Varovanje podatkov v storitvi v oblaku Dropbox

Jernej Flisar, Marko Hölbl
Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Smetanova ul. 17, 2000 Maribor
{jernej.flisar, marko.holbl}@uni-mb.si

Izvleček

Storitev v oblaku Dropbox je zelo razširjena, uporablja jo več milijonov uporabnikov po vsem svetu. Storitev nam omogoča souporabo datotek in sinhronizacijo podatkov med več računalniki. Podatki so shranjeni v oblaku in so nam vedno dosegljivi. Ker so podatki shranjeni pri ponudniku storitve, se poraja vprašanje glede varnosti in zasebnosti shranjenih podatkov. V prispevku smo obravnavali varnostne mehanizme storitve Dropbox in izpostavili varnostne pomanjkljivosti, ki smo jih odkrili. Za zmanjšanje tveganja pri uporabi storitve Dropbox smo razvili programsko rešitev Secure Share, ki jo je mogoče uporabiti pri uporabi storitve za varovanje shranjenih podatkov. Prednost razvite rešitve pred drugimi orodji je, da podpira funkcionalnosti za souporabo podatkov z drugimi uporabniki in tako omogoča varno uporabo storitve Dropbox z vsemi njenimi funkcionalnostmi.

Ključne besede: Dropbox, varnost, Secure Share, SecretSync, BoxCryptor, TrueCrypt.

Abstract

Protection of Data in the Dropbox File Hosting Service

Dropbox is a very popular file sharing cloud service and has millions of users. It can be used for sharing and synchronizing data on multiple devices. Data is stored in the cloud and can always be accessed. Because the data is stored on the provider's side, issues of data privacy and security arise. In this paper, we address the security mechanisms of Dropbox and discuss potential security weaknesses. Furthermore, we review tools that enable a safer use of Dropbox. However, none of these tools support encryption when using sharing in Dropbox. Therefore we develop a software solution that addresses this issue and enables secure use of the Dropbox with all its functionalities.

Key words: Dropbox, security, Secure Share, SecretSync, BoxCryptor, TrueCrypt.

1 UVOD

Storitev računalništva v oblaku je veliko. Mednje sodijo storitve, ki ponujajo hrambo podatkov v oblaku (Zhang, Cheng & Boutaba, 2010). Ena izmed teh storitev je Dropbox, ki je bila predstavljena leta 2007 in je v prvih dveh letih pridobila dva, do leta 2010 pa že dvajset milijonov uporabnikov (Geron, 2011). Na začetku leta 2012 je imela storitev že preko petdeset milijonov uporabnikov po vsem svetu (Dropbox, 2012). Storitev omogoča shranjevanje, sinhronizacijo in souporabo podatkov z drugimi uporabniki. Podatki so shranjeni v oblaku, zato lahko do njih dostopamo povsod. Pri tem pa se pojavi vprašanje varnosti shranjenih podatkov.

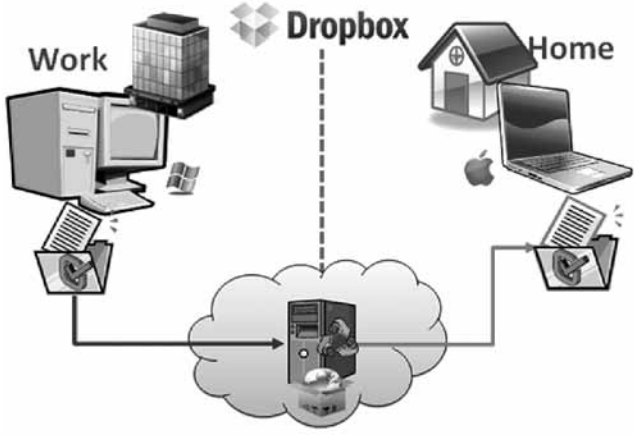
Islovar definira varnost podatkov kot stanje, pri katerem je zagotovljena zaupnost, celovitost in razpoložljivost podatkov. V tem primeru varnost podatkov zagotavlja ponudnik storitve tako, da ta nima dostopa in vpogleda v podatke svojih uporabnikov. Varnost je namreč največja skrb računalništva v oblaku, kar je potrdila tudi raziskava Harvard Business Review, v kateri je nekaj čez 50 odstotkov uporabnikov izrazilo zaskrbljenost, povezano z varnostjo podatkov (Knorr, 2011). Tako tudi Dropbox ni imun na varnostne pomanjkljivosti, kar je razvidno iz številnih virov (Cardwel, 2011; de Icaza, 2011; Kovach, 2011; Mulazzani, Schrittwieser, Leithner, Huber & Weippl, 2011; Newton, 2011). Sodobni standardi aplikacij v oblaku težijo k temu, da je treba varnost nadgraditi (Zhou, Zhang, Xie, Qian & Zhou, 2010) zato tudi Dropbox potrebuje izboljšane mehanizme za varovanje podatkov.

V članku bomo predstavili varnostna tveganja in grožnje zasebnosti storitve Dropbox ter varnostne incidente, povezane z omenjeno storitvijo. Prav tako bomo obravnavali programske rešitve za obravnavanje tveganj in pokazali, da imajo tudi te določene pomanjkljivosti. Predstavili bomo programsko rešitev SecretShare, ki naslavlja pomanjkljivosti obstoječih programskih rešitev za varovanje podatkov v storitvi Dropbox.

V naslednjem razdelku bomo na kratko predstavili storitev v oblaku Dropbox, njeno delovanje in varnostne mehanizme, ki jih vključuje. V tretjem razdelku bomo identificirali varnostne težave in pomanjkljivosti storitve Dropbox. Predzadnji razdelek predstavlja ukrepe, ki jih lahko izvedejo uporabniki, da zavarujejo svoje podatke, shranjene na Dropboxu. Opisali bomo orodja, ki so na voljo, jih primerjali in izpostavili njihove pomanjkljivosti. V zadnjem razdelku bomo opisali aplikacijo, ki naslavlja varnostne pomanjkljivosti in omogoča varno souporabo podatkov, shranjenih na Dropboxu.

2 DROPBOX

Dropbox je brezplačna storitev v oblaku, ki omogoča sinhronizacijo podatkov med več računalniki oz. med več različnimi napravami (slika 1). Storitev je na voljo od leta 2007, upravlja pa jo podjetje Dropbox inc. Začetnika in ustanovitelja Dropboxa sta Drew Houston in Arash Ferdowsi. Dropbox ima danes že več kot 50 milijonov uporabnikov (Dropbox, 2012). Bil je ena izmed prvih storitev za hrambo podatkov v oblaku in je trenutno med najbolj popularnimi (Vaughan-Nichols, 2013). Podobne storitve so SugarSync, iCloud in SkyDrive (Turim-Nygrem, 2012).



Slika 1: **Sinhronizacija podatkov med več računalniki oz. prenosnimi napravami (Dropbox, 2012)**

Dropbox ni samo storitev za hrambo lastnih podatkov v oblaku, omogoča tudi souporabo datotek z drugimi uporabniki. Do podatkov lahko dostopamo z različnih odjemalcev (računalnik, mobilne naprave idr.) ter prek spletnega vmesnika. Prav tako storitev podpira pregled in nadzor nad različicami dokumentov.

2.1 Delovanje

Večji del storitve Dropbox je razvit v programskem jeziku Phyton (Dropbox, 2012). Na odjemalcu uporabnika se vse lokalne datoteke v označeni mapi sinhronizirajo s strežnikom Dropbox in z vsemi drugimi napravami, ki so v lasti uporabnika. Slika 1 prikazuje sinhronizacijo datotek med več različnimi napravami. Uporabnik shrani datoteko na lokalnem računalniku, kopija te datoteke se prenese na storitev in na vse druge naprave, ki so v lasti uporabnika.

Dropbox datoteke razdeli na kose velikosti 4 MB. Kadar uporabnik doda novo datoteko v Dropbox mapo na lokalnem računalniku, aplikacija izračuna prstni odtis datoteke z zgoščevalno funkcijo SHA – 256 (Mulazzani idr., 2011). Izračunano vrednost pošlje na strežnik storitve. Tam preveri, ali že obstaja kakšna datoteka s to izračunano vrednostjo. V primeru, da ne obstaja, prenese na oblak kopijo datoteke uporabnika. Če datoteka že obstaja, pa datoteke ne prenese v oblak, temveč naredi povezavo na to datoteko. S tem Dropbox prihrani prostor in omrežni promet ter pospeši sinhronizacijo podatkov (Cachin & Schunter, 2011).

Za dodatno povečanje učinkovitosti vpeljuje Dropbox tehniko delta kodiranja (angl. delta encoding). Tehnika omogoča, da se na strežnik naložijo samo tisti deli datotek, ki so bili spremenjeni pri predhodni sinhronizaciji s strežnikom (Dropbox, 2012).

2.2 Mehanizmi in tehnike varovanja podatkov

Dropbox zagotavlja več varnostnih mehanizmov za komunikacijo s storitvijo, prenos in shranjevanje podatkov. Za komunikacijo in prenos podatkov uporablja SSL/TLS (angl. Secure Socket Layer/Transport Layer Security), medtem ko za varovanje shranjenih podatkov uporablja šifrirni algoritem AES-256. Za fizično varovanje in varnostne kopije podatkov skrbijo Amazonove storitve (Dropbox, 2012).

Varovana povezava

Za varovanje povezave med odjemalcem in strežnikom uporablja Dropbox protokol SSL (angl. Secure Socket Layer); to je protokol, prek katerega lahko varno pošiljamo podatke. Podatki, ki jih pošiljamo prek SSL so namreč zavarovani s šifriranjem. SSL omogoča, da so podatki, ki jih odjemalec pošilja storitvi v

oblaku Dropbox, zavarovani in nedostopni napadalcem oz. tretjim osebam.

Šifriranje podatkov

Vse datoteke, shranjene na Dropboxu, so šifrirane. Za šifriranje uporabljamo algoritem AES z 256-bitnim ključem. AES (angl. Advanced Encryption Standard) je mednarodni standard za šifriranje in dešifriranje podatkov s simetričnim ključem in velja za varni šifrirni algoritem (NIST, 2001a). Prav tako ni poznan noben učinkovit napad na AES (Ferguson, Schneier & Kohno, 2011). Zaradi 256-bitne dolžine ključa je neučinkovit tudi napad z izčrpnim iskanjem ključa (angl. Exhaustive Key Search).

Uporabljeni šifrirni ključi so neodvisni od uporabnika, saj ta nanje nima vpliva. Ker s šifrirnimi ključi upravlja Dropbox, ni poznano, kako se dodeljujejo ključi in kje se hranijo (Kassner, 2011). Zaradi uporabe šifriranja so shranjeni podatki nedostopni oz. neberljivi drugim uporabnikom.

Amazonove storitve

Za shranjevanje podatkov uporablja Dropbox Amazonovo storitev Simple Storage Service (Dropbox, 2012). Tako je varnost podatkov v veliki meri odvisna od nje.

Podjetje Amazon ponuja številne storitve ter ima veliko izkušenj pri razvoju in načrtovanju velikih in varnih podatkovnih centrov. Glede fizične varnosti infrastrukture imajo pri Amazonu zelo visok vojaški standard (Amazon, 2012). Podatkovni centri so nastanjeni na različnih lokacijah, vgrajene imajo različne kontrole dostopa. Fizični dostop ima samo avtorizirano osebje, ki se mora trikrat overiti z dvema načinoma identifikacije (Two-factor authenticaion[1]) (Rouse, 2005). Prenos podatkov do Amazonovih storitev poteka prek HTTPS. Uporablja različne načine mehanizmov kontrole dostopa:

- IAM (Identity and Access Management),
- ACLs (Access Control Lists) in
- avtentikacijsko povpraševanje (angl. query string authentication).

Dostopnost do podatkov in zanesljivost storitve naj bi bila po trditvah Amazona 99,99-odstotna. Načrtovana je tako, da zagotavlja razpoložljivost podatkov tudi v primeru, če sočasno prenehata delovati dva podatkovna centra (angl. facilities) (Amazon, 2012).

3 VARNOSTNE POMANJKLJIVOSTI STORITVE

Kljub vsem varnostnim mehanizmom smo identificirali določene varnostne pomanjkljivosti, s katerimi je lahko ogrožena varnost shranjenih podatkov. V nadaljevanju bomo obravnavali varnostna tveganja za podatke, shranjene v oblačni storitvi Dropbox.

3.1 Upravljanje s šifrirnimi ključi

Kljub temu da je za šifriranje uporabljen algoritem AES-256, se poraja vprašanje upravljanja s šifrirnimi ključi. Z njimi namreč upravlja Dropbox. Iz tega bi lahko sklepali, da lahko Dropbox dostopa do podatkov, shranjenih na njegovi storitvi v oblaku (De Icaza, 2011). V Dropboxovem pravilniku zasebnosti (angl. private policy) je namreč navedeno, da imajo zaposleni v podjetju Dropbox prepovedan vpogled v datoteke uporabnikov. Največkrat je človek najšibkejši člen verige varovanja, zato se porajajo pomisleki o ustreznosti varovanja podatkov (Cachin & Schunter, 2011). Celo pri »velikanu« Googlu so zaposleni zlorabljali podatke uporabnikov (Popkin, 2010).

Naslednja kočljiva točka v pogojih uporabe storitve Dropbox je dejstvo, da ima Dropbox pravico oz. je zavezan k temu, da podatke uporabnikov posreduje organom pregona. Tudi tako lahko pride do zlorab (Gaddis, 2011).

3.2 Datoteka config.db

Varnostno tveganje pomeni tudi datoteka config.db, ki se namesti na uporabnikov računalnik skupaj z odjemalcem Dropbox. V datoteki config.db so zapisani podatki za overjanje s storitvijo Dropbox. Podatki so shranjeni v formatu SQLite. Zaradi varnostne zasnove, ki jo uporablja Dropbox, je datoteka varnostno kritična. Najzanimivejši podatki v datoteki so:

- e-mail – elektronski naslov uporabnika računa,
- dropbox_path – pot do datoteke, v kateri se nahaja mapa Dropbox,
- host_id – identifikacija sistema, ko je ta nameščen in overjen.

Za overjanje tako uporabljamo samo atribut host_id. Če napadalec pride do vsebine datoteke config.db oz. samo do vrednosti atributa host_id, ima dostop do vseh naših podatkov na Dropboxu (Newton, 2011). Tudi v primeru, da uporabnik spremeni geslo, je host_id še vedno veljaven.

[1] Aventikacija na način »nekaj, kar oseba ima (identifikacijsko kartico), in nekaj, kar oseba zna (geslo)«.

Sicer drži, da ima napadalec verjetno tudi neposreden dostop do vaših datotek Dropbox, če ima dostop do uporabnikove config.db datoteke, vendar se kljub temu porajajo določena varnostna tveganja:

- enostaven virus bi lahko bil implementiran v namen pridobiti vsebino datoteke config.db;
- tudi v primeru odkritja takšnega virusa to napadalcu ne bi preprečilo dostopa do vaših datotek Dropbox, saj bi že imel vsebino datoteke config.db;
- prikrit prenos vsebine datoteke config.db je veliko težje odkriti, kot če bi napadalec želel prenašati celotne datoteke, ki jih ima uporabnik na Dropboxu.

Od Dropboxove verzije 1.2 naprej je bila konfiguracijska datoteka spremenjena. Tako imajo novejše verzije šifrirano datoteko config.dbx, kar preprečuje neavtoriziran dostop do vsebine atributa host_id. (Dropbox, 2012).

Storitev je mogoče uporabljati tudi na mobilnih aplikacijah, vendar določene mobilne naprave ne podpirajo varne povezave HTTPS. V teh primerih lahko napadalec prestreza podatke, ki jih pošiljamo ali pridobivamo iz Dropboxa (Cardwel, 2011; Kovach, 2011).

Kljub ukrepom, ki jih ima Dropbox za zagotavljanje varnosti, se je 20. junija 2011 zgodil incident. Tega dne so bili namreč dostopni vsi uporabniški računi brez overjanja. Napako naj bi povzročila posodobitev programske opreme. Uporabniški računi so bili prosto dostopni štiri ure. Po poročanju Dropboxa je bilo takrat aktivnih manj kot odstotek uporabnikov (Wikipedia, 2012).

4 ORODJA ZA VAROVANJE PODATKOV NA DROPBOXU

Iz do sedaj navedenega lahko sklepamo, da obstajajo določena varnostna tveganja pri uporabi storitve Dropbox. Zavedati se moramo, da podatke s tem, ko jih shranjujemo na Dropboxu, izpostavljamo možnosti nezaželenega vpogleda. Da bi preprečili nepooblaščene vpoglede, moramo podatke ustrezno varovati, kar lahko storimo s programskimi rešitvami. S tem lahko izboljšamo varnost podatkov, shranjenih v storitvah v oblakih. Varovanje podatkov je opredeljeno kot onemogočanje dostopa do podatkov nepooblaščenim osebam, tudi ponudniku storitve v oblaku. Rešitev je udejanjena v obliki šifriranja podatkov, kar pomeni, da podatke iz prvotne oblike pretvorimo v neberljivo obliko. Le z ustreznim geslom in ključem je nato mogoče dobiti prvotne, torej berljive podatke.

Vsi progami za šifriranje podatkov na Dropboxu delujejo podobno. Najprej šifrirajo podatke, nato jih predajo programu za shranjevanje v oblaku, ki jih sinhronizira v oblak. Ker sta šifriranje in sinhronizacija podatkov med seboj neodvisna, program za šifriranje ne pozna uporabniškega imena in gesla za Dropbox, Dropbox pa ne gesla za šifriranje oziroma dešifriranje podatkov.

Tudi Dropbox svetuje uporabo orodij za šifriranje, kot je recimo TrueCrypt (Dropbox, 2012). V ta namen smo obravnavali programska orodja, s katerimi lahko šifriramo podatke, ki jih shranjujemo na Dropbox. Programi uporabljajo različne postopke šifriranja, pri vseh pa so uporabljeni postopki varni, saj uporabljajo standardizirane šifrirne algoritme (Ferguson idr., 2011).

V tabeli 1 je predstavljena primerjava programov in njihovih glavnih značilnosti. Orodja smo primerjali glede na kriptografske lastnosti, s katerimi določamo raven varovanja podatkov. Zaščita je odvisna od uporabljenega algoritma in velikosti ključa – večji kot je uporabljeni ključ, višja je raven varnosti šifriranih podatkov (Ferguson idr., 2011).

Orodji TrueCrypt in AxCrypt sta splošno namenski, medtem ko sta SecretSync in BoxCryptor namenjena izključno šifriranju podatkov na Dropboxu. S tega vidika sta seveda tudi bolj primerna za takšno vrsto uporabe, njuna uporaba pa je preprostejša.

Tabela 1: **Primerjava orodij za varovanje podatkov**

Naziv orodja	**TrueCrypt**	**SecretSync**	**BoxCryptor Classic**	**AxCrypt**
Verzija	7.1a	1.3	1.6	1.7
Spletna stran izdelka	www.truecrypt.org	getsecretsync.com, http://www.viivo.com/	www.boxcryptor.com	www.axantum.com/axcrypt/
Podprte platforme	Windows, Linux, Mac OS	Windows, Linux, Mac OS, Android	Windows, Mac Os, Android, iOS	Windows
Cena	Odprtokoden	Do 2GB zastonj	Do 2GB zastonj	Odprtokoden
		Kriptografija		
Šifrirni algoritem[2]	AES, Blowfish, Twofish	AES	AES	AES
Velikost ključa (v bitih)	256	256	128–256	128
		Dropbox		
Upravljanje s ključi	Pri uporabniku	Na spletni storitvi	Pri uporabniku	Pri uporabniku
Način šifriranja podatkov	V celoti	Po datoteki	Po datoteki	Po datoteki
Šifriranje nazivov datotek	Podprto	Ni podprto	Podprto	Ni podprto
Souporaba podatkov	Ni podprto	Ni podprto	Ni podprto	Ni podprto

Vsi primerjani programi so brezplačni, vsaj v osnovni različici. Najučinkovitejše varovanje podatkov zagotavlja TrueCrypt, saj lahko izbiramo in kombiniramo med več različnimi šifrirnimi algoritmi (TrueCrypt, 2012). Nadloga pri uporabi je vnaprejšnje določanje velikosti šifrirnega navideznega pogona oz. datoteke. Težko je namreč predvidevati, koliko prostora bomo potrebovali. Prav tako je treba datoteko (navidezni pogon) najprej zapreti, da se lahko sinhronizira z oblakom, to pa lahko marsikomu povzroča nevšečnosti. S podobnimi težavami se srečujemo tudi pri uporabi AxCrpyta, saj ne omogoča samodejnega šifriranja datotek. Datoteke je namreč treba šifrirati in dešifrirati ročno. Tukaj sta v prednosti SecretSync in BoxCryptor, ki podatke šifrirata samodejno. Za razliko od TrueCrypta uporabljata šifriranje po posameznih datotekah. Največja razlika med njima je pri upravljanju s šifrirnimi ključi. Pri SecretSync z njimi upravlja storitev, pri BoxCryptorju pa uporabnik. Zaradi tega se zdi BoxCryptor primernejša izbira, saj zagotavlja večjo neodvisnost od ponudnika.

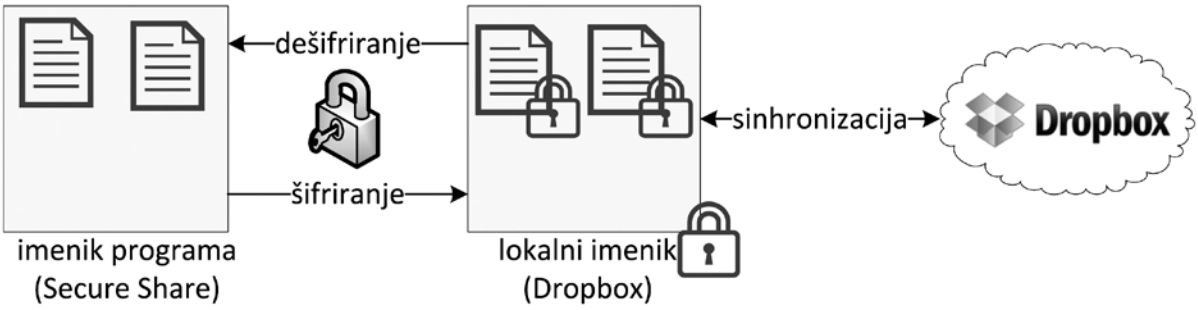
Težava nastane, ko želimo šifrirati podatke in omogočiti dostop do njih tudi drugim (izbranim) uporabnikom. Dropbox sicer omogoča deljenje datotek, vendar tega ne moremo več uporabljati, če uporabljamo katero izmed navedenih rešitev. Zaradi tega se poraja potreba po programski rešitvi, ki bi to omogočala.

5 SECURE SHARE

Kot smo ugotovili v prejšnjih razdelkih, je za zagotavljanje večje varnosti podatkov, shranjenih na Dropboxu, te treba dodatno zavarovati s šifriranjem. Obravnavali smo tudi prednosti in slabosti uporabe obstoječih orodij, s katerimi lahko šifriramo podatke. Ugotovili smo, da imajo vsi programi določene pomanjkljivosti, vendar je najbolj izstopajoče dejstvo, da souporaba datotek med uporabniki ni mogoča, če uporabljamo katero izmed obravnavanih programskih orodij.

Za zagotavljanje omenjene funkcionalnosti smo razvili novo programsko rešitev – Secure Share. Secure Share deluje podobno kot SecretSync, saj zagotavlja dodaten sloj nad podatki Dropbox. Slika 2 prikazuje njegovo delovanje. Šifrirni ključi so shranjeni pri uporabniku kot pri programskem orodju Box Cryptor. Prednost takšne rešitve je neodvisnost od delovanja in dosegljivosti ponudnika oz. storitve.

[1] (Ferguson, Schneier & Kohno, 2011)



Slika 2: **Delovanje šifriranja in sinhronizacije podatkov na Dropbox**

5.1 Predstavitev rešitve

Da bi dosegli čim večjo uporabnost orodja na vseh operacijskih sistemih, smo se odločili implementirati orodje v programskem jeziku Java. Uporabili smo najnovejšo različico Jave SE 7. Dodatnih knjižnic nismo vključevali, saj ima Java že v osnovi vključene implementacije potrebnih in preizkušenih šifrirnih algoritmov (Oracle, 2012).

Za šifriranje podatkov rešitev uporablja simetrične in asimetrične kriptografske algoritme. Pri simetričnih algoritmih imamo samo en zasebni ključ, s katerim šifriramo in dešifriramo podatke. Ti algoritmi so hitri in varni, težko pa je varno izmenjati ključ. Asimetrični algoritmi pa uporabljajo par ključev – zasebnega in javnega. Uporabnik si ustvari dva med seboj povezana ključa in enega objavi. Vsi, ki mu hočejo poslati sporočilo, bodo uporabili njegov javni ključ za šifriranje sporočila. Dešifriral pa ga bo lahko le uporabnik s svojim zasebnim ključem, ki je poznan samo njemu. Asimetrični šifrirni algoritmi so računsko bolj zahtevni kot simetrični in zato počasnejši (Ferguson idr., 2011).

Za šifriranje podatkov smo uporabili šifrirni algoritem AES z velikostjo ključa 256 bitov. Šifrirni algoritem je varen, vsestransko uporaben in hiter. Največjo velikost ključa, ki jo predvideva standard, smo uporabili z namenom zagotavljanja visoke ravni varovanja podatkov. Ker je AES bločna šifra, smo za način šifriranja uporabili veriženje šifriranih blokov (angl. Cipher Block Chaining – CBC) (NIST, 2001b). Za generiranje 256-bitnega ključa, ki je dejansko psevdonaključno število, smo uporabili javanski razred javax.crypto.KeyGenerator.

Da bi zagotovili varno izmenjavo ključev pri implementaciji funkcionalnosti za souporabo podatkov med več udeleženci, je bilo treba izbrati tudi asimetričen šifrirni algoritem (angl. Asymmetric Encryption Algorithm). Ker je v praksi najbolj splošno uporaben, smo uporabili algoritem RSA (Ferguson idr., 2011). Za dolžino parov ključev smo izbrali 2048 bitov, kar je tudi največja možna dolžina pri trenutni implementaciji v Javi (Oracle, 2012). Za generiranje parov ključev poskrbi razred java.security.KeyPairGenerator.

Za shranjevanje nastavitvenih lastnosti in šifrirnih ključev uporabljamo tri datoteke:

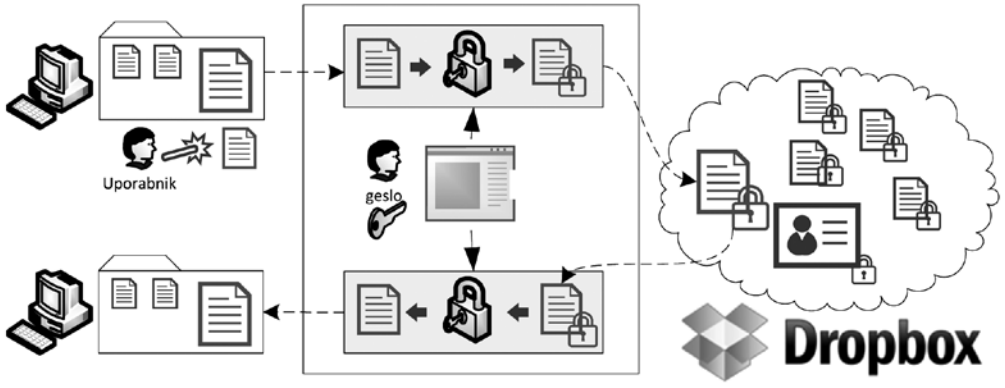
- Host.xyz: shranjeni so podatki o e-naslovu uporabnika ter lokacija mape Secure Share in lokalne mape Dropbox;
- Config.xyz: shranjuje podatke o uporabniku; datoteka se shranjuje v imeniku Settings, v katerem je nameščena aplikacija; podatki, ki jih hranimo, so e-naslov, geslo, šifrirni ključ, javni in zasebni ključ ter vrednost soli (angl. salt);
- Keys.xyz: vsebuje podatke o ustvarjalcu imenika, ki je bil dodan za souporabo, ter seznam javnih ključev oz. uporabnikov, ki imajo dostop do skupnega imenika.

Datoteke so šifrirane z uporabniškim geslom, kar onemogoča napadalcem pridobivanje nastavitvenih podatkov uporabnika.

Prikaz osnovnega delovanja šifriranja je viden na sliki 3. Uporabnik shrani datoteko v lokalnem imeniku programa Secure Share. Ko programska rešitev prepozna spremembo v imeniku, začne s postopkom šifriranja:

1. prebere šifrirani uporabniški ključ za simetrično šifriranje;
2. z uporabniškim geslom dešifrira simetrični ključ;
3. prebere vsebino nove ali spremenjene datoteke;
4. s simetričnim ključem šifrira novo ali spremenjeno datoteko in jo nato prekopira na Dropbox.

Dešifriranje poteka podobno:
1. program zazna spremembo v imeniku Dropbox;
2. prekopira vsebino datoteke;
3. pridobi uporabniški ključ za dešifriranje;
4. prekopira dešifrirano datoteko v lokalni imenik uporabnika.

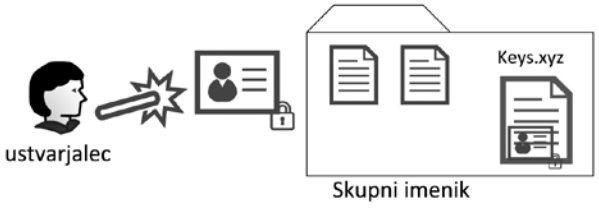


Slika 3: **Prikaz osnovnega poteka šifriranja**

Program tako vodi dvojno evidenco datotek. Lokalne izvorne in šifrirane na Dropboxu. Simetrični ključ, ki se uporablja za šifriranje, je shranjen v Dropboxovem imeniku in je zato vedno dosegljiv uporabniku. Zaradi varnosti je ključ šifriran z uporabniškim geslom.

Za implementacijo šifriranja podatkov za souporabo le-teh med več uporabniki smo uporabili asimetrično šifriranje za varno izmenjavo simetričnega ključa. Pri izvedbi je bilo treba poznati delovanje funkcionalnosti souporabe datotek v Dropboxu, ki jo bomo na kratko opisali v nadaljevanju.

Ko uporabnik doda določen imenik v souporabo, se zanj ustvari sejni ključ. Ključ ustvari aplikacija Dropbox tistega uporabnika, ki je prvi dodal imenik v skupno uporabo, in ta uporabnik je nato zadolžen za nadaljnjo distribucijo ključa. Ključ nato uporabljamo za šifriranje in dešifriranje datotek v imeniku, ki je v skupni rabi. V datoteko *keys.xyz* se zapiše, da je sejni ključ ustvarjen in kateri uporabnik ga je ustvaril (slika 4).

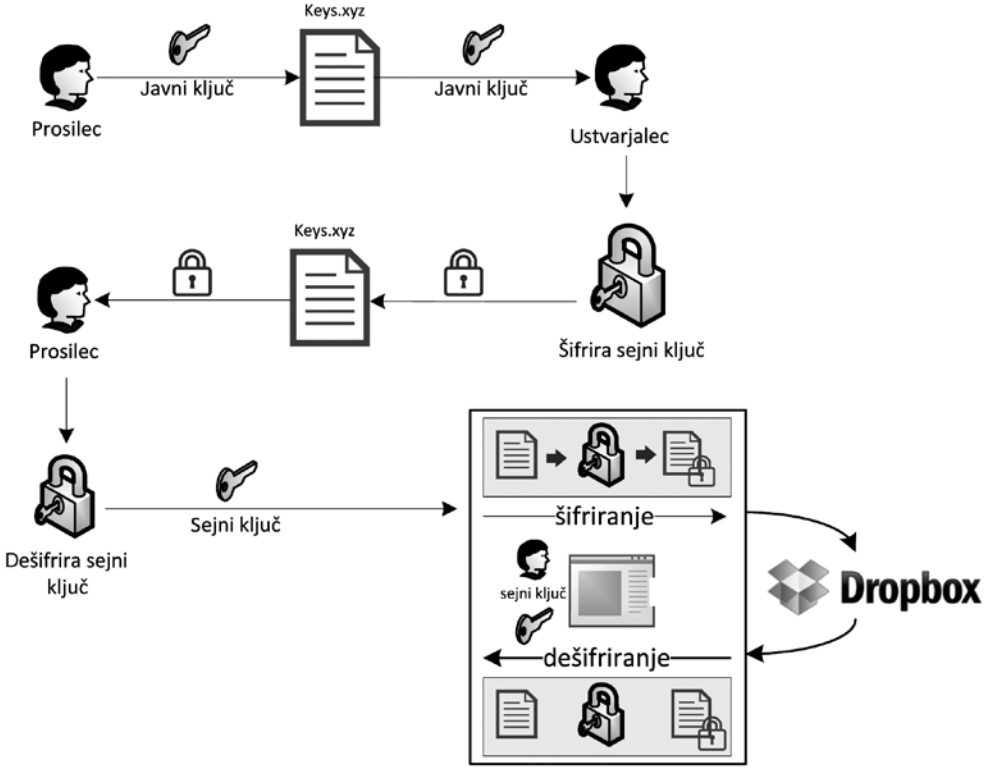


Slika 4: **Začetek postopka za šifriranje datotek v souporabi**

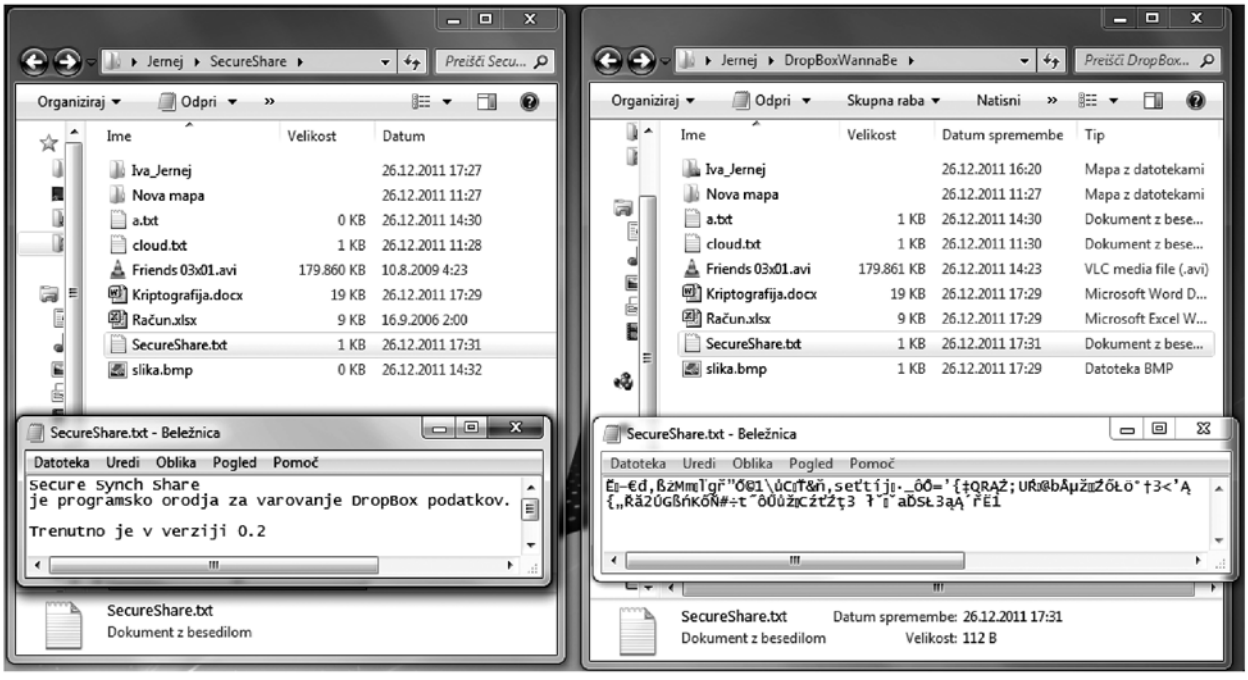
Da bi drugi uporabnik oz. uporabniki (v nadaljevanju prosilec) lahko začeli dešifrirati ali šifrirati datoteke v skupnem imeniku, mora najprej pridobiti ustrezen sejni ključ. Proces izmenjave sejnega ključa poteka takole (slika 5):
1. prosilec spremeni vsebino datoteke *keys.xyz* s tem, da ji doda vrednost svojega javnega ključa;
2. ustvarjalec skupnega imenika prepozna spremembo datoteke, prebere javni ključ prosilca ter šifrira z njim sejni ključ mape; spremembe shrani nazaj v datoteko keys.xyz;
3. prosilec zazna ponovno spremembo datoteke keys.xyz, prebere šifrirano vrednost sejnega ključa in ga dešifrira z zasebnim ključem; s tem pridobi vrednost sejnega ključa;
4. vsi uporabniki nato uporabljajo ta sejni ključ za šifriranje datotek za skupni imenik.

Ko so izmenjani ključi, poteka šifriranje datotek simetrično. Postopek se ponovi posebej za vsak skupni imenik ter za vsakega uporabnika.

Predstavljena rešitev je preprosta za uporabo in deluje popolnoma samodejno. Izvorne podatke shranjuje lokalno na računalniku uporabnika v posebnem imeniku, ki ga določi uporabnik. Ti podatki se nato šifrirajo in sinhronizirajo z mapo Dropbox. Na sliki 6 vidimo, kako so prikazani izvorni in šifrirani podatki na Dropboxu.



Slika 5: **Postopek izmenjave sejnega ključa**



Slika 6: **Prikaz izvornih in kriptiranih datotek, ki so med seboj sinhronizirane**

Pri dodajanju uporabnikov v skupni imenik se – vsaj z vidika uporabnika – nič ne spremeni. Ko doda uporabnik določen imenik v souporabo drugim uporabnikom, se datoteke samodejno začnejo šifrirati s skrivnim ključem, ki je poznan samo uporabnikom tega imenika.

Trenutna različica programske rešitve Secure Share ima tudi možnosti nadgradnje in izboljšave. Izpostavili bi optimizacijo branja datotek in njihovega šifriranja glede na njihovo velikost, s čimer bi lahko izboljšali odzivni čas. Izboljšati je mogoče tudi implementacijo izmenjave sejnega ključa oz. njegovo distribucijo. Trenutno lahko ključ distribuira le uporabnik, ki ustvari skupen imenik. Nadgradnja bi lahko omogočala, da bi sejni ključ distribuirali vsi uporabniki, ki ga posedujejo (za določen imenik v skupni rabi).

6 SKLEP

V prispevku smo predstavili programsko rešitev za varovanje podatkov na Dropboxu, imenovano Secure Share. Implementirana je v programskem jeziku Java, kar omogoča uporabo na več platformah. Rešitev omogoča lokalno šifriranje podatkov, preden te prenesemo v Dropboxov oblak. Dodatne mehanizme varovanja s pomočjo šifriranja je smiselno vpeljati, ko imamo opravka s korporativnimi uporabniki in občutljivimi (tudi zaupnimi) podatki. Pri analizi varnostnega vidika storitve Dropbox smo namreč ugotovili, da storitev ni popolnoma varna, kljub temu da uporablja varno povezavo in šifriranje podatkov (AES),. Varnostno tveganje pomeni upravljanje s ključi za šifriranje. Kljub temu da je šifriranje po standardu AES-256 zelo varno, je ključ pod nadzorom ponudnika shrambe v oblaku. Prav tako incident, ki se je pripetil, nakazuje, da ima storitev Dropbox določena tveganja in da je treba vpeljati dodatne varnostne mehanizme. Primerjali smo tudi orodja za varovanje podatkov in ugotovili, da sta orodji za šifriranje podatkov, kot sta TrueCrypt in SecretSync, primerni za dodatno varovanje podatkov. Podatke šifrirata lokalno, pri uporabniku. Do podatkov ima tako dostop le overjeni uporabnik, saj se šele šifrirani podatki prenesejo na Dropbox. Ob njuni uporabi pa nastopijo težave, saj se uporabnost Dropboxa lahko zmanjša. Težava je predvsem v omejeni zmožnosti souporabe podatkov (z drugimi uporabniki), saj je ne omogočajo omenjeni programi za varovanje. Predstavljena programska rešitev Secure Share rešuje omenjeni problem, kar je njena poglavitna prednost pred obstoječimi orodji oz. programskimi rešitvami. Funkcionalnost je realizirana z uporabo asimetričnega šifriranja, kar zagotavlja varno izmenjavo ključa za šifriranje podatkov, ki so v skupni rabi.

VIRI IN LITERATURA

[1] Amazon. (2012). Amazon Simple Storage Service (Amazon S3). Dostopno na http://aws.amazon.com/s3/ [oktober 2012].

[2] Cachin, C. & M. Schunter (2011). A cloud you can trust. IEEE Spectrum 48 (12) (December): 28–51. doi:10.1109/MSPEC.2011.6085778.

[3] Cardwel, M. (2011). Dropbox Mobile: Less Secure Than Dropbox Desktop. Dostopno na https://grepular.com/Dropbox_Mobile_Less_Secure_Than_Dropbox_Desktop [oktober 2012].

[4] De Icaza, M. Dropbox Lack of Security (2011). Dostopno na http://tirania.org/blog/archive/2011/Apr-19.html [oktober 2012].

[5] Dropbox. (2012). Dropbox. Dostopno na https://www.dropbox.com [oktober 2012].

[6] Geron, T. (2011, November 4). Dropbox Hits 25M Users, Expanding Internationally - Forbes. Forbes. Dostopno na http://www.forbes.com/sites/tomiogeron/2011/04/18/dropbox-ramping-up-towards-mainstream/ [januar 2013].

[7] Jeremy L. Gaddis. (2011). Why I Use Jungle Disk and Tarnsnap. Evilrouters. Dostopno na http://evilrouters.net/2011/04/20/why-i-use-jungle-disk-and-tarsnap/ [oktober 2012].

[8] Ferguson, N., Schneier, B. & Kohno, T. (2011). Cryptography Engineering: Design Principles and Practical Applications. John Wiley & Sons.

[9] Kassner, M. (2011). Dropbox: Convenient? Absolutely, but is it secure? Dostopno na http://www.techrepublic.com/blog/security/dropbox-convenient-absolutely-but-is-it-secure/5618.

[10] Knorr, E. (2011). Cloud computing by the numbers. InfoWorld. Retrieved May 29, 2012, from http://www.infoworld.com/t/cloud-computing/cloud-computing-the-numbers-983.

[11] Kovach, S. (2011). Don't Use Dropbox's Mobile Apps To Store Sensitive Files. Dostopno na http://articles.businessinsider.com/2011-03-14/tech/30018925_1_mobile-apps-private-files-sensitive-files [oktober 2012].

[12] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, & Aoying Zhou. (2010). Security and Privacy in Cloud Computing: A Survey. In 2010 Sixth International Conference on Semantics Knowledge and Grid (SKG) (str. 105–112). Presented at the 2010 Sixth International Conference on Semantics Knowledge and Grid (SKG), IEEE. doi:10.1109/SKG.2010.19

[13] Mulazzani, M., S. Schrittwieser, M. Leithner, M. Huber & E. Weippl (2011). Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space. In USENIX Security, 8:5–5. http://www.usenix.org/event/sec11/tech/full_papers/Mulazzani6-24-11.pdf.

[14] Newton, D. (2011). Dropbox Authentication: Insecure by Design. Dostopno na http://dereknewton.com/2011/04/dropbox-authentication-static-host-ids/ [oktober 2012].

[15] NIST. (2001a). Announcing the ADVANCED ENCRYPTION STANDARD (AES). Federal Information Processing Standards Publication 197 (FIPS PUBS). Dostopno na http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[16] NIST. (2001b). Recommendation for Block Cipher Modes of Operation: Methods and Techniques (NIST Special Publication 800-38A 2001 Edition). Washington, DC: U. S. Government Printing Office. Dostopno na http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.
[17] Oracle. (2012). Java Cryptography Architecture. Dostopno na http://docs.oracle.com/javase/7/docs/technotes/guides/security/StandardNames.html [oktober 2012].
[18] Popkin A. S., H. (2010). Google Had at Least Two Creepy Stalker Engineers. Technolog. Dostopno na http://www.technolog.msnbc.msn.com/technology/technolog/google-had-least-two-creepy-stalker-engineers-127006 [oktober 2012].
[19] Rouse, M. (2005). What Is Two-factor Authentication? WhatIs.com. Dostopno na http://searchsecurity.techtarget.com/definition/two-factor-authentication [oktober 2012].
[20] TrueCrypt. (2012). TrueCrypt - Free Open-Source Disk Encryption - Documentation - Version History. Dostopno na http://www.truecrypt.org/docs/?s=version-history [oktober 2012].
[21] Turim-Nygren, M.(2012). Best of the cloud: 7 top cloud storage services compared. Dostopno na http://www.digitaltrends.com/computing/the-7-best-cloud-storage-services-compared [december 2012].
[22] Vaughan-Nichols, S. J. (2013). The top 10 personal cloud-storage services. ZDNet. Dostopno na http://www.zdnet.com/the-top-10-personal-cloud-storage-services-7000011729/ [februar 2013].
[23] Wikipedia. (2012). Dropbox (service). Wikipedia, the Free Encyclopedia. Wikimedia Foundation, Dostopno na http://en.wikipedia.org/w/index.php?title=Dropbox_(service) [oktober 2012].
[24] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), 7–18.

▪

Jernej Flisar je tehniški sodelavec na Fakulteti za informatiko, računalništvo in informatiko Univerze v Mariboru. Diplomiral je leta 2010 in magistriral leta 2012. Njegova raziskovalna področja zajemajo semantični splet, varovanje podatkov in računalništvo v oblaku.

▪

Marko Hölbl je diplomiral leta 2004 in doktoriral leta 2009 na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Trenutno je na tej fakulteti zaposlen kot docent. Raziskovalno se ukvarja z informacijsko in računalniško varnostjo, s kriptografijo in z varnostjo e-poslovanja..