METODE ZA PROVERU STATUSA I VALIDNOSTI DIGITALNIH SERTIFIKATA

METHODS FOR CHECKING STATUS AND VALIDITY OF DIGITAL CERTIFICATES

Mladen Veinović[1], Aleksandar Mišković[2]
[1]Univerzitet Singidunum, Beograd; mveinovic@singidunum.ac.rs
[2]Visoka tehnička škola, Kragujevac; amiskovic@kg.ac.rs

Sažetak
Upravljanje ključevima kojima se potpisuju digitalni sertifikati je veoma važan korak u obezbeđivanju mrežnih servisa. Digitalni sertifikat ima ograničen rok važenja, zapisan u odgovarajućem polju prema standardu X.509, koji se nakon isteka tog roka mora opozvati. Čest slučaj u praksi je da se digitalni sertifikat opozove pre isteka roka važenja. Sertifikaciono telo je u obavezi da javno objavljuje listu opozvanih sertifikata (*Certificate Revocation List* – CRL). U nekim slučajevima moguće je da se umesto liste opozvanih sertifikata koristi protokol za proveru statusa i validnosti sertifikata u realnom vremenu (*Online Certificate Status Protocol* – OCSP) koji daje pozitivan ili negativan odgovor o statusu digitalnog sertifikata. Treći metod se zasniva na korišćenju modela geografski distribuiranog servera za opoziv ključeva, a samim tim i digitalnih sertifikata. U ovom radu analiziraju se različite metode za proveru statusa i validnosti digitalnih sertifikata, mehanizmi opoziva sertifikata i njihova implementacija u PKI sistem sa osvrtom na moguće zloupotrebe.
Ključne reči: CRL, OCSP, *Key revocation*

Abstract
Management of keys used for digital signatures is an important step in providing network services. Digital certificate has a limited validity period, it is written in the corresponding box according to the standard X.509, that needs to be revoked after the expiration period. In practice, a digital certificate is often revoked before the expiration date. A Certification Authority is obliged to publish the Certificate Revocation List (CRL). In some cases, instead of the CRL, it is possible to use Online Certificate Status Protocol (OCSP), which gives a positive or a negative response to the status of a digital certificate. The third method is based on the use of a geographic server distribution model for key revocation, and thus also the digital certificates. This paper analyzes different methods for checking the status and validity of digital certificates, certificate revocation mechanisms and their implementation in the PKI considering also possible abuses.
Key words: CRL, OCSP, Key revocation

1.Uvod

Postojeći protokoli, tehnike i algoritmi koji se koriste u asimetričnoj kriptografiji bezbedni su ukoliko privatni ključ koji se koristi ostane tajna. Veoma je važno da se vest o kompromitovanju privatnog kjuča brzo prenese kroz mrežu. Međutim, isto toliko je važno da korisnik PKI (*Public*

Key Infrastructure – PKI) sistema pre upotrebe proveri status i validnost digitalnog sertifikata, a samim tim i privatnog ključa kojim je on potpisan.
Cilj upravljanja ključevima je da se obezbedi dostupnost ključeva za obe strane u komunikaciji, kao i dostupnost i efikasno upravljanje informacijama o ključevima koji su povučeni iz upotrebe. Sertifikaciono telo je u obavezi da objavljuje listu opozvanih sertifikata i da vodi računa da ona bude ažurna i dostupna svim korisnicima PKI sistema.
Dokumentom RFC5280 [1.] definisan je način izdavanja CRL liste, odgovarajući upravljački protokol i niz operacionih protokola (HTTP, LDAP,...) za dostavljanje CRL liste do klijenata. Povezanost u realnom vremenu na Internetu danas je veoma izražena, samim tim javlja se i potreba za proverom validnosti i statusa sertifikata u realnom vremenu. Kao dodatak ili zamena za liste opoziva koristi se OCSP protokol koji je definisan dokumentom RFC2560 [2.]. Pored ova dva najčešće korišćena metoda, dat je i prikaz modela geografski distribuiranog servera za opoziv ključeva u realnom vremenu koji nudi nova rešenja u ovoj oblasti [3.].

2. Provera statusa i validnosti digitalnih sertifikata

Veliki problem za korisnike digitalnih sertifikata predstavlja to što se podaci o opozvanim sertifikatima, od strane sertifikacionog tela (*Certification Authority* – CA), objavljuju najčešće jednom dnevno. Ovakav način upravljanja informacijama o povučenim sertifikatima može dovesti do toga da se neki sertifikati koriste iako su već povučeni.

1.1. Lista opozvanih sertifikata – CRL

Standardom X.509 definisan je metod povlačenja digitalnih sertifikata iz upotrebe i izdavanje potpisane CRL liste od strane CA. Ovako potpisana lista, privatnim ključem CA, omogućuje korisnicima da budu sigurni u informacije koje CRL lista sadrži. CRL lista je binarna datoteka koja sadrži informacije o listi povučenih sertifikata i razlozima zbog kojih su isti povučeni, nazivu izdavaoca CRL liste, vremenu kada je CRL lista izdata i vremenu kada će sledeća CRL lista biti izdata.
CA periodično kreira CRL listu na bazi primljenih zahteva za opoziv izdatih digitalnih sertifikata. Kada istekne rok važenja digitalnog sertifikata, njegov status se više ne prikazuje u okviru CRL liste. Ova mera pomaže da se minimizuje veličina CRL liste i smatra se da status povučenosti nema značaja za sertifikat kome je istekao rok važenja.
Najrasprostranjeniji protokol koji se koristi u PKI sistemima za pristupanje CRL listama unutar X.500 direktorijuma je LDAP (*Lightweight Directory Access Protocol*) protokol. Pored LDAP protokola u upotrebi je i metod slanja CRL liste svim korisnicima (*push* metod), kao i objavljivanje CRL liste na odgovarajućem WEB sajtu sertifikacionog tela sa koga korisnici mogu preuzeti CRL datoteku (*pull* metod, kao što je i preuzimanje CRL liste sa X.500 direktorijumskog servera).
Glavni nedostatak povlačenja sertifikata putem objavljivanja CRL liste je nepostojanje uniformnog i brzog načina da se ažurna CRL lista dostavi svim korisnicima PKI sistema. Kod većine PKI sistema korisnici su sami zaduženi da preuzmu ažurnu CRL listu. Od trenutka kompromitacije digitalnog sertifikata, pa do trenutka dok se na svim korisničkim uređajima i serverima ažurira CRL lista može proći dosta vremena. Pored ovog nedostatka do značajnog usporavanja rada neke PKI aplikacije može doći ukoliko korisnici imaju potrebu da veoma često

koriste CRL listu. Sama CRL lista može biti veoma velika i do značajnog usporavanja rada neke PKI aplikacije dolazi zbog neophodnosti korisnika da uvek raspolažu sa poslednjom verzijom CRL liste, koju preuzimaju sa veoma zauzetog direktorijumskog servera ili neke druge CRL distribucione tačke.
U PKI sistemu potrebno je veoma precizno odrediti koliko se često kreira i publikuje CRL lista. Prečesto publikovanje CRL liste i njeno preuzimanje od strane korisnika može zagušiti čitav PKI sistem, dok nedovoljno često publikovanje može dovesti do toga da se koriste digitalni sertifikati koji su već povučeni.

3.2. Protokol za proveru statusa sertifikata u realnom vremenu – OCSP

OCSP protokol napravljen je kao dodatak, a u nekim slučajevima i kao zamena, za metodu povlačenja sertifikata putem periodičnog izdavanja CRL liste. OCSP protokol omogućava klijentima da u realnom vremenu provere status i validnost digitalnog sertifikata.
U toku provere digitalnog sertifikata OCSP klijent kreira zahtev za OCSP validacijom i upućuje ga OCSP serveru. Tom prilikom OCSP klijent suspenduje sopstveni proces validacije sve dok ne dobije odgovor od OCSP servera. OCSP server po prijemu zahteva proverava da li je poruka dobro formatirana, da li je server konfigurisan da obezbedi zahtevani servis i da li zahtev sadrži sve potrebne informacije. Ukoliko bilo koji od ova tri uslova nije zadovoljen, OCSP server će poslati poruku o grešci. U suprotnom, ukoliko su svi uslovi zadovoljeni, OCSP server će poslati definitivni odgovor. Definitivni odgovori mogu biti: *good*, *revoked* i *unknown*. Svi definitivni odgovori moraju biti potpisani i prema RFC2560 dokumentu [2.] za potpis se može koristiti:

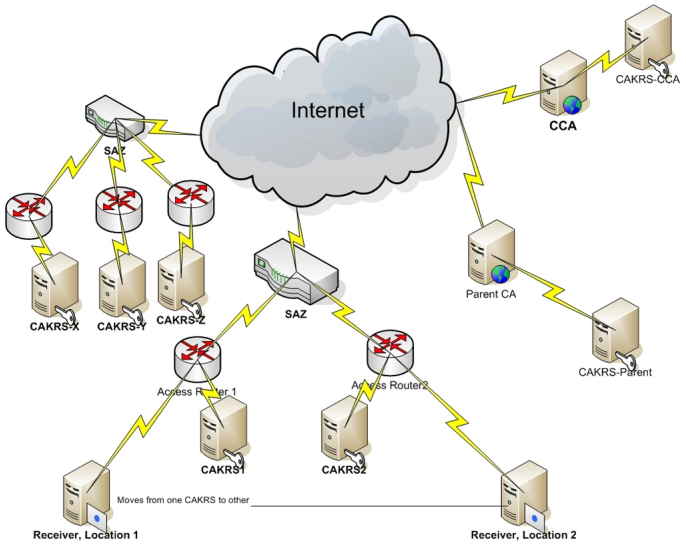
- Privatni ključ sertifikacionog tela koje je izdalo digitalni sertifikat u upitu;
- Privatni ključ autorizovanog OCSP servera. Ovakav server je u posedu posebnog sertifikata izdatog direktno od strane sertifikacionog tela koje je izdalo i sertifikat u upitu;
- Privatni ključ pouzdanog OCSP servera, čiji se javni ključ smatra pouzdanim od strane podnosioca zahteva.

Osim definitivnih odgovora, predviđeni su i odgovori koje bi OCSP server mogao da šalje u izuzetnim slučajevima: *malformedRequest*, *internalError*, *tryLater*, *sigRequired* i *unauthorized*.
Iako se u dokumentu RFC2560 [2.] navodi da je moguće koristiti pouzdani OCSP server čiji se javni ključ od strane klijenta smatra pouzdanim, u praksi se kao podrazumevan, a vrlo često i kao jedino podržan metod izbora OCSP servera kome će se uputiti upit o statusu digitalnog sertifikata, koristi OCSP server koji je naveden u samom digitalnom sertifikatu koji se proverava. Naime, kao standardno proširenje u dokumentu RFC5280 [1.] definisano je polje *AuthorityInfoAccess* u kome je navedeno kako se pristupa CA informacijama i servisima izdavača digitalnog sertifikata koji ima ovo proširenje.
Kod poznatih implementacija OCSP servera, kao što su *OpenSSL* i *Microsoft Windows Server* 2008, izvor informacija koje služe kao osnov za odgovore su statične liste opoziva (CRL) koje se dostavljaju OCSP serveru. OCSP server se koristi da u realnom vremenu saopšti klijentima informacije sadržane u CRL listama koje su mu dostavljanje.
Dva najčešće korišćena pristupa za implementaciju ovog protokola su T-OCSP (*Traditional Online Certifi cate Status Protocol*) i D-OCSP (*Distributed Online Certifi cate Status Protocol*). T-OCPS je, kao i CRL metod, veoma centralizovan protokol u kome postoji jedan server koji direktno komunicira sa svim korisnicima koji zahtevaju dokaz o validnosti digitalnog sertifikata. Kod D-OCSP protokola, postoji jedan validacioni autoritet koji kontroliše informacije o

validnosti digitalnih sertifikata i više nezavisnih servera koji ovu informaciju prosleđuju korisnicima [4.]. OCSP kao jedinstvena tačka na kojoj se može proveriti status sertifikata može predstavljati jedinstvenu tačku otkaza i metu za DoS (*Denial of Service*) napade. Dokumentom RFC5019 [5.] je predviđen niz mera kako bi se izbeglo opterećenje OCSP servera i obezbedila skalabilna implementacija. Potrbno je istaći da je D-OCSP protokol manje osteljiv na DoS napade u odnosu na T-OCSP protokol. OCSP protokol, nezavisno od konkretne implementacije, ima fundamentalnu slabost jer u nekim situacijama dozvoljava nepotpisane odgovore, a time i odgovore bez mogućnosti da se proveri njihova autentičnost.

2.3. Model geografski distribuiranog servera za opoziv ključeva

Prema istraživanjima koja su sprovedena ovaj metod je predstavljen kao pouzdaniji, brži i skalabilniji u odnosu na postojeća PKI rešenja u raznim zemljama [3.]. On pruža optimizovanu autentifikaciju ključa i zasniva se na automatskom traženju geografski distribuiranih servera sertifikacionih tela za opoziv ključeva (*CA's Key Revocation Server* - CAKRS) na osnovu najboljih dostupnih mrežnih servisa.
Ovaj model je kompatibilan sa postojećim šemama PKI sistema i ne zahtava promenu istih. On je zadržao mehanizam opozivanja digitalnih sertifikata i ključeva koji se koristi u PKI sistemu ali smanjuje kašnjenje u dobijanju informacija o opozvanim ključevima i obezbeđuje dostupnost CRL liste u svakom trenutku čak i za one korisnike koji veoma često menjaju svoju fizičku lokaciju u mreži.
Pre svega, predlaže se korišćenje nove distribuirane CAKRS šeme koja je prikazana na slici 1.



Slika 1. Distribuirana CAKRS šema [3.]

Mreža se deli na najjače dostupne zone (*Strongest Availability Zones* – SAZ). Ruter detektuje novog korisnika (*receiver*) u SAZ-u i šalje mu RQM (*Router QueryMessage*) zajedno sa SAZ opcijama. Nakon prijema RQM poruke sa SAZ opcijama korisnik izvršava lokalno obavezujuće ažuriranje sa novim SAZ-om. Lista adresa CAKRS servera uključena je u RQM poruku sa SAZ opcijama. Korisnik bira najbliži CAKRS server u okviru istog SAZ-a i zamenjuje adresu starog

CAKRS servera novom adresom CAKRS servera u usvojenom SAZ-u. Administrator mreže, ili neko drugo ovlašćeno lice, skladišti informacije u vezi sa CAKRS serverima u SAZ. Manuelna konfiguracija SAZ i CAKRS opcija potrebna je za propagiranje RQM poruke kroz određeni konfiguracioni interfejs rutera.
Izbor najbližeg CAKRS servera vrši se uz pomoć posebnog algoritma [3.] koji prepoznaje sledeća tri slučaja:

- Može biti samo jedan CAKRS server u SAZ-u;
- Može biti više od jednog CAKRS servera u SAZ-u;
- CAKRS server može biti nedostupan u SAZ-u.

Nedostatak ovog metoda se ogleda u tome što se ruter u okviru SAZ zone oglašava svim novim korisnicima porukom koja nosi informacije o SAZ opcijama i listom CAKRS servera. Na taj način predloženi metod se izlaže istim bezbedonosnim rizicima koji prate hijerarhiske i distribuirane PKI sisteme. Ovo bi se moglo izbeći korišćenjem IP autentifikacionog zaglavlja (*Authentication Header* - AH), korišćenjem bezbednog VPN (*Virtual Private Network*) tunela između servera i korisnika ili korišćenjem IPSec protokola za komunikaciju između servera i korisnika. Ovaj metod odgovara nacionalnom ili internacionalnom nivou implementacije i nije pogodan za male intranet mreže. Potrebno je da postoji jedno centralno sertifikaciono telo na nacionalnom nivou, koje se u ovoj šemi zove *Controller of Certifying Authorities* (CCA), ili više njih na internacionalnom nivou koji su izvršili unakrsnu sertifikaciju.

3. Zaključak

U okruženju sa različitim platformama i aplikacijama koje se koriste, teško je nametnuti jedinstvenu politiku upotrebe i povlačenja digitalnih sertifikata. Bez unakrsne sertifikacije to je nemoguće izvesti sa digitalnim sertifikatima koji ne pripadaju istom domenu. Nepostojanje striktne, unapred poznate hijerarhije sertifikacionih tela, otežava sprovođenje jedinstvene i univerzalno priznate politike upotrebe sertifikacionih tela.
U ovom radu predstavljene su najčešće korišćene metode i protokoli za proveru statusa i validnosti digitalnih sertifikata i ukazano je na nedostatke i moguće zloupotrebe istih. Dat je i prikaz i jedne alternativne metode koja koristi nova rešenja u ovoj oblasti. Sve ove metode, pored navedenih nedostataka, osetljive su na tzv. napad "čovek u sredini" (*Man in the middle*) i napad ponavljanja (*replay attack*). Pravilna implementacija ovih metoda i smanjenje perioda važenja CRL liste u značajnoj meri će smanjiti osetljivost na ove pretnje.
Za problem opozivanja digitalnih sertifikata ne postoji univerzalno rešenje, međutim postoje određeni pristupi ovom problemu koji olakšavaju proveru statusa i validnosti digitalnih sertifikata.

Literatura

[1.] D.Cooper, S.Santesson, S.Farrell, S.Boeyen, R.Housley, W.Polk (2008): "RFC5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile".
[2.] M.Myers, R.Ankney, A.Malpani, S.Galperin , C.Adams (1999): "RFC2560: X.509 Internet Public Key Infrastructure,Online Certificate Status Protocol - OCSP".
[3.] S.Misra, S.Goswami, G.P.Pathak, N.Shah, I.Woungang (2010): "Geographic server distribution model for key revocation", *Telecommunication Systems*, Volume 44, Springer.

[4.] CoreStreet (2006): "Vulnerability Analysis of Certificate Validation Systems", (white paper), (pristup 01.02.2012.),
[dostupno na http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.117.395].
[5.] A. Deacon, R. Hurst (2007): "RFC5019: The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments".