CoreStreet
REAL TIME CREDENTIALS

Analisi Della Vulnerabilita' Dei Sistemi Di Convalida Dei Certificati Digitali

Un'analisi delle minacce ai sistemi di revoca dei certificati digitali

Indice

ANALISI DELLA VULNERABILITA' DEI SISTEMI DI CONVALIDA DEI CERTIFICATI DIGITALI

Un'analisi delle minacce ai sistemi di revoca dei certificati digitali

Introduzione

Il Dipartimento della Difesa degli USA (DoD) sta realizzando la più grande infrastruttura di Chiavi Pubbliche (PKI) del mondo. Quando sarà completata, essa servirà applicazioni abilitate alla chiave pubblica (PKE) utilizzate da oltre 4 milioni di impiegati del DoD e da altri 3-4 milioni di utenti delle Ditte che lavorano per il DoD. Un componente critico di questa PKI è il metodo di convalida dei certificati di validità. Per essere efficace, il metodo di convalida scelto deve essere capace di servire decine di milioni di utenti mantenendo alte prestazioni, un'elevata affidabilità in modo sicuro e costo-efficace.

Questo documento tratta gli aspetti inerenti la sicurezza dei tre più comuni metodi di convalida dei certificati: Liste di revoca certificati (CRL), Protocollo Tradizionale di stato dei certificati on-line (T-OCSP) e Protocollo Distribuito di stato dei certificati on-line (D-OCSP) [1].

Ciascuno dei suddetti sistemi ha una propria differente architettura. Nel CRL la CA (Certificate Authority) pubblica periodicamente la CRL in una o più directories dalle quali la lista può essere prelevata dagli utenti collegati. L'architettura di base del T-OCSP è mostrata nella figura

---

[1] L'Online Certificate Status Protocol (OCSP) è lo standard emergente dell'IETF (Internet Engineering Task Force) destinato al controllo della validità dei certificati digitali nel corso di una determinata transazione. Prima dell'arrivo di OCSP, i risk manager non avevano a disposizione un sistema per effettuare in modo semplice un duplice controllo sulla validità di un certificato. OCSP permette invece di condurre queste verifiche in tempo reale, risparmiando tempo e denaro, e fornendo alle attività di e-business un sistema più rapido, semplice e affidabile per la validazione dei certificati digitali rispetto a quello offerto dal tradizionale scaricamento ed elaborazione delle CRL (Certificate Revocation Lists). Rilasciate dalle Certification Authority (CA), le CRL sono liste di certificati e di possessori non validi.

1. Entrambi i sistemi (CLR e T-OCSP) sono altamente centralizzati.

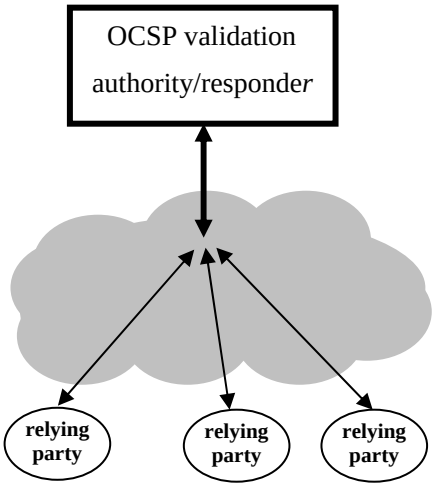

Figura 1 - Architettura OCSP Tradizionale. In questa architettura c'è una o, al più, un numero limitato di autorità che comunicano con tutte le applicazioni collegate per fornire attestazioni di validità.

La Figura 2 mostra l'architettura di base D-OCSP. Tale sistema si basa sul principio di tenere separati i dati sensibili e le applicazioni da proteggere dalle procedure di fornitura dello stato di validità dei certificati degli utenti collegati. L'approccio progettuale del sistema consente di realizzare l'architettura distribuita mostrata di seguito.

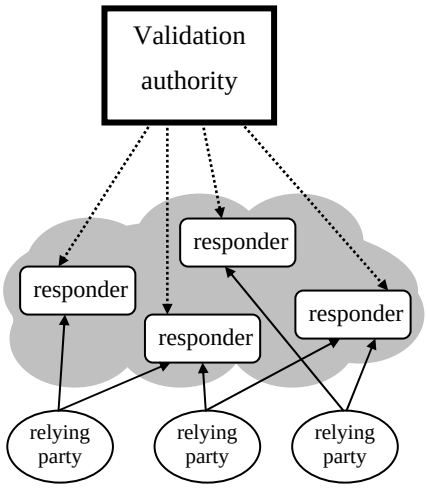

Figura 2 - Architettura Distribuita per la convalida dei certificati. In questo sistema, c'è un'autorità che controlla il rilascio dei certificati di validità ed un numero illimitato di "risponditori liberi" che forniscono questi certificati alle applicazioni collegate.

Il presente documento analizza le minacce che possono essere portate dall'esterno a questi tre sistemi di convalida degli utenti.

1. Metodologia

La metodologia impiegata per valutare la sicurezza dei tre sistemi di convalida dei certificati pone l'attenzione su quattro aree: vulnerabilità, minacce, probabilità di sfruttamento e contromisure. Esse sono definite come segue:

- **Vulnerabilità**: è una debolezza del sistema o un punto in cui un sistema è attaccabile; tale debolezza potrebbe essere sfruttata per violare la sicurezza del sistema.
- **Minaccia:** è un possibile pericolo per il sistema quale una persona, componente del sistema o evento il quale potrebbe causare una compromissione della sicurezza delle operazioni del sistema stesso.
- **Probabilità di sfruttamento**: è il risultato dell'analisi di quanto sia verosimile che una data vulnerabilità venga sfruttata; essa considera sia l'ambiente in cui il sistema opererà che le contromisure utilizzate per contrastare la minaccia.
- **Contromisura**: è un'azione, apparecchiatura, procedura o tecnica per proteggere il sistema contro le minacce alla sicurezza delle sue operazioni.

Ogni sistema basato su computer ha delle vulnerabilità correlate con la sicurezza. Alcune di queste possono essere facili da sfruttare (es. sistemi con passwords facili da decifrare) mentre altre possono richiedere un tale dispendio di tempo e risorse da rendere altamente improbabile un loro sfruttamento. (es. attacco in forza per aprire una chiave RSA a 2048 bit).

Le vulnerabilità sono caratteristiche dei sistemi presi in analisi. Esse possono esistere per molte ragioni quali: un progetto non accurato, sistemi di codifica non accurati, operazioni non in sicurezza o difficoltà /costi per realizzare e implementare sistemi più sicuri.

Le minacce sono proprietà o elementi dell'ambiente in cui il sistema sotto analisi andrà ad operare. Ambienti differenti pongono minacce differenti. Una minaccia è uno scenario reale nel quale una vulnerabilità è sfruttata e può provenire da un qualsiasi numero di fonti: attacchi esterni, attacchi interni, errori accidentali di utenti, errori dei processi di sistema, ecc. Le minacce possono aumentare quando vengono scoperte delle ulteriori vulnerabilità. Comunque, le vulnerabilità del sistema rimangono costanti. Un sistema può avere una certa vulnerabilità non sfruttabile però nell'ambiente in cui opera.

In questo documento:

- vengono prese in considerazione quattro tipi di vulnerabilità comuni ai tre metodi di certificazione: CRL, T-OCSP, D-OCSP;
- sono identificate le minacce associate a queste vulnerabilità e valutate la probabilità di sfruttamento da parte di un attaccante;
- ove necessario, saranno altresì anche discusse le possibili contromisure.

2. Interruzione del servizio (DoS)

Il DoS è un'azione o serie di azioni o circostanze che impediscono a un sistema o a qualche sua risorsa di funzionare con efficienza ed affidabilità. In conseguenza di ciò, negare l'accesso significa che gli utenti del sistema non riescono ad utilizzare le risorse di cui hanno bisogno quando ne hanno bisogno. Per i sistemi di validazione di certificati in rete, l'affidabilità è particolarmente importante dal momento che anche un minimo rallentamento in servizio può avere ripercussioni sull'intera rete.

Negli ultimi anni gli attacchi del tipo DoS sono diventati molto di moda [2] . I sistemi che sono centralizzati e impiegano del tempo per completare una transazione sono altamente soggetti agli attacchi di questo tipo.

Da notare che un attacco DoS può colpire chiunque utilizzi il servizio.

a. Vulnerabilità

Tutti e tre i sistemi di validazione sono vulnerabili agli attacchi del tipo DoS. L'attuale metodo CRL del Dipartimento della Difesa è il più vulnerabile poiché impiega tempi lunghi per scaricare i grandi files CRL (5-6 Mbytes). Ciò è chiaramente dimostrato dal fatto che gli utenti DoD stanno già sperimentando inaccettabili indicazioni di accesso negato anche nella pratica quotidiana.

Il metodo T-OCSP è altrettanto altamente suscettibile di attacchi DoS dal momento che in tale metodo ciascuna risposta è firmata in modo digitale in tempo reale, un processo che richiede tempo. In aggiunta, T-OCSP è un metodo altamente centralizzato a causa dei costi associati di gestione di molteplici autorità T-OCSP che devono essere collocate ed impiegate in sicurezza, analogamente a quanto è richiesto per l'operatività di una Autorità Certificativi (CA).

Il metodo D-OCSP è il meno vulnerabile agli attacchi DoS. Il D-OCSP ha un'architettura fortemente distribuita nella quale i risponditori sono economici da impiegare e non richiedono particolari sistemazioni e servizi di sicurezza. Un'architettura distribuita si è dimostrata la miglior difesa contro gli attacchi "servizio rifiutato".

---

[2] Il 21 ottobre 2002 un attacco plurimo DoS è stato condotto contro i 13 server DNS che assicurano il transito primario a quasi tutto il traffico Internet. L'attacco, il più massiccio a tutt'oggi, è fallito a causa dell'architettura distribuita dei server di root di Internet, 5 di questi server hanno rilevato l'attacco e sono rimasti disponibili per assicurare il traffico ordinario su Internet durante l'attacco.

b. La Minaccia

Tra i vari tipi di minaccia vi è una minaccia DoS dovuta a un sovraccarico del sistema con richieste di verifica di validità dovute ad un imprevedibile numero di contemporanee richieste di verifica.

Una seconda minaccia è costituita dalla perdita di accesso al server o ai servers che forniscono il servizio di validazione dei certificati la quale comporterà un DoS per tutti gli utenti

Una ulteriore minaccia può essere costituita da un attaccante (o da un gruppo di attaccanti) i quali possono sovraccaricare il servizio di validazione con false richieste impedendo, così, la disponibilità del servizio per gli utenti legittimi.

c. Probabilità di sfruttamento

Coloro che intendono condurre un attacco DoS potrebbero facilmente sfruttare il metodo di validazione CRL semplicemente perché esso impiega molto tempo a scaricare le pesanti liste CRL . L'attuale sistema di certificazione CRL del DoD è, in pratica, già in stato DoS per le normali richieste degli utenti legittimi. Similmente, il sistema T-OCSP è altrettanto suscettibile di blocco perché impiega un tempo circa 20 volte più lungo per firmare una risposta di quanto non venga impiegato per generare ed inviare una richiesta.

Il sistema D-OCSP è il più difficile da attaccare per due ragioni:

- l'architettura fornisce molte più fonti da cui attingere i dati di validità di un utente;
- il tempo per generare e inviare una risposta è uguale al tempo necessario per generare ed inviare una richiesta. Gli attacchi DoS sono considerati estremamente seri per l'impatto che hanno sull'intera utenza.

d. Contromisure

La più efficace contromisura per contrastare sia la minaccia in questione che i sovraccarichi si ottiene con l'uso di una ridondanza multipla di certificazioni della validità all'accesso. La minaccia derivante dalla perdita di connettività può essere contrastata con l'impiego di reti ridondanti e/o l'uso di sorgenti locali di informazioni di stato di certificato.

L'architettura D-OCSP è l'ideale per queste contromisure perché l'aggiunta di servers che non devone essere protetti è economica e può essere fatta in ogni luogo e senza la necessità di particolari postazioni sicure. Nel caso del T-OCSP, invece, l'aggiunta di ulteriori servers è costosa sia per le tanto diverse dislocazioni che per l'impiego; essa, inoltre, crea problemi di gestione e complicate procedure di ripristino. Infine, aggiungere servers addizionali nel

caso CRL non è molto efficace a causa del lungo tempo impiegato per scaricare files di 5MB, tempo molto più lungo di quanto ne occorra per richiedere un download. Perciò un attacco diffuso del tipo “interruzione del servizio”, avrà probabilmente sempre successo contro un sistema CRL.

3. Intrusione

Per intrusione si intende un tentativo deliberato di penetrare in un sistema informatico. Spesso gli intrusi sono più interessati ai tentativi di intrusione in siti web ad alto profilo che allo sfruttamento delle possibilità di manipolare il sistema una volta penetrati in esso. Tuttavia, nel caso dei sistemi di validazione di certificati la motivazione dell'intruso è probabilmente da ricercarsi con la possibilità di sfruttamento di dati ed informazioni e ciò costituisce un grande rischio in caso di attacchi proprio con lo scopo di effettuare una compromissione.

a. Vulnerabilità

Ogni sistema connesso in rete è soggetto a possibili intrusioni. La vulnerabilità dei sistemi di validazione CRL e D-OCSP a questi attacchi è virtualmente nulla perché nessuno dei due consente traffico in ingresso al server che svolge le operazioni di accredito e memorizza dati sensibili per la sicurezza. Per contro, il sistema T-OCSP è permeabile agli ingressi indesiderati alla sua autorità di certificazione (CA) rendendola, così, vulnerabile agli attacchi intrusivi.

b. La minaccia

Ogni volta che un sistema informatico consente accessi dal mondo esterno c'è pericolo che dall’esterno si possa scoprire un difetto nella sicurezza del sistema e guadagnare così l'accesso a dati sensibili e/o informazioni/sistemi riservati. Nel caso di sistemi di validazione degli accessi, la minaccia è che l'intruso possa manipolare i certificati di accredito, revocando certificati validi e rendendo validi certificati revocati.

c. Probabilità di sfruttamento

E' virtualmente impossibile per un intruso attaccare con successo sistemi CRL o D-OCSP dal momento che questi non permettono l’accesso ai loro elementi accreditati. Il livello del sistema T-OCSP al quale un intruso può condurre un attacco dipenderà dalla robustezza e dal corretto utilizzo degli elementi di prevenzione anti-intrusione del sistema.

d. Contromisure

Le contromisure standard anti-intrusione, come l'introduzione di firewalls, possono essere usate per mitigare la minaccia,. Queste comunque non eliminano la minaccia nei sistemi T-OCSP dal momento che essi sono progettati per permettere ad utenti esterni sconosciuti di connettersi agli elementi del sistema.

4. Aggiornamento della risposta di validità

Un importante concetto per ogni discussione sulla validazione dei certificati è quello dello stato di aggiornamento della risposta di validità (R.F). Il tempo di aggiornamento della risposta di validità. misura quanto è attuale lo stato di validità di un certificato quando esso raggiunge l'applicazione di un partner collegato. In generale, l'aggiornamento scatta quando un nuovo dato di revoca è ricevuto dalla CA il quale quindi deve essere aggiunto al successivo CRL. Idealmente, un nuovo CRL dovrebbe essere rilasciato ogni qualvolta un certificato è revocato. Questo approccio, comunque, è impraticabile per la maggior parte degli impieghi. Si consideri, ad esempio, lo scenario DoD. Il Dipartimento della Difesa ha circa 4,4 milioni di utenti e un tasso di revoca di certificati di circa il 17%. Ciò comporta che, in media, si ha una revoca ogni 2 minuti. Chiaramente non sarebbe pratico rilasciare un nuovo CRL ogni 2 minuti [3].

L'attuale policy del DoD è di rilasciare un CRL ogni 24 ore, validi per 96 ore. La finestra di vulnerabilità può andare da 24 a 96 ore, in dipendenza di quando il partner collegato riceve il prossimo aggiornamento di CRL. Per la classe 4 di certificazione del DoD, un CRL deve essere disponibile entro 4 ore dalla notifica di revoca per "compromissione di chiave".

a. Vulnerabilità

Tutti e tre i sistemi sono vulnerabili ad un aggiornamento non tempestivo delle risposte di validità. Il grado di aggiornamento dei dati di validità è determinato dalla valutazione se si può correre il rischio di mantenere validi certificati scaduti rispetto alle impegnative procedure di emissione di CRL.

Entrambi i metodi T-OCSP e D-OCSP dipendono dalla ricezione degli aggiornamenti di revoche di validità dalla CA sotto forma di CRL. Tutti e tre i sistemi, perciò, hanno

---

[3] Il 25 ottobre 2002 è stato emesso un Avviso CERT per informare gli utilizzatori del protocollo di autenticazione Kerberos di un sovraccarico nel traffico causato dall'esterno il quale avrebbe permesso di accedere ai server di root consentendo di apportare ogni modifica voluta al centro di distribuzione delle chiavi di Kerberos. Questo esempio serve a dimostrare che anche solidi sistemi di sicurezza sono vulnerabili agli attacchi se connessi ad una rete. L'unico modo per eliminare la vulnerabilità è di non consentire accessi alla rete.

essenzialmente la stessa modalità di aggiornamento. E' importante notare che l'aggiornamento delle richieste di validità risposta, in entrambi i sistemi T-OCSP e D-OCSP non è determinato da quando la risposta è firmata. L'aggiornamento è determinato da quando la CA ha rilasciato un dato di revoca via CRL.

Dal momento che il metodo D-OCSP richiede pochi minuti per pre-firmare tutte le risposte OCSP, si crea un leggero ritardo nel rendere i nuovi dati di revoca disponibili per i risponditori. Nell'esempio del DoD, con 9 milioni di certificati da pre-generare, questa differenza equivale a ritardare il rilascio dei CRL di circa 10-15 minuti. Questo inconveniente può essere superato aggiungendo processori più veloci o in maggior numero per velocizzare il processo di pre-firma.

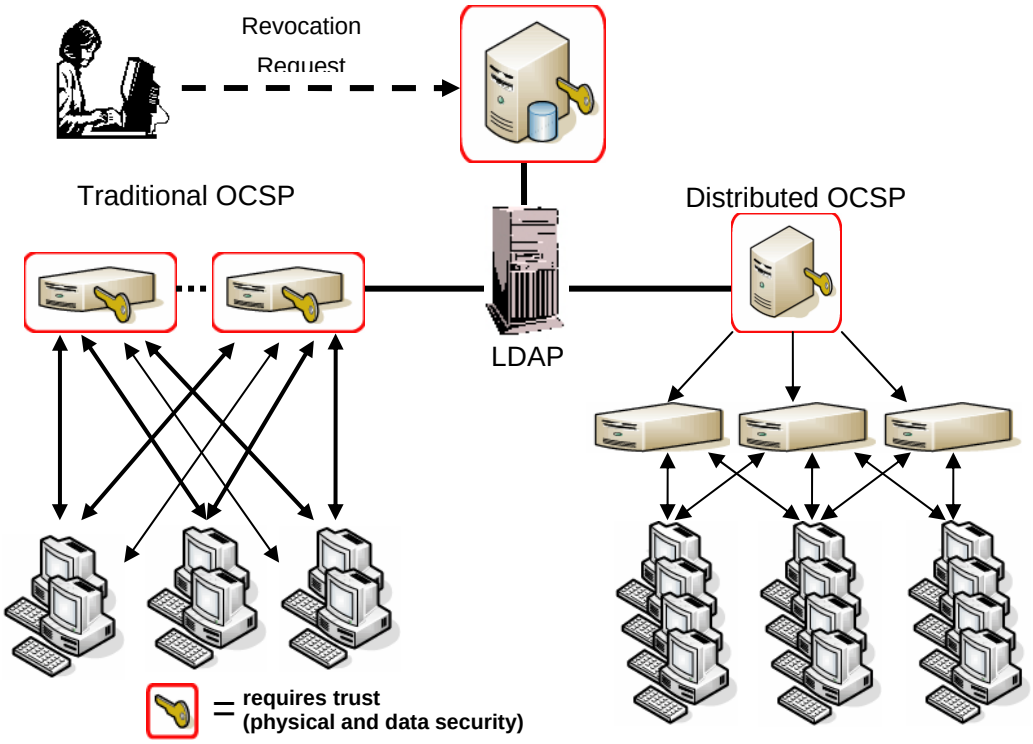

Figura 3 - Aggiornamento della risposta di validità. L'aggiornamento della risposta di validità è controllato dalla CA la quale invia una notifica iniziale di revoca di certificato via CRL. Una comune falsa interpretazione è che l'aggiornamento OCSP sia effettivo da quando esso è firmato ciò che chiaramente non avviene come desumibile dalla figura.

b. Minaccia

La minaccia alla sicurezza è rappresentata dal fatto che qualcuno il cui certificato è stato revocato possa ancora usare tale certificato finché il dato di revoca sia ricevuto dall'applicazione correlata.

c. Probabilità di sfruttamento

La minaccia più significativa è associata ai certificati che vengono revocati per dimissioni o termine dell'incarico di un legittimo possessore. In questo caso, il possessore del certificato può ancora autenticarsi al sistema e pertanto può continuare ad accedervi o usare le risorse correlate con la validità del suo certificato. I certificati che sono revocati a causa di una potenziale compromissione (es. perdita di una carta di accesso) non sono facilmente sfruttabili perché l'accesso alle chiavi private richiede l'autenticazione dell'utente.

d. Contromisure

Dal momento che lo sfruttamento di dati obsoleti è limitato, in pratica, a utenti legittimi che si sono dimessi o hanno lasciato l'incarico, le procedure di sicurezza dovrebbero prevedere la restituzione della carta di accesso o di altri strumenti di memorizzazione di chiavi private come standard del processo di termine dell'incarico.

5. Riproduzione

La riproduzione è definita come la registrazione di un legittimo messaggio da parte di una persona che intende utilizzare il messaggio senza autorizzazione. Un esempio, è quello di un messaggio di trasferimento fondi il quale potrebbe comportare una riproduzione illegittima molto proficua.

a. Vulnerabilità

Nell'esempio del DoD, l'informazione di revoca del certificato è aggiornata ogni 24 ore ed è valida per 96 ore. Come conseguenza, tutti e tre i sistemi sono suscettibili di attacchi di ripetizione. La vulnerabilità si sviluppa come segue. Il CRL_1 è rilasciato con il certificato in questione ancora valido. Dopo il rilascio del CRL_1, ma prima del CRL_2, il certificato in questione è revocato. Ora è possibile, per un attaccante, replicare i dati dal CRL_1 impedendo al partner collegato di ricevere l'informazione aggiornata (es. da CRL_2, CRL_3 e CRL_4). In questo caso il periodo di vulnerabilità è di 72 ore. Da notare che può essere usato un metodo per eliminare questa vulnerabilità, come discusso nel paragrafo Contromisure di seguito riportato.

b. Minaccia

La minaccia è rappresentata da qualcuno che può registrare la risposta di stato del certificato (CRL o OCSP) quando il certificato è valido e, poi, replicare la risposta dopo

che il certificato è stato revocato. Nel caso del DoD la minaccia è limitata al periodo in cui CRL_1 è valido.

c. Probabilità di sfruttamento

Lo sfruttamento di questa vulnerabilità è tecnicamente difficile e richiede alcune spiegazioni. La figura successiva mostra le predisposizioni richieste.

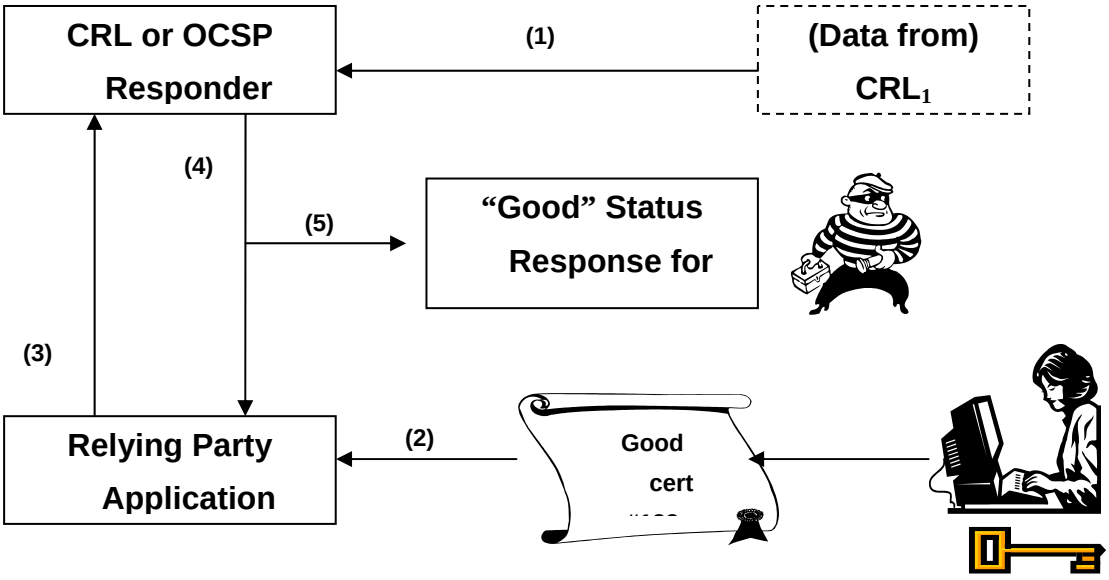

Figura 4 - Set-up per un attacco di replica. La predisposizioni per la riproduzione richiede la conoscenza di quando un certificato valido sta per essere revocato nonché l'intercettazione e la registrazione dell'ultima, o di una delle ultime, risposta in corso di validità.

Per sfruttare questa vulnerabilità un violatore dovrebbe prima sapere quale certificato (o certificati) sta/stanno per essere revocato/i. Ciò sarebbe difficile per una violazione occasionale, così la maggior parte delle minacce di replica proviene da possessori legittimi di certificati che stanno per essere dimissionati o per lasciare l'incarico. La preparazione alla violazione comincia quando l'ultimo CRL relativo al certificato in questione (es. #123) è ancora valido (in questo caso CRL_1). L'attaccante deve, in qualche modo, inviare una richiesta all'utenza che intende violare usando il certificato "valido" [4]. Ciò comporterà da parte dell'utenza l'emissione di una richiesta di validità per il certificati #123 al risponditore dal quale normalmente riceva un CRL o una risposta OCS. L'attaccante, allora, capta e copia la risposta (4 & 5) che viene inviata all'applicazione dell'utenza.

[4] Da notare che non è insignificante poiché l'applicazione dell'utenza richiederà prova del possesso della chiave privata associata con il certificato prima di processare la richiesta. Da notare anche che non si presume che l'attacante abbia ottenuto a questo punto il controllo della chiave privata.

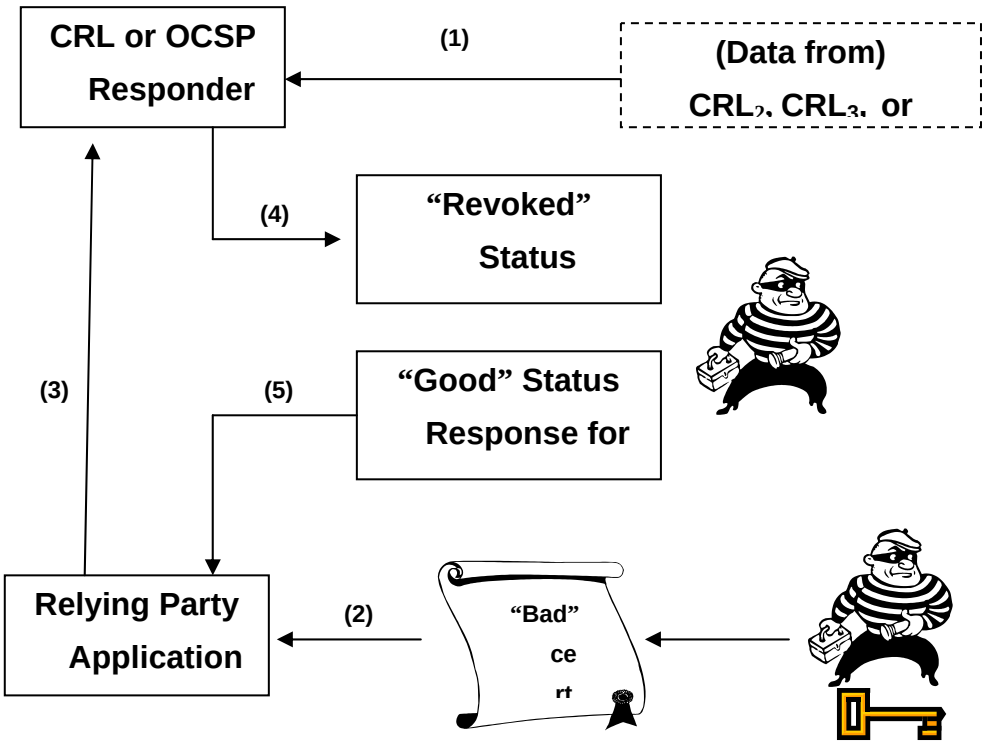

Figura 5 - Effettuazione di una riproduzione. L'esecuzione di una riproduzione è difficile perché richiede coordinamento e la prova di essere in possesso della chiave privata associata al certificato revocato che si cerca di sfruttare.

Nello scenario sopra rappresentato, l'effettuazione della riproduzione può iniziare una volta che CRL_2 è stato emesso e può continuare fino alla scadenza naturale di CRL_1 (es. 96 ore dall'emissione). In questo frangente, l'attaccante sottopone una richiesta (2) all'applicazione dell'utenza usando il certificato revocato (o "cattivo"). L'attaccante deve avere ottenuto il controllo della chiave privata associata (es. sia il possesso della chiave privata che la capacità di autenticarsi al sistema nel quale essa è memorizzata per ottenere la possibilità di suo uso) dal momento che l'applicazione dell'utenza richiederà una prova di possesso di tale chiave prima di soddisfare la richiesta. L'applicazione dell'utenza allora sottopone una richiesta di validità del certificato #123, come d'uso,. A questo punto, l'attaccante deve intercettare la risposta di "stato revocato" impedirle di raggiungere l'applicazione e sostituirla con la vecchia risposta salvata attestante che il certificato #123 è ancora valido.

E' importante notare che non tutti i certificati sono vulnerabili a questo attacco ma solo quelli che sono stati revocati durante il periodo di validità di un dato CRL. Considerata la difficoltà, per un attaccante esterno di avere accesso a una chiave privata di utente e di autenticarsi in maniera propria, la minaccia più significativa è associata ai certificati che sono revocati a causa di dimissioni o fine del servizio di un legittimo utente che già

possedeva le proprie chiavi private e poteva legittimamente utilizzarle.

d. Contromisure

Sapendo che la minaccia principale di riproduzione è limitata ai legittimi possessori di certificati che sono stati dimessi o che hanno lasciato il servizio, è importante prevedere la restituzione della carta di accesso o di altri strumenti di memorizzazione di chiavi private come parte del processo di termine del servizio.

La riduzione del periodo di validità del CRL potrebbe ridurre il periodo di vulnerabilità. Ciò tuttavia potrebbe comportare l'attivazione indesiderata del DoS se l'utente e l'autorità OCSP non fossero in grado di ottenere CRL aggiornati durante tale periodo ridotto.

Nel metodo T-OCSP la minaccia di riproduzione può essere virtualmente eliminata attraverso l'uso di un elemento casuale. Usando questo metodo, l'utenza inserisce un numero casuale (nonce) nella richiesta che invia al risponditore. Il risponditore allora include questo numero casuale nella sua risposta firmata assicurando, così, che la risposta non è stata replicata [5]. Questo sistema, comunque, aumenta la possibilità di DoS ed elimina l'uso di risposte nascoste che sono critiche per un sistema che serve un grande numero di utenti.

6. Conclusioni

Il DoS è la vulnerabilità più critica delle quattro esaminate dal momento che è la più facile da sfruttare e colpisce tutti gli utenti di un sistema. La contromisure di aggiungere servers addizionali da cui le applicazioni degli utenti possono ottenere conferme di validità è efficace solo con i sistemi basati sull'approccio D-OCSP.

L'intrusione è una vulnerabilità solo per i sistemi T-OCSP perché tale metodo è progettato per consentire a utenti esterni sconosciuti di connettersi all'autorità accreditata. Quanto siano efficaci le relative contromisure è difficile predirlo, in quanto l'efficacia dipende dall'assenza di difetti di progetto non noti e dall'attivazione ed impiego di appropriate contromisure.

L'aggiornamento della risposta alle richieste di validità di un certificato è determinato dalle misure di sicurezza adottate. Tutti e tre i metodi hanno virtualmente la stessa vulnerabilità. La minaccia di sfruttamento è bassa perché limitata a legittimi possessori di certificati revocati eventualmente risentiti perché hanno dovuto lasciare l'incarico. La riconsegna della chiave privata da parte di questi individui è una contromisura efficace.

Gli attacchi per riproduzione sono tecnicamente difficili da eseguire con successo. In aggiunta, il pericolo di sfruttamento è basso dal momento che la minaccia è simile a quella associata con l'aggiornamento della risposta. L'uso della contromisura "nonce" nel metodo T-OCSP elimina la minaccia di riproduzione ma aumenta la vulnerabilità DoS.

Il ritiro delle chiavi private dai possessori legittimi che lasciano il servizio è una contromisura efficace per i casi CRL e D-OCSP.

Da una prospettiva generale di sicurezza, il metodo D-OCSP offre la massima sicurezza rispetto alle minacce esterne discusse in questo documento. Esso fornisce la migliore protezione contro gli attacchi tipo Dos, non è vulnerabile agli attacchi di intrusione ed ha una contromisura efficace contro la scarsa e difficilmente sfruttabile minaccia di riproduzione.

Il metodo T-OCSP è suscettibile di attacchi DoS che non sono facilmente mitigati dalla ridondanza di servers che possono servire come contromisura. Esso è anche vulnerabile agli attacchi di intrusione. L'attacco di riproduzione può essere effettivamente eliminato con l'uso di una contromisura "nonce".

L'approccio CRL è il meno accettabile dal punto di vista della sicurezza per la sua alta vulnerabilità all'attacco DoS. Non è vulnerabile agli attacchi di intrusione ed ha una contromisura efficace contro la scarsa e difficilmente sfruttabile minaccia di riproduzione.

7. Bibliografia

Russell, Deborah and Gangemi,G. T. Sr., Computer Security Basics, O' Reilly & Associates. Inc, Sebastopol, CA, 1992.