Ochrana elektronických dokumentov

Obhajoba diplomovej práce

Bc. Martin Bajaník

Fakulta informatiky
Masarykova univerzita
396204@mail.muni.cz

Brno, 10. februára 2017

Cieľ diplomovej práce

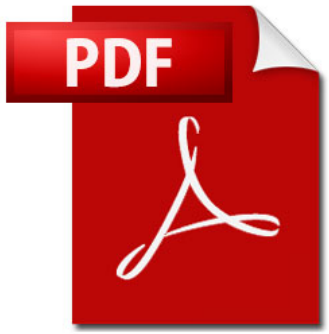
- Poskytnúť ucelený prehľad ochrán, implementovaných v najrozšírenejších formátoch, s dôrazom na ochranu dôvernosti dokumentov založenej na heslách.
- Vytvoriť distribuovaný systém na obnovu zabudnutého hesla.
- Pomocou vytvoreného nástroja zhodnotiť schopnosť formátov odolať útokom hrubou silou a použitelnosť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

Ochrana elektronických dokumentov

Spôsob ochrany

- Šifrovanie - dôvernosť
- Digitálne podpisy - autenticita a integrita

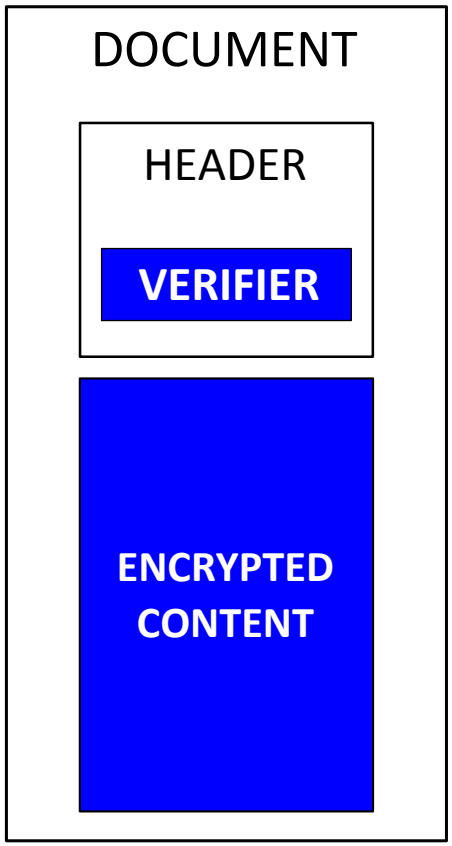
Populárne formáty



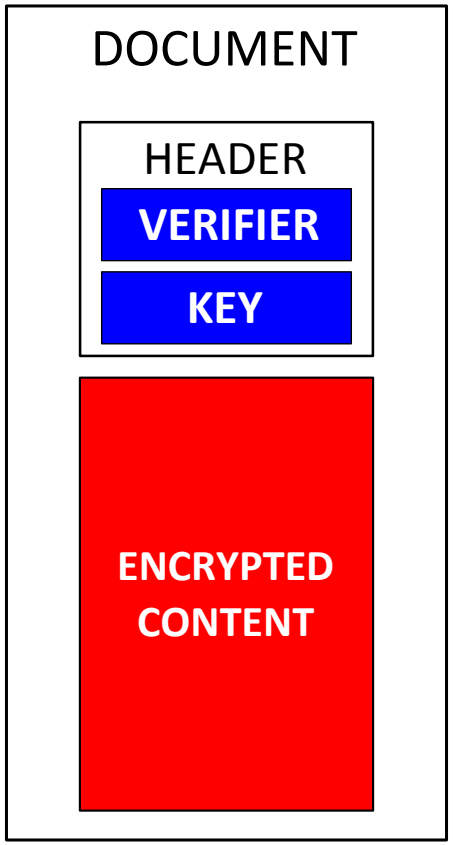
Šifrovanie na základe hesla

1.  password → **USER_KEY** = KDF(password)

2. A



2.B



KEY = RNG()

MS Office Document Cryptography Structure

Šifrovanie na základe hesla

- Open Office XML (ECMA-376)
- Štandardné šifrovanie (Office 2007)
  - 50 000 iterácií
  - SHA-1
- Agilné šifrovanie (Office 2010 a vyššie)
  - 100 000 iterácií
  - SHA-1
  - Konfigurovateľné užívateľom

Portable Document Format

Šifrovanie na základe hesla

- Samostatný šifrovací modul (*Standard Security Handler*)
- PDF 1.1 - 1.3
  - 50 iterácií MD5
- PDF 1.4 - 1.7
  - 50 iterácií MD5 a 19 iterácií RC4
- PDF 1.7 s modulom verzie 5
  - 1 iterácia SHA-256
- PDF 1.7 s modulom verzie 6
  - 32 iterácií SHA-2 a AES-128

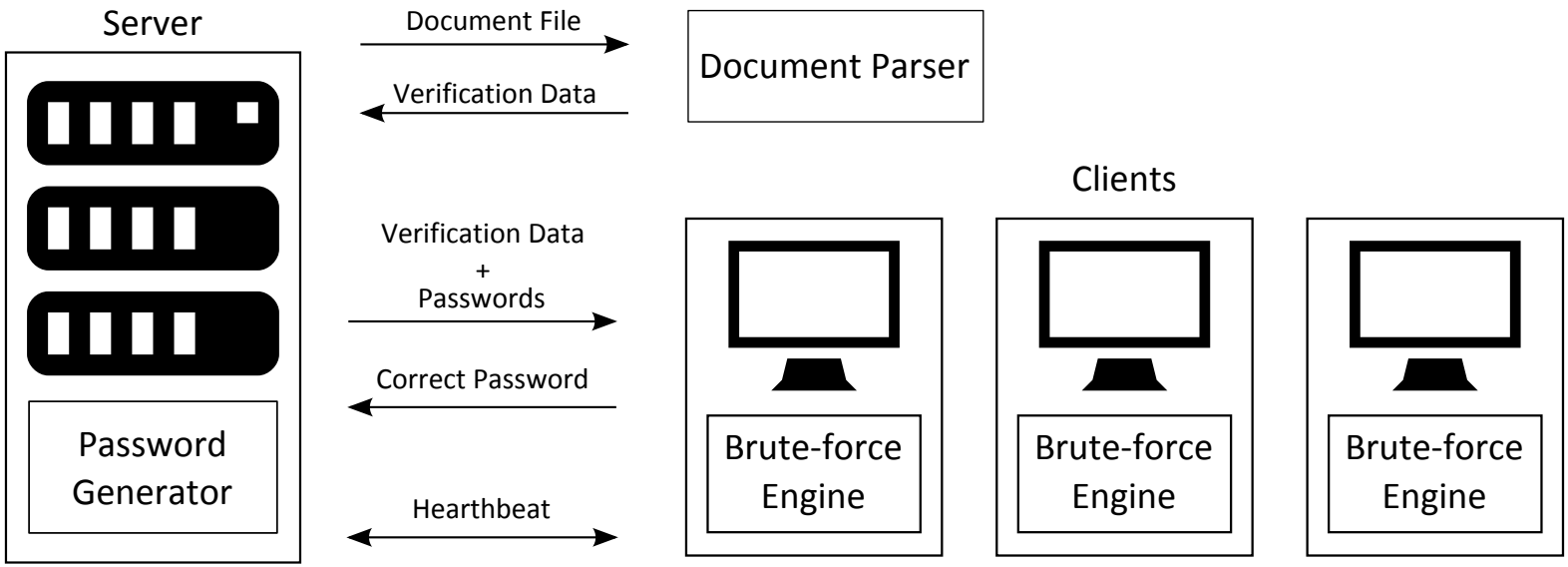
Open Document Format

Šifrovanie na základe hesla

- Verzia 1.0 - 1.2
  - 1024 iterácií PBKDF2 s HMAC-SHA1 (RFC 2898)
  - Počet iterácií konfigurovateľný

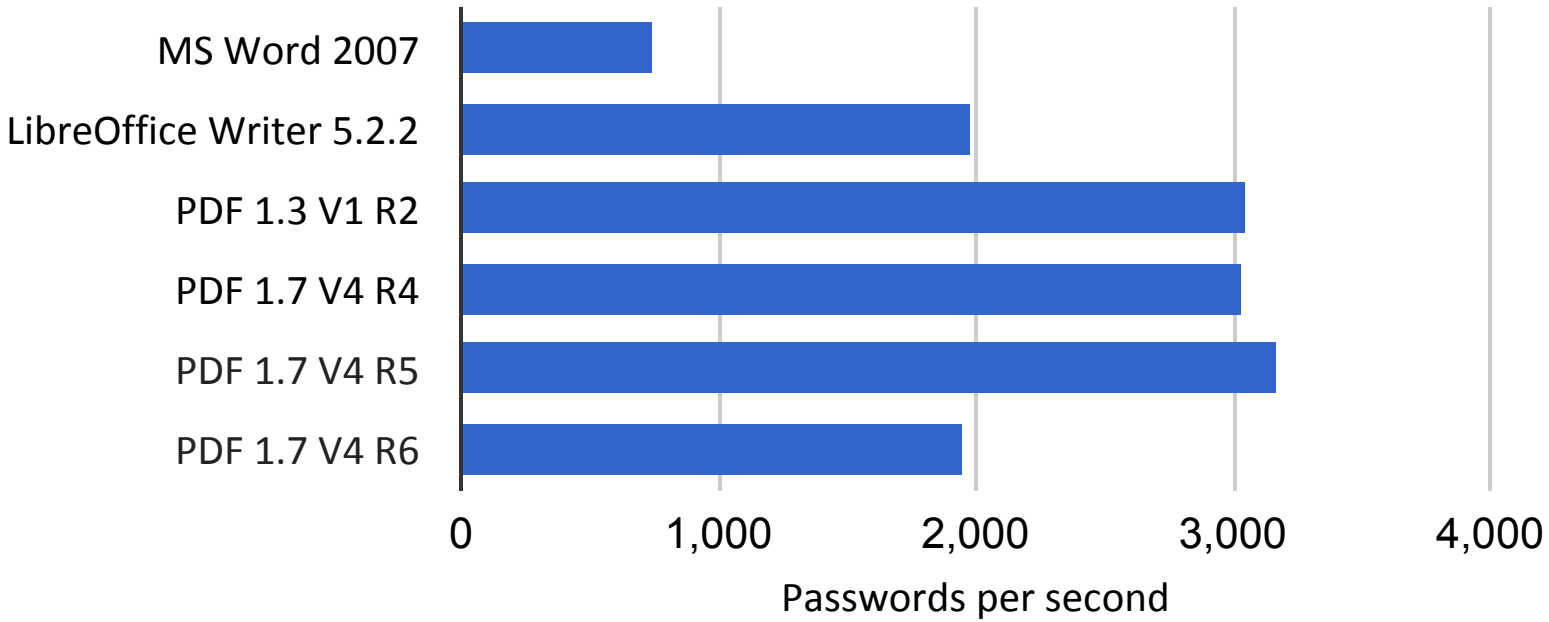
Kľúčové vlastnosti

- 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)

Záver

Hlavné prínosy práce

- Ucelený popis ochrán implementovaných v populárnych formátoch elektronických dokumentov.
- Zhodnotenie dostupných ochrán a testovanie odolnosti voči útokom hrubou silou.
- Vytvorený funkčný distribuovaný systém na obnovu zabudnutého hesla s dôrazom na:
  - rozšíriteľnosť vďaka modulárnemu prístupu,
  - efektívnosť vďaka paralelizácii na viac úrovniach a
  - jednoduchú použiteľnosť.

Otázky

Ďakujem za pozornosť.

Otázky z posudkov

- 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?

Štandardné vs. agilné šifrovanie

- Binárny formát vs. XML
- Fixné algoritmy a parametre vs. CNG (*CryptoAPI: Next Generation*)
- Šifrovací kľúč (tzv. *intermediate key*)
- Integrita (*Encrypt then MAC*).

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.

Ďalšie ochrany

Ochrana proti zápisu (MS Office)

- Uplatnenie iba z pohľadu UX.

Šifrovanie pomocou asymetrickej kryptografie (PDF)

- Dokument šifrovaný pomocou RC4.

Digitalné podpisy

- Microsoft Office a Open Document Format
  - XML Signature Syntax and Processing (W3C)
- Portable Document Format
  - Pokročilá funkcionalita a robustné algoritmy.

Porovnanie implementácii ODT

Apache OpenOffice vs. LibreOffice

	LibreOffice	**Apache OpenOffice**
checksum-type	SHA-256	SHA-1
algorithm-name	AES-256	Blowfish CFB
start-key-derivation-name	SHA-256	SHA-1
key-derivation-name	PBKDF2	PBKDF2
iteration-count	1024	1024
key-size	32	16

Šifrovanie dokumentov - algoritmy

- Microsoft Office
  - Štandardné šifrovanie - AES-128, AES-192, AES-256 (ECB)
  - Agilné šifrovanie - Windows OS API (CNG)
- Portable Document Format
  - RC4, AES-128 (CBC)
  - Dĺžky kľúčov 40-128 bitov
- Open Document Format
  - 1.0 a 1.1 - Blowfish CFB
  - 1.2 - Triple DES, AES-128, AES-192, AES-256 (CBC)
    - XML Encryption Syntax and Processing (W3C)