

Remote client authentication

Sono sempre di più i dispositivi che oggi si collegano alla rete in remoto, questo impone una particolare attenzione per garantire la security. L'efficacia di approcci variabili e combinati in funzione delle minacce

di Giuseppe Badalucco

I dispositivi che oggi chiedono di attestarsi sulla rete sono in continua crescita per numero e tipologia (laptop/desktop/netpc e smartphone). Il modo in cui questi client si autenticano si dispiega lungo un continuum che va dall'utilizzo di una password statica, all'impiego della biometria, all'utilizzo di una infrastruttura Pki, servendosi, per rendere più sicura la sessione, di strumenti di sicurezza quali smart card, schede di memoria e quant'altro. Ogni combinazione di client, metodi di autenticazione, dispositivi di sicurezza ha una certa resistenza agli attacchi oggi in circolazione.

MOBILITÀ WIRELESS DIFFUSA

Chi qualche anno fa vaticinava l'avvento della mobilità wireless diffusa, oggi possiamo dirlo, aveva visto giusto. I milioni

di laptop e smartphone aziendali che si connettono da remoto alle Lan aziendali hanno innalzato in maniera esponenziale la quantità e il valore delle informazioni immagazzinate nella memoria di questi dispositivi: credenziali di accesso alla posta elettronica e agli applicativi aziendali, catalogo prodotti, anagrafica clienti, ma anche quelle che servono per collegarsi alla banca di fiducia.

Il rovescio della medaglia? Fenomeni come la perdita e il furto dei dati, per una buona metà oggi imputabile a un utilizzo scorretto o fraudolento di dispositivi mobili. Tra le fonti di vulnerabilità lo schema di autenticazione remota utilizzato, il software di sicurezza installato all'interno degli strumenti utilizzati, la robustezza dei dispositivi di sicurezza, siano essi hardwa-

re o software, e naturalmente il livello di complessità e efficacia degli attacchi diretti all'acquisizione di credenziali e dati.

Preservare la sicurezza senza compromettere l'accessibilità degli utenti non è un compito agevole. Per questo le aziende sono sempre più interessate a trovare delle risposte convincenti al bisogno di sicurezza connesso agli accessi remoti e all'autenticazione.

DUE METODOLOGIE DI AUTENTICAZIONE REMOTA

Negli ultimi mesi sono comparsi sul mercato nuovi prodotti software che utilizzano un approccio poco sfruttato per ovviare al problema di ottenere un livello di sicurezza efficace durante una sessione di autenticazione remota. Grazie a tecnologie brevettate, queste soluzioni sono in grado

di creare un univoco fingerprint ricavato dalle caratteristiche del dispositivo (desktop, netpc, laptop e smartphone compresi) che si attesta sulla rete. La soluzione, sfruttando il gran numero di informazioni che si possono ricavare dall'hardware, poniamo di un netbook, verifica tramite un software installato sul dispositivo stesso e sul server l'identità dello user che richiede l'autenticazione.

Un discorso a parte meriterebbe il collegamento protetto alle risorse di storage. Protocolli di accesso sicuro, funzioni di controllo, sistemi di audit trail, oltre a funzioni di sicurezza sempre più avanzate, come la crittografia sui canali di comunicazione locale e remota sono sempre più diffusi. «Le nostre soluzioni – ci dice

Roberto Salucci, solutions consultant di Hitachi Data Systems (www.hds.com/it/) – rivedono l'accesso all'ambiente di gestione del sottosistema storage attraverso meccanismi di controllo basati sull'identificazione del ruolo di chi sta accedendo al sistema, sulle password, e tramite l'utilizzo di un protocollo sicuro di tipo Ssl per il colloquio tra lo storage administrator e il sottosistema storage».

Dunque ogni metodologia di autenticazione remota ha prerogative proprie a seconda dell'architettura per la quale è stata pensata. Si tratta di individuare il modello di autenticazione che meglio si presta alle esigenze specifiche e si integra con l'architettura dei sistemi. Dal nostro punto di vista la scelta del metodo di autenticazione migliore è quello che mette la sicurezza al primo posto. E da questo assunto partiremo senza peraltro dimenticare che una maggiore security qualche volta va a scapito della semplicità d'uso e degli obiettivi del business. Per esempio l'accesso a un applicativo aziendale via Web tramite semplici credenziali, quali nome utente e password, in molti casi è la soluzione migliore per quelle aziende più interessate al contenimento dei costi di svi-



Roberto Salucci
solutions consultant
di Hitachi Data Systems



Elio Molteni
security solution strategist
di CA



Emilio Turani
country manager di Stone-
soft Italia, Svizzera Italiana,
Grecia e Turchia

Preservare la sicurezza senza compromettere l'accessibilità degli utenti non è un compito agevole

luppo, formazione del proprio personale e assistenza tecnica rispetto alle conseguenze di un accesso non autorizzato.

PUBLIC KEY INFRASTRUCTURE

Rispetto alle password statiche o a quelle generate per la singola autenticazione, metodi entrambi ancora molto diffusi, i sistemi che sfruttano la crittografia a chiave pubblica (Pki) sono tecnicamente più sicuri. La crittografia a chiavi asimmetriche assicura l'autenticazione dell'utente, la cifratura del traffico di rete, l'integrità dei dati e la tutela dell'identità delle parti. Le eventuali debolezze esulano secondo alcuni esperti da problemi di natura tecnologica. Il loro handicap principale, rileva **Elio Molteni, security solution strategist di CA** (www.ca.com/it/), «risiede nel fatto che i servizi di generazione e distribuzione di chiavi, di emissione e pubblicazione di certificati, di gestione dei registri dei certificati emessi e delle liste di sospensione e revoca sono costosi e complicati».

Le operazioni di controllo della validità del certificato, aggiunge **Emilio Turani, country manager di Stonesoft Italia, Svizzera Italiana, Grecia e Turchia** (www.stonesoft.com/it/), «basate su li-

ste di revoca di certificato sono il più delle volte tralasciate o ignorate».

Il deployment di una infrastruttura Pki richiede l'interazione di numerosi componenti - registration authority, certification authority, Web server - il cui coordinamento è demandato in genere alla redazione di policy che stabiliscono, nel modo più dettagliato possibile, come comportarsi in ogni frangente.

Questa oggettiva complessità della Pki, rileva **Giuliano Bertoletti, pre-sales engineer, Technological Department di Symbolic** (www.symbolic.it/), si traduce in ulteriori costi, diretti e indiretti, che finiscono per limitare la loro diffusione.

L'autenticazione basata su Pki si fonda sul paradigma "trusted third party" vale a dire sulla fiducia accordata a una terza parte per l'autenticazione. Per questo in caso di smarrimento o furto del certificato digitale e della relativa chiave privata, l'utente in genere li revoca presso la terza parte che li ha rilasciati. «L'infrastruttura Pki prevede che i controlli avvengano tramite l'uso delle Certificate revocation list (Crl); in realtà queste verifiche solo raramente vengono effettuate», ci dice **Antonio Forzieri, principal consultant di Symantec Services Group** (www.symantec.com/it/). Lo stesso utente poi può incorrere in pericoli aggiuntivi qualora si affidi a più di una certification authority, con il rischio di accreditare potenziali authority truffaldine: «L'utente malintenzionato infine potrebbe fornire informazioni false a una certification authority fidata che, in caso di superficialità, potrebbe rilasciare un certificato valido a un utente del quale non ha verificato l'identità», ci spiega Forzieri.

Di natura strutturale è la critica mossa da **Alexander Moiseev, managing director di Kaspersky Lab Italia** (www.kaspersky.com/it/), che evidenzia come il modello abbia mostrato la sua debolezza soprattutto nell'Internet banking: «Mentre la crittografia è abbastanza for-

te per la protezione contro le intercettazioni e la modifica dei dati di rete, il modello non regge contro le infezioni locali. Una volta che il computer è infetto e la vittima effettua l'autenticazione, il criminale informatico può intervenire sulla sessione aperta dall'utente facendo credere alla vittima che vi sia un ritardo di rete oppure che il server sia sovraccarico e nel frattempo utilizzare la connessione aperta per azioni fraudolente».

BIOMETRIA

L'autenticazione biometrica effettuata dal server avviene nel rispetto di tre assunzioni base, proprie del processo biometrico. Le informazioni devono essere riproducibili, difficili da contraffare e differenti le une dalle altre. La veridicità della prima assunzione è controversa; di certo le informazioni catturate dal client possono essere riprodotte solo con una certa approssimazione. In altre parole l'autenticazione basata sul controllo biometrico non è in grado di generare un risultato univoco; l'identità della persona potrà essere riconosciuta solo con una certa approssimazione. Questa debolezza è alla base del noto fenomeno dei falsi positivi in conseguenza del quale in alcuni casi l'identità di clienti autorizzati non viene correttamente riconosciuta oppure vengono autenticati soggetti non autorizzati. Oggi questa percentuale di errori può essere perfezionata e contenuta; ma esiste comunque la possibilità di riprodurre per scopi fraudolenti alcune misurazioni biometriche come la scansione dell'iride o le impronte digitali; inoltre così come avviene per le password statiche le informazioni biometriche possono essere utilizzate per autenticazioni ricorrenti avvenute anche a intervalli di tempo notevoli.

Questi limiti sono ancora un ostacolo alla diffusione della biometria, in particolare su reti insicure come Internet.



Giuliano Bertoletti
pre-sales engineer, Technological department
di Symbolic



Antonio Forzieri
principal consultant
di Symantec Services Group



Alexander Moiseev
managing director
di Kaspersky Lab Italia

Contro gli attacchi Mitm l'uso di protocolli crittografici robusti come Sll e Tsl non è sufficiente

LA SICUREZZA DEI SISTEMI DI AUTENTICAZIONE

A ogni sistema di autenticazione corrisponde un certo grado di robustezza agli attacchi. Questo è senz'altro un aspetto da considerare quando si sceglie a quale sistema affidarsi. Phishing, malicious software, attacchi man-in-the-middle (Mitm) sono tutte tipologie di aggressione accomunate dal target, vale a dire il client sul quale i meccanismi di protezione sono di norma meno avanzati rispetto a quelli presenti lato server. La minaccia Mitm, in grande ascesa, è tipicamente un attacco di rete. A differenza del phishing un'offensiva Mitm non necessariamente compromette le credenziali dello user.

Qualcuno suddivide gli attacchi Mitm in esterni e interni, caratterizzando questi ultimi come quelli che scaturiscono da worm o rootkit che, installandosi in modo subdolo e automatico, si insediano all'interno di Pc o smartphone. Tutti i sistemi di autenticazione qui richiamati sono vulnerabili agli attacchi Mitm.

L'obiettivo di questo attacco non è di impadronirsi delle credenziali dell'utente, quanto di intercettare i messaggi che vengono scambiati tra client e server. In questo processo la prima criticità è la tenden-

za dello user a ignorare gli avvisi che segnalano la presenza di certificati non validi o non affidabili. In questo modo si apre la strada a chi attacca per contraffare un canale cifrato di trasmissione delle informazioni oppure per modificare i dati della negoziazione.

DIFESA MITM

Per far fronte agli attacchi Mitm l'impiego di protocolli crittografici robusti come Sll e Tsl non è di per sé sufficiente. **Emilio Turani** (Stonesoft), sottolinea come sia indispensabile che tra le entità che effettuano la comunicazione sia presente un elemento che verifichi in maniera indipendente la bontà della trasmissione. «A questo scopo è sufficiente la presenza di firewall e/o Ips che controllino i parametri fondamentali della connessione come i numeri di sequenza dei pacchetti e i flag Tcp dei pacchetti stessi».

Sabrina Mazzanti, marketing manager di RSA Italia (<http://italy.rsa.com>), rileva altresì «la necessità di monitorare le transazioni a rischio e le attività che vengono effettuate dopo la fase di login poiché i fraudster hanno sviluppato tecnologie che consentono di bypassare l'autenticazione con gli attacchi man-in-the-browser (nuova forma di Mitm, ndr)».

Questo tipo di aggressione è disegnato per intercettare i dati quando vengono scambiati tra un utente e un'applicazione online. Le cose funzionano all'incirca in tale modo: una volta inserito un trojan nel browser dell'utente è possibile fare in modo che questo s'innesci in concomitanza con l'accesso a specifici siti Web. Una volta attivato, il trojan man-in-the-browser può intercettare e manipolare, in tempo reale, qualsiasi informazione l'utente online inserisca. Per prevenire questo attacco evoluto è necessario approvare esplicitamente ogni transazione, per esempio il trasferimento di denaro da un conto all'altro, utilizzando un dispositivo di sicurezza come una smart card da un laptop. «Il di-

positivo di sicurezza infatti assicura che le informazioni che il display visualizza non possono essere successivamente modificate firmandole digitalmente», ci spiega **Mazzanti** (RSA).

DIFESA DA PHISHING E MALWARE

Non c'è qui bisogno di ricordare l'ampiezza dei fenomeni malware e phishing. Desta impressione semmai constatare che alla crescita nel numero delle minacce non c'è stata alcuna diminuzione della loro efficacia.

Ogni metodo di autenticazione remoto deve perciò misurarsi con questa realtà. Con il semplice utilizzo delle sole password non è possibile ovviare al problema del phishing, neppure utilizzando quelle con durata limitata nel tempo che pur riducono lo spazio temporale utile per portare a termine attacchi di phishing.

Detto questo le tecniche di phishing sortiscono maggiori risultati a fronte di dispositivi di autenticazione basati sulle Pki o biometrici?

Secondo **Gianni Genta**, partner **ATS - Advanced Technology Solutions** (www.atscom.it), «i meccanismi di autenticazione "forte" basati su certificati digitali o, ancor più, su impronte biometriche limitano in modo significativo i rischi di furto di identità digitale poiché le informazioni utilizzate per il riconoscimento sono difficilmente esportabili all'esterno dei token sicuri nei quali sono memorizzati». Di fatto l'utente risulta implicitamente protetto perché non è in grado di rispondere alla richiesta di informazioni. Come detto in precedenza molto più efficace è l'autenticazione combinata di Pki e un dispositivo di sicurezza, per esempio un laptop che utilizzi un lettore di smart card. Naturalmente utilizzando uno smartphone occorre limitare la possibilità di eseguire in modo arbitrario codice da terzi stabilendo sino a che punto questo codice può avere accesso alle smart card.

Quando è possibile è poi sempre bene sensibilizzare anche gli utenti sulle minacce e sul corretto utilizzo della tecnologia installata. Gli attacchi di phishing sono in continua evoluzione; «è importante che le



Sabrina Mazzanti
marketing manager
di RSA Italia



Gianni Genta
partner ATS - Advanced
Technology Solutions

Se l'utente fosse accorto, la Pki non sarebbe necessaria per proteggerlo dai tentativi di truffa

aziende affrontino il problema anche dal punto di vista della formazione dell'utente per aumentare la consapevolezza verso il problema», afferma Genta.

Una maggiore consapevolezza da parte dell'utilizzatore finale, come sottolinea **Giuliano Bertoletti** (Symbolic), è sempre auspicabile: «Se l'utente fosse accorto, la Pki non sarebbe necessaria per proteggerlo dai tentativi di truffa. Basterebbe verificare la validità del certificato quando il browser si connette al (presunto) server della propria banca e fare attenzione a cosa appare nella barra degli Url quando si viene reindirizzati». In pratica però questo non accade e allora «chi può, passa all'uso della Pki e dei token, che consentono una salvaguardia maggiore perché delegano all'hardware e soprattutto a chi gestisce la Pki buona parte delle responsabilità inerenti la sicurezza dell'utente», ammette Bertoletti.

PAROLA D'ORDINE: SEMPLIFICARE

Per il call center aziendale il moltiplicarsi dei dispositivi e delle connessioni si traduce in più chiamate e più problemi da risolvere: verifica della connettività, monitoraggio degli accessi autorizzati, protezione dei dati e così via.

Lo staff It è già impegnato su molte problematiche. La parola d'ordine è semplificare le procedure di accesso remoto. La corretta configurazione spesso richiede conoscenze informatiche avanzate. Inoltre spesso i parametri di configurazione cambiano velocemente soprattutto quando ci si appoggia alla rete di hotel e aeroporti.

Senza dubbio la maniera più semplice per scansare qualche complicazione di troppo è quella di eliminare o comunque ridurre le installazioni di software sui dispositivi aziendali. Un applet Java nel browser evita il problema di installare software e aggiornarlo. Se proprio, non è possibile eliminarli tutti riuscire almeno a unificarli è già un passo avanti.

Il processo di autenticazione è più agevole da monitorare quando si riescono a registrare tutti gli accessi degli utenti. Una lista di tutti coloro che sono autorizzati ad accedere da remoto a un certo applicativo unita all'analisi dei log relativi alle connessioni da remoto ci restituirà il quadro completo di chi e quando accede a cosa. Inoltre ci dirà la frequenza con cui avvengono gli accessi. Ci sarà chi utilizza periodicamente un certo accesso, chi lo farà prevalentemente in certi orari, chi meno frequentemente, chi solo in circostanze particolari, un occhio allenato è in grado dall'analisi dei log di trarre più di una considerazione sul flusso complessivo di dati e sulle eventuali anomalie.

Qualora si renda necessario limitare gli accessi a determinati utenti può essere una decisione utile e tempestiva per evitarsi guai potenziali in futuro. Lo stesso accorgimento può essere adottato per i dati e le applicazioni ai quali gli utenti sono autorizzati ad accedere da remoto. Non tutti i database o le applicazioni devono essere accessibili a tutti; inoltre può essere utile prevedere a protezione dei dati una parziale o totale cifratura dei dati. La disponibilità di un numero limitato di applicazioni accessibili da remoto può ridurre, lo diciamo ancora una volta, i problemi; tuttavia perché queste limitazioni siano efficaci è fondamentale che siano inserite in maniera armonica nel più ampio sistema di policy aziendali. **DM**