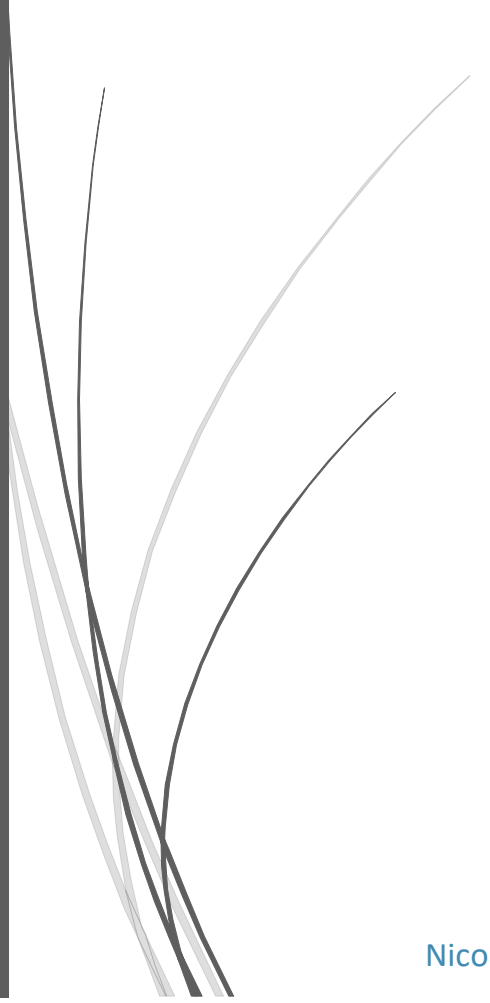
2019-2020

Bank Robbery

Formal Methods for Secure Systems Project



Nicola Barsanti Gianluca Tumminelli

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.

Figura 1 Esempio di una struttura bancaria

2 Dettagli attacchi

Nella seguente sezione andremo ad analizzare nel dettaglio i seguenti attacchi:

- **Attacco fisico** con la seguente configurazione dei pesi di preferenza:
  - **Cost:** 0.4
  - **Detection:** 0
  - **Payoff:** 0.6
- **Attacco informatico** con la seguente configurazione dei pesi di preferenza:
  - **Cost:** 0
  - **Detection:** 0.4
  - **Payoff:** 0.6

Un ulteriore caso di studio è una modalità d'attacco che combina i due tipi di attacco e che presenta la seguente configurazione dei pesi di preferenza:

- **Cost:** 0.4
- **Detection:** 0.4
- **Payoff:** 0.6

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 individuato l'accesso gli 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.

- **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 individuazione del 25%. Tuttavia, in caso di fallimento la probabilità di essere scoperti è quasi certa e l'abbiamo ipotizzata intorno al 95%.

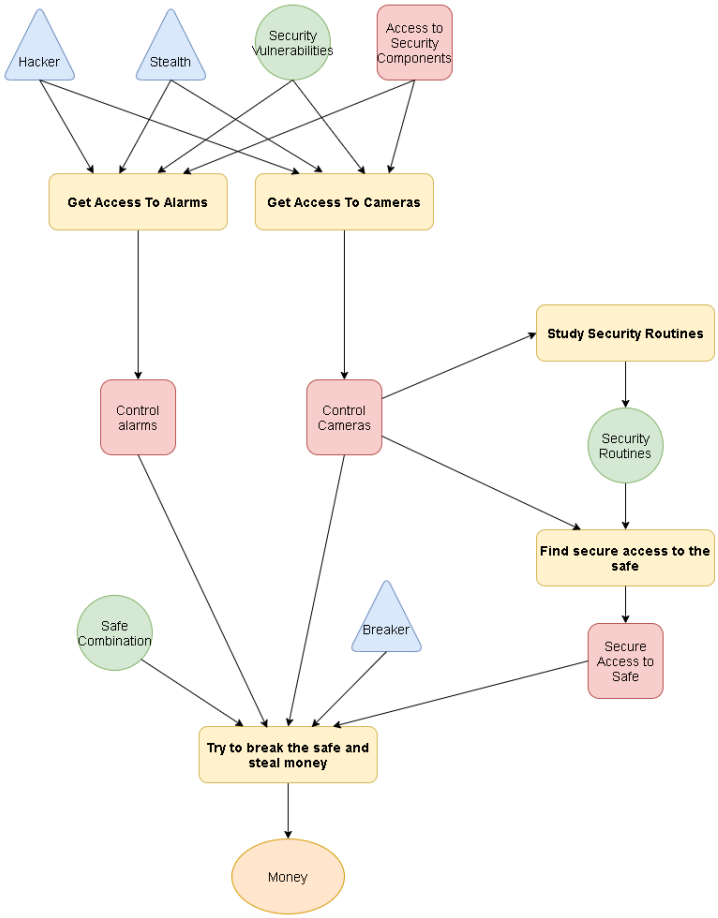


Figura 2 ADVISE attacco fisico

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 ottenerne l'accesso e trovare le credenziali del direttore in modo da poter trasferire il denaro della banca. Inoltre, hanno anche una conoscenza di social engineering che permette di poter ottenere le credenziali degli utenti della banca tramite phishing. Per finire questo team ha una elevata capacità di rimanere anonima anche in caso di fallimento.

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

- **Phishing**: in questo passo l'attaccante tramite le sue abilita di social Engineering invia e-mail per ingannare un utente e ottenere le sue credenziali. 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 ad un massimo di 5000. Le probabilità di successo di tale attacco sono stimate all'1%. Gli hacker utilizzano un metodo d'attacco tale da che non ci siano possibilità che vengano scoperti.

- **Transfer Customer Money:** in questo passo l'attaccante utilizzando le credenziali sottratte all'utente per rubare 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%. Le probabilità di venire scoperto dopo aver fallito l'attacco sono del 10%.

- **Cyber Attack**: in questo passo si utilizzano le skill di hacking e le conoscenze delle debolezze dei sistemi di sicurezza della rete informatica, l'attaccante 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% in quanto il livello di sicurezza della rete di una banca è molto elevato. Le probabilità di essere scoperti dopo aver completato con successo questo attacco sono del 5%, mentre nel caso in cui l'attacco fallisce tale probabilità è dell'1%.

- **Infect the system**: in questo passo l'attaccante infetta la rete informatica della banca utilizzando le capacità di hacking insieme alla backdoor creata nell'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%. Abbiamo considerato due tipi di fallimento il primo è generico e dovuto al fatto che non è stato possibile infettare con successo il sistema ed ha probabilità del 65% di manifestarsi con il 5% di probabilità di venire rintracciati. Mentre il secondo caso viene causato dall'individuazione e cancellazione da parte di un sistemista della backdoor creata con una probabilità che accada del 30% e con un rischio di venire individuati del 5%.

- **Get Director Credentials**: questo passo permette all'attaccante di ottenere le credenziali del direttore della banca tramite l'utilizzo delle conoscenze di hacking e della backdoor ottenuta in precedenza. Per tale attacco è stato stimato un costo di 55 e un tempo d'esecuzione che può variare da un massimo di 25 a un minimo di 5 in base alle abilità dell'avversario nell'hacking. Le probabilità di successo sono stimate al 10% con una probabilità di essere scoperti del 5%. Anche in questo attacco abbiamo considerato due tipi di fallimento il primo è dovuto all'incapacità di ottenere le credenziali del direttore e ha una probabilità del 60% che si manifesta con il rischio di venire scoperti al 5%. Mentre il secondo caso viene provocato dall'individuazione e cancellazione della backdoor creata da parte di un sistemista con una probabilità che accada del 30% e con un rischio di venire individuati del 5%.

- **Get Safe Combination**: in questo passo l'attaccante tramite le sue abilità di hacking e l'utilizzo della backdoor ottiene la combinazione della cassaforte da utilizzare opzionalmente durante il passo dell'apertura della cassaforte. Questo attacco presenta un punto di fusione tra le due tipologie di attacco. Per tale attacco è stato stimato un costo di 60 e un tempo d'esecuzione che può variare da un massimo di 25 a un minimo di 5 in base alle abilità dell'avversario nell'hacking. Anche in questo attacco abbiamo considerato due tipologie di fallimento, la prima è dovuta all'incapacità di ottenere la combinazione della cassaforte e ha una probabilità di manifestazione del 60% e il rischio di venire individuati al 5%. Mentre il secondo caso viene provocato dall'individuazione e cancellazione della backdoor creata da parte di un sistemista con una probabilità che accada del 30% e con un rischio di venire individuati del 5%.

- **Transfer Bank Money**: questo attacco permette di ottenere digitalmente i soldi di una banca tramite l'accesso al sistema e l'utilizzo delle credenziali del direttore. Il costo di tale attacco è di 5 e il tempo d'esecuzione è fisso ad un valore di 5. La probabilità di successo è stimata al 80% con una

probabilità di venire rintracciati del 5%. In caso l'attacco fallisca la probabilità di venire individuati passa al 10%.

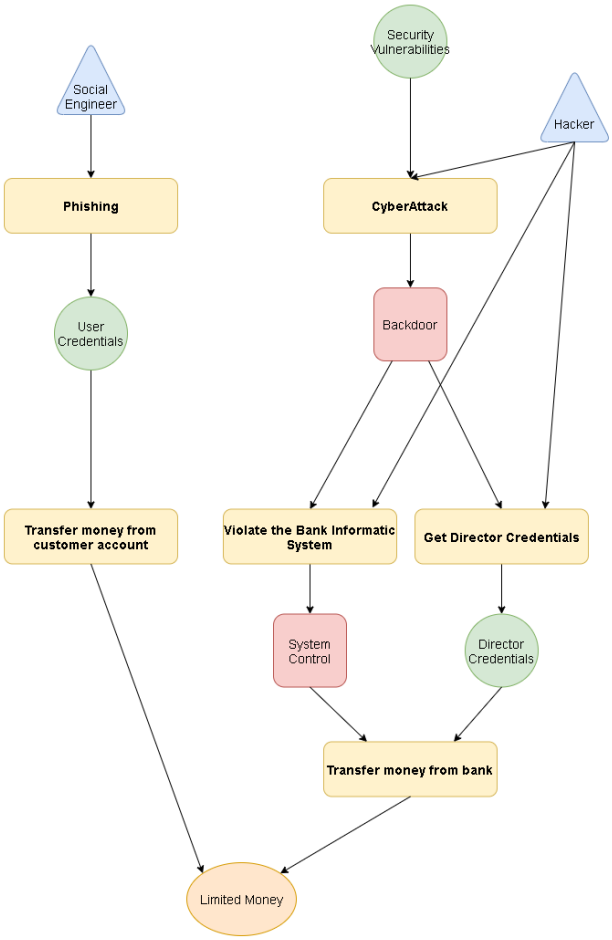


Figura 3 Attacco Informatico

2.3)Attacco combinato

Combinando i due tipi d'attacco otteniamo un attacco molto più articolato, in cui i due team collaborano per poter sottrare soldi alla banca o direttamente dai suoi clienti(attacco di phishing). In particolare, nell'attacco informatico oltre a tentare di rubare i soldi dalla banca digitalmente, gli hacker cercheranno di sottrare al passo **Get Safe Combination** la combinazione della banca. Tale combinazione verrà utilizzata dai ladri per aprire la cassaforte in modo più efficace (meno costoso) rispetto a scassinarla.

Gli obiettivi che verranno raggiunti saranno ottenere i soldi dalla cassaforte(dall'attacco fisico) e ottenere i soldi dal conto corrente di un cliente o direttamente dal deposito digitale di una banca. Una scelta importante che abbiamo preso è quella di considerare il guadagno ottenuto con un attacco fisico maggiore rispetto a quello ottenuto da un attacco informatico. Tale scelta è stata presa considerando che c'è un limite del denaro elettronico che può venir spostato in una sola volta.

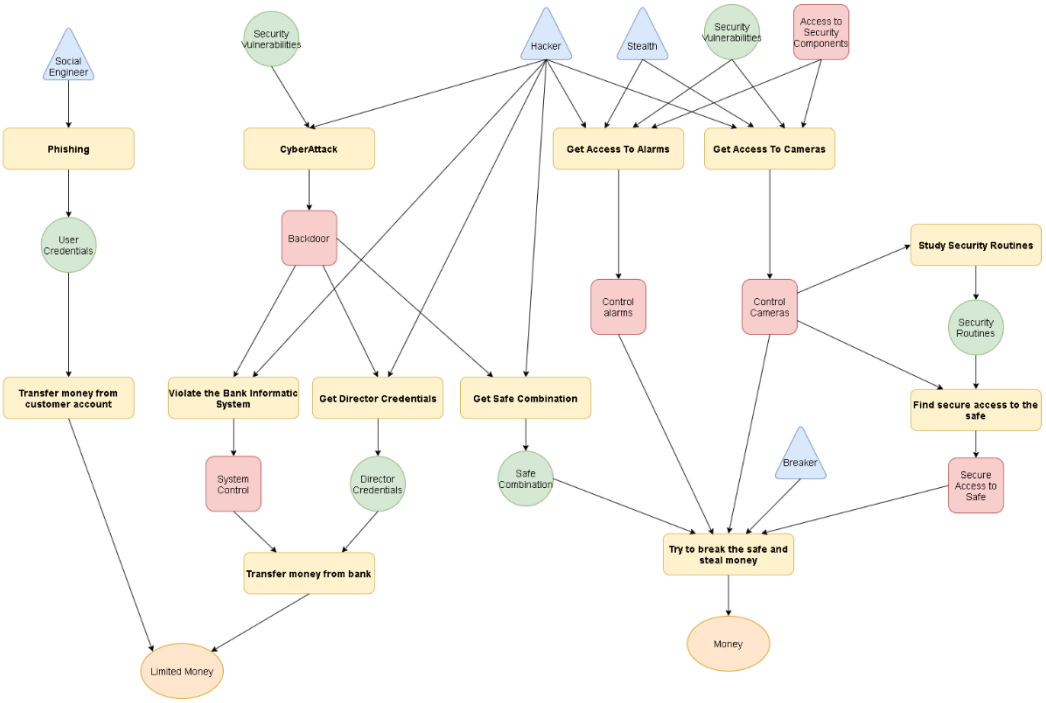


Figura 4 Attacco completo

3) Analisi

In questa sezione analizzeremo i risultati ottenuti dalle simulazioni effettuate sui modelli d'attacco descritti nel capitolo precedente. Nel dettaglio analizzeremo l'andamento dei tre tipi d'attacco nel tempo tramite l'utilizzo di variabili di reward.

3.1)Analisi attacco fisico

Dal *Grafico 1* possiamo osservare come la sicurezza complessiva della banca sia correlata alla difficoltà ad ottenere l'accesso alle telecamere, agli allarmi. In particolare, si avrà una probabilità diversa da zero che l'avversario ottenga i soldi a tempo t=3500. Per ciò se si controllano i sistemi di sicurezza con un intervallo temporale minore o uguale a 3500 si garantisce la completa sicurezza della banca con una probabilità del 95%, dovuto alla accuratezza con cui si ottengono i dati.

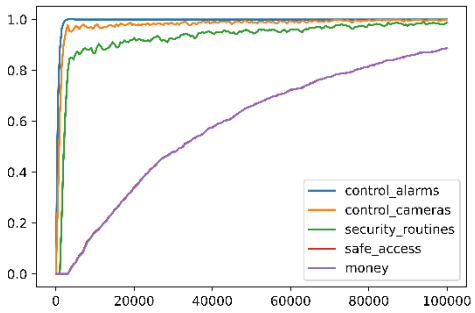


Grafico 1

Le variabili reward per questo attacco sono:

- **control_camera:** le telecamere della banca vengono sabotate
- **control_alarms**: gli allarmi della banca vengono disattivati
- **security_routines:** vengono ottenuti i percorsi delle pattuglie
- **safe_access:** si ottiene l'accesso alla cassaforte
- **money:** ottenimento del denaro dalla cassaforte

3.2) Analisi attacco Informatico

Nell'attacco informatico gli avversari hanno due rami da percorrere un ramo dove si tenta l'attacco di phishing e un attacco dove viene effettuato un attacco alla rete informatica della banca.

Dal *Grafico 2* si nota come la curva che descrive la probabilità nel tempo di ottenere i soldi quasi si sovrappone con la curva che descrive l'ottenimento delle credenziali utente. Da questo si può osservare come l'attacco di phishing sia la strada preferita dagli hacker, poiché con questo tipo d'attacco il rischio di essere rintracciati è minimo. Dal grafico si nota che a partire dal tempo 3000 la probabilità del furto dei soldi sia maggiore di 0. Per garantire con un 95% di accuratezza la sicurezza del servizio informatico della banca è necessario, ogni 3000 istanti di tempo generare nuove credenziali per gli utenti e controllare la presenza di una back door.

Un'altra misura interessante è quella di istruire i propri clienti in modo da diminuire drasticamente la probabilità che a un utente vengano rubate le credenziali.

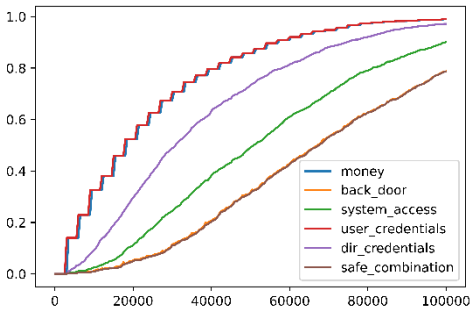


Grafico 2

Le variabili reward per questo attacco sono:

- **back_door:** creazione di una backdoor nella rete della banca

- **system_access:** ottenimento dell'accesso del sistema informatico della banca
- **user_credentials:** ottenimento delle credenziali dell'utente della banca
- **dir_credentials:** ottenimento delle credenziali del direttore della banca
- **safe_combination**: ottenimento della combinazione della cassaforte della banca
- **money:** ottenimento soldi elettronici della banca

3.3) Analisi attacco combinato

Mettendo in combinazione l'attacco fisico e l'attacco informatico otteniamo un nuovo tipo d'attacco più articolato. Nel *Grafico 3* si nota come l'attacco preferito è l'attacco di phishing e di conseguenza si ha una probabilità di ottenere i soldi digitali mediamente più elevata rispetto ad ottenere i soldi dentro la cassaforte. Il risultato è abbastanza prevedibile poiché i sistemi di sicurezza di una banca sono molto sicuri ed è facile farsi individuare scegliendo questo attacco, mentre con il phishing anche se i tempi sono più lunghi il rischio di venire rintracciati è quasi nullo. La conclusione è che per diminuire la vulnerabilità di una banca si può:

- controllare e resettare periodicamente i dispositivi di sicurezza della banca.
- Far modificare periodicamente le password ai clienti
- Controllare la presenza di eventuali back door nella rete informatica della banca.

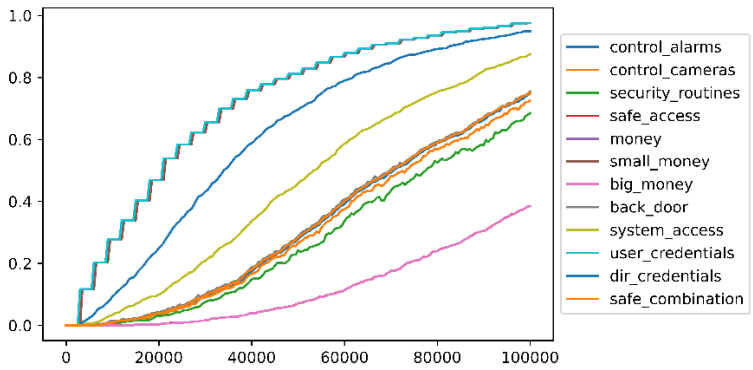


Grafico 3

Le variabili reward per questo attacco sono:

- **control_camera:** le telecamere della banca vengono sabotate
- **control_alarms**: gli allarmi della banca vengono disattivati
- **security_routines:** vengono ottenuti i percorsi delle pattuglie
- **safe_access:** si ottiene l'accesso alla cassaforte
- **back_door:** creazione di una backdoor nella rete della banca
- **system_access:** ottenimento dell'accesso del sistema informatico della banca
- **user_credentials:** ottenimento delle credenziali dell'utente della banca
- **dir_credentials:** ottenimento delle credenziali del direttore della banca
- **safe_combination**: ottenimento della combinazione della cassaforte della banca
- **big_money:** soldi ottenuti dall'attacco fisico
- **small_money:** soldi ottenuti dall'attacco informatico
- **money:** ottenimento del denaro dalla cassaforte(**small_money + big_money**)