

Estratto dal rapporto FDIC "Putting an End to Account Hijacking Identity Theft"

(dicembre 2004 e supplemento giugno 2005, pubblicato su www.fdic.gov)

MISURE TECNICHE PER CONTRASTARE I FURTI DI IDENTITÀ A DANNO DEI TITOLARI DI CONTI CORRENTI BANCARI

Nello studio del *Federal Deposit Insurance Corporation (FDIC)*, sono analizzate le tecnologie che possono essere usate per attenuare il rischio dei furti di identità in generale e il *phishing* sui conti correnti in particolare.

SOFTWARE DI SCANSIONE

I software di scansione esaminano continuamente Internet alla ricerca di indizi che possano far ritenere che una determinata istituzione sia oggetto di un attacco di *phishing*. A tal fine vengono ricercati sul *web* con cadenza giornaliera: a) ricorrenze del nome dell'azienda, della marca, dei marchi di fabbrica, degli slogan, ecc...b) nomi dei domini (DNS) che somigliano al nome dell'azienda, secondo predeterminati criteri. I software di scansione aiutano le istituzioni finanziarie a individuare siti che potrebbero simulare l'appartenenza all'azienda stessa, ovvero che dichiarano illegalmente di avere un legame con l'istituzione finanziaria. Un'istituzione finanziaria può acquistare e attivare software di scansione per conto proprio, oppure può esternalizzare il servizio; quest'ultimo è il caso più frequente per le piccole istituzioni finanziarie.

STRUMENTI DI ANALISI DEI LOG DEL SERVER

Simili ai software di scansione, tali strumenti analizzano il *server* dell'istituzione finanziaria, fornendo informazioni sull'attività quotidiana dell'infrastruttura telematica aziendale e aiutando così a scoprire attività sospette indicative di attacchi di *phishing* in corso. I log sono voluminosi e costosi da consultare; i software in questione sono in grado di analizzarli ed estrarre informazioni utili per il "*Network administrator*" nel giro di qualche minuto. In tal modo, è possibile monitorare l'evoluzione di eventuali tentativi di frode ed è facilitata l'identificazione dei "pirati". Tale attività può essere esternalizzata, anche se il software non richiede una complessa implementazione.

AUTENTICAZIONE DELLE E-MAIL

Le *e-mail* ingannevoli, apparentemente provenienti da un'istituzione finanziaria, sono il primo passo di un attacco di *phishing* che può portare a indebiti prelievi sui conti correnti. L'inganno è agevolato dal fatto che l'*e-mail* non è autenticata dal mittente. L'autenticazione delle *e-mail* consente di eliminare il *domain spoofing* verificando, attraverso l'IP address (IPA) del *server* mittente, che le *e-mail* provengano da dove dichiarano di venire. Questo standard può anche consentire di riconoscere i tentativi fraudolenti di registrare domini con un nome simile a quello dell'istituzione finanziaria presa di mira. Il processo di autenticazione è il seguente:

- il mittente invia una *e-mail* al destinatario;
- il servizio di posta riceve la *e-mail* e il *server* ricevente controlla, sulla base di una lista pubblica di DNS, il nome del dominio del mittente verificando che l'indirizzo IP del *server* del mittente coincide con quello pubblicato nella lista;
- se il controllo dà esito positivo, la *e-mail* viene recapitata, altrimenti viene scartata.

L'autenticazione richiede la cooperazione di più soggetti con diverse responsabilità: gli *Internet Server Providers (ISP)*, l'*Internet Engineering Task Force (IETF)*⁵⁹ e le società fornitrici di software.

⁵⁹ Lo IETF è un organismo indipendente costituito da sistemisti, operatori, vendors e ricercatori, che si occupa del buon funzionamento di Internet e della sua evoluzione.

AUTENTICAZIONE DELL'UTENTE

L'utente viene autenticato attraverso la presentazione di credenziali. Generalmente si intende per "credenziale" una o più dei seguenti elementi: qualcosa che l'utente "sa" (es. la *password*); qualcosa che l'utente "ha" (es. il *token*, che può contenere un certificato digitale); qualcosa che l'utente "è" (in questo caso si parla di caratteristiche biometriche, es. le impronte digitali). Quando l'autenticazione dell'utente utilizza congiuntamente due di questi sistemi, si parla di autenticazione "a due fattori". L'autenticazione attraverso certificati digitali è considerata generalmente come una tra le più sicure tecnologie di autenticazione. Si ha inoltre una mutua autenticazione quando anche la pagina web del sito dell'istituzione è protetta da un certificato SSL (*Secure Socket Layer*): in questo caso il *browser* dell'utente verifica che la *Certification Authority* che ha emesso il certificato sia accreditata e se il certificato sia ancora valido o meno.

Si descrivono di seguito alcune modalità tecniche che consentono, in associazione all'utilizzo di *userid* e *password*, di effettuare una autenticazione a due fattori:

Segreti condivisi Si tratta di domande personali poste al momento dell'autenticazione e delle quali il "pirata informatico" verosimilmente non conosce le risposte. Una forma più recente di questa tecnica riguarda l'aver concordato all'inizio un segreto, rappresentato da una parola o da un'immagine, in modo che l'utente possa riconoscere l'autenticità della comunicazione ricevuta dalla presenza della parola/immagine inizialmente concordata. Va posta particolare attenzione, in questo caso, alla frode cosiddetta *man in the middle* che potrebbe consentire al "pirata", spacciandosi per l'utente, di acquisire in modo fraudolento il segreto condiviso.

Token Possono essere raggruppati principalmente in tre tipologie: l'*USB token*, la *smart card* e il generatore di *password*.

1. *USB token*: è grande quanto la chiave di una serratura a cilindro; contiene normalmente un microprocessore e usa un sistema forte di crittazione; si introduce nella porta USB del computer e non richiede nessuna installazione aggiuntiva; è costituito da un unico pezzo e l'eventuale tentativo di forzatura lo renderebbe inutilizzabile; è in grado di memorizzare certificati digitali da usare in ambiente PKI.

2. *Smart card*: concettualmente simile all'*USB token*, la *smart card* ha le dimensioni di una carta di credito e richiede, per il suo riconoscimento, un hardware specifico e l'installazione del software associato.

3. *Generatori di password*: si tratta di dispositivi che producono un codice di accesso utilizzabile una sola volta - *one time password* - (OTP); l'OTP viene visualizzato sul piccolo schermo del *token*. Esiste una versione a più bassa tecnologia, consistente in una scheda con più parole chiave da scoprire e usare in sequenza negli accessi; questa soluzione presenta lo svantaggio della complessità di gestione a carico dell'azienda finanziaria, costretta a tenere traccia e a verificare le *password* fornite ai clienti; essa è comunque più economica dell'*USB token*, non richiedendo apparecchiature aggiuntive.

Tecnologie biometriche L'autenticazione avviene in questo caso per mezzo di caratteristiche fisiche o fisiologiche (p.es. impronte digitali, riconoscimento facciale, caratteristiche vocali, tipicità della scrittura sulla tastiera). Durante il processo di registrazione le caratteristiche fisiche e/o fisiologiche concordate vengono valutate e convertite in un modello matematico; questo viene registrato in un database per le successive elaborazioni. A tale proposito, il *National Institute of Standards and Technology* (NIST) ha sviluppato uno standard, denominato *Common Biometric Exchange File Format* (CBEFF) - per descrivere i dati a sostegno delle tecnologie biometriche. Normalmente vengono aggiunti controlli per evitare l'uso fraudolento di fotografie o registrazioni. Esistono due tipologie di problemi in cui la presente tecnologia può incorrere: accettare una credenziale falsa e scartare una credenziale valida. Infatti, a differenza della *password* che può solo essere corretta o errata, i sistemi a tecnologia biometrica si basano su una probabilità di riconoscimento: se il valore viene fissato troppo in basso si rischia di accettare utenti non accreditati, mentre se viene fissato troppo in alto si rischia di rifiutare l'accesso al legittimo proprietario.

Si riportano di seguito alcuni esempi di impiego di tecnologie biometriche:

1. Riconoscimento delle impronte digitali

Questa tecnologia è considerata tra le più mature e accurate per l'identificazione biometrica. L'apparecchiatura per la scansione va installata presso ogni utente (è quindi una soluzione "non portabile") ed è generalmente considerata tra le più facili da installare e da usare tra le tecnologie biometriche.

2. Riconoscimento facciale

La bontà del sistema di riconoscimento attraverso il riconoscimento facciale dipende molto dell'ambiente in cui viene usato. È facile da usare (basta disporre di una *web-cam* e del software di riconoscimento), non è intrusivo ed è perciò ben accettato dell'utente.

3. Riconoscimento dello stile di battitura sulla tastiera

Esistono software che consentono il riconoscimento dell'utente attraverso le caratteristiche del movimento delle mani sulla tastiera. Non è necessaria nessuna installazione aggiuntiva di hardware. Alcuni sistemi si limitano a riconoscere l'utente all'atto del *logon*, altri continuano il monitoraggio durante l'intera sessione.

AUTENTICAZIONE DEL DISPOSITIVO FISICO

È una tecnologia relativamente nuova che prevede l'utilizzo di un software residente che riconosce l'impronta univoca del PC. Lo svantaggio consiste nel fatto che il cliente proprietario del conto non può comunque accedere ai propri dati se non ha fatto prima autorizzare l'hardware da cui accede. Anche se non è necessario né hardware né software aggiuntivo, l'azienda finanziaria dovrà prevedere procedure di recovery che consentano di utilizzare il sistema da parte del legittimo utente nel caso di problemi di accesso.

TRUSTED PLATFORM MODULE (TPM)

Si tratta di un dispositivo, inserito direttamente nell'hardware del computer, che usa un chip per memorizzare *password*, certificati digitali e chiavi di crittografia. La TPM agisce come un *caveau* virtuale e usa lo standard PKI. Il chip è a prova di scasso e l'integrità viene verificata al momento dello start-up. I due svantaggi tipici di questa tecnologia sono: a) incapacità di riconoscere software non autorizzato o non collegato con il sistema operativo in uso; b) alti costi di conversione, una volta che il prodotto sia stato usato. Nonostante questi chip vengano installati su molti PC distribuiti dalle maggiori aziende, essi sono in realtà, ad oggi, disinseriti. L'idea è promettente, ma i sistemi operativi e il supporto applicativo non sono ancora diffusi.

INTERNET PROTOCOL ADDRESS (IPA) & LOCALIZZAZIONE GEOGRAFICA

L'idea alla base è di utilizzare l'IPA assegnato nella sessione all'utente per filtrare eventuali richieste fraudolente, tenendo conto che l'IPA può cambiare nel tempo e che a volte non è possibile associare all'IPA il suo attuale proprietario. Sono in commercio prodotti software in grado di setacciare Internet alla ricerca di informazioni sulle IPA. Il software effettua dei controlli in tempo reale confrontando i dati attuali con i profili degli accessi per individuare eventuali accessi non autorizzati. Oltre a questi controlli sono anche disponibili alcune tecnologie in grado di stabilire dove l'utente è localizzato geograficamente ovvero dove non può trovarsi al momento della transazione.

AUTENTICAZIONE FUORI BANDA

Con questo termine si indicano tutte quelle tecniche finalizzate ad autenticare l'utente attraverso un canale diverso da quello su cui l'utente sta facendo transitare i suoi dati. Oltre a ridurre il rischio di frodi, queste tecniche consentono anche di prevenire errori sui dati significativi. Ad esempio, all'inizio della transazione viene generata una chiamata telefonica, una *e-mail* o un SMS, e solo dopo che è arrivata la conferma, la transazione può procedere.

* * *

Il rapporto della FDIC pone l'enfasi sui sistemi di autenticazione a due fattori quale strumento per ridurre drasticamente il rischio di frodi a danno dei clienti di istituzioni

finanziarie. Viene quindi fornita una elencazione, non esaustiva, di istituzioni finanziarie che adottano, o stanno per adottare, sistemi della specie.

| Esempi di adozione di sistemi di autenticazione a due fattori negli USA | | | |
|---|---|---|---|
| AZIENDA | TECNOLOGIA | APPLICAZIONE | STATO |
| E-Trade Bank | OTP hardware token | Internet Banking | Progetto pilota |
| Bank of America | Tecnologie a 2 fattori | Accesso a internet per impiegati e clienti (aziende) | Funzioni per interni (estate '05) funzioni per l'esterno (aut/inv 2005) |
| Sovereign Bank | OTP hardware token | Business banking: clienti aziendali e istituzionali | In produzione |
| ABN AMRO | OTP hardware token | Gestione <i>on-line</i> della tesoreria | In produzione |
| ING Direct | Segreti condivisi a rotazione | Internet Banking | In produzione |
| Standford Federal Credit Union | Autenticazione del dispositivo fisico | Internet Banking | In produzione |
| Purdue Employees Federal Credit Union | Biometrica: Impronte digitali | Centri servizi automatizzati | In produzione |
| San Antonio City Employess Federal Credit Union | Biometrica: geometria della mano e tipicità della scrittura con la tastiera | Accesso alla cassetta di sicurezza; accesso degli impiegati alla rete | In produzione |
| Commerce Bank | OTP hardware token | Internet Banking per clienti aziendali | In produzione |
| Wachovia | OTP hardware token | Internet Banking | Allo studio |
| Dollar Bank | OTP hardware token | Internet Banking per clienti aziendali | In produzione |

| Esempi di adozione di sistemi di autenticazione a due fattori a livello internazionale | | | |
|--|---------------------------------------|---|-----------------|
| AZIENDA | TECNOLOGIA | APPLICAZIONE | STATO |
| Australian Bankers Association | Tecnologie varie a due fattori | Internet Banking | Progetto pilota |
| Bank of Valletta | OTP hardware token | Internet Banking, telephone banking, centro servizi per i clienti, mobile banking | In produzione |
| Rabobank | OTP hardware token | Internet Banking | In produzione |
| SEB Bank | OTP hardware token | Internet Banking | In produzione |
| SwedBank | OTP hardware token | Internet Banking | In produzione |
| Banca di Tokyo – Mitsubishi | Biometrica: geometria della mano | ATM | Marzo 2006 |
| Surugo Bank Shizuoka Prefecture | Biometrica: geometria della mano | ATM | In produzione |
| Mizuho Bank | Biometrica: geometria della mano | ATM | In produzione |
| Sumitomo Mitsui Bank | Biometrica: geometria della mano | ATM | Marzo 2006 |
| Citibank, UK Division | Tastiera virtuale sullo schermo | ATM | Allo studio |
| First National Bank del Sudafrica | OTP hardware token | Internet Banking | In produzione |
| Royal Bank of Scotland | OTP hardware token | Internet Banking | In produzione |
| Loyal Bank | OTP hardware token | Internet Banking | In produzione |
| Fortis, NV | OTP hardware token | Internet Banking | In produzione |
| Gruppo Aval | Autenticazione del dispositivo fisico | Internet Banking | Luglio 2005 |
| Barclays | Tastiera virtuale sullo schermo | Internet Banking | In produzione |
| | Autenticazione fuori banda | Internet Banking | Allo studio |