2019-2020

Formal Methods for Secure Systems Project

Nicola Barsanti Gianluca Tumminelli

Bank Robbery

**Indice**

**1 Introduzione**

In questo progetto abbiamo valutato il livello di sicurezza di una banca tramite l’utilizzo del modello **ADVISE**(ADversary VIew Security Evaluation).

Attraverso Mobiüs abbiamo simulato due diversi tipi di attacchi che possono essere effettuati per sottrarre soldi a una banca e ai suoi clienti. In particolare abbiamo analizzato un attacco fisico in cui gli avversari provano un attacco diretto alla banca ed uno informatico dove gli avversari tentano di infiltrarsi nella rete informatica e da questa sottrarne i soldi oppure rubare le credenziali degli utenti tramite un attacco di phishing e sottrarne i soldi direttamente dal conto corrente.

Per dettagliare ogni tipo d’attacco si sono considerati attaccanti professionisti che hanno le giuste conoscenze e abilità. In particolare, abbiamo considerato due tipi di avversari:

* **Rapinatore esperto**: predilige un attacco rischioso ma con probabilità di successo elevate, bassi costi di esecuzione e alti guadagni
* **Hacker**: predilige un approccio più cauto ma con tempi e probabilità di fallimento più alte e un guadagno più basso dovuto al limite della quantità di denaro trasferibile telematicamente.

Dal lato della banca invece abbiamo considerato un sistema di sicurezza sofisticato che comprende l’uso di allarmi, telecamere e pattuglie lungo i corridoi d’accesso alla cassaforte. Il sistema informatico della banca è considerato altamente sicuro e controllato periodicamente da sistemisti allo scopo di verificare eventuali violazioni ai dispositivi di sicurezza o la presenza di backdoor.

Immagine che contiene testo, mappa

Descrizione generata automaticamente

Figura Modello ADVISE

**2 Dettagli attacchi**

Nella seguente sezione andremo ad analizzare nel dettaglio gli attacchi descritti nel grafico di *Figura1.*

**2.1 Attacco fisico**

Per l’attacco fisico si è preso in considerazione un team di ladri professionisti che hanno le capacità adatte per ottenere il controllo delle telecamere e degli allarmi della banca. Essi hanno inoltre le qualità necessarie per entrare furtivamente all’interno della banca e accedere alla stanza di controllo. Conoscono inoltre le vulnerabilità dei sistemi di sicurezza utilizzati e di sfruttarle per trovare un percorso sicuro per la cassaforte e scassinarla.

I passi dell’attacco per poter raggiungere l’obbiettivo **Money** sono i seguenti:

* **Get Access To Alarm**: è l’attacco che permette di ottenere in caso di successo il controllo degli allarmi della banca. Per far ciò l’avversario ha bisogno innanzitutto di conoscere le vulnerabilità del sistema di allarme e notevoli conoscenze da hacker per poterle sfruttare. Inoltre l’attaccante necessita di capacità furtive per poter raggiungere un punto di accesso per prenderne il controllo. Per questo step abbiamo previsto un costo per l’avversario di 30, un tempo d’esecuzione dell’attacco che varia da una durata di 5 ad un massimo di 30 dipendente dal livello delle abilità di hacking possedute dall’avversario. Le probabilità di successo di questo attacco sono dell’ 1% in quanto i sistemi di sicurezza di una banca sono molto protetti e difficili da raggiungere. Gli attaccanti sono abili ma hanno comunque una probabilità di essere scoperti nel tentativo di manomettere gli allarmi del 5% in caso di successo e del 30% in caso di fallimento.
* **Get Access To Cameras**: è l’attacco che permette di ottenere il controllo delle telecamere della banca. Per far ciò l’avversario ha bisogno innanzitutto di conoscere le vulnerabilità del sistema delle telecamere e di avere notevoli conoscenze da hacker per poterle sfruttare. Inoltre necessita di capacità furtive per poter raggiungere un punto di accesso e prenderne il controllo. Per questo attacco è stato stimato un costo di 30 per l’avversario, un tempo di esecuzione dell’attacco che può variare da un massimo di 30 a un minimo di 5 in base alle abilità dell’avversario nell’infiltrarsi nel sistema di video sorveglianza. Le probabilità che questo attacco abbia successo e porti al controllo delle telecamere sono stimate all’1%, poiché il sistema di sorveglianza è protetto in modo che sia molto difficile ottenerne il controllo dei dispositivi di video sorveglianza e soprattutto raggiungere indisturbati la sala di controllo delle telecamere. La probabilità di essere scoperti dopo aver completato con successo questo attacco sono del 15% tenendo conto di possibili meccanismi di rilevamento della manomissione delle telecamere. Invece, le probabilità di essere scoperti dopo aver fallito l’attacco sono più alte del 40% tale percentuale è dovuta dalle possibilità di essere scoperti da eventuali guardie.
* **Study Security Routines**: è il passo che permette al team di ladri di osservare e studiare la routine del personale di sicurezza, per ottenere il percorso delle pattuglie e il loro tempi. Per effettuare questo step è necessario il controllo delle telecamere dalle quali osservare lo spostamento delle guardie. Abbiamo stimato un costo di 5 e un tempo di 1000 dovuto al fatto che, per studiare le ronde di guardia bisogna semplicemente osservare i vari turni e non è richiesta una presenza fisica all’interno della banca dovendo solo accedere in maniera remota alle telecamere. Per la stessa ragione le probabilità di successo sono del 75% e le probabilità di essere individuati sono nulle. Abbiamo tuttavia considerato due tipi di fallimento, il primo è generico e dovuto al fatto che non è stato possibile individuare le routine del personale e ha una probabilità del 15% di manifestarsi. Mentre il secondo è dovuto alla scoperta della precedente violazione delle telecamere e possiede una probabilità del 10% di verificarsi. Inoltre a seguito dell’individuazione dell’accesso questo verrà rimosso facendo perdere il controllo delle telecamere agli attaccanti.
* **Find Secure Access**: questo passo permette di individuare un percorso sicuro alla cassaforte utilizzando le telecamere per analizzare i possibili accessi e la conoscenza dei percorsi degli agenti di sicurezza. Il costo di tale attacco è di 5 ed il tempo di esecuzione è di 2000 ma, la sua probabilità di successo è solo del 10% poiché si suppone che i percorsi di pattuglia siano organizzati in modo tale da lasciare per poco tempo un punto scoperto. Anche in questo step abbiamo due tipologie di fallimento, si può avere a causa dell’impossibilità di trovare un valido percorso di accesso con una probabilità del 70% altrimenti, nel caso venga scoperto l’accesso delle telecamere, con una probabilità del 20%. Nel caso venga indivuato l’accesso l’attaccanti perderanno sia il controllo delle telecamere sia la conoscenza dello schema delle pattuglie la quale verrà riorganizzata dalla banca a seguito dell’individuazione della violazione.
* Immagine che contiene testo, mappa

  Descrizione generata automaticamente**Safe Break**: questo passo permette di ottenere accesso al denaro tramite l’apertura (per scassinamento o per conoscenza della combinazione) della cassaforte. Per far ciò si deve avere accesso agli allarmi e alle telecamere, conoscere un percorso sicuro alla cassaforte e possedere o le capacità da scassinatore. Il costo dell’attacco è di 40 in caso si utilizzi la combinazione viceversa, nel caso si opti per scassinare il caveau, di 70. Ipotizzando che nel momento in cui si va ad effettuare la rapina gli attaccanti si siano ben preparati, ottenendo il controllo di tutti i meccanismi di sicurezza e un accesso sicuro, abbiamo stimato la probabilità di successo intorno 75% e una probabilità di indivudazione del 25%. Tuttavia in caso di fallimento la probabilità di essere scoperti è quasi certa e l’abbiamo ipotizzata intorno al 95%.

Figura 2 ADVISE attacco fisico

**2.2 Attacco informatico**

Per l’attacco informatico si è preso in considerazione un team di hacker esperti che hanno le conoscenze necessarie per entrare all’interno della rete informatica della banca tramite l’utilizzo di una back door e ottenuto l’accesso trovare le credenziali del direttore o il controllo del sistema bancario in modo da poter trasferire telematicamente il denaro della banca nei propri account. Gli attaccanti possono avere anche una conoscenza di social engineering che permette loro di poter ottenere le credenziali degli utenti della banca tramite l’utilizzo di tecniche di phishing. A causa della natura degli attacchi informatici, gli attaccanti hanno una elevata capacità di rimanere anonimi anche in caso di fallimento tuttavia gli attacchi richiedono molto tempo e risorse per essere eseguiti e il guadagno risulta inferiore in quanto si suppone la banca preveda delle misure di sicurezza aggiuntive non violabili(ad esempio richiesta la firma dei titolari dei conti in sede) per il trasferimento di somme di denaro ingenti.

I passi per ottenere i **Digital Money** sono:

* **Phishing**: in questo step l’attaccante tramite le sue abilita di social Engineering invia grandi quantitativi di e-mail con lo scopo di ingannare qualche utente e ottenere le sue credenziali bancarie. Il costo di tale attacco è di 50 e il tempo di esecuzione può variare a seconda delle capacità di social engineering da un minimo di 3000 al massimo di 5000. Le probabilità di successo di tale attacco sono dell’1% dovuto alla poca probabilità che gli utenti si facciano ingannare ma allo stesso tempo fornisce probabilità nulle di individuazione sia in caso di successo che di fallimento.
* **Transfer Customer Money:** in questo step l’attaccante utilizzando le credenziali sottratte all’utente ruba i soldi dal conto corrente dell’utente ottenendo così i **digital money**. Il costo di tale attacco è di 5 come il tempo di esecuzione. Le probabilità di successo sono dell’ 80% con una probabilità di essere scoperti del 5%, mentre nel caso di fallimento la probabilità di venire individuati è del 10%.
* **Cyber Attack**: in questo step utilizzando le skill di hacking e le conoscenze delle debolezze dei sistemi di sicurezza della rete informatica, l’attacca riesce a generare una back door nella rete della banca. Il costo è di 70 e i tempi variano a seconda delle capacità di hacking tra un minimo di 30 e un massimo di 60. La probabilità di successo è dell’1% considerando l’elevato livello di sicurezza della una rete di una banca, con la probabilità di essere scoperti dello 5%, mentre nel caso di fallimento è dell’1%. Questo perché è più probabile essere scoperti se si entra all’interno della rete invece che fallire e rimanere fuori dalla rete.
* **Infect the system**: in questo step l’attaccante infetta la rete utilizzando la capacità di hacking unita alla backdoor creata all’attacco precedente, per ottenere l’accesso completo alla rete. Il costo dell’attacco è di 65% e il tempo varia da 10 a 30 in base alle skill di hacking. La probabilità di successo è del 5% con probabilità di essere individuati del 5%. In caso di fallimento si ha o il caso generico che ha probabilità del 65% di accadere con il 5% di probabilità di essere scoperti e il caso di essere scoperti per l’individuazione da parte di un sistemista della backdoor con la probabilità del 30% e rischio di essere scoperti del 5%. In caso di individuazione della backdoor si ha la predita di essa.
* **Get Director Credentials**
* **Get Safe Combination**
* **Transfer Bank Money**