří počítačovou sítí.
- **Trojsky kon** - Program, který úmyslně provádí nějakou skrytou činnost (Krádež hesel, Mazání souborů, Vytváření zadních vrátek, Připojování přes síť k jiným počítačům). Neprovádí replikaci. (Netbus, BackOrifice, Subseven).
- **Logicka bomba** - Nereplikuje se. Část kódu, která se aktivuje na základě splnění naprogramované podmínky. Typicky provádí nějakou destrukční činnost. Příklad – Program zničí data, jakmile jeho autor zmizí z výplatní listiny.
- **Specificky internetové typy malware**
    - *JAVA* – Stažený kód interpretovaný na klientském počítači. Ochrana pomocí „pískoviště“ – Sandbox
    - *ActiveX* – Nativní spustitelný kód, stažený z internetu. Může provádět cokoli (žádné pískoviště). Ochrana podepisováním.

Techniky skryvania:

- *Spoofing/Stealth* – Filtrace volání operačního systému tak, aby program byl neviditelný (rootkit)
- *Šifrování* – Šifrování kódu programu
- *Polymorfismus* – Způsobí, že virus vypadá po každé replikaci zcela jinak. Mutační stroje.

Netradiční typy malware

- *Spam* - Hromadná nevyžádaná pošta. Nekalé obchodní praktiky – Direct mail. Podvodné zvyšování provozu webu. Uměle vygenerované odkazy na web. Pro podvody. Phishing. Krádež identity. Získávání hesel a jiných autentizačních informací.
- *Phishing*- Nalákání na podvodný web.
- *Spyware*- Software který: Sbírá osobní informace. Bez vědomí uživatele. Zaznamenávání kláves – Keyloggery.
- *Boty* – Vyuzitie: „Keystroke loggers" pro získávání hesel a čísel kreditních karet. Útoky DDOS (Distributed Denial of Service) – Proti významným serverům. Přeposílání spamu: 70-80% veškerého spamu. Warez. Zásoba pro budoucí využití.
- *Root Kity* - Rootkit je softwarový balík určený k tomu, aby vytvořil, utajil a spravoval prostředí pro útočníka na kompromitovaném stroji.
    - Binary rootkits – Modifikace systémových souborů
    - Kernel rootkits – Modifikace komponent kernelu
    - Library rootkits – Přepisují systémové knihovny

  Cíle: Správa přístupu útočníka » Vytvoří zadní vrátka (backdoor) a udržuje je, poslouchá na portu a čeká na příkazy (UDP listener). Bez poslouchání na portu (sniffer) pro snížení možnosti odhalení. Správa lokálního přístupu. Práva roota. Ochrana před jinými rootkity. Lividace důkazů. **Skrývání**:

  Zmodifikovaných souborů
  Procesů útočníka
  Používaných síťových připojení

2. Funkce prosazující bezpečnost (řízení přístupu, autentizace, skryté kanály, audit, přenos dat).

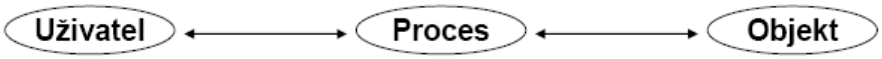
Základním účelem bezpečnostních funkcí BF je zajištění CIA (Confidentality, Integrity, Availability) + účtovatelnosti (identifikace a monitorování důležitých událostí.

Mezi další účely BF může patřit:

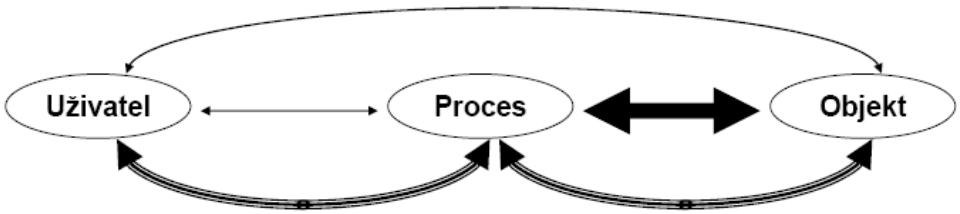
- autentizace vs. anonymita (není možné zjistit, kdo akci provedl) / pseudonymita (provádění akce pod bezpečným pseudonymem);
- audit vs. nemožnost sledování.

Riadenie pristupu

-zarucuje dovernost a integritu.



- **nepovinné řízení přístupu:**
  - uživatel, proces a objekt dostávají identifikaci
  - přístupová práva k objektu může měnit běžný uživatel (vlastník) – UNIX
  - v rámci systému lze použít pouze jeden stupeň utajení
- **povinné řízení přístupu**
  - uživatel, proces a objekt mají bezpečnostní atributy <stupeň utajení, kategorie>
  - běžný uživatel nemůže měnit atributy a ani přístupová práva
  - atributy a přístupová práva
    - administrativně určuje správce
    - se nastavují automaticky tak, aby odpovídaly bezpečnostní politice (viz modely bezpečnosti)
  - lze použít více stupňů utajeni



- **minimální** – k některým objektům je možno přistupovat pouze pomocí privilegovaných procesů
- **základní** – uživatel má práva k procesům a objektům (UNIX)
- **vyšší** – přístup na základě kombinace uživatel/proces/objekt (seznam přístupových práv)

Skryté kanály

Zarucuju dovernost.

předávání informace v rozporu s bezpečnostní politikou.

- šířka pásma skrytého kanálu
- paměťové skryté kanály
  - existence / neexistence souboru

    - atributy souboru
    - délka souboru
    - stav sdílených prostředků (V/V zařízení)
    - NIKOLI obsah souboru - v tom zabrání
- časové skryté kanály
    - zatížení procesoru
    - zatížení V/V zařízení
- kombinované
    - směr pohybu diskové hlavy...

Opětné použití objektů

Zarucuju dovernost.

- objekt přidělený procesu
    - nesmí obsahovat žádné informace od předchozího vlastníka
    - nesmí mít žádné autorizace zbylé od předchozího vlastníka
- mechanismy
    - fyzické zničení objektu
    - mazání obsahu objektu
    - šifrování obsahu objektu
- hrozby
    - sbírání smetí (scavenging)

DVB

Zarucuje integritu

- princip DVB (Důvěryhodná Výpočetní Báze) - zajišťuje schopnost systému
    - chránit sám sebe
    - spravovat chráněné objekty
- ochrana DVB
    - DVB je je schopna chránit sama sebe před vnějšími vlivy a fyzickým útokem
- nemožnost obejít DVB
    - veškerý přístup k chráněným objektům musí být prováděn přes DVB

Fyzická integrita

- evidence fyzického útoku
    - ochranné nálepky, pečetě, světlocitlivá barva
- odezva na fyzický útok
    - zničení objektu při útoku, upozornění na útok
- odolnost proti fyzickému útoku
    - útok je velmi obtížný až nemožný

Návrat (zálohování)

Zarucuje integritu.

- schopnost vrátit se k předchozímu stavu
  - po chybě uživatele
  - po fyzickém útoku
  - po zničení dat (poruchou, požárem...)
- metody
  - transakce
  - zálohování dat na nezávislá média
    - fyzické uložení záložních médií
    - interval zálohování
    - počet záložních kopií

Oddělení rolí

Zarucuje integritu.

- definice různých rolí pro různé funkce
- 1 - základní oddělení rolí
  - správce X uživatel (viz UNIX)
- 2 - oddělení rolí správců
  - více rolí správců (sezení, audit, péče o programy...)
- 3 - oddělení rolí uživatelů
  - více rolí uživatelů (ne pouze skupiny)

Autonomní testování

Zarucuje integritu.

- systém je schopen ověřit, že se nachází v bezpečném a správném stavu
  - testování funkce hardware
  - testování integrity software (kontrolní součty, kryptografické testy integrity)
    - úmyslné změny software a konfigurace - viry, trojské koně
- 1 - manuální autonomní testování
  - vyžaduje zásah člověka
- 2 - autonomní testování při inicializaci
- 3 - autonomní testování během činnosti

Přidělování prostředků

Zarucuje dostupnost.

- kontrola množství prostředků a služeb přidělovaných procesům a uživatelům
  - prostor na disku
  - čas procesoru
  - doba relace
  - počet tiskových stran
- 1 – kvóty

    - uživatelům jsou přiřazeny kvóty čerpání prostředků
- 2 - opatření proti neposkytnutí služby
    - žádný uživatel nemůže vyčerpat prostředky systému
- 3 - prioritní přidělování
    - uživatelům nebo skupinám lze přiřadit priority přidělování prostředků

Identifikace a autentizace

Zarucuje uctovatelnost.

- Identifikace - zjišťění totožnosti uživatele
- Autentizace - ověření totožnosti uživatele na základě to, že uživatel:
    - něco zná
        - heslo, PIN
    - něco vlastní
        - klíč, magnetická karta, smart karta, autentizační kalkulátor
    - někým je
        - antropometrická autentizace
        - hlas, otisk prstu, vzorek sítnice, tvar dlaně
- slabá X silná autentizace (kryptografická)
- jednosměrná X obousměrná autentizace

Audit

Zarucuje uctovatelnost.

Provádí rozpoznávání, záznam a možnost analýzy událostí významných pro bezpečnost.

- ochrana auditních dat
    - bezpečnostní správce
- fyzické uložení auditních dat
    - diskový prostor !!
- granularita auditních dat
    - podrobnost dat X objem dat
- analýza auditních dat
    - podpůrné prostředky, UI
- detekce a poplach
    - okamžitá odezva systému na události

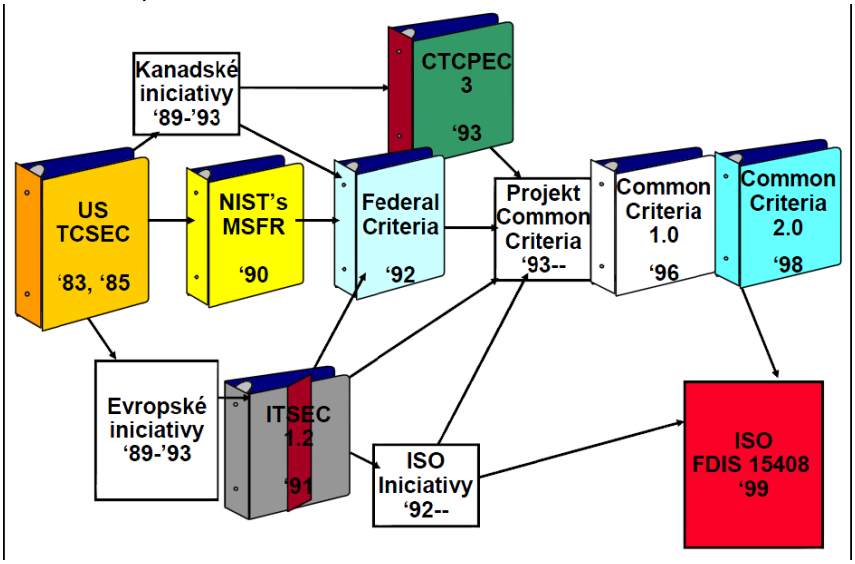
Bezpečnosť prenosu dát

Bezpečným přenosem dat se zabývá norma ISO 7498-2, ve které jsou definovány podmínky na CI + autentizaci, autorizaci a nepopiratelnost.
Bezpečný přenos tedy musí umožňovat:

- v případě spojení **autentizaci spojení** (při navazování spojení ověření prohlašované identity), v případě zasílání zpráv **autentizaci odesílatele**;
- krom důvěrnosti spojení a zasílání zpráv i **důvěrnost toku dat** (proti sbírání metainformací zpráv – časy, délky, adresáti);
- integritu spojení bez opravy a integritu zasílání zpráv;
- **nepopiratelnost odesílatele** a **nepopiratelnost doručení** (např. potvrzení u emailu).

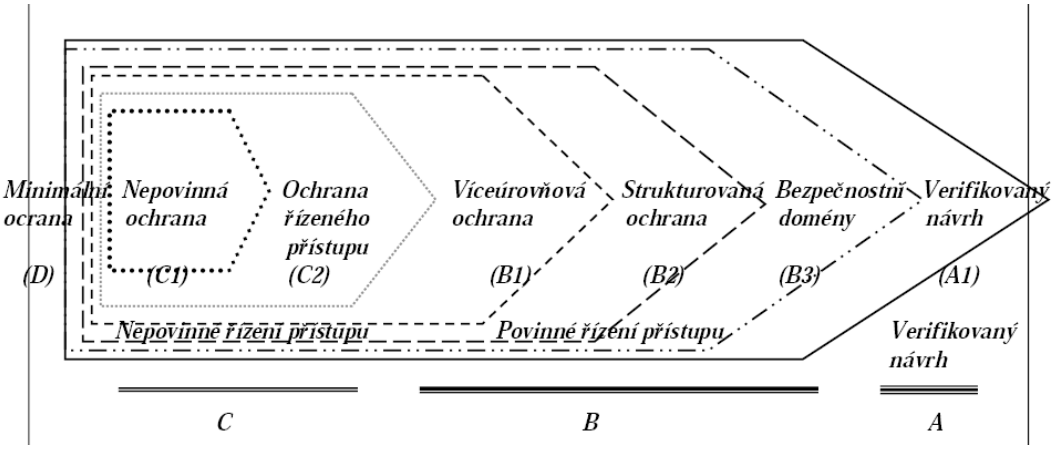
3. Kritéria hodnocení bezpečnosti informačních systémů, historie, kritéria CC (Common Criteria).

Je potřeba nějakého obecně příjmaného dokumentu, který by v sobě popisoval nejen vlastnosti bezpečného IS, ale i způsob, jak si tyto vlastnosti vykládat při inspekci již existujících IS. Slouží tedy nejen uživatelům (*„Je náš IS bezpečný?“*), ale i vývojářům (*„Jak vypadá a jak je udělán bezpečný IS?“*) a případným hodnotitelům/auditorům.



TCSEC

TCSEC (Orange book) neboli **Trusted Computer System Evaluation Criteria** je první takovouto publikací, za kterou stojí americké DoD. Je v ní zmiňována a rozebírána bezpečnostní politika, účtovatelnost, zaručitelnost, dokumentace, analýza skrytých kanálů, architektura systémů, specifikace a verifikace návrhu.



Zavádí následující **úrovně zabezpečení**:

- **C1 (nepovinná ochrana)** – počítá s nepovinným řízením přístupu a případnou identifikaci a autentizaci;
- **C2 (ochrana řízeného přístupu)** – opětovné použití a audit;
- **B1 (víceúrovňová ochrana)** – povinné řízení přístupu pro některé objekty, neformální model bezpečnostní politiky;

- **B2 (strukturovaná ochrana)** – důvěryhodná cesta pro přihlášení, princip nejmenších privilegií (co není povoleno je zakázáno), formální model bezpečnostní politiky, analýza skrytých kanálů, správa konfigurace;
- **B3 (bezpečnostní domény)** – referenční monitor, omezení při vytváření kódu, požadavky na dokumentaci a testování;
- **A1 (verifikovaný návrh)** – formální metody pro analýzu a verifikaci, důvěryhodná distribuce.

Neoficiální pohled na předchozí úrovně:

- C1, C2 - prosté vylepšení existujících systémů, které neohrožuje aplikace;
- B1 – závažnější rozšíření existujících systémů (především MAC), některé aplikace vyžadují úpravy;
- B2 – zásadní změny oproti stávajícím systémům, většina aplikací beze změn nebude fungovat;
- B3 – typicky systémy, které nedosáhly na úroveň A1;
- A1 – systém musí být navržen a implementován od základu, nutné využití netradičních metod.

Mezi nedostatky TCSEC patří, že směšuje v jednom dokumentu různé úrovně abstrakce, málo se zabývá integritou dat a neřeší komunikaci a počítačovou síť. Nerozlišuje funkčnost (*„Co je implementováno?“*) a zaručitelnost (*„Je to implementováno správně?“*).

ITSEC

IT Security Evaluation Criteria. Evropská klika zhodnocovacích kritérií vytvořena z národních norem Anglie, Německa, Francie a Holandska. Založena na systematickém a dokumentovaném přístupu k zhodnocení. Rozlišuje produkty a systémy. Oproti TCSECu vnímá rozdíl mezi funkčností a zaručitelností.
Zavádí **třídy funkčnosti**:

- kompatibilní F-C1, F-C2, F-B1, F-B2, F-B3 – které odpovídají úrovním TCSEC;
- zvýšené nároky F-IN, F-AV, F-DI, F-DC – pro systémy s většími požadavky na určitou doménu funkčnosti (dostupnosti, integrita, spolehlivost datového přenosu).

Zaručitelnost je členěna do šesti kategorií:

- E1 – jsou definovány bezpečnostní cíle, má neformální popis architektury;
- E2 – neformální popis návrhu, kontrola nad konfigurací, distribuční kontrola;
- E3 – korespondence mezi kódem a bezpečnostním cílem;
- E4 – formální model bezpečnostní politiky, strukturovaný přístup k designu, analýza zranitelností vyplývajících z návrhu;
- E5 – korespondence mezi návrhem a kódem, analýza zranitelnosti zdrojového kódu;
- E6 – formální metody architektury a mapování návrhu na bezpečnostní politiku.

Sílu bezpečnostních mechanismů kategorizujeme jako:

- **základní** – mechanismus chrání proti náhodným poruchám, avšak může být narušen kvalifikovanými útočníky;
- **střední** – mechanismus chrání proti útočníkům s omezenými příležitostmi a prostředky;
- **vysokou** – mechanismus může být narušen pouze útočníkem, disponujícím vysokou úrovni znalostí, příležitostmi a prostředky, útok se zkrátka vymyká běžné praxi.

Síla mechanismů se dotýká znalostí (míru vědění, kterou musí osoba mít, aby byla schopna zaútočit), prostředků (objem vynaložených prostředků k úspěšnému útoku – čas, vybavení) a příležitostí (faktory, které obecně není schopen útočník ovlivnit – kooperace s jinou osobou, pravděpodobnost výskytu specifických okolností). **Komplotem** rozumíme druh příležitosti, kdy je požadavek na asistenci jiné osoby, lze ho dělit na samostatný (bez asistence), s asistencí uživatele, s asistencí správce.

	Samostatný	S uživatelom	So správcom
V minutách	0	12	24
V dňoch	5	12	24
V mesiacoch	16	16	24
	Bez vybavenia	Bezne vybavenie	Specialne vybavenie
Zaciatocnik	1	-	-
Skuseny	4	4	-
Expert	6	8	12

Sečteme-li faktory z tabulky času/komplotu a znalosti/vybavení, lze sílu mechanismu ohodnotit podle výsledné tabulky jako:

V=1	Sila nie je ani zakladna
1 < V < 21	Sila je zakladna
12 < V < 24	Sila je stredna
24 < V	Sila je vysoka

Kritéria CC (Common Criteria)

Common Criteria CC neboli hodnocení bezpečnosti IT podle normy ISO/IEC 15408 je mezinárodně uznaným standardem popisujícím bezpečnost nejen IS. K CC existuje i **Common Criteria Evaluation Methodology CEM**, které se zabývá způsobem evaluace kritérií naznačených v CC.

Zavádí **profily ochrany PO** pro kategorie produktů a **bezpečnostní cíle BC** pro konkrétní typy produktů.

Požadavky na funkčnost (F)** lze kategorizovat do:

- **tříd** – seskupení rodin, které jsou stejně zaměřěny (např. FCS – kryptografická podpora);
- **rodin** – seskupení komponent, které mají stejný bezpečnostní cíl ale různou sílu či příslušnost (např. FDP_ACC ve třídě ochrany uživatelských dat politika řízení přístupu)
- **komponent** – nejmenší volitelná sada prvků, která může být použita v BC nebo PO (např. FDP_ACC.1 pro řízení přístupu k podmnožinám).

Zaručitelnost podle CC se zabývá základy pro prokázání, že IT produkt nebo systém splňuje bezpečnostní cíle. Zaručitelnost je tedy ochranou proti špatnému návrhu, implementačním chybám či neefektivním opatřením a mechanismům.

CC rozlišuje následující **úrovně zaručitelnosti**:

- EAL1 – funkčně testovaný;
- EAL2 – strukturálně testovaný (odpovídá C1);
- EAL3 – metodicky testovaný a kontrolovaný (odpovídá C2);
- EAL4 – metodicky navrhovaný, testovaný a přezkoumávaný (odpovídá B1);
- EAL5 – semiformálně navrhovaný a testovaný (odpovídá B2);
- EAL6 – testovaný se semiformálně ověřeným návrhem (odpovídá B3);
- EAL7 – testovaný s formálně ověřeným návrhem (odpovídá A1).

EAL4 umožňuje svědomitému návrháři dosáhnout maximálně možné zaručitelnosti bezpečnosti, založené na dobrých metodologiích, vývojových praktikách a nepříliš velkých odborných znalostí. Je to nejvyšší úroveň pro běžně vyráběné produkty.

Stejně jako existuje hierarchie požadavků funkčnosti, existují i hierarchie **požadavků na zaručitelnost (A**)**.

Modely specifikace lze rozdělit následovně:

- **neformální** – zapsaná v přirozeném jazyce, přičemž nepodléhá žádným omezením;
- **poloformální (semiformální)** – vyžaduje užití některé omezující notace spolu s množinou konvencí, může mít buď grafickou podobu, nebo být založena na omezeném použití přirozeného jazyka.
- **formální** – zapsaná ve formální notaci, která využívá dobře definovaných matematických pojmů.

Při vývoji lze použít model bezpečnostní politiky, funkční specifikace, architektury, aj.

4. Management bezpečnosti – standardy.

Celková bezpečnostní politika (CBP)

- Globální popis cílů organizace, jejího IS a zabezpečení
- Cíl
  - ochrana majetku, pověsti a činnosti instituce
- Dokument
  - nadčasový, nezávislý na použité technologii, (horizont 5-10 let)
  - přijatý vedením organizace jako vnitroinstitucionální norma
  - závazný dokument, veřejný dokument
- Stanovuje
  - citlivé informace, ostatní citlivá aktiva a jejich klasifikaci
  - jednoznačné (hierarchické) zodpovědnosti & práva & pravomoci
  - minimální sílu použitých bezpečnostních mechanismů
- Stručný a srozumitelný, úplný dokument
  - otázky a konflikty lze vyřešit odkazem na paragrafy CBP

Systémová bezpečnostní politika (SBP)

- Systémová bezpečnostní politika
  - Definuje způsob implementace celkové bezpečnostní politiky IT v konkrétním prostředí
  - Stanovuje soubor principů a pravidel pro ochranu IS
  - Zabývá se volbou konkrétních technických, procedurálních, logických a administrativních bezpečnostních opatření
  - Částečně i volbou fyzických a personálních bezpečnostních opatření, pokud tyto mohou ovlivnit bezpečnost IS
  - Implicitně se zabývá bezpečností elektronické (počítačové) části IS
  - Pokud je IS příliš rozsáhlý a různorodý, je vhodné vypracovat samostatně systémovou bezpečnostní politiku pro různé oblasti nebo subsystémy

Tvorba bezpečnostní politiky

- BP nikdy nevzniká jednorázovou akcí
- životní cyklus tvorby BP lze zjednodušeně vyjádřit následujícími (opakovaně) prováděnými kroky
  - 1. posouzení vstupních vlivů
  - 2. analýza rizik
  - 3. vypracování BP
  - 4. implementace BP
  - 5. nasazení BP, kontrola její účinnosti a vyslovování závěrů

Normy a standardy

- TR 13335 - Guidelines for the Management of IT Security
  - ČSN ISO/IEC TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti IT 1-3

- BS7799 - Code of Practice for Information Security Management
    - ČSN ISO/IEC 17799 Informační technologie – Soubor postupů pro řízení informační bezpečnosti
- ISO 27001
    - nová mezinárodní norma pro Systém správy informační bezpečnosti (Information Security Management System, ISMS)

Modely bezpečnosti

Formální vyjádření části bezpečnostní politiky

- podle řízení přístupu
    - povinné řízení přístupu
    - nepovinné řízení přístupu
- podle klasifikace informace
    - jednoúrovňové X víceúrovňové
- podle cílů, které zajišťují
    - modely důvěrnosti
    - modely integrity
    - modely dostupnosti
- entity
    - uživatel, proces, objekt, subjekt

Monitor

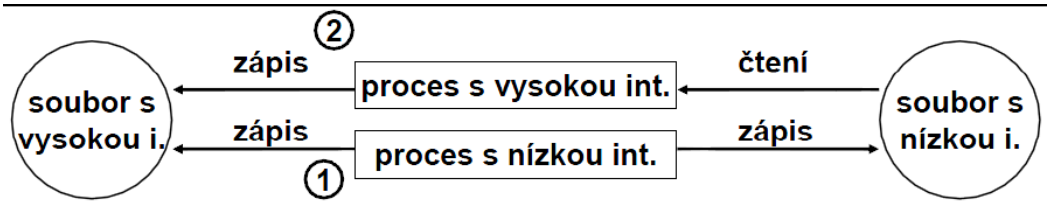
je prostředkem pro lokalizaci bezpečnostních funkcí do jednoho místa. Mezi požadavky na monitor patří, že je neobejitelný, že je odolný proti útoku (je schopen zajistit si integritu) a je dostatečně malý, aby mohl být podroben analýze správnosti.

Bell-LaPadulův model důvěrnosti:

- ohodnocení – stupeň důvěry v subjekt C(s) a úroveň důvěrnosti objektu C(o);
- ochrana ① – subjekt s může číst objekt o, pokud $C(s) \geq C(o)$;
- omezení ② – pokud subjekt s může číst objekt o, pak může modifikovat objekt p, když $C(p) \geq C(o)$, čímž je zaručeno, že neprozradí, co nemá;

Bibův model integrity:

- ohodnocení – stupeň integrity subjektu *I*(*s*) a úroveň integrity objektu *I*(*o*);
- ochrana ① – subjekt *s* může modifikovat objekt *o*, pokud $I(s) \geq I(o)$;
- omezení ②– pokud subjekt *s* může číst objekt *o*, pak může modifikovat objekt *p*, když $I(o) \geq I(p)$, čímž je zaručeno, že nepokazí takový objekt;



Modely dostupnosti

- Systém kvót
  - každý uživatel má omezeno množství prostředků, které mu lze přidělit
    - prostor na disku, prostor v paměti, čas procesoru, délka relace, počet tiskových stran....
- Amorosův model
  - každý uživatel má prioritu p a prostředek kritičnost c
  - funkce prevent(p,c) říká, zda se má prostředek uživateli poskytnout
- Yu-Gligorův model
  - spravedlnost - uživatel nebude blokován navždy, pokud je možnost, aby pokračoval
  - simultánnost - uživatel někdy dostane všechny možnosti, jak pokračovat
  - dohoda uživatelů - současné požadavky uživatelů na službu jsou uspořádány podle analýzy všech ostatních požadavků.

5. Analýza rizik (vstupy, výstupy, jednotlivé generace).

Proces analýzy rizik

- Identifikace aktiv
- Stanovení zranitelných míst a hrozeb
- Stanovení rizik
- Výpočet očekávané roční ztráty (ALE, Annual Loss Expectations)
- Volba bezpečnostních opatření
- Určení ročních úspor

Výpočet ALE

- Riziko
  - škodlivý efekt uskutečnění hrozby
  - škodlivý efekt využití zranitelného místa
- Riziko závisí na :
  - P - pravděpodobnost výskytu bezpečnostního incidentu (např. V jednotkách výskytů za rok)
  - C - průměrná škoda vzniklá tímto incidentem
- Riziko se vypočte jako R = P . C

1. Generace

- Vlastnosti metod první generace
- Předpoklady:
  - oblast možných řešení je silně omezena
  - každé z řešení je značně univerzální
  - vliv bezpečnostních opatření je vyjádřen jako snížení pravděpodobnosti výskytu hrozby nebo snížení vlivu hrozby

VULAN

- Oblast zranitelnosti
- Míra příležitosti útočníka
- Míra znalostí útočníka
- Čas potřebný pro útok
- Vybavení potřebné pro útok

Výsledkem je zjištěná míra zranitelnosti komponenty.

2. Generace

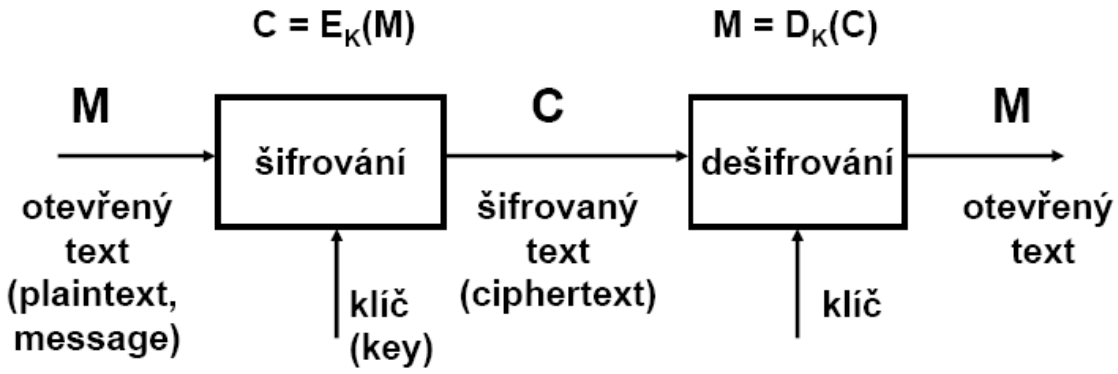
- Mechanistické inženýrské metody
- Vlastnosti:
  - zobrazují problém do velkého množství částečných řešení
- Vývojové prostředky:
  - návrh shora dolů
- Bezpečnostní prostředky:
  - Zjišťují odděleně:
    - Aktiva
    - Hrozby
    - Zranitelná místa

3. Generace

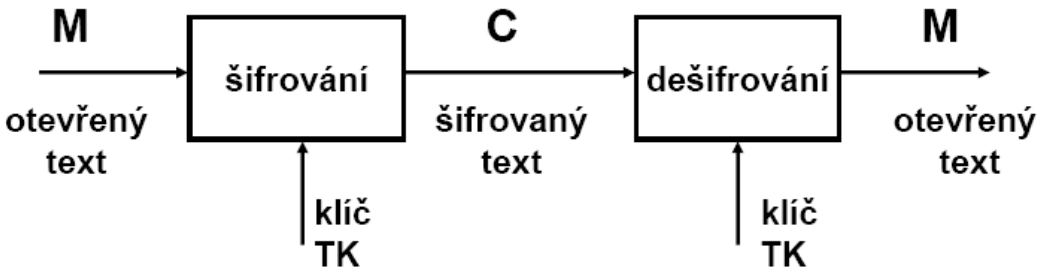
- Logicko-transformační metody
- Vychází z toho, že model pro analýzu rizik musí znat nejenom strukturu systému, ale i jeho funkčnost
- Např. SSADM-CRAMM

6. Bezpečnost přenosu dat (symetrická a asymetrická kryptografie, algoritmy, režimy blokových šifer).

Kryptografie:



Symetrický algoritmus



S tajným klíčem

- Uživatelé se dohodnou na stejném tajném klíči
- Sdílené tajemství
- Útoky (COA, KPA)
- „Bezpečný algoritmus“
- Útok silou
- Zarucuje D, A, I. N nie, pretoze nemozem pred tretou stranou dokazat ze som spravu poslal ja alebo ten druhy.

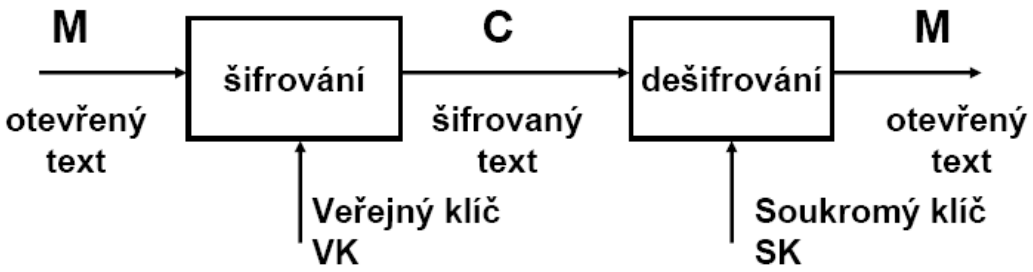
Symetrické algoritmy

- DES – 56 bit
- 3DES – 112 bit
- IDEA – 128-bit keys, PGP used in early versions
- RC2 – “Ron’s code” (Ron Rivest), variable size key
- RC5 – variable size key

- Skipjack – 80-bit key, 32 rounds, NSA initially classified
- AES – variable size key

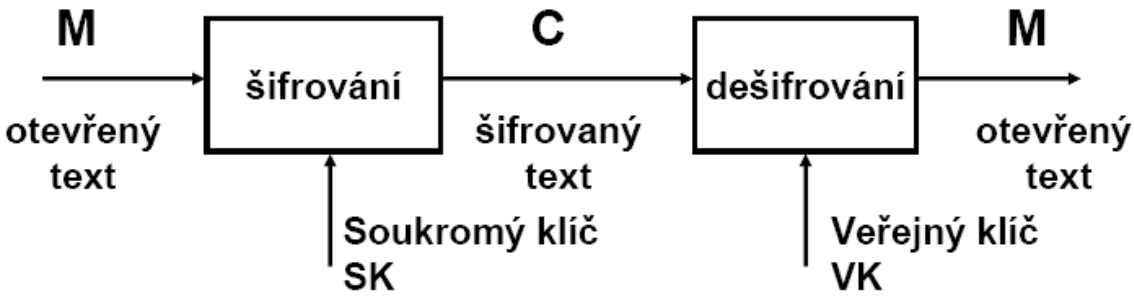
Asymetrický algoritmus

1 Možnosť:



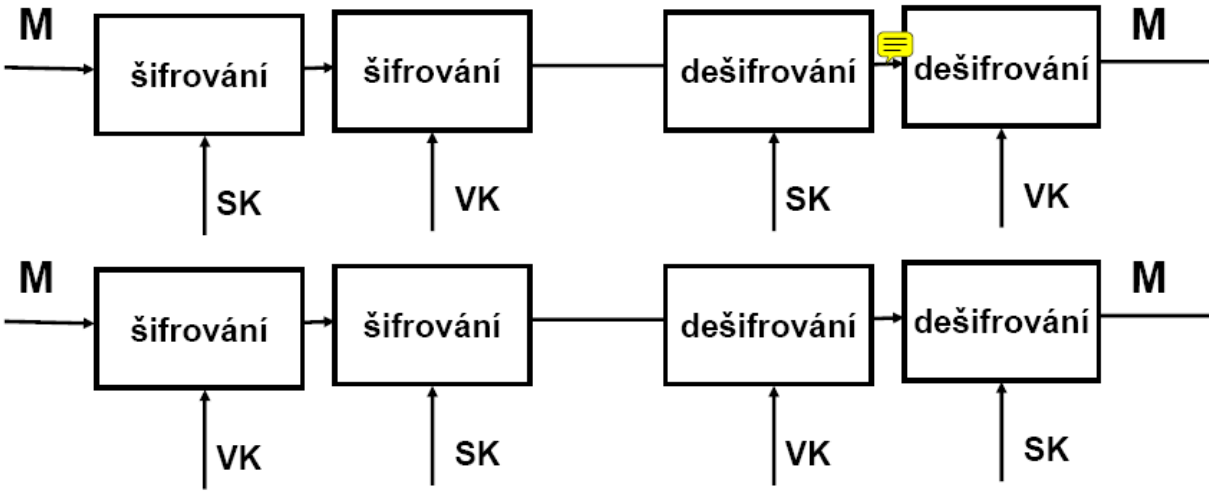
Uživatel tají soukromý klíč, zveřejní veřejný klíč. **Duvernost** – ANO, **Autentizacia** – NIE (pretoze ktokolvek moze poslat zasifrovanu spravu verejnym klucom), **Integrita** – NIE (je mozne zahodit original spravu a vytvorit vlastnu a podvrhnut ju), **Nepopieratelnost** – NIE

2 Možnosť



- Uživatel tají soukromý klíč, zveřejní veřejný klíč
- Elektronický podpis
- **Dovernost** – NIE (ktokolvek 17it u spravu desifruje), **Autentizacia** – ANO (odosielatel je len jeden) **Integrita** – ANO (Iba odosielatel ju moze vyrobit), **Nepopieratelnost** – ANO (existuje len JEDEN sukromny kluc – cize sa nemoze vzdat zodpovednosti za zaslanu spravu)

3 Možnosť



Zaručuje všetky 4. 99% pripadov sa pouziva prva varianta pretoze je tam priestor pre archivaciu aby som sa dostal k sprave aj ked stratim SK (tam kde je ta zlta bublina).

Hašovací funkce

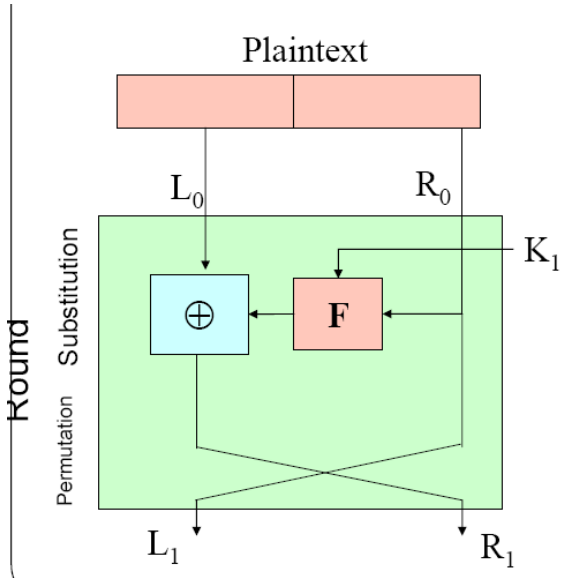
- Hašovací funkce, charakteristika zprávy, jednocestná funkce, message digest, digest, hash, hash function, one way function
- je to funkce F taková, že
  - je aplikovatelná na argument libovolné velikosti
  - její výstupní hodnota má konstantní délku (zpravidla 128, 160 nebo 256 bitů)
  - lze rychle spočíst F(x)
  - pro dané y je výpočetně nezvládnutelné nalézt takové x, aby platilo F(x)=y (first preimage resistance)
  - pro dané x je výpočetně nezvládnutelné nalézt takové x'<>x, aby platilo F(x')=F(x) (second preimage resistance)
  - je výpočetně nezvládnutelné nalézt takové x' a x, x'<>x, aby platilo F(x')=F(x) (collision resistance)
- implementace
  - MD2, MD4, MD5
  - SHS (Secure Hash Standard), SHA

Bloková šifra

- 64 bitové bloky dat (nyní 128 až 256)
- 264 možných bloků otevřeného textu, alespoň 264 odpovídajících bloků zašifrovaného textu
  - Existuje 264! možných zobrazení
- Proč nevytvořit náhodné zobrazení?
  - Byla by třeba 264 * 64-bitová tabulka ≈ 1021 bitů
  - $14 quadrillion
  - Přenos klíče znamená přenos nové tabulky
- Ideální náhodné zobrazení aproximujeme pomocí několika komponent, řízených hodnotou klíče

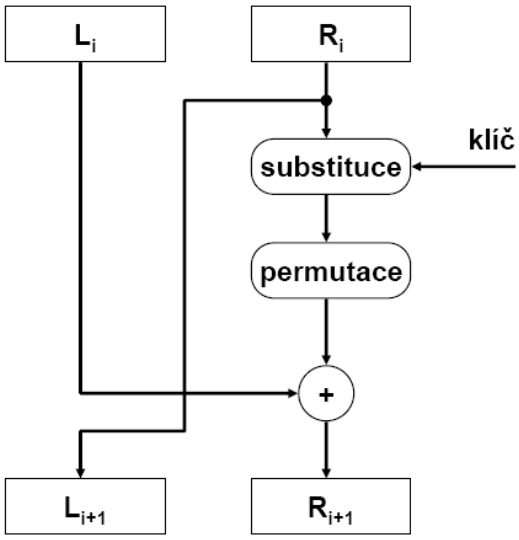
Feistelova šifra

- Základ některých symetrických šifer
  - Horst Feistel pracoval pro IBM v roce 1973
  - IBM's Lucifer algoritmus, založený na Feistelově principu,byl základem pro algpritmus DES v roce 1977
- Mnoho jiných algoritmů používá Feistelův princip
- Mimo Feistelův princip jsou však i jiné iterativní principy



Algoritmus DES

- vyvinut IBM v r. 1976 na zakázku NBS (nyní NIST)
- Na základě algoritmu Lucifer od IBM
- Modifikován NSA
  - Změna S-Boxů
  - Redukovaná délka klíče ze 128 na 56 bitů
- Přijat jako standard v r. 1976
- Zašifroval nejvíce bitů ze všech algoritmů
- NBS - National Bureau of Standards
- Požadavky na DES
  - musí zajišťovat vysokou bezpečnost
  - musí být přesně specifikovaný
  - bezpečnost nesmí záviset na utajení algoritmu
  - musí být realizovatelný pomocí hardware
  - musí být rychlý
- symetrický šifrovací algoritmus tajným klíčem
- šifruje bloky dat o šířce 64 bitů klíčem o velikosti 56 bitů
- Feistelova šifra s dodatečnou počáteční permutací IP
- Komplikovaná funkce F
- 16 kol
- 56-bitový klíč, posuvy a permutace vytvářejí 48-bitové subklíče pro každé kolo



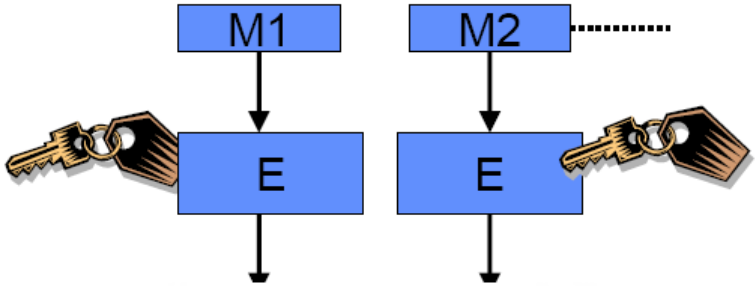
DES - slabiny a pochybnosti

- Velikost bloku a klíče
  - Je více bloků než klíčů
  - Pro jeden blok 264 zpráv > 256 klíčů
  - Zašifrovaný konstantí blok nemůže nabýt všech 264 možných hodnot
- 56-bitový klíč je příliš krátký
  - vedou se úvahy o případné úspěšnosti útoku silou
- Komplementární klíče
- Mezi klíči existují tzv. slabé klíče
- při generování klíče je třeba kontrolovat, zda nejde o slabý nebo poloslabý klíč
- Návrh S-boxů nebyl zveřejněn - možnost “zadních vrátek”
- pokud by S-boxy byly nějakou lineární funkcí, autor S-boxů může snadno šifru rozbít
- Není zcela jasné, zda 16 cyklů je postačující pro bezpečné zašifrování
- Utok silou

Režimy blokových šifer

ECB (Electronic Code Book)

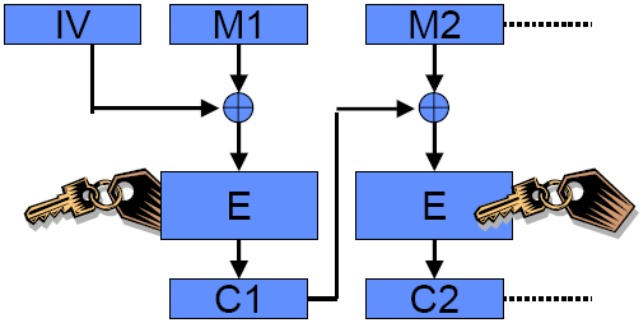
- vezmem sifrovanu spravu, rozsekam ju na bloky, kazdy enzavisle zasifrujem a vysledky poskladam do vyslednej spravy.



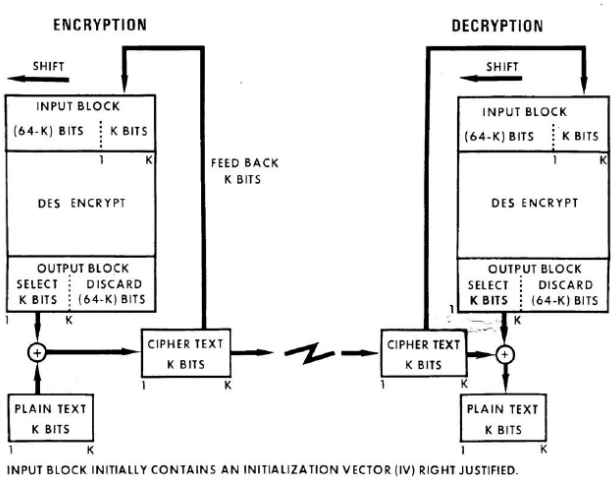
Umožňuje slovníkové útoky, repetíciu blokov, preskladanie blokov.

Cipher Block Chaining (CBC)

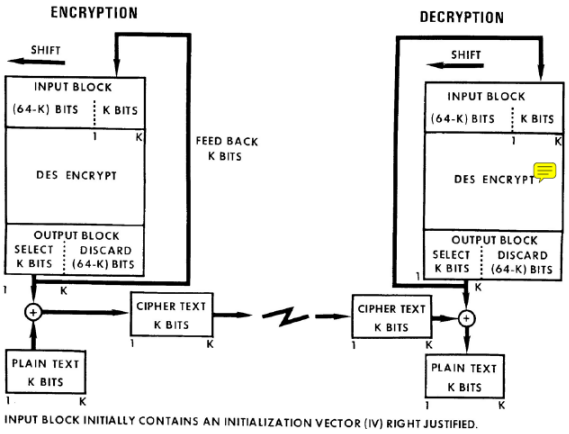
- spravu rozsekam na bloky, kazdy blok zifrujem oddelene ale pred tym ako ho zasifrujem tak ho “zorujem” zasifrovanou hodnotou predchodzieho bloku (prvy sa sifruje nejakou inicializacnou hodnotou) - nejde manipulovat s blokmi..



Cipher Feedback (CFB)



Output Feedback (OFB)



3DES, DES-EDE

- Velikost klice 112 bitů
- Velikost bloku 64 bitů
- ANSI X9.17, ISO 8732 standard
- Double DES není bezpečný
    - CPA útok Merkle-Hellman meet-in-the-middle - 2n+1 pokusů

International Data Encryption Algorithm (IDEA)

- Šifruje 64-bitové bloky pomocí 128-bitového klíče
- Podobně jako DES:
    - Pracuje v kolech (rounds)
    - Operace je stejná pro šifrování i dešifrování
- Od DESu se liší:
    - Navržena, aby byla efektivní v software
    - Nepoužívá S-boxy a P-boxy

AES: The Next Generation

- Advanced Encryption Standard (FIPS PUB 197)
    - Má odstranit nedostatky DES
    - Založený na algoritmu Rijndael algorithm
        - Joan Daemen and Vincent Rijmen, Belgie
    - U. S. od Nov. 26, 2001, platný od May 26, 2002
    - Délky klíčů 128, 192 a 256 bitů
    - Velikost bloku 128 bitů
        - Platí pro AES, Rijndael dovoluje i jiné velikosti
- Délky klíčů a počet kol
    - AES-128 – 10 kol
    - AES-192 – 12 kol
    - AES-256 – 14 kol

Asymetrické algoritmy

- Knapsack
    - Knapsack – první algoritmus, Merkle-Hellman, 1976
- Faktorizace čísel
    - RSA
    - Diffie-Hellman
- Diskrétní logaritmus
    - DSS (DSA)
    - El Gamal
- Eliptické křivky
    - Např. ECDSA

Algoritmus RSA

- Rivest, Shamir, Adelman 1978

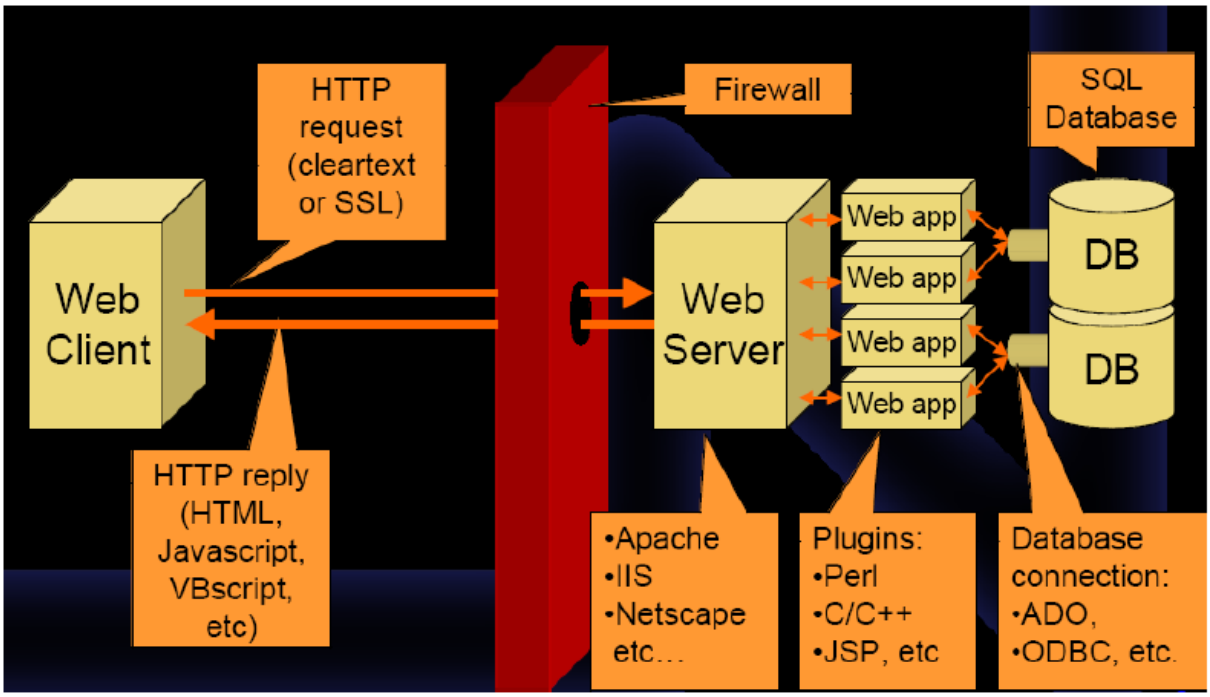
    - Údajně objeven už v GCHQ (Ellis a Cocks) v roce 1973
- Asymetrický šifrovací algoritmus s veřejným klíčem
- Založený na problému faktorizace velkých čísel
- Funguje jako bloková šifra, kde blok je celé číslo mezi 0 a n
- Klíče
    - n: veřejný modulus
    - e: veřejný exponent (typicky 3 nebo 216+1)
    - d: soukromý exponent
    - p,q: činitele (factors) modulu n
        - $n = p \times q$
    - Musí platit vztah
        - $d \times e \bmod (p-1)(q-1) = 1$
    - Veřejný klíč je (n,e).
    - Soukromý klíč je (n,d).
    - Postup
        - Vygeneruj prvočísla p a q, n=pq
        - Spočti $\Phi(n)=(p-1)(q-1)$ (Eulerova funkcia)
        - Zvol hodnotu $e<\Phi(n)$ takovou, že $\gcd(\Phi(n),e) = 1$
        - Spočti d tak, že $d = e^{-1} \bmod \Phi(n)$
- <u>Šifrování / Dešifrování 1</u>
    - Zpráva m (celé číslo)
    - Zašifrovaný text c (celé číslo)
    - Šifrování veřejným klíčem
        - $c = me \bmod n$
    - Dešifrování soukromým klíčem
        - $m = cd \bmod n$
    - Použití
        - Utajení
- <u>Šifrování / Dešifrování 2</u>
    - Zpráva m (celé číslo)
    - Zašifrovaný text s (signature)
    - Šifrování soukromým klíčem
        - $s = md \bmod n$
    - Dešifrování veřejným klíčem
        - $m = se \bmod n$
    - Použití
        - Elektronický podpis

Digital Signature Algorithm (DSA)

- Navržen NISTem v r. 1991 jako standard (DSS)
- Založen na diskrétních logaritmech
- Má některé nevýhody
    - Nedá se použít pro šifrování nebo distribuci klíčů
    - Rychlejší než RSA při podpisu ale pomalejší při verifikaci
    - Přichází v době, kdy už je značně rozšířeno RSA
    - Obavy, zda neobsahuje zadní vrátka od NIST
- Velikost klíče původně 512 bitů, později zvětšena na 1024 bitů

7. Bezpečnost webových aplikací, typické útoky.

Typická webová aplikácia:

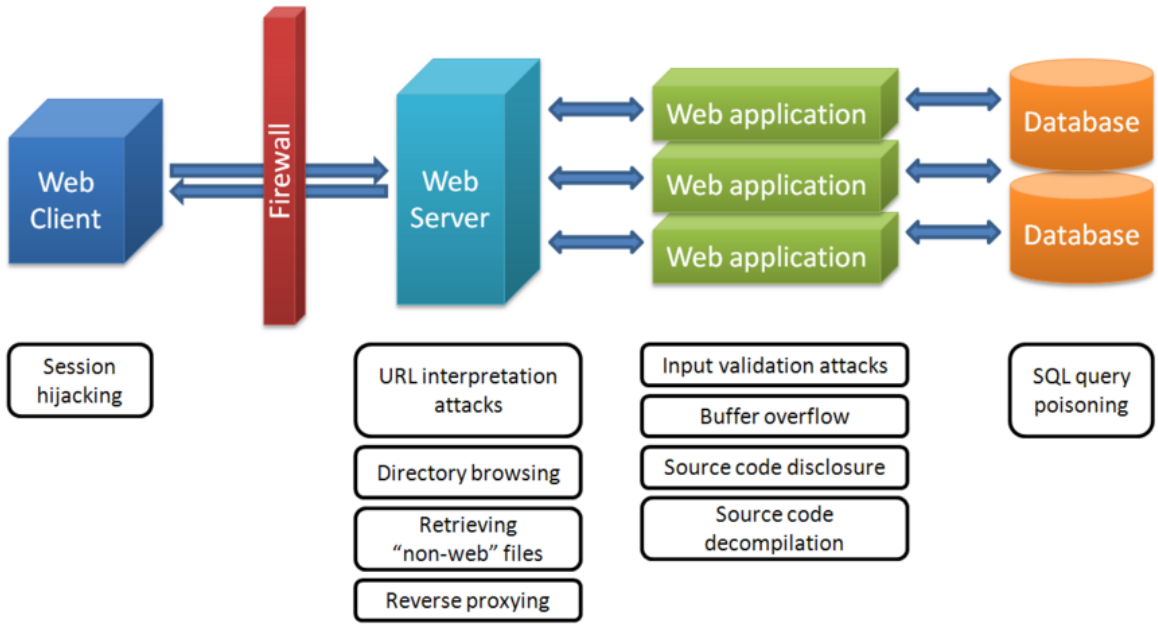


Ciele útočníka

- Cesy, Databázová štruktúra, programovací jazyk, databázový systém a pod.
- Zdrojové kódy
- Data

Typy útokov

- URL interpretation attacks
- Input validation attacks
- SQL injection attacks
- Impersonation attacks
- Buffer Overflow attacks



URL Misinterpretation.

Webový server nezvládne zparsovať URL dobre (unicode).

Protiopatrenia:

- Fix od dodávateľa
- Inšpekcia konfigurácie web servera

Directory Browsing

- Získanie celej adresárovej štruktúry
- Zvyčajne keď neexistuje súbor „index“

Protiopatrenia:

- Web server config lock-down
- Zakázať vypisovanie adresárovej štruktúry

Získavane newebových súborov

- .zip, backup súbory a pod
- Skúšať /2005/? Alebo /January/?

Protiopatrenia:

- Zbaviť sa súborov, ktoré nie sú potrebné

Odhalenie zdrojových súborov

- Na základe zrojákov je možné zistiť iné chyby

Input Validation

- Všetky inputy musia byť validované

SQL Query poisoning

- Parametre zo vstupu sú použité v SQL dotaze
- Je možné prenášať aj cez URL: http://10.0.0.1/index.php?item=3+or+1=1
- Možné spustenie procedúr

Session hijacking

Ide o získanie validnej session, aby sa útočník mohol pomocou nej dostať k informáciám.

Protiopatrenia:

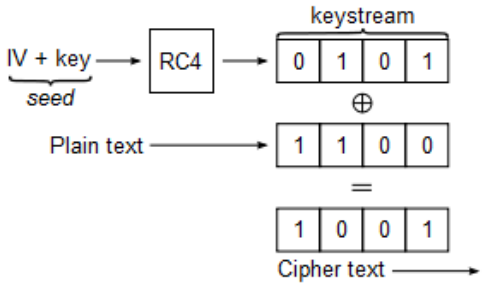
- Trakovanie ID Session na strane servera
- Časové známky, IP Adresy..
- Kryptografické Session ID

8. Bezpečnost bezdrátových sítí, útoky, způsoby kryptografického zabezpečení.

- WiFi, WiMax, Bluetooth, RFID, others, ..
- WLAN - 802.11 (WiFi)
- WMAN - 802.16 (WiMax)

WEP

- Wired Equivalent Privacy
- WEP – 40, WEP – 104 (veľkosti kľúča), inicializačné vektory 12b a 24b.
- Používa šifru RC4 – stream cipher
- Na kontrolu využíva CRC



Autentizácia pomocou zdieľaného kĺúča:

- Klient pošle *Auth. Request* na AP (Access Point). Ten pošle *plain challange* (nejaký čistý text). Klient ho zašifruje zdieľaným kľúčom a pošle to späť. AP si to dešifruje a porovná. Ak sa rovnajú pošle *Accept*, inak *Reject*.

Problémy WEP

- Znovu použitie Inicializačného Vektora
- Kľúč sa mení veľmi zriedkavo
- CRC – možnosť zmeniť správu

WPA

- WiFi Protected Access
- Od 802.11i
- RC4
- 128b kľúč, 48b IV
- TKIP
    - Temporal Key Integrity Protocol
    - Dynamická zmena kľúča každým paketom
    - sériové číslo paketov (Proti útoku Replay)
- CRC nahradené MIC
    - Message integrity code
    - Výpočet algoritmom Michael

- Ak 2 framy neuspejú pri kontrole identity, sieť sa reštartuje a generujú sa nové kľúče

WPA2

- CCMP – založené na blokovej šifre AES
- Povinné pre všetky WiFi-certified zariadenia

802.1x

- Autentizácia založená na tzv. portoch
- 3 porty/entity
  - Supplicant – klient, ktorý sa chce pripojiť
  - Authenticator – AP, ktorý pripája Supplicanta
  - Authentication Server (RADIUS) – Vykonáva autentizačný proces na základe informácií od Supplicanta.
- Kroky autentizácie
  - Port je nastavený len na komunikáciu 802.1x – neautorizovaný stav
  - Keď sa klient pripojí, authenticator mu pošle *EAP – Request*
  - Supplicant odpovie *EAP – Response*
  - Authenticator to prepošle na Authentication Server
  - Ak prijme, port sa zmení na autorizovaný a je povolený traffic
  - Ak sa Supplicant odhlási, pošle *EAP – logoff* a port sa nastaví späť na nautorizovaný.

EAP

- Extensible authentication protocol
- Definuje formát správ
- EAPOL – EAP over the LAN

RADIUS

- Remote Authentication Dial In User Service
- AAA služby – Autentizácia, Autorizácia, Accounting (účtovanie)
- Klient/server architektúra
- Klient
  - AP
  - VPN Server
  - Network switch

Hrozby

MAC Filtering a MAC Spoofing

Ak mám zabezpečenie filtrovaním MAC adries, je možné ju odchytiť a pripájať sa na základe tejto MAC adresy

Man-in-the-middle

Útočník prinúti klienta pripojiť sa na svoj Soft AP, ktorý ma pripojený na reálny AP a tak odpočúvať jeho komunikáciu.

Denial of Service

Bobmardovanie AP požiadavkami s cieľom zhodiť sieť.

Caffe Latte

- Útočí na Windows wireless stack
- Je ním možné preraziť WEP
- Používa na to záplavu ARP požiadaviek