PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3706 di giovedì 28 gennaio 2016

Sicurezza informatica: le sigle e i neologismi da conoscere

In materia di sicurezza informatica sono molti gli acronimi e i neologismi che un professionista della security deve conoscere. Che cosa è una CA? Che significa E2EE? E cosa sono SPIT e madware? Di Adalberto Biasiotti.

Con la tecnologia che oggi corre a velocità impensabili nel passato può non essere semplice, anche per un professionista della security, conoscere tutti i nuovi acronimi, sigle e neologismi correlati al mondo della sicurezza informatica.
Per questo motivo raccogliamo alcuni brevi articoli che Adalberto Biasiotti ha scritto e che ? come dice lo stesso Biasiotti ? "potranno togliere qualche professionista dall'imbarazzo legato ad un silenzio od una risposta non corretta".
Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0143] ?#>

Cosa è una CA?

Le crescenti preoccupazioni, legate ad un uso indiscriminato di Internet da parte di criminali, giocano un ruolo fondamentale degli enti, che permettono di individuare con certezza l'identità digitale di un soggetto.

Una **certificate authority** (CA) è un ente fiduciario che emette dei documenti elettronici, che permettono di verificare l'identità digitale di un soggetto su Internet. I documenti elettronici, che sono chiamati certificati digitali, rappresentano un aspetto essenziale di una rete sicura di comunicazione e giocano un ruolo importantissimo nella gestione di una infrastruttura di chiave pubblica (PKI). Questi certificati per solito includono la chiave pubblica del titolare, la data di scadenza del certificato, il nome del titolare ed altre informazioni ad esso afferenti. I sistemi operativi e gli applicativi di navigazione mantengono una lista di certificati, che vengono utilizzati per verificare se quelli emessi sono validi.

Anche se, almeno in teoria, un qualsiasi ente può emettere certificati digitali per garantire la sicurezza delle comunicazioni, nella gran parte dei casi i siti Web e di commercio elettronico usano certificati che sono stati emessi da enti commerciali CA. Per solito, maggiore è il tempo da cui la CA sta funzionando, maggiore è il numero dei certificati emessi.

Perché questi certificati possono davvero essere garantistici, essi devono poter essere utilizzati anche in ambienti compatibili con sistemi di navigazione e sistemi operativi oggi desueti; questo concetto viene normalmente chiamato "**ubiquità**".

In tempi recenti, il livello di fiducia nelle CA è stato messo a dura prova per la presenza di certificati fraudolenti. È capitato infatti che gli hacker siano riusciti a penetrare nelle reti di varie CA, emettendo certificati digitali a nome di siti di grande rilievo, come Twitter e Microsoft.
Purtroppo i protocolli che si basano su una verifica a catena della validità del certificato sono vulnerabili a un certo numero di attacchi, tra cui uno dei più popolari è quello chiamato *man-in-the-middle*, laddove un soggetto criminale si interpone fra il richiedente e il destinatario di un certificato.

Nel momento in cui un solo certificato emesso da una CA è compromesso, si può ritenere che tutti certificati emessi da questa CA possano essere stati compromessi.
Ecco il motivo per cui le garanzie afferenti alla integrità dei certificati emessi da una CA rappresentano un aspetto fondamentale del rapporto fiduciario tra ente emittente e titolare del certificato.

E2EE: che significa?

La sicurezza informatica è in continua evoluzione ed in analoga evoluzione sono gli strumenti relativi. Ecco la decodifica di un acronimo che sempre più spesso viene menzionato dagli esperti.

È bene che i lettori prendano rapida confidenza con questo acronimo, che significa **End to End Encryption**.
Con questa **protocollo di cifratura**, un messaggio viene cifrato nel sistema informativo del mittente e soltanto il destinatario è capace di decifrarlo. Nessun soggetto intermedio, sia esso un fornitore di servizi Internet, o un fornitore di applicativi oppure un hacker, può leggere o manipolare il messaggio.

Le chiavi criptografiche usate per la criptografia e decifratura del messaggio sono archiviate soltanto sui sistemi informativi terminali, il che è possibile grazie all'uso di sistemi di criptografia a chiave pubblica.
Anche se in questo contesto lo scambio di chiavi è considerato pressoché inviolabile, almeno utilizzando gli algoritmi e le potenze di calcolo oggi disponibili, esistono tuttavia almeno **due debolezze potenziali**, che non fanno riferimento ad algoritmi matematici.

Innanzitutto, ogni sistema informatico terminale deve ottenere la chiave pubblica dell'altro sistema terminale, ed un attaccante, che abbia la possibilità di fornire ad uno od entrambi i sistemi terminali la chiave pubblica dell'attaccante, potrebbe eseguire una attacco di impersonamento, normalmente chiamato *man-in-the-middle attack*.
Inoltre, la sicurezza va a farsi benedire se entrambi i sistemi informatici terminali sono stati penetrati in modo tale che un attaccante possa vedere i messaggi prima e dopo che essi siano stati criptografati e decifrati.

Ad oggi, il metodo normalmente utilizzato per garantire che una chiave pubblica sia effettivamente la chiave legittima, creata dal legittimo destinatario, è quello di inserire la chiave pubblica in un certificato, che è stato firmato digitalmente da un'autorità di certificazione ? CA.
Poiché la chiave pubblica che caratterizza un'autorità di certificazione è distribuita largamente ed è ben nota, si può contare sulla sua legittimità ed un certificato segnato con questa chiave pubblica si può presupporre legittimo.
Almeno per ora!

Neologismi da conoscere: SPIT e madware
Nulla può maggiormente imbarazzare un professionista della security di non essere in grado di rispondere a un quesito afferente a temi avanzati di sicurezza. Per questa ragione offrirò di frequente ai lettori delle sintetiche illustrazioni di acronimi, per lo più provenienti da paesi anglosassoni, che potranno togliere qualche professionista dall'imbarazzo legato ad un silenzio od una risposta non corretta.

SPIT (*spam over Internet telephony*) è un neologismo che fa riferimento alla trasmissione di messaggi, in blocco, sulle **comunicazioni telefoniche via Internet**. Anche se molte attività commerciali utilizzano già i messaggi vocali per promozioni di marketing, questo tipo di attività è assai più invasivo, perché il mittente può inviare migliaia di messaggi in blocco, invece di selezionare ogni numero separatamente.
Per integrare correttamente la telefonia, tramite computer, spesso i telefoni sono classificati in gruppi e operatori di pochi scrupoli possono catturare questi gruppi in modo da trasmettere, in forma massiccia e simultanea, messaggi promozionali. È bene ricordare che i messaggi telefonici che sono smistati tramite IP sono molto più difficili da tracciare e quindi il potenziale per attività fraudolente è assai più elevato.

Viene invece chiamato con il nome di **madware** una forma aggressiva di pubblicità mirata agli smartphones e tablet. Il nome nasce dall'accoppiamento di mobile (m) e di pubblicità (adware), ed è stato creato da un'azienda specializzata nella protezione di siti informatici da attacchi elettronici.

Tipicamente, questo applicativo viene installato su un apparato, quando l'utente dà la sua approvazione a ricevere dei messaggi pubblicitari, in cambio di una app gratuita. La invasività di questi applicativi fraudolenti può essere molto elevata, perché l'app può tenere sotto controllo il comportamento di un utente e può perfino intervenire, modificando la programmazione dell'apparato, sino al punto che il tono di chiamata di una comunicazione telefonica può essere trasformato nel lancio di un messaggio promozionale!

Per aumentare la probabilità che un utente distratto possa essere infettato da queste app, i progettisti creano dei banner di grandi dimensioni, che catturano quasi tutto lo schermo.
Come al solito, la migliore forma di prevenzione è quella di leggere molto attentamente la informativa che viene offerta, invece di pigiare subito il tasto di accettazione, senza aver ben capito che cosa si stia realmente accettando.

Un efficace applicativo antimalware, specialmente progettato per uso su apparati mobili, rappresenta, almeno per oggi, una utile difesa.

Adalberto Biasiotti

 Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it