ATTACCHI AD ATM

Luca Mortaro

Anno Accademico 2009/2010

Indice

- 1.Storia ATM
- 2.Funzionamento ATM
- 3.Attacchi all'ATM:

3.1. Attacchi fisici

3.2. Lebanese Loop

3.3. Skimming attack

3.4. Virus e worm

3.5. Phishing

3.6. Insider attack

3.7. Competitor Attack

3.8. Decimalization attack

1. Storia ATM

Il primo Bancomat fu sviluppato dalla società inglese De La Rue e installato a Enfield Town (zona nord di Londra) il 27 giugno 1967 presso la Barclays Bank. In Italia compare nel 1976, a Ferrara: la Cassa di Risparmio di Ferrara fu la prima banca italiana ad installarlo.
Tuttavia l'invenzione vera e propria è oggetto di controversie addirittura tra tre inventori:

- John Sheperd-Barron che fu insignito nel 2005 del titolo di OBE (O_cer of the Order of the British Empire).
- Luther George Simjian che registrò, nel 1930 a New York un brevetto.
- Don Wetzel e altri due ingegneri che registrarono un brevetto il 4 giugno 1973.

Il modello inaugurato nel 1967 accettava soltanto voucher monouso, che venivano trattenuti dalla macchina. Per rendere più difficili i furti l'apparecchiatura funzionava con diversi principi, tra cui radiazioni e magnetismo a bassa coercitività che veniva rimosso dal voucher in fase di lettura.

L'idea del personal identification number (PIN) venne sviluppata nel 1965 dall'ingegnere inglese James Goodfellow, anch'egli titolare di alcuni brevetti in materia.

2. Funzionamento ATM

Il sistema sfrutta per l'identificazione del richiedente una tessera plastificata (*badge*) corredata di una banda magnetica e (solo in quelle più moderne) di un microchip, che il cliente inserisce in un apposito lettore. La tessera viene attivata digitando sulla tastiera del distributore un codice numerico di sicurezza (PIN), che deve essere mantenuto segreto dal possessore; questo viene criptato e se la stringa criptata corrisponde a quella memorizzata o ricalcolata sul calcolatore centrale l'operazione può essere eseguita, diversamente al terzo tentativo sbagliato la tessera viene *catturata* dal distributore ed il servizio viene cautelativamente sospeso. Con il servizio Bancomat è inoltre possibile usufruire di altre operazioni connesse, come il pagamento di bollette, il versamento di contanti e assegni, la lettura del saldo, la stampa degli estratti conto o della lista dei movimenti e ricariche ai telefoni cellulari; si possono inoltre effettuare pagamenti negli esercizi commerciali provvisti di POS. Il servizio Bancomat, con la relativa tessera, è fornito dalla maggior parte degli istituti bancari ed ha costi e modalità di funzionamento variabili a seconda delle condizioni stabilite tra la banca ed il cliente. In generale i distributori possono appartenere anche a una banca diversa da quella presso cui il cliente ha il conto, se questa appartiene allo stesso circuito gratuitamente altrimenti è legata al pagamento di una commissione. Nella maggior parte dei Paesi Europei, la tessera è fornita gratuitamente ed i prelievi effettuati presso qualsiasi banca sono anche gratuiti.

Il funzionamento degli ATM è basato su due concetti fondamentali: PIN e PAN.

Il ***PIN*** (Personal Identification Number) è usato dal possessore di conto per identificarsi alla banca che ha emesso la carta ATM ed è usato come mezzo per autenticare un'operazione finanziaria. Poiché tali operazioni devono essere eseguite in modo sicuro (ad esempio se qualcuno viene a conoscenza del PIN potrebbe accedere al conto dell' utente illecitamente) è necessario che il PIN sia condiviso solamente tra l'utente e la banca che detiene il conto. Per mantenere segreto il PIN, durante la trasmissione tra l'ATM e la banca che detiene il conto, viene utilizzata una cifratura. Ma prima di essere cifrato il PIN è configurato in un buffer di 8-byte chiamato "PIN Block" (PB). Il risultato codificato è chiamato EPB (Encrypted PIN Block).

Associato al conto di ogni utente c'è un numero di conto conosciuto come ***PAN*** (Personal Account Number). La banca usa il PAN per identificare quale conto è usato per una transazione bancaria.

Quando gli ATM e le reti EFTPOS (Electronic Funds Transfer at the Point of Sale) furono introdotti nei tardi anni '70, una chiave, detta chiave di zona, era condivisa direttamente tra le due banche che desideravano comunicare.

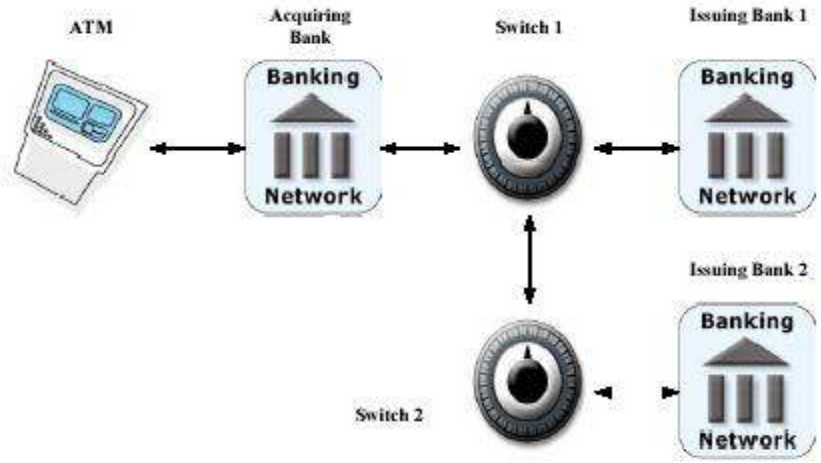
Tale tecnica aveva 2 inconvenienti:

1. una banca non poteva comunicare con una nuova banca se non stabiliva prima la chiave di zona;

2. il processo per stabilire le chiavi di zona con tutte le banche, con cui si voleva comunicare, era oneroso in termini di tempo e denaro.

Perciò si richiese l'uso di depositi dove poter memorizzare un gran numero di chiavi: gli *switch*.

La figura è un semplice diagramma che rappresenta una rete ***EFTPOS***:



Semplice rappresentazione della rete EFTPOS

Lo schema illustrato nella figura precedente è spiegato come segue:

Un dispositivo ATM è connesso con la banca acquirente,cioè la banca responsabile di far iniziare la transazione di un utente.

La banca acquirente è collegata ad uno switch, che ha il compito di inviare la richiesta dell'operazione alla banca con la quale l'utente ha il conto.

Per raggiungere la banca di destinazione la comunicazione può dover attraversare più switch, a seconda della posizione della banca nella rete.

Vediamo più in dettaglio il funzionamento dello schema illustrato in figura. L'utente inserisce la carta nello sportello ATM e digita il PIN. La banca acquirente condivide una chiave, detta chiave di

zona, con lo switch al quale è collegata. La banca acquirente cifra il PIN con la sua chiave di zona e lo invia allo switch-1. A questo punto lo switch-1 prende il PIN Block e lo invia allo switch-2, collegato alla banca detentrice del conto.

La banca acquirente e la banca che detiene il conto hanno chiavi di zona diverse e quindi cifrature differenti del PIN.

Per questo motivo è necessario che i due switch gestiscano in modo opportuno la comunicazione tra le due banche, e quindi la manipolazione del PIN, in particolare lo switch-2 dovrà cifrare il PIN BLOCK inviatogli dallo switch-1 in modo tale che la banca detentrice del conto possa decifrarlo in maniera corretta.

Esistono tre funzioni di base per la gestione dei PIN:

1. Cifratura del PIN;

2. Traduzione del PIN tra chiavi di zona;

3. Verifica del PIN.

La prima operazione è un processo banale. Il PIN viene formattato in un blocco di 8 byte in chiaro e cifrato usando il DES o il 3DES.

La seconda operazione indirizza la richiesta del possessore di conto dalla banca su cui si effettua la connessione, alla banca con la quale l'utente detiene il conto. Questa operazione è effettuata perché le due banche hanno cifrature differenti del PIN, quindi (riferendoci alla figura precedente) lo switch-2 deve convertire (tradurre) il PIN Block inviatogli dallo switch-1 in modo tale che la banca detentrice del conto possa decifrarlo con la sua chiave di zona ed ottenere il PIN corretto.

La terza operazione serve alla banca per verificare se il PIN associato ad un conto è corretto.

Il compito degli Auto-Teller-Machines è quello di fornire un'interfaccia con l'utente, pertanto prevedono periferiche di I/O come monitor, tastiera, lettore di schede magnetiche e/o smartcard, un dispositivo per fornire il denaro richiesto e una telecamera. Gli ATM generalmente utilizzavano un sistema operativo della IBM (OS/2).

Ora gli ATM usano Windows Xp e TCP/IP.

I punti in cui la rete EFTPOS è maggiormente vulnerabile sono i seguenti:

- Nello sportello ATM;
- nella rete che unisce la banca acquirente con la banca detentrice del conto.

Nel primo caso molto dipende dall'utente, infatti ci sono delle regole che un possessore di conto deve rispettare per evitare di essere truffato.

L'utente deve:

- accertarsi che non ci sia nessuno a spiarlo mentre digita il PIN;
- verificare che lo sportello ATM sia integro (cioè senza nessuna manomissione);
- non tenere la carta ATM ed il codice PIN nello stesso posto in modo da evitare che se un malintenzionato trovi uno trovi anche l'altro.

Inoltre lo sportello ATM utilizza due metodi di protezione:

- se entro 30 secondi dall'erogazione del denaro l'utente non lo ritira il denaro viene ripreso dallo sportello;
- se l'utente inserisce per tre volte consecutive il PIN errato lo sportello non eroga il denaro e non restituisce la carta ATM.

Nel secondo caso invece difendersi è più difficile, comunque ogni banca ed ogni switch può proteggersi da eventuali attacchi rispettando i seguenti punti:

- aggiornare sistematicamente i dispositivi di sicurezza;
- essere vigile aumentando le verifiche.

Questo sicuramente non è abbastanza perché oltre alle banche e gli switch, ogni altro punto della rete attraverso cui transita il PIN Block deve essere protetto; potrebbe infatti accadere che ci sia uno sniffer in un punto qualsiasi della rete, quindi il gestore della rete deve sistematicamente controllarla utilizzando dispositivi di sicurezza sempre aggiornati.

3. Attacchi all' ATM

Si riportano alcuni dati pubblicati dall'Enisa, un'associazione dell'UE che si occupa della sicurezza delle reti.

Nel 2008, il Consiglio europeo ATM Security Team (East) ha calcolato 383.951 sportelli automatici in Europa e oltre 1,5 milioni di sportelli automatici in tutto il mondo.

Il 72% del numero totale di distributori automatici di banconote europee si trova in cinque paesi: Regno Unito, Spagna, Germania, Francia e Italia.

Il numero totale di distributori automatici europeo è aumentata del 6% rispetto all'anno precedente.

Con l'aumento del numero di sportelli automatici in Europa vi è stato anche un aumento significativo del numero totale degli attacchi segnalati ATM. Il totale delle perdite hanno raggiunto 485,15 milioni di euro nel 2008.

Un recente rapporto pubblicato dalla East dice che nel 2008, i reati connessi ATM in Europa, sono aumentati del 149% rispetto all'anno precedente. Secondo il rapporto, questo aumento delle frodi ATM è legato principalmente ad un aumento drammatico dei cosiddetti attacchi di ATM-skimming. Nel corso del 2008, un totale di 10.302 incidenti di card skimming sono stati segnalati in Europa. Ma più inquietante sono le recenti notizie di attacchi che sfruttano prontamente malware disponibile e avanzato che ha infettato le reti ATM e ATM stessi.

Secondo la stessa relazione, le aggressioni contro gli utenti dei distributori automatici di banconote europee sono diminuite del 29% principalmente a causa di una diminuzione del numero di rapine segnalate. Tuttavia i casi di ATM attacchi fisici contro gli stessi sportelli automatici sono aumentati del 32%. Nonostante le perdite di denaro per questi attacchi sono inferiori a quelli di altri crimini di ATM, questi attacchi continueranno a rimanere di grande preoccupazione per l'industria.

3.1. Attacchi fisici

Riporto un Articolo del quotidiano "Il Resto Del Carlino":

Reggio Emilia, 23 gennaio 2010. Hanno usato un escavatore rubato, che hanno poi abbandonato sul posto, per asportare la cassa bancomat della filiale del Credito emiliano di Bibbiano, nella Val d'Enza reggiana. L'hanno poi caricata su un furgone e sono fuggiti, con un bottino di circa 40 mila euro.

Gli attacchi fisici sono effettuati con l'intenzione di accedere al denaro contante all'interno della cassaforte bancomat. Alcuni dei metodi più comuni comprendono

- attacchi esplosivi (gas e non-gas) e di taglio (ad esempio fiamma ossidrica, lancia termica, punta di diamante).
- La rapina può verificarsi anche quando i distributori automatici sono sotto manutenzione. Quando il personale che trasporta il denaro da o verso un bancomat è attaccato, o quando la cassetta di sicurezza ATM è aperta e le cassette di cassa sostituite.

3.2. Lebanese loop

Con la tecnica chiamata "Lebanese Loop" il truffatore entra in possesso del Bancomat e del relativo Pin. Viene applicato un dispositivo che blocca la tessera all'interno dello sportello, il cliente viene "soccorso" dal truffatore che lo invita a digitare il codice di accesso (questo permette al ladro di memorizzare la sequenza segreta), quindi non appena il titolare del Bancomat si allontana, il truffatore provvede a recuperare la tessera.

3.3 Skimming attack

La frode prevede l'applicazione di apparecchi per la cattura dei dati delle carte detti **skimmer** (dispositivo sovrapposto alla fessura nella quale viene introdotta la carta) secondo il seguente schema:

- applicazione e rimozione più volte al giorno, anche dopo un breve lasso di tempo (es. mezz'ora) in un qualsiasi giorno della settimana, particolarmente in orari in cui l'agenzia è chiusa al pubblico;
- i dati raccolti dallo skimmer vengono, in alcuni casi, radiotrasmessi ad un complice nelle vicinanze dell'ATM che con un PC portatile li registra per il successivo uso; in altri casi i dispositivi vengono rimossi fisicamente;
- sono catturate tutte le informazioni presenti sulla carta anche in caso di carte multifunzione (II e III traccia) per consentire frodi sia in Italia (circuito Bancomat/PagoBancomat) che all'estero (circuiti CIRRUS/Maestro);
- i dati vengono catturati con finte tastiere sovrapposte alle originali o con microcamere posizionate in modo da inquadrare la tastiera.

I dati così raccolti vengono utilizzati, per le frodi sui circuiti internazionali, anche a distanza di mesi, rendendo in tal modo molto difficile contrastare il fenomeno. Con gli sviluppi delle tecniche su esposte diventa ancor più importante l'opera di controllo degli ATM in dotazione alle agenzie. Le autorità competenti pertanto raccomandano , oltre all'ispezione delle apparecchiature in occasione dell'ingresso quotidiano in agenzia, un periodico controllo durante le eventuali uscite infra-giornaliere (per la pausa caffè, incontri con la clientela, pagamenti alle Poste o altro...).
L'attenzione dovrà essere portata alla rilevazione dei dispositivi di cui sopra (finti frontali, pellicole sulle tastiere, lettori aggiuntivi di carte, telecamere, plafoniere modificate) considerando:

- che gli skimmer (leggeri e non) assumono la forma di una cornice, in plastica o in metallo, intorno alla fessura originaria per l'introduzione della carta ;
- che in questo caso (ma anche in caso dell'apposizione di un finto frontale) la porzione di carta che normalmente sporge dal lettore, dopo l'operazione di prelevamento, risulta ridotta rispetto al normale;
- che le micro telecamere (per la cattura del PIN) vengono in genere poste nelle plafoniere e comunque in posizioni atte ad inquadrare la tastiera racchiusa in contenitori di plastica.

- che le finte tastiere sono del tutto simili alle originali.

3.4 Virus e worm

La migrazione del S.O. degli ATM a Windows Xp ha esposto gli ATM ai problemi di sicurezza tipici di un PC. Gli ATM sono suscettibili ad essere infettati da virus e altri software dannosi.Il software dannoso è iniettato nell' ATM attraverso attacchi alla rete, o in altri dispositivi infetti. Una volta installato su ATM, il software "maligno" raccoglierà informazioni relative alla carta e PIN.

I bancomat di due banche americane sono stati infettati, nell'agosto del 2003, da un worm che si propaga attraverso una vulnerabilità nella sicurezza di Windows. La notizia, riportata qualche tempo fa da SecurityFocus.com, è stata ora ufficialmente confermata da 'Diebloid', il produttore che ha costruito gli ATM colpiti dal worm.
Secondo l'azienda, la scorsa estate un numero non precisato di bancomat su cui girava Windows XP Embedded sono stati spenti perché infettati da Welchia (anche noto come Nachi), un worm "buono" scritto per debellare un suo simile, Blaster, che ha però finito per intasare le reti di molte aziende, fra cui il sistema di check-in di Air Canada. Entrambi i virus si diffondono sfruttando una falla di Windows XP, 2000, NT e Server 2003.

"È un segno premonitore di ciò che accadrà in futuro - ha commentato Bruce Schneier, ricercatore presso la Counterpane Internet Security- Macchine con scopi specifici, come gli ATM, non sono mai stati colpiti da virus. Ora che usano un sistema operativo general purpose come Windows XP Embedded, Diebold dovrà aspettarsi molti problemi del genere in futuro".

Un dirigente di Diebold, Steve Grzymkowski, ha spiegato che la sua azienda ha migrato i propri ATM su esplicita richiesta delle banche da OS/2 di IBM, sistema ancora discretamente diffuso in ambito bancario, a Windows.
"Ci hanno detto che preferivano Windows - ha detto Grzymkowski - perché ha migliori capacità grafiche e un look familiare".
Diebold ha fatto sapere che, per evitare incidenti come quello dell' estate 2003, nel prossimo futuro includerà nei suoi distributori automatici un firewall in grado di bloccare eventuali tentativi di attacco. Proprio nel novembre dello stesso anno, l'azienda ha stipulato un accordo con Sygate Technologies per "fornire una protezione superiore contro le minacce di sicurezza del software che hanno come bersaglio gli ATM". "La sicurezza - si legge in un recente comunicato di Diebold - sta crescendo d'importanza con la migrazione degli ATM verso Windows e le reti TCP/IP".

Nel mese di aprile 2009, gli sportelli automatici in Russia sono stati infettati da malware sofisticati. Il malware è stato in grado non solo di raccogliere i dati della carta, ma anche il PIN.

I criminali hanno ottenuto l'accesso fisico all'interno degli ATM interessati, e tale accesso fisico è stato poi sfruttato per mettere in funzione software non autorizzato e dispositivi sugli ATM, utilizzati per intercettare informazioni sensibili. Il trojan, che secondo quanto sostiene Sophos sarebbe in circolazione da novembre 2008, utilizza un buon numero di funzioni non documentate per annidarsi nel sistema operativo Windows analizzando i dati per lo schermo e la stampante e ovviamente passando sotto scansione le transazioni finanziarie (vale a dire le richieste di denaro inserite allo sportello) in valuta ucraina, russa e statunitense. Il trojan Troj/Skimer-A, che per Sophos rappresenta il primo caso di malware pensato per operare esclusivamente su ATM, non è dotato di routine di propagazione autonome ed è quindi necessario che venga installato direttamente sulla macchina per poter avviare l'infezione.

3.5 Phishing

Questo tipo di frode sono progettati per indurre l'utente a fornire il numero della carta e il PIN per la loro carta di credito. Il ladro invia una e-mail fingendosi una banca e sostenendo che le informazioni dell'account siano incomplete, o che l'utente ha bisogno di aggiornare le sue informazioni di account per impedire che esso venga chiuso. L'utente è invitato a cliccare su un link e seguire le istruzioni fornite. Il collegamento è comunque fraudolento e indirizza l'utente verso un sito creato dai ladri e progettato per assomigliare alla banca dell'utente. Il sito indirizza l'utente ad inserire informazioni sensibili come numeri di carta e PIN. Le informazioni vengono raccolte dai ladri e utilizzate per creare le carte fraudolente, prelevare fondi dal conto dell'utente e fare acquisti.

Questo tipo di attacco è molto frequente ma evitare rischi è semplice: NON UTILIZZARE I CODICI se non per accedere personalmente a banca via internet e per confermare disposizioni da sè già impostate.

In particolare, non fornire mai le password:

1. per effettuare un presunto sblocco dell'utenza o per confermare presunte vincite di concorsi.
   Ricorda che si può richiedere l'eventuale sblocco delle utenze solo in Agenzia.
2. nella pagina di login della banca via Internet.
   Ricorda che per accedere al Servizio sono richiesti solo codice di adesione e pin.
3. all'interno di una pagina con una simultanea richiesta di più password dispositive.
   Ricorda che la banca non richiede in nessun caso il contemporaneo inserimento di più password per confermare un'unica operazione in un'unica pagina.

Semplici indicazioni per evitare spiacevoli sorprese:

- Prima di inserire password in un sito è opportuno verificare sempre la presenza del prefisso "https: //" e del "lucchetto chiuso".
- Le banche non chiedono mai via email di confermare dati personali o codici riservati (numero carta di credito, password, ecc.).
- Le banche non chiedono in nessun caso il contemporaneo inserimento di più password per confermare un'unica operazione in un'unica pagina.
- Proteggi il tuo computer con un AntiVirus aggiornato.

3.6 Insider attack

Presuppone l'esistenza di un membro (insider - da qui il nome) che può essere sia un impiegato di un istituto finanziario, sia un individuo che abbia ottenuto accesso alla rete finanziaria, anche se attraverso qualche tecnica di hacking tradizionale. L'attaccante comincia la frode monitorando il flusso delle transazioni per un certo periodo, e memorizzando i PIN block cifrati e i numeri di conto ad essi associati che passano attraverso il sistema. Utilizzando una routine per decifrare i PIN criptati, come ad esempio il Decimalization attack di cui parleremo, sono estratti i numeri di PIN in chiaro attraverso una sequenza di richieste al modulo hardware di sicurezza. Dopo aver ottenuto una lista di numeri di conto (ed anche informazioni aggiuntive) insieme con i corrispondenti PIN, l'attaccante può portare l'assalto vero e proprio all'istituto di credito. Per sfruttare questa lista,

l'attaccante acquista una serie di "white cards" (carte bianche) ed un lettore/scrittore di carte (facilmente reperibili su Internet per una cifra che si aggira attorno ai 600 €). Su ognuna di queste schede egli scrive le informazioni sul conto rubate, creando un duplicato in tutto e per tutto uguale alla carta ancora in possesso del malaugurato correntista. Queste carte sono poi distribuite ad una rete di complici, che effettuano periodiche "visite" agli ATM dell'area. Ogni carta potrà essere usata una sola volta al giorno prelevando il limite giornaliero, in un ATM casuale . Per potersi rendere conto di quanto possa fruttare un attacco del genere vediamo un esempio numerico: sia *n* il numero dei conti compromessi, *p* il periodo medio entro cui le transazioni truffaldine vengono scoperte, ed *l* il limite giornaliero per il prelievo. Il valore totale *F* della frode sarà: $\boldsymbol{F = n \; x \; p \; x \; l}$:

$$n = 5000; \; p = 2; \; l = 1000 \text{ €}$$

L'ammontare totale della frode sarà quindi di **10,000,000 €**.

Sottrarre un grande numero di conti è molto semplice grazie all'efficienza degli attacchi. Un trojan o una porzione di codice malizioso potrebbero rubare molti milioni di conti in pochi giorni. Quindi l'organizzatore della frode potrebbe rubare un quantitativo di denaro altissimo.

3.7 Competitor attack

Un utente può usare la sua scheda su reti diverse dalla rete della banca di emissione del conto. Come risultato, un possessore del conto può essere attaccato su qualsiasi rete attraverso cui il suo PIN viaggi. Questo include le reti dei concorrenti. Così un concorrente potrebbe scegliere di portare un attacco di tipo “Insider attack” contro i clienti di una particolare istituzione. Inoltre, come amministratori della loro rete, è possibile per loro usare i benefici supplementari e i poteri che sono associati ai privilegi dell'amministratore per effettuare questo. Combinato con tempo e accesso illimitato, il successo dell'attacco è garantito.

Comunque, la ricompensa non sono i soldi rubati ma piuttosto gli effetti successivi. La pubblicità negativa e il danno per le relazioni con i clienti, che sorgerebbero dopo tale attacco, potrebbero distruggere la credibilità di una banca. Da questo risultato trarrebbe profitto il concorrente. Questo ha il vantaggio che non c'è alcuna connessione tra complici e assalitore (in questo caso l'istituzione del concorrente). Non c'è nessuna alcuno spostamento di denaro incriminante che conduce all'assalitore e nessun bisogno di eliminare le prove.

3.8 Decimalization attack

Il metodo IBM 3624-Offset fu sviluppato per supportare la prima generazione di ATM e fu largamente adoperato. Il metodo fu progettato in modo che gli ATM offline sarebbero stati capaci di verificare i PIN dei clienti senza avere bisogno di memorizzare i conti da manipolare in un database di record. Inoltre, fu sviluppato uno schema dove i PIN dei clienti potevano essere calcolati a partire dal numero di conto del cliente stesso a partire da una cifratura con chiave segreta. Il numero di conto è reso disponibile al cliente su scheda magnetica, quindi l'ATM ha bisogno solo di

immagazzinare in modo sicuro una sola chiave crittografica. Il numero di conto è rappresentato usando cifre ASCII, e poi interpretato come un input esadecimale per l'algoritmo di cifratura DES. In seguito viene fatta la cifratura con la chiave segreta "PIN generation"; l'output è convertito in esadecimale e solo le prime quattro cifre non vengono scartate. Inoltre poiché le quattro cifre potrebbero contenere le cifre 'A'-'F', non disponibili su una tastiera numerica standard, e che quindi potrebbero confondere i clienti, esse sono mappate con cifre decimali usando una "Tavola di decimalizzazione".

Tavola di decimalizzazione

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**

Numero di conto 4 5 5 6 2 3 8 5 7 7 5 3 2 2 3 9

Cifratura DES 3 F 7 C 2 2 0 1 0 0 CA 8 A B 3

Scarto cifre non usate e prendo 3F7C

Mapping con la tavola di decimalizzazione 3572

Passi per cambiare il PIN iniziale

PIN iniziale 3572 (+)

Offset 4244 (=)

New PIN 7816

Nell'esempio il PIN di 3F7C diventa 3572. Per permettere ai possessori della carta di cambiare il proprio PIN, si somma al PIN originale un Offset (associato univocamente ad ogni numero di conto), generando così un nuovo PIN. Quando un ATM verifica un PIN, sottrae semplicemente l'offset e confronta il risultato ottenuto con il PIN iniziale. L'Offset è un numero di max 4 cifre che di base viene impostato a 0000 e che serve qualora l'utente per qualche motivo, faccia richiesta di

un nuovo PIN. Dal momento che non e' possibile cambiare il suo numero di conto ci si limita ad aggiungere un certo valore al PIN originario. L'Offset viene registrato nella carta stessa. I centri di controllo delle banche e gli ATM usano Hardware Security Module (HSM), che offrono protezione da possibili attacchi portati da impiegati corrotti della banca. Un HSM è un processore su cui gira un software che offre servizi relativi alla crittografia e alla sicurezza. Possono utilizzare vari algoritmi crittografici quali il DES, 3DES, RSA e SHA1. Hanno elevate prestazioni crittografiche e validano fino a 60 PIN / sec.

Le *Application Programming Interface* API (*Interfaccia di Programmazione di un'Applicazione*), sono ogni insieme di procedure disponibili al programmatore, di solito raggruppate a formare un set di strumenti specifici per un determinato compito. È un metodo per ottenere un'astrazione, di solito tra l'hardware e il programmatore, o tra software a basso ed alto livello. Le API permettono di evitare ai programmatori di scrivere tutte le funzioni dal nulla.

L'API dell'HSM:

- contiene operazioni per generare e verificare i PIN;
- decifra le chiavi di zona quando vengono scambiate tra banche;
- supporta un'ampia gamma di funzioni per la gestione della chiave.

. Qualunque impiegato della banca che ha accesso al computer HSM, può effettuare operazioni come la verifica di un PIN, mentre altre operazioni, come il settaggio di nuove chiavi di cifratura, possono essere effettuate solo con l'autorizzazione da parte di più impiegati fidati. Un esempio di funzione per la verifica del PIN è mostrato:

Encrypted_PIN_Verify

```
 A_RETRES , A_ED ,                          // return codes 0,0=yes 4,19=no
 trial_pin_kek_in , pinver_key ,            // encryption keys for enc inputs
(UCHAR*)"3624 " "NONE “                     // PIN block format
" F"                                        // PIN block pad digit
(UCHAR*)" " ,
trial_pin ,                                 // encrypted_PIN_block
 I_LONG(2) ,
(UCHAR*)"IBM-PINO" "PADDIGIT" ,             // PIN verification method
I_LONG(4) ,                                 // # of PIN digits = 4
"0123456789012345"                          // decimalisation table
“4556238577532239"                          // PAN_data (account number)

"0000 “                                     // offset data
```

Codice di esempio per Verifica del PIN

Gli input cruciali a Encrypted_PIN_Verify sono la tavola di decimalizzazione, il PAN_Data (che contiene il numero personale dell'account) e l'Encrypted Pin Block (EPB).

Supponiamo che un impiegato di banca malintenzionato, si sia impossessato di un PAN_Data e tramite la funzione Encrypted_PIN_Verify può effettuare vari attacchi passando come input la tavola di decimalizzazione, il PAN_Data, l'offset e l'EPB. Alcuni circuiti bancari permettono l'inserimento di PIN di prova in chiaro quando non viene utilizzata la tavola di decimalizzazione. In questo caso è necessario abilitare il comando CCA *Clear_PIN_Encrypt*, che creerà un EPB a partire dal PIN scelto. Quando l'inserimento del PIN in chiaro non è disponibile per l'attaccante, egli può solamente inserire il PIN in un ATM reale e quindi intercettare l'EPB corrispondente ad ogni tentativo. In ogni caso l'attaccante può solamente ottenere blocchi di PIN cifrati; egli sarà quindi costretto a passare, come argomento della funzione Encrypted_PIN_Verify, gli EPB di prova che intende utilizzare per l'attacco.

La funzione ritorna true o false, a seconda che il PIN sia corretto o no.

Il tipo di attacco più conosciuto individuato da Mike Bond e Piotr Zielinski ricercatori della University of Cambridge è chiamato: Attacco alle Tavole di Decimalizzazione.

- **Fase 1:**

  vengono determinate quali cifre sono presenti nel PIN da ricercare.

- **Fase 2:**

  sono testati tutti i PIN composti con le cifre identificate nella fase precedente.

Questo attaccho può essere effettuato solo da un dipendente della banca che ha accesso alla funzione Encrypted PIN Verify.

Per effettuare l'attacco l'assalitore ha a disposizione:

- tavola di decimalizzazione modificata
- EPB (PIN di prova cifrato)
- PAN DATA

Poniamo D_{orig} come tavola di decimalizzazione originale. Per una data cifra *i*, consideriamo una tavola di decimalizzazione binaria D_i che gode della seguente proprietà: D_i ha 1 nella posizione *x* se e solo se D_{orig} ha la cifra *i* in quella posizione. In altre parole:

$$D_i[x] = 1 \text{ se } D_{orig}[x] = i$$

$$D_i[x] = 0 \text{ altrimenti}$$

Ad esempio, per una tavola standard :

D_{orig} =

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5

D_3 =

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0

Nella prima fase, confrontiamo il PIN originale mappato con la tavola di decimalizzazione D_i e il PIN di prova 0000 tramite la funzione Encypted_PIN_Verify. Il test fallisce quando il PIN originale contiene la cifra i. Ad esempio se il PIN è 7816 e la tavola di decimalizzazione è D_7 la funzione farà un matching tra 1000 e e 0000. In questo modo, effettuando al più 10 confronti, è possibile determinare tutte le cifre che compongono il PIN originale.

Nella seconda fase dell'attacco, per ottenere il PIN ricercato, è necessario provare tutte le possibili combinazioni delle cifre trovate nella prima fase. Il numero di combinazioni possibili è strettamente legato al numero di cifre differenti contenute nel PIN. La seguente tabella mostra tutte le possibili combinazioni necessarie a trovare un PIN quando esso è composto da una, due, tre o quattro cifre differenti.

Simboli che compongono il PIN	Possibilità
A	AAAA(1)
AB	ABBB(4), AABB(6), AAAB(4)
ABC	AABC(12), ABBC(12), ABCC(12)
ABCD	ABCD(24)

Dalla tavola si evince che, quando il PIN da trovare è composta da 3 differenti cifre (3° riga della tabella), tutte le possibili combinazioni di PIN formati da queste cifre, sono 36, e rappresentano il caso peggiore per l'attaccante. Inoltre è necessario sommare a queste 36 ipotesi le 10 ipotesi necessarie per determinare tutte le cifre che compongono il PIN ottenute nella fase precedente, per cui, nel caso peggiore, questo approccio necessiterà di 46 tentativi.

AABC	**ABCA**	**ABAC**	**ACBA**	**CBAA**	**BCAA**	**BACA**	**CABA**	**CAAB**	**BAAC**	**ACAB**	**AACB**
BBAC	**BACB**	**BABC**	**BCAB**	**CABB**	**ACBB**	**ABCB**	**CBAB**	**CBBA**	**ABBC**	**BCBA**	**BBCA**
CCAB	**CABC**	**CACB**	**CBAC**	**BACC**	**ABCC**	**ACBC**	**BCAC**	**BCCA**	**ACCB**	**CBCA**	**CCBA**

Tabella delle combinazioni con 3 cifre differenti

L'attacco permette a qualcuno che ha accesso al sistema informatico di una banca per determinare il PIN di una carta bancomat in una media di 15 tentativi, invece della media 5.000 attesa per un PIN a 4 cifre.

Questo tipo di attacco è noto come un attacco API perchè si basa su sfruttando una debolezza del Application Programming Interface (API) di HSM.

Riferimenti bibliografici

[1] http://alessandrobottoni.wordpress.com/tag/cartedicredito/

[2] http://www.cartedipagamento.com/frodi_carte_credito_4.htm

[3] http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-560.pdf

[4]http://www.dia.unisa.it/~ads/corso-security/www/CORSO-0304/ATM_0304/index.html

[5] http://www.dia.uniroma3.it/~dispense/merola/critto/tesine/bancomat.pdf

[6] http://www.enisa.europa.eu/

[7] http://www.primonumero.it/attualita/news/docs/1203519999.pdf