

Ochrana elektronických dokumentov

Obhajoba diplomovej práce

Martin Bajaník

Fakulta informatiky
Masarykova univerzita
`martin.bajanik@gmail.com`

Brno, 16. februára 2017

Cieľ diplomovej práce

- Poskytnúť ucelený prehľad ochrán, implementovaných v najrozšírenejších formátoch, s dôrazom na ochranu dôvernosti dokumentov založenej na heslách.
- Vytvoriť distribuovaný systém na obnovu zabudnutého hesla.
- Pomocou vytvoreného nástroja zhodnotiť schopnosť formátov odolať útokom hrubou silou a použiteľnosť systému na obnovu hesla.

Ochrana elektronických dokumentov

Spôsob ochrany

- Šifrovanie - dôvernosť
- Digitálne podpisy - autenticita a integrita

Populárne formáty



MS Office Document Cryptography Structure

Implementované ochrany

- Šifrovanie podľa ECMA-376.
 - Štandardné šifrovanie.
 - Agilné šifrovanie.
- Digitálne podpisy.
- Ochrana proti zápisu.

Zhrnutie

- Neustále zlepšovaná miera zabezpečenia a používané algoritmy.
- Udržiavaná spätná kompatibilita.

Portable Document Format

Implementované ochrany

- Šifrovanie.
 - *Standard Security Handler*
 - *Public-Key Security Handler*
- Digitálne podpisy.

Zhrnutie

- Otázne spôsoby šifrovania.
- Pokročilá funkcionálna spojená s digitálnymi podpismi.

Open Document Format

Implementované ochrany

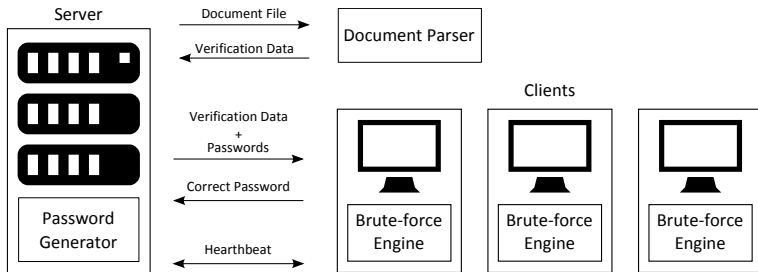
- Šifrovanie.
- Digitálne podpisy.

Zhrnutie

- Jednoduchý a efektívny spôsob ochrany.

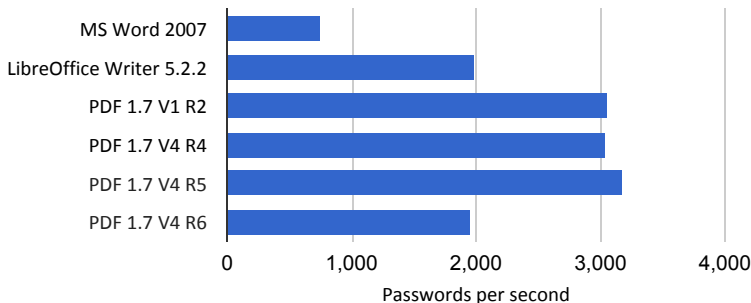
Kľúčové vlastnosti

- Klient – server architektúra
- Modularita a paralelizmus



Návrh systému na obnovu zabudnutého hesla.

Obnova hesla dokumentov hrubou silou



Priemerná rýchlosť verifikácie správnosti hesla (počet pokusov za sekundu).

Obnova hesla dokumentov hrubou silou

	MS Word 2007	LibreOffice Writer 5.2.2	PDF 1.7 V4 R5
3	< 25 seconds	< 9 seconds	< 6 seconds
4	< 10 minutes	< 4 minutes	< 2.5 minutes
5	< 5 hours	< 2 hours	< 1.1 hours
6	< 5 days	< 2 days	< 1.2 days
7	< 17 weeks	< 7 weeks	< 4.2 weeks
8	< 9 years	< 3.5 years	< 2.1 years

Odhadovaný čas na dokončenie procesu obnovy hesla danej dĺžky.

Záver

Hlavné prínosy práce

- Ucelený popis ochrán implementovaných v populárnych formátoch elektronických dokumentov.
- Vytvorený funkčný distribuovaný systém na obnovu zabudnutého hesla s dôrazom na použiteľnosť a rozšíriteľnosť.

Otázky

Ďakujem za pozornosť.

Pripomienky oponenta

- Diskuze algoritmů dostupných přes API v OS Windows (str. 8) mohla být podrobnější.
- Co je to veřejná část certifikátu X.509?
- Zajímavé by bylo zmínit, proč byla vybrána MS právě tato fixní hesla (strana 11).
- Jsou násobné podpisy (např. v sekci 3.3:2) na stejné úrovni nebo hierarchicky řazené.