

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA
Zavoda za elektroničke sustave i obradbu informacija

Seminarski rad iz kolegija
Sustavi za praćenje i vođenje procesa

Eksploracija skrivenih informacija u javno dostupnim dokumentima i datotekama

3. lipnja 2007.

Profesor:
mr.sc. Predrag Pale

Student:
Denis Siladi
JMBAG: 0036391063
Računarstvo, 5. godina
e-mail: denis.siladi@fer.hr

Sadržaj

1. UVOD	1
1.1. CURENJE INFORMACIJA U KONTEKSTU INFORMACIJSKE SIGURNOSTI	1
1.2. META PODACI.....	2
2. PREGLED SKRIVENIH INFORMACIJA U OSNOVNIM FORMATIMA ZAPISA: DOC, PDF, JPEG	4
2.1. MS WORD DATOTEKE.....	4
2.1.1. Analiza skrivenih informacija u MS Word datotekama	4
2.1.2. Načini pregleda meta podataka	7
2.1.3. Preventivne mjere – kako ukloniti meta podatke	8
2.1.4. Primjer zloporabe meta-podataka	9
2.2. PDF DATOTEKE.....	9
2.2.1. Analiza skrivenih informacija u PDF datotekama.....	9
2.2.2. Primjeri.....	9
2.3. JPEG DATOTEKE	10
2.3.1. Analiza skrivenih informacija u JPEG datotekama - EXIF.....	10
2.3.2. Primjeri.....	10
3. ZAKLJUČAK	14
4. REFERENCE.....	15

1. Uvod

Svrha ovog dokumenta je dati kratki pregled načina eksplotacije skrivenih informacija u javno dostupnim dokumentima. Dokument će dati uvid u skrivene informacije koje se mogu naći u najrasprostranjenijim digitalnim dokumentima, Microsoft Word, PDF i JPEG formata; te ukazati na važnost sprječavanja curenja informacija i implikacije koje navedene mogu izazvati u jednoj poslovnoj sredini. Također će biti prikazani alati s kojima je do osjetljivih informacija moguće doći ali i pripadni primjeri koji ilustriraju ozbiljnost problema.

1.1. Curenje informacija u kontekstu informacijske sigurnosti

Danas kada je ideja o sveopćoj umreženosti postala stvarnost i kada se računalni sustavi spojeni na nesiguran Internet koriste u svim sferama ljudske djelatnosti briga o računalnoj sigurnosti postaje nužnost u poslovnoj politici svake organizacije. Iako je većina organizacija već načinila prvi korak u susret brizi o računalnoj sigurnosti i osiguravanju vrijednih i osjetljivih podataka, najčešće kroz implementiranje antivirusnih i vatrozidnih sustava, oni sami nisu dovoljni. Spomenuta rješenja sprječavaju određene vektore napada ali se ne mogu smatrati cjelovitom zaštitom, a osobito ne u situacijama curenja informacija.

Kako se danas komunikacija u poslovnom svijetu gotovo u potpunosti odvija digitalnim putovima, a važni dokumenti prenose najčešće u obliku Microsoft Word ili PDF dokumenata nužno je razmotriti situacije u kojima navedeni dokumenti sadrže osjetljive i povjerljive informacije na prvi pogled nevidljive korisniku. Implikacije mogu biti brojne a u poslovnom svijetu su direktno ili indirektno vezane za finansijske gubitke. Zamislimo samo situaciju u kojoj se povjerljive finansijske informacije mogu doznati kroz na prvi pogled nevidljive informacije u javno objavljenim dokumentima ili kada se drugi kritični podaci nalaze skriveni iza običnih dokumenata. Reputacija tvrtke zbog navedenih propusta može biti narušena, a ovi propusti mogu generirati finansijske gubitke koji se očituju kroz gubitak povjerenje korisnika u tvrtku.

Od početka osamdesetih godina kada je Internet zaživio u obliju kakvog poznajemo danas, Internet se razvijao nevjerojatnom brzinom i stvorio novu, digitalnu, dimenziju, okosnicu brojnih tehnologija bez kojih je poslovanje u današnjem svijetu nezamislivo. Brojne tehnologije te činjenica kako brzinu razvoja samog Interneta nisu mogli pratiti i sigurnosni aspekti stvorili su nove tipove korisnika koji su u stanju iskoristiti sigurnosne propuste u mrežnim konfiguracijama, aplikacijama i web stranicama te načiniti veliku štetu kompromitiranoj organizaciji. Ovi zlonamjerni korisnici, popularno zvani hakeri raspolažu odličnim poznavanjem problematike što im omogućuje pronalaženje sigurnosnih propusta i preuzimanje kontrole nad računalima neke organizacije, a prvi korak u napadu na računalnu infrastrukturu čini izviđanje odnosno prikupljanje informacija o tvrtki koje zlonamjernim korisnicima mogu znatno olakšati napad. Informacije koje zlonamjerni korisnici mogu dobiti iz skrivenih podataka unutar javno objavljenih dokumenata najčešće ih pripremaju za provođenje napada putem socijalnog inženjeringu, danas najuspješnijeg oblika kompromitiranja čak i tehnički najsigurnijih informacijskih

sustava; s druge strane informacije poput korisničkih imena, imena računala i drugih tehničkih podataka koji se također nalaze skrivene u velikom broju digitalnih dokumenata znatno mogu olakšati posao zlonamjernim korisnicima.

Kako je Internet okolina koja osigurava anonimnost i ne poznaje državne granice hakeri mogu izvršavati svoje napade s bilo kojeg mesta u svijetu, a uporaba drugih kompromitiranih sustava, *proxy* poslužitelja i sličnih metoda tijekom tih napada čini otkrivanje napadačeva identiteta izuzetno teškim ako ne i nemogućim. Nakon upada na sustav napadač će poduzeti korake kojima će zamaskirati svoju prisutnost te uporabom *backdoor* programa i *rootkit* tehnologije omogućiti daljnji pristup kompromitiranom sustavu čak i kada se sigurnosni propust pomoću kojega je sustav inicijalno kompromitiran ispravi.

Činjenica da su ključne informacije za napad dostupne u javno objavljenim dokumentima dovodi do zaključka kako je briga o ovom problemu itekako bitna, a malo ulaganje u edukaciju korisnika o problematici može spriječiti velike potencijalne probleme.

1.2. Meta podaci

Kako bi shvatili izvor problema kojega adresira ovaj dokument, potrebno je najprije objasniti sastavne elemente današnjih digitalnih dokumenata, a ključan element u ovoj priči čine meta-podaci.

Meta podaci predstavljaju podatke koje nose informacije o drugim podacima koji se mogu nalaziti unutar dokumenata, aplikacije ili općenito neke okoline. Meta podaci su, u stvari, podaci o podacima, i danas ih sadrži većina digitalnih formata bez obzira bili to digitalni dokumenti ili multimedijalni formati. Primjerice u MS Word dokumentima meta podaci su pohranjeni u "Properties and Custom Properties" sekciji datoteke u specijaliziranom formatu zvanom "OLE (Object Linking and Embedding) structured storage". OLE pruža strukturiranu sustav pohrane za poveznice i objekte unutar dokumenta. S obzirom da su informacije pohranjene unutar OLE u dokumentu, meta-podaci nisu vezani za računalo ili mrežnu sredinu već se oni prenose skupa sa dokumentom.

Koncept meta podataka nije nov; ideja je izvorno potekla iz sredina koje su se bavile razvojem softvera, gdje je rad u skupini i razmjena podataka nužnost. Meta podaci se mogu zamisliti kao dnevnik podataka povezanih s postupkom kreiranja dokumenata.

Kako je Microsoft Word kao tekstualni procesor tijekom godina postao doslovce standard u poslovnoj sredini većina problema veznih uz curenje informacija kroz meta podatke vezana je upravo za njega. Interesantno je kako je sam Microsoft još davne 2001. godine tvrdio da je MS Word dizajniran kako bi adresirao problem skrivenih podataka unutar word dokumenata, te kako bi zadovoljio potrebe poslovnih i pravnih korisnika u sredinama koje aktivno surađuju i razmjenjuju velike količine podataka. No situacija u stvarnosti je bila malo drugačija, tipično Word dokumenti sadrže sljedeće podatke:

- *Ime autora*

- *Inicijali autora*
- *Ime tvrtke*
- *Ime računala korisnika (autora)*
- *Ime mrežnog poslužitelja ili oznaka čvrstog diska gdje je datoteka bila pohranjena*
- *Druga svojstva dokumenta i sažetak*
- *Nevidljivi dijelovi ugrađenih OLE objekata*
- *Imena svih prijašnjih autora*
- *Revizije dokumenta*
- *Verzije dokumenta*
- *Informacije o predlošku*
- *Skriveni tekst*
- *Komentari u dokumentu*

Neki meta podaci unutar Word dokumenta su potrebni za formatiranje i pohranu objekata poput slike tablica itd. Meta podaci mogu biti prilično korisni kada se radi u sredini koja zahtjeva zajedničku suradnju više osoba na kreiranju dokumenata. Negativna ili pozitivna strana informacija sadržanih u kategoriji meta podataka ovisi isključivo kako se dokument stvara i između koga se on dijeli. Ukoliko se definiraju pravila unutar organizacije vezana za dijeljenje dokumenata te educiraju korisnici o meta podacima sadržanim u najčešće korištenim digitalnim formatima potencijalni slučajevi curenja informacija mogu se svesti na minimum.

Kroz gore naveden meta-podatke jasno se razaznaju određene kategorije, te se tako meta-podaci mogu podijeliti na sljedeća tri tipa: korisnički generirane meta podatke, automatski generirane meta podatke te sistemske meta podatke.

Korisnički generirani meta podaci – su oni podaci koje korisnik sam kreira unutar nekog digitalnog dokumenta, dobar primjer je kratki opis koji je vidljiv u svojstvima word dokumenta

Automatski generirani meta podaci – su oni podaci koje generira alat pomoću kojega nastaje dokument, primjerice informacije o osobi koja je posljednja radila na dokumentu

Sistemske meta podaci – su oni podaci koje generira operacijski sustav ili neka okolina, najbolji primjer za ovaj tip podataka su EXIF informacije koje se pohranjuju zajedno s digitalnim fotografijama kreirane putem nekog digitalnog fotoaparata

2. Pregled skrivenih informacija u osnovnim formatima zapisa: doc, pdf, jpeg

Većina korisnika danas nije upoznata s problemom oko skrivenih podataka u digitalnim dokumentima i drugim digitalnim sadržajima. Danas meta-podatke ne sadrže samo oni najjednostavniji formati dok su u većini drugih oni normalna pojava. Ovaj seminar obraditi će nekoliko osnovnih formata te prikazati kakve sve informacije mogu biti skrivene u njima, kako do tih informacija doći kako ih obrisati i na kraju navesti nekoliko interesantnih primjera iz stvarnog života. Zbog opsega i količine danas dostupnih digitalnih formata ovaj seminar uzet će u obzir MS Word format dokumenta, PDF (engl. *Portable Document Format*) i često korišten slikovni format JPEG.

2.1. MS word datoteke

Kako je već bilo rečeno u prvom poglavlju MS Word datoteke sadrže brojne meta podatke, a kako je ovaj alat postao standardom u uporabi u poslovnim okruženjima te je u povijesti imao veći broj nedostataka glede skrivenih informacija upravo će on biti detaljno analiziran.

2.1.1. Analiza skrivenih informacija u MS Word datotekama

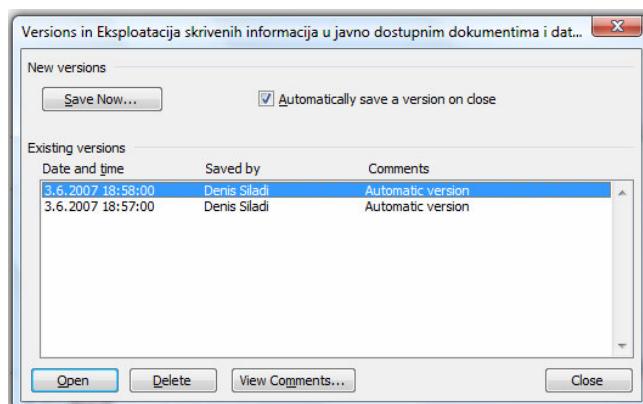
Procjena rizika prilikom definiranja neke politike u sklopu organizacije bitan je čimbenik, na isti način treba pristupiti analizi skrivenih informacija u MS Word dokumentima. Mnogi koji aktivno koriste MS Word dokumente smatraju kako nisu ugroženi ovim problemom samo iz razloga što nemaju uključenu „Track Changes“ opciju; no ipak postoji nekoliko drugih načina kako se meta podaci mogu stvarati i skrivati unutar MS Word dokumenta. Zbog toga korisnici često nisu svjesni kako se meta podaci stvaraju i integriraju unutar word dokumenta samo zbog činjenice što to nigdje nije prikazano. Razmatranje koje slijedi odnosi se na način kako se meta podaci kreiraju.

1. *Opcija Versions...*

ako je uključena predstavlja takozvane automatski generirane odnosno pasivne meta podatke. Ovu opciju je moguće uključiti u izborniku *File -> Versions...* i omogućuje korisnicima pohranu prijašnjih inačica dokumenta stvarajući tako jedan oblik dnevnika izmjena. Ukoliko je opcija „**automatically save a version on close**“ uključena svaki puta prilikom zatvaranja programa za obradu teksta – Word, trenutna inačice dokumenta se snima unutar OLE baze bez da se o tome korisnik eksplicitno obaveštava. Iako se prilikom postojanja različitih inačica u sklopu dokumenta u statusnoj traci pojavljuje mala ikonica, neiskusnom korisniku ona će zasigurno promaći. Kao takve, razne inačice dokumenta čuvaju se unutar dokumenta pružajući uvid u izmjene svakome tko ima pristup dokumentu.

Primjer zlorabljenja prikazat ćemo kroz situaciju u kojoj osoba od povjerenja – neka ona bude osobni bankar radi na dokumentu kojega je kreirala neka druga osoba i bez znanja bankara omogućila opciju „*Versions*“. Pretpostavimo kako će

bankar raditi na tom dokumentu tijekom tjedan dana te nakon nekoliko izmjena finalnu inačicu poslati osobi koja je dokument izvorno kreirala. Zahvaljujući uključenoj opciji *Versions* ta osoba će imati mogućnost pregleda svih izmjena koje je bankar u dokumentu načinio, vidjeti put kojim je dokument nastajao i vjerojatno vidjeti neke osjetljive podatke koji iako nisu sadržani u finalnoj verziji dokumenta, jesu sadržani u nekoj od prethodno snimljenih inačica.



Slika 1: Versions izbornik u programu MS Word 2003.

2. Opcija “Track Changes” i “Hidden Deletions”

Drugi primjer kreiranja meta podataka bez znanja korisnika uključuje opciju *Track Changes*, mogućnost Microsoft Word alata da prati promjere u dokumentu. Opcija *Track Changes* iznimno je korisna i omogućuje većem broju korisnika da vrlo jednostavno rade na jednom dokumentu prateći sve nastale promjene. Ova funkcija je također dobro došla prilikom revizije dokumentacije što je u poslovnim sredinama vrlo česta procedura. Primjerice ukoliko jedan korisnik izmjeni nešto u dokumentu, od ostatka teksta, drugačijom bojom, će biti prikazane izmjene, a obrisani tekst će biti prikazana uz desnu stranu dokumenta u posebnim okvirima (NAPOMENA: Iako je način prikaza izmjena moguće mijenjati navedeni način prikaza je podrazumijevan u Word 2003 tekstu procesoru).

Pri podrazumijevanim postavkama svi korisnici znaju kako se podaci o izmjenama kreiraju jer su promjene eksplisitno prikazane uz radni tekst, no kako je način prikaza moguće mijenjati, sve tragove o uključenoj opciji *Track Changes* moguće je sakriti od korisnika, što nas dovodi do primjera prikazanom u prethodnom paragrafu. Ukoliko se iz izbornika **Tools** bira opcija **Options** te u novootvorenom izborniku tab **Track Changes**, moguće je promijeniti način prikaza praćenja izmjena. Opcija **Hidden Deletions** tako neće prikazivati obrisani tekst, iako će se informacije o njemu pohranjivati, a ako se sve stavke podese kako to prikazuje slika 2. iako uključen Track Changes obični korisnik neće uočiti.

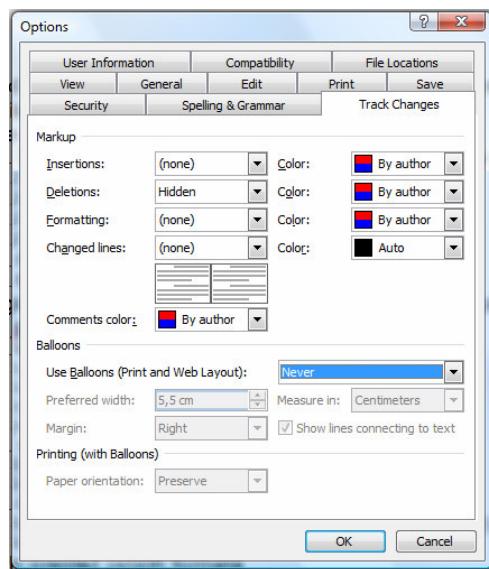
3. Properties

Izborom stavke *Properties* iz izbornika *File* vidljivi su neki meta podaci koji se generiraju automatski bez obzira na postavke u programu. Ove informacije bez

Eksplotacija skrivenih informacija

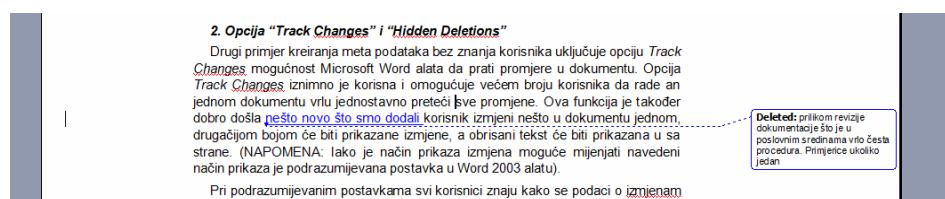
u javno dostupnim dokumentima i datotekama

obzira koliko se činile bezazlenima, mogu sadržavati informacije poput imena svih korisnika koji su radili na dokumentu, njihovih korisničkih imena s kojima su prijavljeni, kada se dokument ispisivao i na koji pisač i druge informacije, koje ponekad mogu znatno olakšati posao zlonamjernih korisnika.

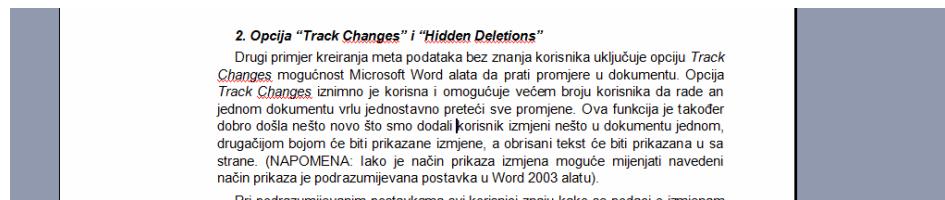


Slika 2: Dijaloški okvir prikazuje postavke koje su zaslužne za skrivanje informacija o praćenju izmjena.

Slika 3. i slika 4. prikazuju kako izgleda Word dokument s uključenim praćenjem izmjena uz podrazumijevane postavke i uz postavke prikazane na slici 2. Korisnici koji nemaju omogućenu alatnu traku **Reviewing** neće vidjeti je li opcija Track Changes uključena dok će ona u pozadini spremati sve podatke o izmjenama.



Slika 3: Word dokument s uključenom opcijom praćenja izmjena



Slika 4: Isti taj dokument s skrivenim praćenjem izmjena

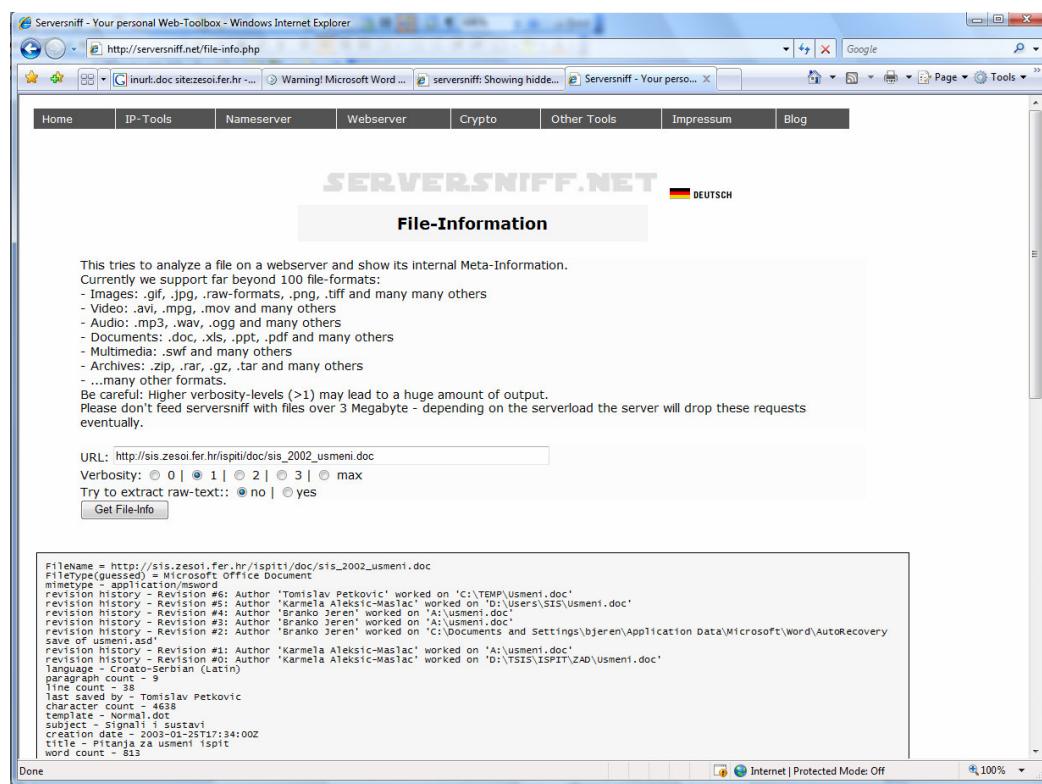
2.1.2. Načini pregleda meta podataka

Postoje dva načina kako se meta podaci mogu pogledati, prvi uključuje uporabu alata pomoću kojih je dokument nastao, a drugi prepostavlja uporabu specijaliziranih alata. U slučaju Word dokumenata većinu meta-podataka moguće je pogledati iz sučelja samog programa, ako se uzmu u obzir načini prikrivanja kreiranja meta podataka objašnjeni u prošlom poglavlju jasno je što najprije treba pogledati kako bi se otkrili tragovi o postojanju meta podataka. Do nekih meta podataka međutim nije moguće doći tako jednostavno te za tu svrhu služe specijalizirani alati koji su u stanju ekstrahirati sve podatke iz Word dokumenata i OLE baza sadržanih u njima.

Tri najpoznatija takva alata potpuno su besplatna te sve podatke koje mogu naći unutar Word dokumenta ekstrahiraju u običan tekstualni format; radi se o:

- Antiword alatu dostupnom na <http://www.winfield.demon.nl/>
- word2x dostupnom na <http://word2x.sourceforge.net/>
- File-Info dostupnom na [http://serversniff.net/file-info.php/](http://serversniff.net/file-info.php)

Posljednji navedeni alat najzanimljiviji je od tri navedena, razlog je to što se radi o Web aplikaciji koja pored Word datoteka prepoznaće preko 100 različitih datotečnih formata. Slika 5. prikazuje alat u radu koji je analizirao jedan od Word dokumenata dostupan na Zavodskim stranicama.



Slika 5: File-Info Web aplikacija u radu

Alat je bio u stanju ekstrahirati informacije o svim autorima dokumenta, putanjama na disku gdje je dokument tijekom obrade bio pohranjen, tko ga je posljednji obrađivao i druge informacije.

Tijekom prikupljanja informacija za ovaj seminarski rad autor je uočio kako gotovo svaki dokument na Internetu ima dostupne ovakve i slične informacije, a među nekim dokumentima je našao i pohranjene inačice odnosno druge skrivene podatke koje su nosile veliki broj informacija koji u izvornom tekstu nije bio vidljiv.

2.1.3. Preventivne mjere – kako ukloniti meta podatke

U svrhu zaštite privatnosti i sprječavanja curenja informacija nužno je objavljivati dokumente bez meta podataka ili sa što manje dostupnih meta podataka. Kako kreiranje ovih informacija zbog načina rada programa nije moguće isključiti, nakon kreiranja dokumenta generirane meta podatke nužno je odstraniti iz dokumenta. Tri su načina kako je to moguće napraviti.

Prvi podrazumijeva pretvaranje Word dokumenta u neki od formata koji sadrže manji broj meta podataka ili u format u koji se meta podaci zbog načina konvertiranja neće prenijeti, tipičan primjer je konvertiranje Word dokumenta u PDF no i ova metoda ima određenih nedostataka, a nije upotrebljiva kada je nužna razmjena dokumenata u izvornom formatu.

Drugi način uključuje ručno analiziranje dokumenta te uklanjanje osjetljivih podataka. Microsoft svjestan nedostataka u svojim formatima objavio je podugačak dokument o ručnom uklanjanju meta podataka iz svojih dokumenata. Dokument je dostupan na sljedećoj adresi: <http://support.microsoft.com/kb/290945> a opisuje brojne postupke uklanjanja meta podataka od onih najjednostavnijih koji prikazuju uklanjanja podataka poput imena korisnika koji je kreirao dokument do onih komplikiranijih koji uključuju primjerice pisanje makro programa namijenjenih pretrazi dokumenta za tzv. *hidden* atributima.

Prethodno spomenuti način uklanjanja meta podataka ima jedan veliki nedostatak a to je vrijeme koje je potrebno uložiti kako bi se dokument počistio od osjetljivih informacija, stoga gore opisane načine danas najčešće zamjenjuju specijalizirani programi kreirani isključivo za ovu namjenu. Prvi ovdje opisani besplatan je a kreirao ga je sam Microsoft; informacije o njemu kao i putanja za dohvrat nalaze se na: <http://support.microsoft.com/kb/834427>; Alat se instalira u obliku add-in proširenja za skup alata iz obitelji Office XP i Office 2003 uredskog paketa te omogućuje uklanjanje svih meta podataka iz dokumenata Office paketa. Također uz alat dolazi komando linijski program pomoću kojega je moguće uklanjati meta podatke na većem broju dokumenata automatizirano.

Pored Microsoftovog besplatnog alata postoji i nekoliko komercijalnih alata od kojih je najpoznatiji *Metadata Assistant*, tvrtke Payne Consulting Group (www.payneconsulting.com). Drugi dostupni alati su: Out-of-Sight tvrtke SoftWise Consulting (www.softwise.net), ezClean tvrtke KKL Software (www.kkl.com) i Workshare Protect tvrtke Workshare (www.workshare.net).

2.1.4. Primjer zloporabe meta-podataka

Za kraj poglavlja o meta podacima sadržanim u Word dokumentima navest ćemo jedan primjer stvarne zloporabe meta-podataka. Prije tri godine jedna američka banka je u postupku odobravanja kredita slala svojim korisnicima formular u obličju Word dokumenta. Problem je nastao kada se otkrilo da je u sklopu tog dokumenta bila uključena opcija *Versions*, a kako banka nije vodila računa, nakon obrade formulara, podatke je iz njega brisala i ponovno slala taj naizgled prazan dokument drugim korisnicima. Kada se ovo otkrilo navedeni dokument sadržavao je osjetljive informacije koje su uključivale podatke o računima, jedinstvene brojeve građana itd. preko 100 korisnika, a naknadno je otkriveno kako se na osnovu tih podataka dogodilo nekoliko krađa identiteta.

2.2. PDF datoteke

Od svog nastanka PDF (engl. *Portable Document Format*) Adobeov format otvorenog standarda zamišljen kao format za razmjenu sadržaja, no u svojoj 8. aktualnoj inačici prerastao je i u format za obradu. Tako danas postoje brojne aplikacije namijenjene obradi pdf dokumenata što za sobom povlači problem meta podataka.

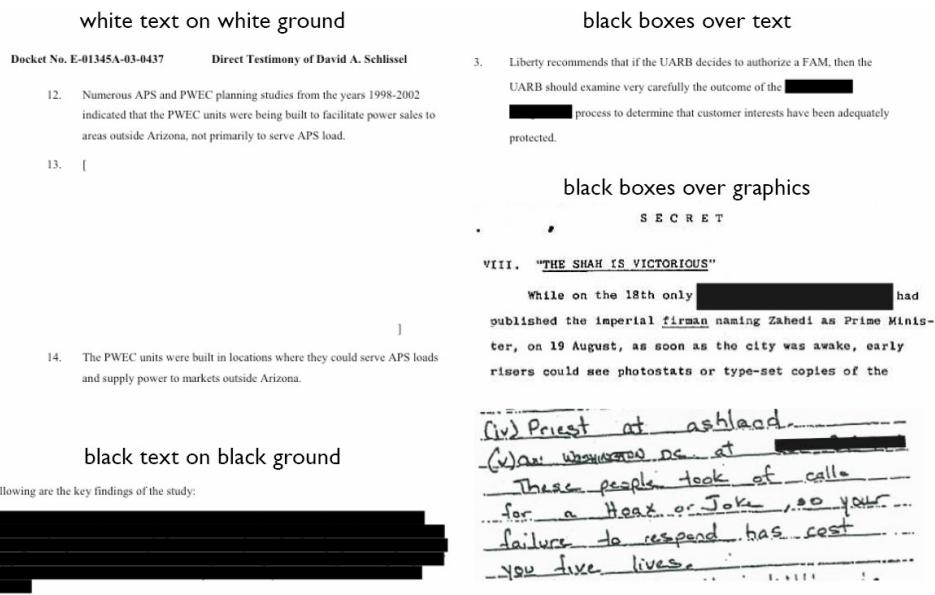
2.2.1. Analiza skrivenih informacija u PDF datotekama

PDF dokumenti nemaju ni približno toliki broj meta podataka kao primjerice dokumenti MS Word formata. PDF iako otvoreni standard prilično je težak za dekodiranje te činjenica da od meta podataka sadrži samo informacije o korisniku, korisničkom imenu prijavljenom na računalo, vremenu kada je dokument nastao i neke statističke informacije čini ga relativno pouzdanim formatom za razmjenu informacija.

Problem nastaje kada su u PDF dokument uključi element obrade odnosno redakcija dokumenata. Ovo je osobito bitno kod dokumenata koji moraju biti javno dostupni no sadrže neke povjerljive informacije koje je nužno sakriti od javnosti. U tu svrhu PDF editori zbog načina PDF standarda u većini slučajeva ne modificiraju izravno sadržaj već ga prikrivaju najčešće iza crnih kvadrata.

2.2.2. Primjeri

Primjer skrivanja iza zacrnjenih površina vidljiv je na slici 6. Iza crnih kvadrata nalaze se i elementi teksta i elementi slike. Doći do tih skrivenih elemenata iznimno je jednostavno i svodi se na običnu operaciju copy-paste. Rješenje predstavlja konvertiranje u PostScript format ili zamjena box operatora s null vrijednostima.



Slika 6: Do skrivenih informacija jednostavno je doći copy-paste operacijom

2.3. JPEG datoteke

Datoteke JPEG formata danas se mogu naći svuda. Zbog svoje rasprostranjenosti i činjenica što su pored TIFF-a jedine podržane standardom EXIF dobar su primjer za prikaz meta-podataka u drugačijem formatu od dosad prikazanih formata za dokumente. EXIF (engl. *Exchangeable image file format*) nastao je kao standard za slikovni format koji se koristi u digitalnim fotoaparatima. EXIF pored same fotografije sadrži i meta informacije. EXIF standard definira osnovni skup meta informacija poput rezolucije, tipa digitalnog fotoaparata, vremena kada je fotografija nastala, ekspozicije, otvora blende i drugih.

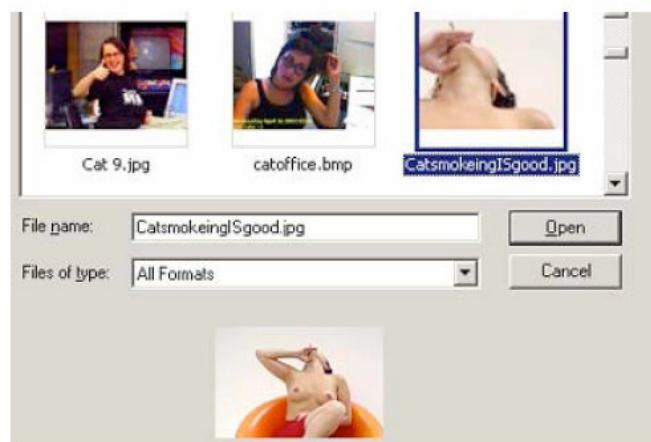
2.3.1. Analiza skrivenih informacija u JPEG datotekama - EXIF

EXIF također definira i proširenja u kojima se mogu pohraniti dodatne informacije poput umanjene slike originala (thumbnail). Kako većina aplikacija za obradu fotografija nepoznate EXIF tagove ne dira u što u većini slučajeva spadaju i thumbnail sličice, obrađene fotografije svoj umanjeni original često zadržavaju. Zbog ovog fenomena, mogu se otkriti primjerice povreda intelektualnog vlasništva, manipulacija programima za obradu slike i druge što će biti navedenu u poglaviju koje slijedi.

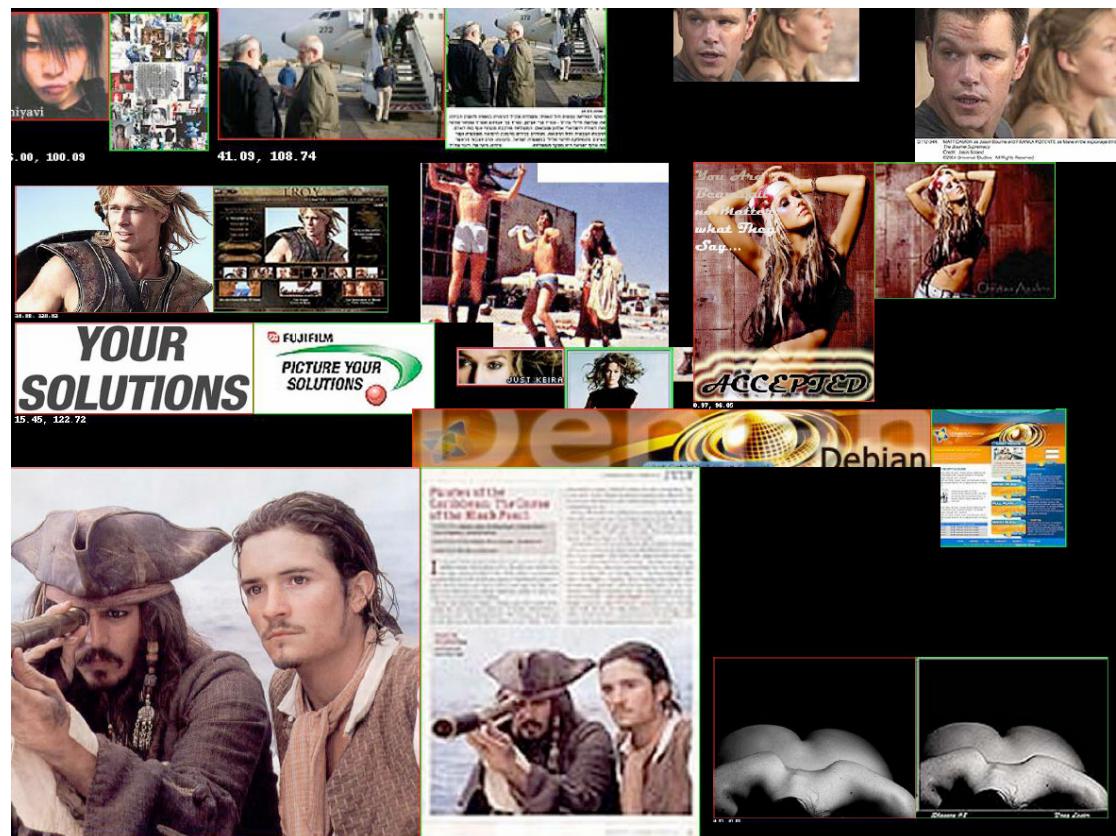
2.3.2. Primjeri

Problem meta podataka skrivenih unutar EXIF standarda popularizirao se prije 2 godine kada je izvjesna mlada moderatorica techtv-a dodala svoju fotografiju na forum, naoko bezazlena fotografija u sebi je krila smanjeni original koji je otkrio neke eksplisitne detalje. Sporna fotografija vidljiva je na slici 7. Pored svojevrsnog zabavnog faktora ovi meta podaci mogu poslužiti prilikom otkrivanja povrede intelektualnog vlasništva ili otkrivanja identiteta što je ilustrirano slikama koje slijede.

Eksplotacija skrivenih informacija u javno dostupnim dokumentima i datotekama



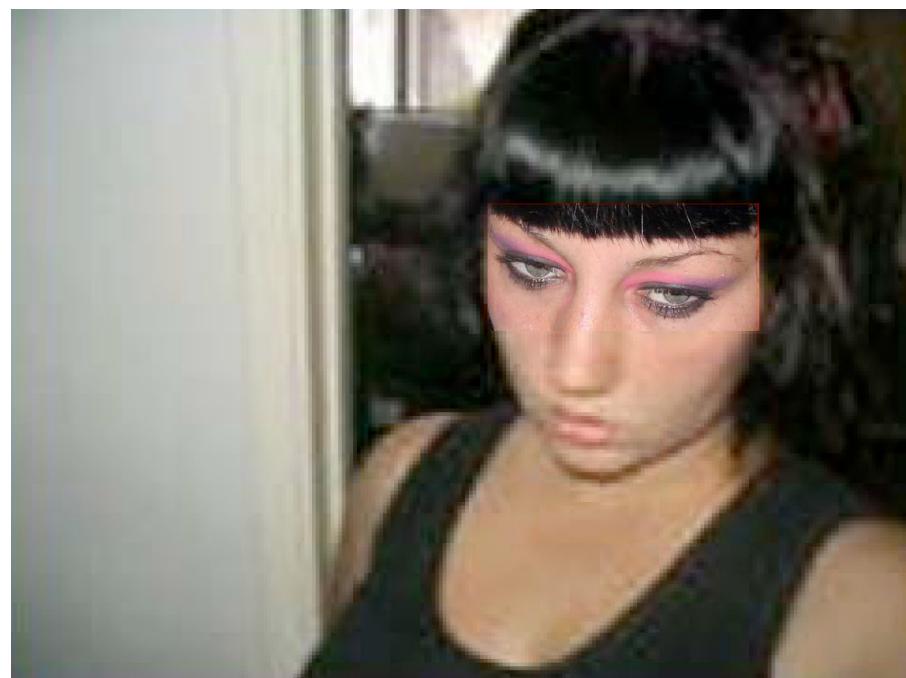
Slika 7: Thumbnail fotografije otkrio je neočekivane detalje



Slika 8: Primjeri povrede intelektualnog vlasništva



Slika 9: Pokušaj prikrivanja identiteta



Slika 10: Thumbnail fotografije otkrio je identitet

Eksplotacija skrivenih informacija

u javno dostupnim dokumentima i datotekama



Slika 11: Primjer rezanja (crop)



Slika 12: A evo i kako je to izgledalo na izvorniku

3. ZAKLJUČAK

Ideja ovoga dokumenta bila je prikazati moguće implikacije curenja informacija putem meta podataka koji se mogu naći danas u gotovo svakom digitalnom formatu te ih malo bliže objasniti. Microsoftov Word se pokazao kao najproblematičniji format (no isto se odnosi na sve formate Office uredskog pakete) od tri ovdje prikazana, ne samo zbog velikog broja meta podataka već i zbog velikog udjela ovog formata u poslovnim okruženjima. Iako ponekad meta podaci ne moraju nositi povjerljive informacije, valja imati na umu da one postoje te treba koristiti alate za njihovo uklanjanje kada god je to moguće ili potrebno. Kada se dokumenti objavljiju javno svakako je preporučljivo ukloniti sve meta podatke koji čak iako se čine bezazlenima mogu u određenim situacijama nanijeti štetu organizaciji. Od kraja devedesetih kada su se počele koristiti i eksplotirati skrivene meta informacije od strane zlonamjernih korisnika pa do danas je postignut veliki napredak kako u edukaciji korisnika tako i u formatima. Office 2003 tako više ne pohranjuje tko je sve radio na dokumentu, a Office 2007 uvodi Open XML format koji je lišen svih osjetljivih meta podataka, te možemo reći kako se zahvaljujući u ulaganje u informacijsku sigurnost problem meta podataka sveo na minimum.

4. REFERENCE

- [1] <http://addbalance.com/usersguide/metadata.htm>
- [2] http://www.stc-psc.org/Newsletter/archivedNewsletters/May_June_2005/newsletter_article.2006-01-06.5409202925
- [3] http://www.payneconsulting.com/pub_books/white_papers/pdf/PayneJuly2006ArticleonMetadata.pdf
- [4] http://www.enewsbuilder.net/techcommander/e_article000507288.cfm?x=b11,0,w
- [5] <http://www.lawpro.ca/LawPRO/metadata.pdf>
- [6] http://www.user-agent.org/word_docs.pdf