24. Ochrana a zabezpečení dat

Zdroje chyb

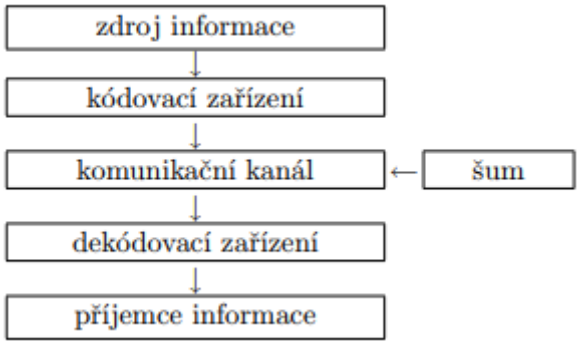
```
Výčet zdrojů chyb:
  - Porucha HW/SW
  - Přírodní katastrofy(Požár,Voda,Výpad elektřiny)
  - Neoprávněný přístup
Pokud se jedná o softwarovou chybu můžou být zdrojem:
  - Syntaxe
  - Sémantická (nekonečný cyklus, spadne, špatný výsledek)
  - Neočekávaná událost(Program neumí vhodně zareágovat na nečekanou
událost)

Následky softwárových chyb Mohou mít dominový efekt s různými následky pro
uživatele.
Některé chyby mají na funkčnost minimální vliv a proto jsou neobjeveny.
Vážnejší mohou vést k zamrznutí programu a následné ztrátě dat.
```

Zabezpečení dat před chybami pomocí kódování

Kódování dat

```
Teorie kódování se zabývá tím, jak rychle a spolehlivě přenášet informace
z jednoho místa na druhé. Mezi její aplikace patří například minimalizace
šumu při přehrávání kompaktních disků, přenos finančních informací po
telefonních linkách, přenos informací mezi dvěma počítači, mezi pevným
diskem
a operační pamětí v jednom počítači.
```




```
Schéma samoopravného kódování
Konstrukce kódovacího a dekódovacího zařízení sleduje několik cílů:
1. rychlé kódování informace,
2. snadný přenos zakódované zprávy,
3. rychlé dekódování přijaté zprávy,
4. opravu chyb způsobených šumem v kanálu během přenosu zprávy,
5. maximalizaci množství informace přenesené za jednotku času.
```

Komprimace dat

Hlavním úkolem při komprimaci (balení) dat je zmenšení objemu dat před jejich uložením nebo přenosem. Dosahuje se toho různými komprimačními postupy. Většinou jsou vyhledány často se vyskytující skupiny znaků a těm je přiřazen krátký binární kód, zatímco zřídka se vyskytující znaky mají přiřazen kód delší. Ve výsledku se tím celková velikost souboru zmenší. Komprimační programy však také plní další úkoly:

- spojení většího množství malých souborů do jediného souboru
- rozdělení velkého souboru na části aby se to vešlo na jedno médium
- ochrana dat heslem

Šifrování dat

Jako zabezpečení dat jsme schopni zašifrovat data za pomocí kryptografie na data šifrovaná, čitelná pouze pro majitele dešifrovacího klíče.
Šifrování dat slouží k jejich ochraně proti nežádoucímu zjištění cizí osobou a uplatňuje se při ukládání dat i při jejich přenosu včetně telekomunikace.

Šifrování souborů se šifruji pomocí zvoleného/vygenerovaného klíče nebo hesla k zašifrování jednotlivých souborů.K otevření takového souboru je potřeba klíč.Pro každodenní práci s počítačem je velmi podstatná otázka zpomalování systému.Dobrá volba je kombinace šifrování a skrytí dat.

Šifrování disků se provádí softwarem, který vštšinou firuje takzvaně Full Disk Encryption.Tato metoda šifruje celý disk včetně oddílu Master Boot Record.Uživatel se nestará, jelikož jsou všechny soubory zašifrované.

Detekce poškozených dat

Může se jednat o mechanické nebo elektronické poškozené HDD.
Vadný harddisk se například vůbec neroztočí a může být elektricky mrtvý, nebo se roztočí a pak zastaví.Další případ je také, že se normálně roztočí,ale klepe.Harddisk nemusí být detekován v BIOS.A takovéto chování poškozuje disk a plotny disku.

U poškozených dat nám můžou data při čtení nebo spuštění vychybovat a hodit hlášku o poškození dat.Buď nám operační systém data vůbec neukáže nebo ukáže atypické soubory s zvláštní příponou a neumožní data přečíst.

Každý operační systém má také registry a v těch můžou být uvedeny neplatné záznamy a operační systém provádí detekci a opravu těchto dat.

Oprava poškozených dat

Oprava poškozených dat může probíhat např. u HDD pomocí SW nástroje Testdisk.Takový to software je schopen zachránit a opravit disk, když se vyskytne chyba v GPT při řazení oddílů.

Při omylném smazání,zformátování,přesunutí dat jsme schopni použít takovýto software na obnovení, jelikož se informace jak byl soubor uložen ztratí, ale data budou přepsána až bude potřeba na jejich místo něco uložit.

Kontrolní součet

Kontrolní součet je doplňková informace, která se předává spolu s vlastní informací a slouží k ověření, zda je vlastní informace úplná a zda při jejím přenosu nedošlo k chybě.
Kontrolní součet je výsledkem nějaké předem určené operace, provedené s vlastní informací.
Prakticky používané metody tedy jako kontrolní součet používají jen menší dodatkovou informaci; jednoduchým příkladem použitelným při předávání řady čísel je součet všech čísel.
Mezi další prakticky používané metody patří například:

- Parita
- Modulo
- Hammningův kód
- Cyklický redundantní součet
- MDA5 (Message-Digest algorithm)
- SHA (Secure Hash Algorithm)

Paritní bit

Paritní bit je redundantní bit přidaný k datovému slovu a obsahuje paritní informaci o počtu jedničkových bitů ve slově.
Paritní bit je určen k jednoduché detekci chyby ve slově.

sudý počet jedniček - sudá (even) parita nebo
lichý počet jedniček – lichá (odd) parita.

Hammingův kód

Hammingův kód, pojmenovaný po Richardu Hammingovi, je lineární kód používáný v oblasti telekomunikací pro detekci až dvou chybných bitů nebo pro opravu jednoho chybného bitu. Základem je Hammingův kód (7,4), ale lze jej zobecnit i na jiné počty datových a paritních bitů.

CRC (- Cyclic Redundancy Check.)

Cyklický redundantní součet je speciální hašovací funkce, používaná k detekci chyb během přenosu či ukládání dat. Pro svou jednoduchost a dobré matematické vlastnosti jde o velmi rozšířený způsob realizace kontrolního součtu.

Kontrolní součet bývá odesílán či ukládán společně s daty, při jejichž přenosu nebo uchovávání by mohlo dojít k chybě. Po převzetí dat je znovu nezávisle spočítán. Pokud je nezávisle spočítaný kontrolní součet odlišný od přeneseného nebo uloženého, je zřejmé že při přenosu nebo uchovávání došlo k chybě. Pokud je shodný, tak téměř jistě k žádné chybě nedošlo. V určitých případech je možné chybu pomocí CRC opravit.

CRC je vhodný pro zjišťování chyb vzniklých v důsledku selhání techniky, avšak jako metoda pro odhalení záměrné změny dat počítačovými piráty je příliš slabý. V tomto případě je třeba používat speciální hašovací funkce určené pro šifrovací algoritmy.

Diagnostický SW

Diagnostický software je používán široce mezi operačními systémy a má za účelem diagnostikovat specifickou část nebo kompletně systém a podat o systému zprávu založenou na svém kódu určeném pro testování.

Takovýto software je schopen otestovat chyby v operačním systému,operační paměti,disky,procesor atd.

SW na testování a údržbu disků

Nejlepší nástroj je ten od výrobce disku spuštěný v offline režimu a přímo nabootován.

Jako software na kontrolu stavu a zdraví disku se označuje CrystalDiskInfo, který je schopen číst S.M.A.R.T data z disků.Tato data zahrnují četnost chyb,roztočení disku.Výrobci disku ví, které hodnoty jsou normální a jaké ne, a takovéto hodnoty zakódují do firmwaru.CrystalDiskInfo je schopen monitorovat tyto hodnoty a vyhodnotí je.
Další software je např. Disk Drill, který je schopen obnovit enormní množství typů souborů.Je schopen obnovit jakýkoliv soubor bez jakýchkoliv znalostí.

SW na otestování operační paměti

MemTest86
Jedná se o jeden z nejstarších a nejvíce známých programů na testování operační paměti.Analyzuje RAM a zkontroluje vše možné typy chyb.Jedná o bootovací program.Po nabootování to vykoná sérii algoritmů a testovacích funkcí aby to prozkoumalo stabilitu a chybovost.Zkouší to sekveční blokování paměti,pohybové inverze, hammer test, a spousty dalších.

Systém windows v sobě má program na otestování operační paměti s názvem Windows Memory Diagnostic, který funguje báječně a také je bootovací.

SW na testování stavu procesorů

Výrobce procesorů intel přímo nabízí svůj program s názvem Intel PDT. Tento software zkontroluje Funkcionalitu všech jader, identifikaci značky, procesorovou operační frekvenci, otestuje specifické schopnosti a udělá zátěžový test.

FireWall

Firewall v počítačové síti blokuje nebo povoluje navazované komunikace na základě předdefinovaných nebo dynamických pravidel a politik. Chrání zařízení, jež jsou zapojena za ním, před různými typy útoků, včetně těch, které umožní útočníkovi převzít kontrolu na zařízením.

Skrz toto místo jde veškerá komunikace mezi sítěmi a proto může komunikaci zpomalovat za bezpečí, a možnost zablokovat jakékouliv službu, která může procházet nebo prochází.
Kategorie firewallu:
- Paketové filtry
- Aplikační filtry
- Stavové paketové filtry s kontrolou známých protokolů

Antivirus

Jedná se o software, který slouží k identifikaci, odstraňování a kontaminaci počítačových virů a jiného škodlivého softwaru.Toto se uskutečňuje za pomocí:
- prohlížení souborů na lokálním disku, která ma za cíl nalézt sekvenci odpovídající definice některého počítačového viru v databázi
- detekci podezřelé aktivity nějakého počítačového programu, který může značit infekci

Úspěšnost závisí na schopnostech antivirového programu a aktuálnosti databáze počítačových virů.

Malware

```
Jedná se o škodlivé programy, které v počítači provádí činnost, se kterou
by uživatel nesouhlasil, kdyby o jeho skutečných záměrech věděl. Označení
malware se nevztahuje na programátorské chyby.
```

Trojský kůň

Červ

Ransomware

Spyware

Adware

Phissing

Man in the middle