Da li su elektronski sertifikati zaista bezbedni?

Stevan A. Milinković

***Sadržaj* — U radu je prikazan nedostatak Infrastrukture javnog ključa (PKI) kod izdavanja digitalnih sertifikata. Upotrebom predloženog scenarija moguće je napraviti lažni sertifikat sertifikacionog tela sa originalnim elektronskim potpisom. Takav sertifikat omogućuje da se lažira bilo koji web sajt, uključujući banke, e-trgovine i ostale koji koriste HTTPS protokol. Opisana tehnika zasnovana je na slabosti kriptografske heš funkcije, poznatom pod imenom MD5 kolizija.**

***Ključne reči* — Digitalni sertifikati, heš kolizija, PKI, sertifikaciono telo.**

I. UVOD

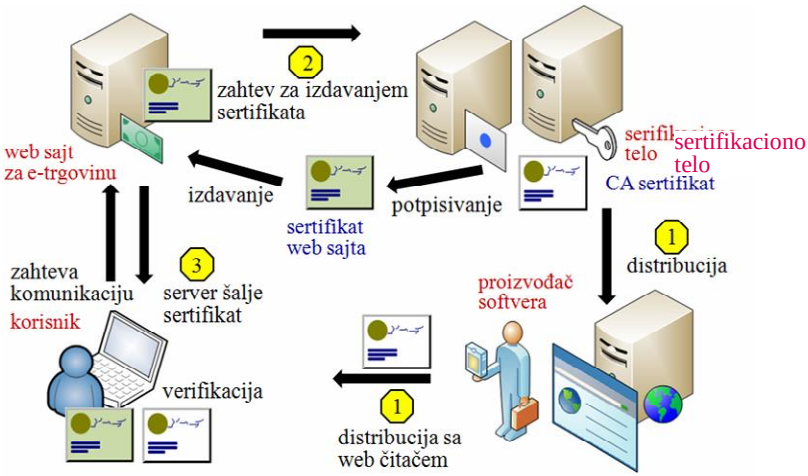
BEZBEDNOST transakcija na Internetu jedan je od postulata elektronske trgovine. Ukoliko bi ona bila narušena, sam smisao elektronske trgovine bio bi doveden u pitanje. Zbog toga se bezbednosti posvećuje značajna pažnja, uz oslanjanje na PKI (Infrastrukturu javnog ključa) [1]. Suština PKI je uspostavljanje poverenja između dva entiteta, koje se zasniva na međusobnoj autentifikaciji i razmeni kriptografskog materijala za buduću šifrovanu komunikaciju. Pri tome, koriste se usluge institucije od visokog poverenja - sertifikaciong tela (engl. *Cetrification Authority* - CA). U okviru digitalnog sertifikata koji izdaje sertifikaciono telo korisniku, nalazi se, pored ostalog, i korisnikov javni kriptografski ključ. Sertifikaciono telo garantuje tačnost podataka u sertifikatu tj. garantuje da javni ključ koji se nalazi u sertifikatu pripada korisniku čiji su podaci navedeni u tom istom sertifikatu. Zbog toga ostali korisnici na Internetu, ukoliko imaju poverenje u sertifikaciono

Stevan A. Milinković, Računarski fakultet univerziteta „Union“, Knez Mihailova 6/VI, 11000 Beograd, Srbija (telefon: +381-11-2633-321; e-mail: smilinkovic@raf.edu.rs).

Rad je u skraćenom obimu izložen na IX međunarodnoj konferenciji o elektronskoj trgovini i elektronskom poslovanju - *e-trgovina*, Palić, 22-24.04.2009.

telo, mogu da budu sigurni da određeni javni ključ zaista pripada korisniku koji je vlasnik pripadajućeg tajnog ključa. Ali, da li treba bezuslovno verovati sertifikacionom telu?

Radi osiguranja tipičnog sajta za elektronsku trgovinu, standardni scenario je otprilike sledeći: Šaljemo legitimni zahtev komercijalnom sertifikacionom telu (najčešće je u pitanju root CA, kao npr. RapidSSL) tražeći sertifikat koji prepoznaju standardni web čitači (Microsoft Internet Explorer, Mozilla Firefox). Sertifikaciono telo potpisuje traženi sertifikat koristeći md5RSA algoritam i vraća ga nama (Sl.1). Međutim, naš legitimni zahtev je tako napravljen da je dobijeni sertifikat u koliziji sa drugim, prethodno pripremljenim, lažnim sertifikatom. Ovaj lažni sertifikat nije sertifikat web sajta, već sertifikat lažnog sertifikacionog tela u lancu (Intermediate CA), koje može da izdaje sertifikate drugim sajtovima ili nižim sertifikacionim telima, a koje će priznati svi web čitači na Internetu.



Sl.1. Upotreba elektronskih sertifikata

Kako je ovo moguće? To se postiže obezbeđivanjem identičnih MD5 heš vrednosti za legitimni i lažni sertifikat. Odatle sledi da digitalni potpis, koji smo dobili od komercijalnog sertifikacionog tela, može jednostavno da se kopira u naš lažni sertifikat, a da on i dalje ostane važeći. Znači, potpis je originalan i ispravan, ali je potpisani dokument lažan. Time je narušena PKI filozofija u kojoj se sertifikacija obavlja zbog toga da bi se izbegle ovakve situacije.

II. KRIPTOGRAFSKE HEŠ FUNKCIJE

Heš (engl. *hash*) funkcije su jednosmerne funkcije kod kojih je ulazna vrednost poruka proizvoljne dužine, a izlazna vrednost niz bajtova fiksne dužine - heš vrednost. To znači da je jednostavno izračunati heš vrednost za datu poruku, ali je voma teško rekonstruisati poruku iz date heš vrednosti. Heš funkcije često se koriste u bezbednosnim primenama, kao što je autentifikacija, provera integriteta, digitalni sertifikati, digitalni potpisi i generatori pseudo-slučajnih brojeva. Zbog toga je potrebno da heš fukcija H ispunjava sledeće uslove:

- Jednosmernost (Preimage Resistance): Za datu heš vrednost h teško je naći poruku m takvu da je $h = H(m)$.
- Slaba koliziona otpornost (Second Preimage Resistance): Za datu poruku m_1 teško je naći drugu poruku $m_2 \neq m_1$ takvu da je $H(m_1) = H(m_2)$.
- Jaka koliziona otpornost (Collision Resistance): Teško je naći različite poruke m_1, m_2 takve da je $H(m_1) = H(m_2)$.

Jedan od najčešćih algoritama za nalaženje heš vrednosti je MD5 [2]. On koristi Merkle-Damgård-ov iterativni algoritam [3] gde se ulaz sastoji od niza bitova koji se popunjavaju da bi se dobio celobrojni umnožak od 512 bitova, tj. ulaznih blokova. Jezgro MD5 čini tzv. kompresiona funkcija. Ulazni blokovi se ubacuju u MD5 sukcesivnim pozivanjem kompresione funkcije, koja koristi svaki ulazni blok radi obnavljanja internog stanja veličine 128 bitova. Ovo stanje se naziva još i unutrašnja međuvrednost heš funkcije (*Intermediate Hash Value* – `IHV`). Kompresiona funkcija kao ulaz uzima unutrašnje stanje `IHV` od 128 bitova i ulazni blok podataka od 512 bitova. Rezultat funkcije je novo stanje `IHV`. Početno stanje `IHV` ima fiksnu vrednost, a krajnje stanje je vrednost tražene heš funkcije.

Ako svaki od ulaznih blokova označimo sa M_1, M_2, ..., M_n (svaki je veličine 512 bitova), početnu vrednost stanja `IHV` sa IHV_0 (128 bitova), a kompresionu funkciju sa `CF`, tada je sekvenca izračunavanja data sa:

$$
\begin{aligned}
IHV_0 &= \text{fiksna vrednost} \\
IHV_1 &= CF(IHV_0, M_1) \\
IHV_2 &= CF(IHV_1, M_2) \\
IHV_3 &= CF(IHV_2, M_3) \\
&\vdots \\
IHV_{n-1} &= CF(IHV_{n-2}, M_{n-1}) \\
IHV_n &= CF(IHV_{n-1}, M_n) \\
MD5 &= IHV_n
\end{aligned}
$$

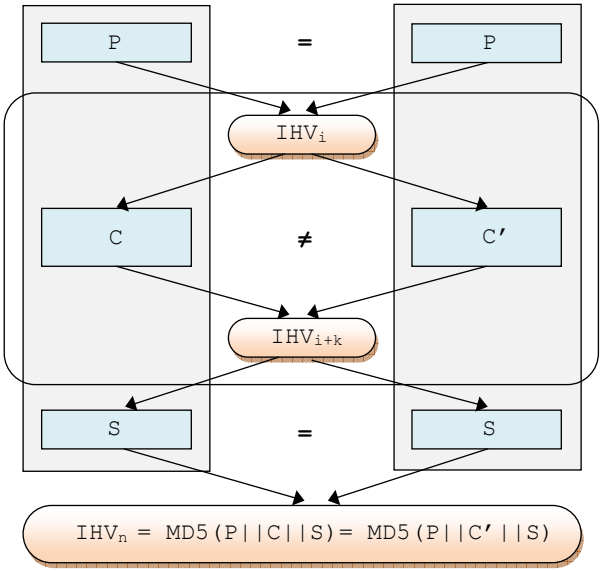
III. MD5 HEŠ KOLIZIJE

Rani rezultati dobijanja pesudo-kolizije kompresione funkcije objavljeni su u radu [4]. U pitanju je bilo nalaženje različitih početnih vrednosti koje daju identičnu heš vrednost. Međutim, nakon objavljivanja rada [5] bilo je jasno da je MD5 podložan napadu, kada je i preporučen prelazak na SHA-1 i RIPEMD-160. Dužina heš vrednosti od 128 bitova bila je dovoljno mala da omogući primenu „rođendanskog napada“ [6].

Marta 2004. započeo je distribuirani projekat MD5CRK koji je trebalo da dokaže nalaženje MD5 kolizije upotrebom rođendanskog napada, ali je ubrzo obustavljen, nakon objavljivanja rada [7] u kome su autori izvestili da su uspešno izvršili napad koji je trajao svega jedan sat.

Ubrzo je objavljen rezultat [8] u kome je prikazana metoda koja radi za svaku početnu vrednost IHV_0. Drugim rečima, metoda za svaki IHV_0 od 128 bitova, proizvodi par $\{\{M_1,M_2\}, \{M_1',M_2'\}\}$, od kojih svaki sadrži dva bloka od 512 bitova, takva da $\{M_1,M_2\} \neq \{M_1',M_2'\}$, kao i

$$IHV_0 = IHV_0'$$
$$IHV_1 = CF(IHV_0,M_1) \neq IHV_1' = CF(IHV_0',M_1')$$
$$IHV_2 = CF(IHV_1,M_2) = IHV_2' = CF(IHV_1',M_2')$$

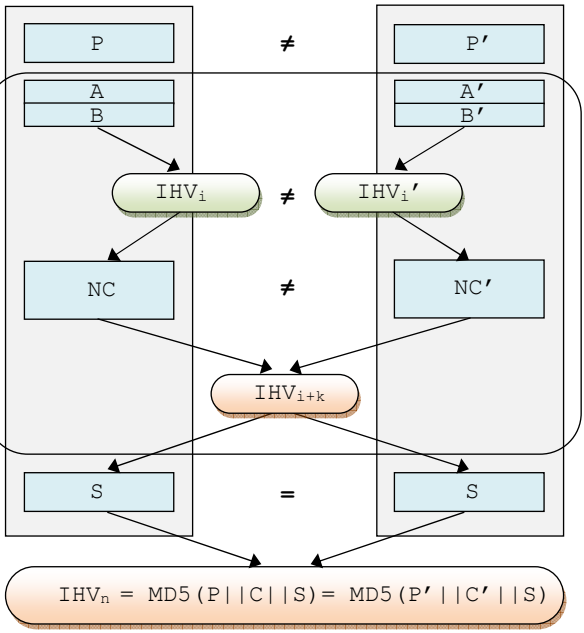


Sl.2. Kolizija bloka $\{C,C'\}$ za istu vrednost IHV_i.

Na osnovu iterativne strukture MD5, kao i na osnovu činjenice da IHV_0 može da ima bilo koju 128-bitnu vrednost, ovakve kolizije mogu da se kombinuju stvarajući duži niz ulaznih blokova. Konkretno, za bilo koji zadati prefiks `P` i sufiks `S`, može se izračunati kolizioni blok `{C,C'}` takav da je `MD5(P||C||S) = MD5(P||C'||S)`.

Terminom "kolizioni blok" naziva se niz bitova koji se ubacuje u drugi niz bitova da bi se postigla kolizija. Jedan kolizioni blok može da sadrži više ulaznih blokova (Sl.2). Kolizioni blok opisan u [8] sastoji se od tačno dva uzastopna ulazna bloka.

Skoro istovremeno, objavljen je rad [9] sa unapređenim algoritmom koji omogućuje pravljenje MD5 kolizije u toku nekoliko sati na običnom notebook računaru, a zatim i rad [10] sa još boljim algoritmom, koji svodi računanje na samo jedan minut, upotrebom tehnike pod nazivom „tunelovanje".



Sl.3. Kolizija sa odabranim prefiksom.

U radu [11] ova metoda je proširena na tzv. koliziju sa odabranim prefiksom (engl. *Chosen-prefix Collision*). To znači da kolizija može da se nađe upotrebom različitih proizvoljnih početnih vrednosti `IHV`, pri čemu metoda može da koristi više od dva ulazna bloka (Sl.3).

Ponovo, na osnovu iterativne strukture MD5, metoda kolizije sa odabranim prefiksom je u mogućnosti da, upotrebom proizvoljnog para odabranih prefiksa `{P,P'}` i bilo kog sufiksa `S`, proizvede kolizione blokove `{C,C'}`, takve da je `MD5(P||C||S) = MD5(P'||C'||S)`.

Za zadati par `{P,P'}` kolizioni blokovi se konstruišu na sledeći način. Prvo se `P` i `P'` popunjavaju nizovima bitova `A` i `A'` proizvoljne dužine da bi se postigla identična dužina `P||A` i `P'||A'`. Sledeće, upotrebom "rođendanskog" postupka proizvode se nizovi bitova `B` i `B'` takvi da rezultujući `P||A||B` i `P'||A'||B'` imaju istu dužinu i da su celobrojni umnošci od 512, a da odgovarajuće `IHV` imaju unapred zadatu strukturu. Tako nastaju tzv. blokovi bliske kolizije (engl. *Near Collision Blocks*) `{NC,NC'}`, koji na kraju omogućuju punu koliziju. Svaki od ovih blokova sastoji se od više 512-bitnih ulaznih blokova. Znači, kada je `C = A||B||NC` i `C' = A'||B'||NC'`, rezultujuće `IHV` vrednosti su identične. Odatle sledi, `MD5(P||C) = MD5(P'||C')`, što dalje znači da i za svaki sufiks `S` važi `MD5(P||C||S) = MD5(P'||C'||S)`.

Kolizija sa odabranim prefiksom ostvarljiva je u praksi, ali je znatno kompleksnija nego kolizija koja se dobija upotrebom identičnih početnih vrednosti za `IHV`. Međutim, s druge strane dobija se kompletna sloboda u izboru oba prefiksa `P` i `P'`. Ovo je od ključnog značaja za pravljenje kolizije sertifikata.

IV. KOLIZIJA SERTIFIKATA

A. Analiza dosadašnjih rezultata

Godine 2005. objavljen je rad [12] u kome je pokazano kako kolizija identičnih `IHV` vrednosti može da se ugradi u par X.509 sertifikata. Glavna ideja je da se kolizioni blokovi sakriju unutar javnog ključa koji se šalje sertifikacionom telu u zahtevu za izdavanje sertifikata. Kolizioni blokovi su pažljivo napravljeni, a izgledaju kao slučajni brojevi. Kada se sakriju unutar javnog ključa, koji je za posmatrača običan niz slučajnih brojeva, teško mogu da se otkriju čak i najpažljivijom pretragom. Kolizione blokove moguće je sakriti i unutar RSA modula, uz obezbeđivanje da parovi modula i dalje predstavljaju proizvod velikih prostih brojeva. Na taj način je pokazano kako se može napraviti par X.509 sertifikata sa identičnim MD5 heš vrednostima

onog dela koji se potpisuje, pa samim tim i sa identičnim CA potpisima. Ovo predstavlja kršenje fundamentalnih principa infrastrukture javnog ključa. Ali, imajući u vidu da prefiksi kolizionih ulaza moraju da budu jednaki, sertifikati su pokazivali isti identitet, što je sprečavalo njihovu realnu upotrebu.

Međutim, na osnovu rada [13], pojavila se mogućnost upotrebe MD5 kolizije odabranog prefiksa. To znači da je bilo moguće odabrati bilo koji par prefiksa u sertifikatu, koji se ubacuje pre RSA modula, a zatim dobiti sertifikate sa različitim odabranim identitetima i različitim javnim ključevima (koji kriju kolizione blokove), ali sa identičnim MD5 heš vrednostima onog dela koji se potpisuje, odnosno sa identičnim CA potpisim.

Ovo je bio veliki napredak, ali je postojalo ozbiljno ograničenje ukoliko bi takav zahtev bio upućen pravom sertifikacionom telu. Naime, napadač mora da odabere kompletan prefiks pre početka kolizionog procesa. Ovo uključije i ona polja nad kojima napadač nema direktnu kontrolu, kao što je period važenja i serijski broj potpisanog sertifikata. Uspešno predviđanje sadržaja tih polja znači imati značajnu kontrolu nad operacionim procedurama sertifikacionog tela, što je u principu vrlo teško postići. Dodatno, u radu [14] upotrebljen je 8192-bitni par RSA ključeva, koji još uvek nisu prihvaćeni od strane mnogih sertifikacionih tela.

Krajem 2008. god. grupa istraživača uspela je da dobije lažni sertifikat potpisan od strane komercijalnog sertifikacionog tela. Prvi korak je bio da se identifikuju sertifikaciona tela koja još uvek koriste MD5. Nažalost, nije moguće utvrditi koju heš funkciju koristi sertifikaciono telo direktno iz CA sertifikata, već samo iz sertifikata koje to telo potpisuje. U roku od nedelju dana specijalno napisan spajder je pretražio web i sakupio više od 100 000 SSL sertifikata, od kojih je oko 30 000 bilo potpisano od strane CA koji se nalaze u listi poverenja web čitača Firefox. Tu se nalazilo šest CA koji su potpisali sertifikate sa MD5 u 2008. i to su: RapidSSL, FreeSSL, TC TrustCenter AG, RSA Data Security, Thawte i verisign.co.jp. Od navedenih 30 000 sertifikata, oko 9000 je bilo potpisano upotrebom MD5, a 97% njih je izdao RapidSSL. Saznanje da toliki broj sertifikacionih tela i dalje koristi MD5 bilo je pravo iznenađenje, imajući u vidu da je prva MD5 kolizija bila demonstrirana još sada davne 2004. godine.

B. Postupak pravljenja lažnog sertifikata

Pravi sertifikat je dobijen od sertifikacionog tela slanjem zahteva za izdavanje sertifikata (Certificate Signing Request - CSR). Inicijalni zadatak bio je da se sastave takvi sadržaji CSR i lažnog sertifikata koji će biti maksimalno usaglašeni. Drugi, znatno teži zadatak bilo je predviđanje sadržaja različitih

polja pravog sertifikata i, na osnovu toga, konstrukcija različitih polja u oba sertifikata na način koji će dovesti do MD5 kolizije.

Saglasno sa standardom X.509, svaki od ova dva sertifikata sastoji se od:

- zaglavlja dužine 4 bajta,
- takozvani "deo za potpisivanje", dužine 927 bajtova (Tabela 1),
- naziv algoritma potpisivanja dužine 15 bajtova,
- polje potpisa dužine 131 bajt.

TABELA 1: STRUKTURA DELA KOJI TREBA POTPISATI U PRAVOM SERTIFIKATU.

bajtovi 0 - 3:	Zaglavlje
bajtovi 4 - 8:	Verzija (3, podrazumevana vrednost)
bajtovi 9 - 13:	Serijski broj (643015, postavljen od strane CA, ali je predviđen unapred po postupku opisanom u nastavku)
bajtovi 14 - 28:	Algoritam digitalnog potpisa ("md5withRSAEncryption", postavljen od CA)
bajtovi 29 - 120:	Izdavalac - Distinguished Name (CA standardna vrednost)
bajtovi 121 - 152:	Period važenja sertifikata ("od 3. novembra 2008. 7:52:02 to 4. novembra 2009. 7:52:02", postavljen od strane CA, ali je predviđen unapred)
bajtovi 153 - 440:	Subjekat (onaj kome se izdaje sertifikat) Distinguished Name (Country = "US", Organisation = "i.broke.the.internet.and.all.i.got.was.this.t-shirt.phreedom.org", Organisational Unit (3 postavljena od strane CA) Common Name = "i.broke.the.internet.and.all.i.got.was.this.t-shirt.phreedom.org", Country, Organisation and Common Name - postavljeni su prilikom slanja CSR)
bajtovi 441 - 734:	Informacije o javnom ključu subjekta: bajtovi 441 - 444: zaglavlje bajtovi 445 - 459: algoritam javnog ključa ("RSAEncryption", postavljen prilikom slanja CSR) bajtovi 460 - 468: zaglavlja bajtovi 469 - 729: RSA modul (2048 bitna vrednost, postavljena u CSR) bajtovi 730 - 734: RSA javni eksponent (65537, postavljena u CSR)
bajtovi 735 - 926:	Proširenja: bajtovi 735 - 740: Zaglavlja bajtovi 741 - 756: Upotreba ključa ("digital signature,

		nonrepudiation, key encipherment, data encipherment", postavljeno od strane CA)
	bajtovi 757 - 881:	Identifikator ključa subjekta, CRL distribucione tačke, Identifikator ključa sertifikacionog tela (polja koja postavlja CA, ali koja nisu interesantna u ovom razmatranju)
	bajtovi 882 - 912:	Proširena upotreba ključa ("server authentication, client authentication", postavlja CA)
	bajtovi 913 - 926:	Osnovna ograničenja ("CA = FALSE, Path Length = None", postavlja CA)

Radi dobijanja ovog sertifikata, sertifikacionom telu upućen je zahtev za izdavanje u formatu PKCS#10:

- Deo koji se potpisuje:
  - Broj verzije (1)
  - Zemlja subjekta = "US"
  - Poznato ime subjekta = "i.broke.the.internet.and.all.i.got.was.this.t-shirt.phreedom.org" (ovo CA koristi za polja Organisation i Common Name)
- Algoritam javnog ključa ("RSAEncryption").
- Javni ključ (sastoji se od RSA modula i RSA eksponenta).
- Algoritam potpisivanja ("md5withRSAEncryption").
- Potpis (2048 bitna vrednost izračunata upotrebom privatnog ključa nad delom koji treba potpisati). Ovaj potpis verifikuje sertifikaciono telo upotrebom javnog ključa koji se nalazi u zahtevu za izdavanje sertifikata, kao dokaz da mi zaista posedujemo privatni ključ.

Zahtevi za generisanje para asimetričnih ključeva za pravi sertifikat bili su sledeći: modul veličine 2048 bitova, javni eksponent - uobičajena vrednost 65537. Odgovarajući privatni ključ se čuva i koristi samo za potpisivanje CSR. Kolizioni blokovi sakriveni su unutar modula.

Usklađivanje je pokazalo da 256-ti bajt modula mora da počne od bajta 474. To znači da je na raspolaganju 38 bajtova tekućeg 512-bajtnog MD5 bloka. Prvih 26 bajtova su slučajno odabrani. Preostalih 12 bajtova upotrebljeno je za "rođendanske bitove". Zatim, imamo 3 bloka bliske kolizije od po 512 bitova (tj. svaki je 64 bajta). Celokupni kolizioni blok sadrži 96 + 3 x 512 = 1632 bita, odnosno 204 bajta. Na kraju poslednjeg kolizionog bloka uspostavljena je MD5 kolizija.

U kolizionom bloku ne postoji kontrola nad sadržajem već treba prihvatiti dobijene vrednosti onako kako su izračunate (izgledaju kao slučajni brojevi).

Na kraju, u modulu se nalazi i preostalih 256 - 26 - 204 = 26 bajtova (208 bitova). Oni su upotrebljeni da bi se ispunio zahtev da modul bude proizvod dva prosta broja (koji su poznati samo nama) na takav način da možemo da izračunamo odgovarajući privatni eksponent.

TABELA 2: LAŽNI CA SERTIFIKAT NAPRAVLJEN PREMA STANDARDU X.509.

bajtovi 0 - 3:	Zaglavlje	
bajtovi 4 - 8:	Verzija (3, podrazumevana vrednost)	
bajtovi 9 - 11:	Serijski broj (prozvoljno, u ovom slučaju mala vrednost - 65)	
bajtovi 12 - 26:	Algoritam digitalnog potpisa ("md5withRSAEncryption", zahtevan u CSR)	
bajtovi 27 - 118:	Izdavalac - Distinguished Name (CA standardna vrednost)	
bajtovi 119 - 150:	Period važenja sertifikata ("od 31 jula 2004. 0:00:00 do 2 setembra. 2004. 0:00:00")	
bajtovi 153 - 212:	Subjekat (onaj kome se izdaje sertifikat) Distinguished Name (Common Name = "MD5 Collisions Inc. (http://www.phreedom.org/md5)")	
bajtovi 213 - 374:	Informacije o javnom ključu subjekta:	
	bajtovi 213 - 215:	Zaglavlje
	bajtovi 216 - 230:	Algoritam javnog ključa ("RSAEncryption")
	bajtovi 231 - 237:	Zaglavlja
	bajtovi 238 - 369:	RSA modul (1024 bitna vrednost)
	bajtovi 370 - 374:	RSA eksponent javnog ključa (65537)
bajtovi 375 - 926:	Proširenja:	
	bajtovi 375 - 378:	Zaglavlja
	bajtovi 379 - 395:	Upotreba ključa ("digital signature, nonrepudiation, certificate signing, offline CRL signing, CRL signing")
	bajtovi 396 - 412:	Osnovna ograničenja ("CA = TRUE, Path Length = None")
	bajtovi 413 - 476:	Identifikator ključa subjekta (polja koja nisu interesantna u ovom razmatranju)
	bajtovi 477 - 926:	“tumor” (Netscape ekstenzija)

Polje koje od ovog sertifikata pravi CA sertifikat je “Osnovna ograničenja” ("Basic Constraints") sa vrednošću "CA = TRUE". Izabrana je mala vrednost za serijski broj sertifikata zbog velike verovatnoće da je pravi sertifikat sa ovim brojem odavno istekao (Tabela 2).

Bajtovi 0 - 473 u pravom sertifikatu (sva polja do modula, kao i prvih 5 bajtova modula, koji su u stvari predvidljiva zaglavlja) su fiksirani od strane CA. Ova 474 bajta čine odabrani prefiks na strani pravog sertifikata. Za ovaj sertifikat, izabrana dužina RSA ključa je 2048 bitova. Glavni razlog za ovakav izbor je činjenica da unutar njega mora da se sakrije kolizioni blok. Metoda konstrukcije kolizionog bloka davala je veličinu kolizionog bloka od 1632 bita, tako da je dužina od 2048 bila sasvim prihvatljiva. U današnje vreme, 2048-bitni RSA moduli sasvim su uobičajeni, tako da ni to nije izazivalo neku sumnju.

Na strani lažnog sertifikata, deo koji sadrži moduo javnog ključa ne koristi se za sakrivanje kolizionog bloka. Razlog za ovo je postavljanje CA indikatora u polju "Basic Constraints" na vrednost "TRUE", što je suprotno od originalnog sertifikata. Problem je što se polje "Basic Constraints" pojavljuje u sertifikatu posle javnog ključa, tako da se u lažnom sertifikatu javni ključ i sva proširenja do polja "Basic Constraints" nalaze ispred kolizionog bloka. Da bi se ovo postiglo, iskorišćena je neuobičajena dužina imena subjekta (Distinguished Name) u pravom sertifikatu, koja može da se sažme u odgovarajuću dužinu koji ima Common Name.

U isto vreme, Distinguished Name subjekta u lažnom CA sertifikatu napravljeno je da bude što kraće, da bi omogućilo dovoljno prostora za smeštanje javnog ključa od 1024 bita kao i polja "Basic Constraints", što sve treba smestiti u odgovarajuću oblast polja Distinguished Name pravog sertifikata. Na ovaj način sva potrebna polja koja pripadaju odabranom prefiksu lažnog CA sertifikata mogu da se smeste u prvih 477 bajtova dela za potpisivanje.

Sledeći problem je bilo polje u ekstenziji lažnog CA sertifikata u koje treba sakriti najmanje $3 \times 512 + 96 = 1632$ bita (204 bajta) kolizionog bloka. Ovi podaci izgledaju kao potpuno slučajni (na prvi pogled, nemaju nikakav smisao), jer nad njima nema nikakve kontrole pošto su oni rezultat izračunavanja kolizionog metoda. Drugi problem je što svi podaci odmah iza javnog ključa u pravom sertifikatu moraju da se kopiraju bit po bit u lažni CA sertifikat. Zajedno, ova polja imaju značajnu veličinu, tačnije 427 bajtova.

Ova dva problema zahtevaju neki prostor za sakrivanje 427 bajtova podataka, od kojih neki izgledaju sasvim slučajno, a neki imaju takav sadržaj koji ne bi trebalo da vide čitaoci sertifikata. Rešenje ovog problema je definisanje

tzv. "Netscape Comment" bloka. Ovo je specifična ekstenzija u koju mogu da se smeste bilo kakvi podaci, a koje će većina web čitača ignorisati. Manji problem je što format ovih podataka mora da bude IA5String, dok konkretni sadržaj nije u tom formatu. Većina ASN.1 parsera koji striktno prate standard buniće se zbog ovoga, ali to nije slučaj sa većinom aplikacionog softvera, koji jednostavno ignorišu ovo polje. Moguće je ovih 427 bajtova sakriti i u nekom drugom polju za ekstenzije. Tako npr., postoji sertifikat sa sakrivenim čitavim filmom u formatu MPEG-1 [15].

Ekstenzija za Netscape Comment zahteva zaglavlje od 23 bajta. Znači, sadržaj ekstenzije započinje od bajta 500, tako da to tačno može da bude početak "rođendanskih bitova". Kod pravog sertifikata, gde modul započinje od 474 bajta, prvih 26 bajtova su popunjeni slučajnim vrednostima.

U tehničkom smislu, odabrani prefiksi oba sertifikata završavaju se na bajtu 499. Kolizioni blok započinje od bajta 500. Kao što je već rečeno, ovaj kolizioni blok sastoji se od $96 + 3 \times 512 = 1632$ bita = 204 bajta, tako da se završava na bajtu 703.

Prema tome, od bajta 500 do bajta 926 nalazi se 427 bajtova unutar lažnog sertifikata koja za sam sertifikat nemaju nikakvog smisla. Ovaj veliki nepotrebni blok nazvan je "tumor" (za sada benigni).

Modul javnog ključa pravog sertifikata počinje od 474 bajta. Kako je prethodno objašnjeno, radi usklađivanja sa lažnim CA sertifikatom potrebno je nakako popuniti prvih 26 bajtova, pa je u tu svrhu upotrebljeno 26 slučajnih bajtova. Imajući u vidu da MD5 deli izlazni niz na blokove od po 512 bajtova, potrebno je razmišljati u jedinicama od po 64 bajta. Prema tome, imaćemo 12 neupotrebljenih bajtova, pre nego što krene novi blok od 512 bajtova sa novom `IHV` vrednošću. Znači, na bajtu br. 500 onog dela koji treba potpisati došli smo do stepena gde smo u pravom sertifikatu unutar modula, a u lažnom CA sertifikatu unutar tumora.

Metoda MD5 kolizije sastoji se od dva dela: "rođendanski" deo i deo bliske kolizije. Rođendanski deo se koristi za pripremu sledeću razliku vrednosti za `IHV` za dva sertifikata, na granici između dva 512 bitna bloka. Za rođendanski deo, na raspolaganju je 12 bajtova, odnosno 96 bitova. Zahvaljujući usavršenoj rođendanskoj proceduri, ovo je više nego dovoljno. Tačnije, za ovu proceduru potrebno je samo 72 bita, tako da je preostalih 12 popunjeno nulama.

Treba imati u vidu da su ova 72 rođendanska bita po svojoj prirodi potpuno različita u oba sertifikata i izgledaju kao niz slučajnih bitova. Oni se računaju upotrebom programa za nalaženje kolizije.

Zatim, tu su tri MD5 ulazna bloka, svaki dužine 512 bitova, što je 3 × 64 bajtova, čiji su redni brojevi od 512 do 703 bajta. Svaki od ova tri ulazna bloka konstruisan je upotrebom metoda za nalaženje kolizije sa ciljem da se ponište neke razlike u vrednostima `IHV`. Za razliku od rođendanskih bitova, ovi blokovi bliske kolizije razlikuju se samo u jednom ili dva bita (zato se i zovu "bliska" kolizija – odnosno "samo što nije" kolizija). Na kraju trećeg bloka razlika nestaje, dajući pravu koliziju MD5 kompresione funkcije. Počevši od 704. bajta, sadržaj oba sertifikata je identičan.

U pravom sertifikatu sada imamo 26 + 12 + 3 × 64 = 230 bajtova za modul koji ćemo obeležiti sa *B*. Sada je potrebno dodati niz bitova *S* dužine 208 (ostatak od 26 bajtova) takav da rezultujući niz $B \parallel S$ (2048 bita) predstavlja celobrojnu vrednost po RSA, tj. to je broj $n = p \times q$ gde su p i q prosti brojevi.

U nastavku, u pravom sertifikatu slede eksponent javnog ključa i sve ekstenzije za verziju 3 sertifikata. To zahteva ukupno 197 bajtova. Ove vrednosti, koje u pravom sertifikatu generiše sertifikaciono telo, jednostavno se kopiraju u tumor lažnog CA sertifikata.

Jedno od polja koja se tamo nalaze je i polje "Basic Constraints" u kome je postavljeno "CA = FALSE". Interesantno je da se bajtovi iz ovog bolja takođe nalaze i u tumoru, ali softver za obradu sertifikata ih neće prepoznati, a samim tim neće ni imati neko značenje.

Iza ekstenzija pravog sertifikata i tumora lažnog sertifikata, od bajta 926, deo koji se potpisuje se završava. Sada se poziva MD5 heš funkcija koja daje niz bajtova koji su u koliziji u oba sertifikata.

Na kraju sertifikata sledi polje sa algoritmom potpisa ("Signature Algorithm") kao i polje samog potpisa, koji su sada identični u oba sertifikata.

Upotrebom prethodno opisanog scenarija, pravo i postojeće sertifikaciono telo nam je obezbedilo važeći potpis za sertifikat koji nikada nije ni videlo niti zaista potpisalo.

Potencijal ovog napada je još veći nego što je to dobijanje ispravnog sertifikata za lažni web sajt. Lažni sertifikat može da postane sertifikat sertifikacionog tela drugog nivoa jednostavnim postavljanjem polja "CA = TRUE". Obzirom da mi posedujemo privatni ključ koji odgovara javnom ključu lažnog sertifikata, mi možemo da izdajemo proizvoljan broj sertifikata trećim licima, a da oni budu priznati od strane web čitača kao sertifikati kojima se može verovati.

C. Period važenja i serijski broj sertifikata

Predviđanje perioda važenja sertifikata nije težak problem. Sistemi za izdavanje sertifikata koji koriste RapidSSL i FreeSSL su u potpunosti automatizovani, tako da se svaki sertifikat izdaje tačno 6 sekundi nakon što korisnik klikne na završno dugme "OK" radi kompletiranja kupovine sertifikata. Imajući u vidu da vremenski pečati u polju za period važenja sertifikata koriste granularnost od jedne sekunde, jednostavno treba kliknuti na ovo dugme u proizvoljnom trenutku T–6 sekundi i dobiti sertifikat koji važi od T do T+1 godine.

Prva procena da je za dobijanje kolizionih sertifikata potrebno 3 dana značila je da je bilo potrebno predvideti serijski broj sertifikata tri dana unapred. Većina prikupljenih sertifikata imala je serijske brojeve koji su na prvi pogled bili slučajni i zbog toga teški za predviđanje, ali je primećeno da RapidSSL i FreeSSL koriste sekvencijalne serijske brojeve, tj. brojeve koji se, uz inkrementiranje, izdaju jedan za drugim. U toku rada sertifikacionog tela, ovaj broj se povećava na osnovu broja izdatih sertifikata. Statistička analiza serijskih brojeva od 9251 sertifikata izdatih od strane RapidSSL pokazala je da ovaj broj ima vrlo malu varijansu. U trodnevnom periodu između četvrtka i subote, tipično se izdaje između 800 i 1000 sertifikata.

Uz ove informacije, plan je bio sledeći: U četvrtak uveče kupljen je sertifikat koji je imao serisjki broj S. Na osnovu prethodne statistike, predviđa se da bi u nedelju (vreme T) serijski broj bio malo manji od S+1000. Nekoliko sati pre vremena T, započela bi kupovina sertifikata jednog za drugim, kako bi se serijski broj što više približio ciljanom, dobijajući serijski broj S+999 30 sekundi pre vremena T. Uz malo sreće da CA ne dobije nijedan zahtev tokom ovih 30 sekundi, slanjem zahteva u trenutku T dobiće se sertifikat sa predviđenim serijskim brojem.

D. Pravljenje kolizije

Pravljenje MD5 kolizije u osnovi je opisano u radu [13]. Međutim, da bi se napravila kolizija sertifikata u realnim uslovima, bilo je potrebno uvesti još neka značajna poboljšanja. Osnovna ideja je da se algoritam rastavi na dva dela.

U prvom delu pripremaju se razlike `IHV` na takav način da se mogu koristiti u drugom delu. Ovo se jednostavno radi rođendanskom pretragom za nalaženje takvog para koji ima `IHV` razliku određene strukture. Potrebno je napraviti optimalan izbor između rođendanskih bitova i broja blokova bliske kolizije. Pri tome, glavno opterećenje izračunavanja predstavlja rođendanska pretraga.

U drugom delu, prave se diferencijalne putanje koje su u mogućnosti da eliminišu određene razlike kod `IHV` bitova sa određenom verovatnoćom. Ovo se može nazvati pretraga za blokovima bliske kolizije. U nekoliko ovakvih blokova bliske kolizije, specijalne kombinacije razlika u bitovima mogu da se eliminišu nalaženjem novog diferencijalnog puta, tako da je od krucijanog značaja upotreba algoritama za automatsko nalaženje diferencijalnog puta.

Pvi pokušaj pravljenja kolizije sa odabranim prefiksom trajao je nešto više od jednog dana. Algoritam rođendanskog pretraživanja je računarski najzahtevniji, ali je srećom, veoma pogodan za izvršavanje na IBM Cell procesorima. Iako IBM ove procesore ne prodaje pojedinačno, oni se nalaze u igračkim konzolama Sony PlayStation 3. Na 200 ovakvih konzola koje su činile Linux klaster, rođendanska pretraga trajala je oko 18 sati. Za drugi deo (nalaženje 3 koliziona bloka i eliminaciju `IHV` razlika koje su ostale nakon prvog dela) bilo je potrebno manje od 10 časova na četvorojezgarnom PC računaru. Izvršavanje ovog dela nije pogodno za Sony PlayStation 3 zbog velikih zahteva za memorijom. Obzirom da su se delovi algoritma izvršavali na različitom hardveru, mogla se uvesti i izvesna preklapajuća obrada, tako da je bilo moguće izvršiti 3 pokušaja tokom jednog vikenda ($3 \times 18 + 10 = 64$ sata). Ukupna kompleksnost pravljenja kolizije može se proceniti na 2^{51} poziva MD5 kompresione funkcije, kada je na raspolaganju 30 GB memorije (ravnomerno raspoređene među čvorovima Sony konzola). Vikend je odabran zbog manjeg mrežnog saobraćaja prema sertifikacionom telu.

Ne računajući cenu hardvera (Sony PlayStation 3 je bio na raspolaganju istraživačima u jednoj igraonici), glavni trošak bilo je dobijanje pravog sertifikata u nekoliko pokušaja, najviše zbog lošeg tajminga u predviđanju serijskog broja. Svaki sertifikat kupljen od RapidSSL koštao je 45 USD. Međutim, ovo sertifikaciono telo dozvoljavalo je ponovno izdavanje sertifikata još 20 puta, tako da je jedan zahtev, u stvari, koštao samo 2,25 USD. Istraživači su potrošili ukupno 657 USD na ovom projektu.

E. Provera rezultata

Rezultat prethodno opisanog algoritma, podešavanja i usklađivanja su dva sertifikata koji se mogu učitati sa web lokacije [16]. Pored toga, na sajtu se nalaze i tekstualne datoteke, koje su rezultat izvršavanja programa `dumpasn1` [17] , gde se može dobiti detaljni uvid u oba sertifikata.

Upotreba prethodno opisanog lažnog sertifikata može se proveriti i "uživo". Potrebno je prethodno podesiti sistemski kalendar/časovnik na August 2004, a zatim kliknuti na link [18] ka web sajtu koji su postavili istraživači koji su doprineli ovom značajnom radu. Na sajtu su dati i detaljni

opisi kako je čitav poduhvat realizovan. Ono što je od izuzetne važnosti je da se, prilikom pristupanja ovojm sajtu, web čitač neće buniti, tj. da će prihvatiti sertifikat kao originalan.

F. Značaj postignutog rezultata

Svaki web sajt, bilo da je bezbedan (tj. koristi SSL) ili ne, bilo da je zasnovan na MD5, SHA-1, SHA-256, ili nekom drugom tipu sertifikata, bez obzira koje sertifikaciono telo je izdalo sertifikat, može da se lažira. Znači, nisu samo MD5-zasnovani sertifikati podložni ovom napadu.

Pokazano je da je u praksi moguće napraviti lažni sertifikat sertifikacionog tela, pa ako je to moguće uraditi sada, svakako će biti još lakše uraditi u budućnosti. Na to ukazuju istorijske činjenice. Za algoritme koji su se smatrali "bezbednim", nalazili su se ključevi, u početku teže, a kasnije sve lakše i lakše (DES, MD2, MD4 su samo neki primeri). Teoretski je moguće da je još neko to uradio i da već lažira web sajtove po svom nahođenju.

U kombinaciji sa poznatim slabim tačkama DNS protokola [19], [20] otvaraju se vrata *phishing* napadu koji se praktično ne može otkriti. Bez da i jednog trenutka u nešto posumnjaju, korisnici mogu da budu preusmereni ka malicioznim sajtovima koji izgledaju identično kao banka ili sajt za elektronsku trgovinu. Korisničke lozinke i ostali privatni podaci mogu da padnu u pogrešne ruke.

Ostale aplikacije koje obezbeđuju web komunikaciju upotrebom SSL protokola takođe mogu da budu pod udarom ovog napada (npr. elektronski potpis e-mail-a i slično).

G. Opoziv sertifikata

Interesantno je napomenuti da je jednom napravljen lažni sertifikat vrlo teško opozvati upotrebom mehanizma za opoziv u standardnim web čitačima. Postoje dva metoda za opoziv sertifikata: CRL i OSCP. Do pojave Firefox-a 3 i Internet Explorer-a 7, opcija opoziva bila je standardno isključena. Čak i u najnovijim verzijama, web čitači se oslanjaju na sertifikat očekujući da on sadrži URL koji pokazuje na server sa listom opoziva (engl. *Revocation Server*).

Napravljeni lažni CA sertifikat ima vrlo ograničen prostor, tako da je bilo teško uključiti takav URL, što znači da standardno ni Internet Explorer ni Firefox ne mogu da nađu server sa listom opoziva, da bi se proverila važnost sertifikata.

Kao rešenje ovog problema, sistemski administratori mogu da konfigurišu web čitače da uvek šalju upit kompanijskom OSCP serveru za informaciju o

opozivu, ali ova opcija nije lako ostvariva kod individualnih krajnjih korisnika. To ukazuje na važan problem koji treba rešiti u slučaju sličnih napada na sertifikate. Takve sertifikate što pre treba opozvati.

Još jedan interesantan scenario koji proizilazi iz navedenog je mogućnost DoS (Denial of Service) napada na postojeća sertifikaciona tela. Ako napadač želi da nečiji sertifikat bude povučen, (npr. konkurentska web trgovina), on može da upotrebi opisanu tehniku za dobijanje lažnog sertifikata od istog sertifikacionog tela, koji ima isti serijski broj kao i ciljni sertifikat. Čim se ovaj lažni sertifikat objavi, sertifikaciono telo nema drugog izbora nego da ga povuče. S obzirom da se povlačenje vrši samo na osnovu serijskog broja sertifikata, istovremeno biće povučen lažni ali i pravi sertifikat. Ovaj napad može da bude ubitačan ukoliko je meta napada sertifikat samog sertifikacionog tela. Napadač tako može da izazove povlačenje korenskog sertifikata, a sa njim i svih sertifikata koji zavise od njega u lancu sertifikata.

V. ZAKLJUČAK

A. Šta preduzeti?

Kao prvo, nema valjanog opravdanja za dalje korišćenje razbijenih kriptografskih primitiva, kada već postoje mnogo jača rešenja, kao što je npr. SHA-2.

Drugo, ne postoji zamena za bezbednosnu samosvest. Otvorenost po pitanju bezbednosnih problema, otkrivanje nedostataka i njihova tehnička rešenja od izuzetne su važnosti ako želimo da od Interneta napravimo sigurno okruženje. Saveti od strane eksperata moraju se uzeti najozbiljnije u obzir što pre. Treba zaboraviti na kompanijsku sujetu i ubrzati birokratiju. U opisanom slučaju, izbacivanje MD5 iz upotrebe trebalo je započeti već 2004.

Šta bi trebalo da preduzmu pojedinačni entiteti?

B. Korisnici

Surfovanje webom može da preusmeri korisnika na web sajt koji poseduje lažni SSL sertifikat. Korisnik ne može ništa da preduzme da se ovo ne dogodi. Doduše, on može da pokuša da to otkrije, ali prosečen korisnik weba za to jednostavno nema dovoljno znanja. Korisnik može da klikne na ispravno dugme ili da odabere ispravnu opciju iz menija web čitača u nameri da vidi detalje sertifikata web sajta koji posećuje. Upotrebljena heš funkcija se vidi u polju "Signature algorithm" gde "md5RSA" znači da je za potpis sertifikata upotrebljena MD5 heš funkcija. Ukoliko svi sertifikati u lancu, sve

do korenskog CA sertifikata koriste neku drugu heš funkciju (npr. SHA-1), to znači da sajt nije napadnut opisanim napadom.

Ako se MD5 ipak koristi, prevara može da se otkrije tek na nivou pojedinačnih bitova. Npr., čudno polje "Netscape comment" koje na prvi pogled sadrži vrednost 3, u stvarnosti je polje veličine 427 bajtova, koje se ne može videti na ekranu iz tehničkih razloga. Ekspert koji pregleda sertifikat upotrebom alata kao što je `dumpasn1`, u mogućnosti je da identifikuje takva čudna polja u sertifikatu. Međutim, standardni korisnik najverovatnije neće uočiti ništa.

C. Sertifikaciona tela

Preporučuje se da odmah prekinu izdavanje sertifikata koji su potpisani upotrebom MD5 algoritma. Da bi sprečili napad sa odabranim prefiksom, mogu da dodaju značajan broj slučajnih informacija, što bliže početku sertifikata. Serijski broj je dobro polje za ovu upotrebu jer se nalazi blizu početka sertifikata i dozvoljava upotrebu 20 bajtova koji mogu da budu slučajni. Mnoga sertifikaciona tela već koriste slučajan izbor serijskih brojeva, ali verovatno iz različitih razloga. Neki evropski zakoni o elektronskom potpisu (ali ne i naš) propisuju slučajne serijske brojeve za kvalifikovane SHA-1 sertifikate.

Ostale mere koje sertifikaciona tela mogu da preduzmu je upotreba parametra “Path Length” u polju “Basic Constraints”. Ukoliko CA ima politiku izdavanja sertifikata samo krajnjim korisnicima, ta politika može da se sprovodi postavljanjem parametra “Path Length” na vrednost 0.

U tom slučaju, opisani scenario napada može da se otkrije. Ali, i ovo otkrivanje može da se osujeti izmenom scenarija napada, kada se umesto lažnog CA sertifikata podmetne lažni sertifikat samog web sajta. Ovakav sertifikat može da se napravi na takav način da se kolizioni blok nalazi unutar samog javnog ključa, umesto u neupotrebljenim poljima, što čini otkrivanje izuzetno teškim.

Posebno interesantno pitanje je da li će sertifikaciona tela opozvati postojeće sertifikate potpisane upotrebom MD5. Scenario mogućeg napada bio je poznat još maja 2007, tako da su svi sertifikati od toga datuma potpisani upotrebom MD5 bili kompromitvani. Da li je zaista došlo do zloupotrebe potpuno je irelevantno. Za sada jedini poznati realizovani kontrolisani napad je prethodno opisan u decembru 2008. Ono što jeste važno je da li strane u bezbednoj komunikaciji imaju propisan i ispravan način da provere da li sertifikatima mogu da veruju ili ne.

D. Proizvođači web čitača i operativnih sistema

Proizođači softvera kao što su Microsoft (Windows i Internet Explorer) i Mozilla (Firefox) bi mogli da implementiraju pop-up prozor sa upozorenjem da se pojavio sertifikat potpisan upotrebom MD5. Blokiranje MD5 sertifikata je takođe moguće, ali je to ipak drastična mera. Proizvođači web čitača mogu da implementiraju proveru parametra "Path Length". Imajući u vidu da su proizvođači web čitača ti koji odlučuju koja će se sertifikaciona tela naći u njihovoj listi od poverenja, oni mogu da izvrše dodatan pritisak na ova tela da prihvate ispravne procedure i koriste jake kriptografske primitive.

E. Vlasnici web sajtova

Oni svakako mogu da provere da li njihovo sertifikaciono telo koristi odgovarajuće procedure, u ovom slučaju, da li koriste MD5 u svom elektronskom potpisu. Ukoliko ustanove nepravilnost, oni od svog sertifikacionog tela mogu da traže prelazak na bezbednije heš funkcije.

F. Da li treba preći na SHA-1?

Ukoliko se već ne koristi, zbog inercije celog sistema možda ne bi trebalo uvoditi ovu funkciju, jer je u radu [20] pokazano da je za nalaženje kolizije kod SHA-1 potrebno 2^{62} poziva kompresione funkcije, tako da je samo pitanje trenutka kada će kolizija biti napravljena u razumnom računarskom vremenu. Treba imati u vidu da se kriptografski algoritmi sve više implementiraju na GPU paralelnim arhitekturama, koje nisu skupe, a imaju sve bolje performanse. Zbog toga bi možda trebalo koristiti snažnije heš algoritme, kao npr. SHA-2, mada je i on već na udaru [22].

LITERATURA

[1] W. Kou, Ed., *Payment Technologies for E-Commerce*. Berlin: Springer Verlag, 2003, pp. 1-67.

[2] R. L. Rivest, "The MD5 Message Digest Algorithm", *RFC 1321*, April 1992.

[3] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1996, pp. 321-383.

[4] B. den Boer and A. Bosselaers, "Collisions for the Compression Function of MD5", *Advances in Cryptology, Proceedings Eurocrypt'93, LNCS 765*, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 293-304.

[5] H. Dobbertin, "Cryptanalysis of MD5 Compress", *EUROCRYPT '96 rump session*, Zaragoza, Spain, May 12-16, 1996.

[6] M. Bellare, T. Kohno, "Hash Function Balance and Its Impact on Birthday Attacks", *EUROCRYPT 2004*, Interlaken, Switzerland, May 2-6, 2004, pp. 401–418.

[7] X. Wang, D. Feng, X. Lai and H. Yu, "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD", *Cryptology ePrint Archive*: Report 2004/199. Available: http://eprint.iacr.org/

[8] X. Wang and H. Yu, "How to Break MD5 and Other Hash Functions", In: R. Cramer, Ed., "Advances in Cryptology - EUROCRYPT 2005", vol. 3494 of *Lecture Notes in Computer Science*. Berlin: Springer Verlag, 2005, pp. 19-35.

[9] V. Klima, "Finding MD5 Collisions – a Toy For a Notebook", *Cryptology ePrint Archive*: Report 2005/075. Available: http://eprint.iacr.org/

[10] V. Klima, "Tunnels in Hash Functions: MD5 Collisions Within a Minute", *Cryptology ePrint Archive*: Report 2006/105. Available: http://eprint.iacr.org/.

[11] M. Stevens, "On collisions for MD5", *MSc Thesis*, Eindhoven University of Technology, June 2007.

[12] A. Lenstra and B. de Weger, "On the possibility of constructing meaningful hash collisions for public keys", In: C. Boyd and J. M. G. Nieto, Eds, "Information Security and Privacy - Proceedings of ACISP 2005", vol. 3574 of *Lecture Notes in Computer Science*. Berlin: Springer Verlag, 2005, pp. 267-279.

[13] M. Stevens, A.Lenstra and B. de Weger, "Chosen-prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities", In: M. Naor, Ed., "Advances in Cryptology - EUROCRYPT 2007", vol. 4515 of *Lecture Notes in Computer Science*. Berlin: Springer Verlag, 2007, pp. 1-22.

[14] http://www.win.tue.nl/hashclash/TargetCollidingCertificates/

[15] http://www.cs.auckland.ac.nz/~pgut001/pubs/dave.der

[16] http://www.win.tue.nl/~bdeweger/CollidingCertificates/

[17] http://www.cs.auckland.ac.nz/~pgut001/dumpasn1.c

[18] https://i.broke.the.internet.and.all.i.got.was.this.t-shirt.phreedom.org/

[19] M. Olney, P. Mullen, K. Miklavcic, "Dan Kaminsky's 2008 DNS Vulnerability", *Sourcefire Vulnerability Research Team Report*, Sourcefire, Inc., July 25, 2008.

[20] D. Kaminsky, "Black Ops 2008: It's the end of the cache as we know it", August 2008. http://www.doxpara.com/DMK_BO2K8.ppt

[21] M. Cochran, "Notes on the Wang et al. 2^{63} SHA-1 Differential Path", *Cryptology ePrint Archive*: Report 2007/474. Available: http://eprint.iacr.org/2007/474.

[22] V. Klima, "On Collisions of Hash Functions Turbo SHA-2", *Cryptology ePrint Archive*: Report 2008/003. Available: http://eprint.iacr.org/2008/003.

ABSTRACT

This paper describes a vulnerability in the Internet Public Key Infrastructure (PKI) used to issue digital certificates for secure websites. By application of suggested scenario it is possible to create a rogue certificate, containing original electronic signature. This certificate allows to impersonate any website, including banking and e-commerce sites secured using the HTTPS protocol. Described technique takes advantage of a weakness in the cryptographic hash function, known as an MD5 collision.

Title of the Paper in English:

Are Electronic Certificates Really Secure?

Names of authors:

Stevan A. Milinković