Scuola di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Informatica

Tesi di Laurea

STACKELBERG SECURITY GAMES NEL PROCESSO DI CYBERSECURITY RISK ASSESSMENT

ENGLISH TITLE

MATTEO BOLLECCHINO

Relatore: *Paolo Lollini*

Correlatore: *Manuel Drago*

Anno Accademico 2024-2025

Matteo Bollecchino: *Stackelberg Security Games nel processo di Cybersecurity Risk Assessment,* Corso di Laurea in Informatica, © Anno Accademico 2024-2025

CONTENTS

LIST OF FIGURES

"Le verità scientifiche non si decidono a maggioranza."
— Galileo Galilei

1

INTRODUZIONE

Il cybersecurity risk assessment (CRA) per un sistema ciber-fisico (CPS) è un processo sistematico che le organizzazioni utilizzano per identificare, valutare e mitigare i rischi informatici. In pratica, si tratta di analizzare a fondo il sistema informativo aziendale, identificare potenziali minacce e vulnerabilità, e definire azioni per ridurre i rischi e proteggere i dati sensibili.

La problematica principale di tale procedimento risulta confluire nella modalità con cui viene eseguito che, infatti, consiste in un approccio prettamente qualitativo. Ciò è osservabile anche nell'articolo [3]. Tale modalità di valutazione rappresenta effettivamente un problema, in quanto fornisce un risultato approssimativo sullo stato della sicurezza informatica di un CPS.

Vista la considerazione precedente, è stato ritenuto opportuno elaborare una metodologia che affrontasse la questione da un punto di vista quantitativo. Al suddetto scopo sono stati introdotti gli Stackelberg Security Games (SSGs), uno specifico modello della teoria dei giochi introdotto nell'articolo [5], nel processo di CRA.

La metodologia seguita per tale integrazione consiste, in seguito a una preliminare analisi degli SSGs, in un'integrazione del modello della teoria dei giochi all'interno del processo di CRA per un CPS, evidenziando una possibile mappatura tra gli elementi principali dei due soggetti. Ciò viene evidenziato fornendo uno/due casi di studio.

L'applicazione di tale metodo implicherebbe una progressione del CRA verso una metodologia meno approssimativa e automatica che consenta la restituzione di risultati più precisi.

La tesi si sviluppa in 4/5 capitoli: nel primo capitolo viene descritto lo "state of the art", nel quale vengono analizzati sia la struttura del processo di CRA sia le caratteristiche che contraddistinguono gli SSGs.

Nel secondo capitolo viene indagata, in maggior dettaglio, l'integrazione del modello della teoria dei giochi all'interno del CRA per un CPS con un relativo caso di studio.

Nel terzo capitolo vengono discussi i risultati ottenuti analizzando il caso di studio realizzato, descrivendone inoltre i dettagli implementativi.

Nel quarto, e ultimo, capitolo vengono tratte le conclusioni dell'analisi svolta precedentemente e descritti i possibili sviluppi futuri di tale progetto.

2

STATO DELL'ARTE

2.1 STACKELBERG SECURITY GAMES

Uno dei primi articoli in cui si incappa nel momento in cui si ricercano informazioni riguardanti gli Stackelberg Security Games è proprio l'articolo [5].

Gli *Stackelberg Security Games* (SSGs) sono un modello non cooperativo di teoria dei giochi utilizzato per ottimizzare le strategie di sicurezza in scenari in cui un difensore, con risorse spesso limitate, deve proteggere obiettivi critici da attacchi avversari.

I giochi non cooperativi sono un ramo della teoria dei giochi in cui i giocatori prendono decisioni individualmente, senza la possibilità di stringere accordi vincolanti con gli altri partecipanti. Ogni giocatore cerca di massimizzare il proprio payoff, tenendo conto delle strategie degli avversari.

Gli SSGs si contraddistinguono in ambito di teoria dei giochi dalla relazione esistente tra i propri agenti, ovvero difensore e attaccante. Infatti, il difensore agisce per primo e deve distribuire un numero limitato di risorse su un determinato insieme di target. L'attaccante, invece, ha una visione completa del sistema, quindi, dopo aver osservato la strategia del difensore, seleziona la propria strategia di attacco.

La definizione di strategia in un gioco cambia a seconda dell'entità che viene considerata. Il difensore sceglie una singola azione deterministica, come ad esempio, proteggere un obiettivo specifico con certezza. L'attaccante, invece, conoscendo questa scelta, può reagire di conseguenza in modo ottimale. La strutturazione di un gioco basandosi sulle strategie pure spesso non è la scelta ottimale per il difensore, poiché un attaccante informato può facilmente aggirare la difesa. In alternativa possono essere usate le strategie miste, le quali si basano sulle probabilità che un determinato ente compia un'azione. Infatti, il difensore assegna probabilità a

diverse azioni come, ad esempio, proteggere vari obiettivi con una certa distribuzione di probabilità. Questo introduce incertezza per l'attaccante, rendendo più difficile l'elaborazione di un attacco ottimale. È spesso preferibile tali tipi di strategie negli SSGs poiché migliorano la sicurezza complessiva delle risorse.

Un elemento centrale all'interno di un gioco è il concetto di payoff, interpretabile come un guadagno o una perdita per una determinata entità all'interno del SSG. Generalmente, l'obiettivo degli agenti è quello di massimizzare il payoff adottando una strategia ottimale, quindi sarà in tale senso che i giocatori faranno delle scelte piuttosto di altre.

In teoria dei giochi, un gioco a somma zero descrive una situazione in cui il guadagno o la perdita di un partecipante è perfettamente bilanciato da una perdita o un guadagno di un altro partecipante in una somma uguale e opposta. Se alla somma totale dei guadagni dei partecipanti si sottrae la somma totale delle perdite, si ottiene zero. Invece, situazioni in cui i partecipanti possono guadagnare o perdere insieme sono indicate come giochi non a somma zero. Ad esempio, se un paese con un eccesso di banane commercia con un altro paese che ha un eccesso di mele, entrambi trovano beneficio nella transazione: si è quindi di fronte a un gioco non a somma zero.

Perché un SSG è quasi sempre non a somma zero?

I motivi ricadono sui seguenti fatti:

- Il costo della perdita per il difensore, come ad esempio vite umane, reputazione, danni, può essere molto più alto del guadagno dell'attaccante.
- Il fallimento dell'attaccante può non essere un grande vantaggio per il difensore.
- In scenari reali, le motivazioni degli attori sono asimmetriche (terroristi vs forze dell'ordine, hacker vs azienda, ecc.).

In un gioco non a somma zero, il difensore deve ottimizzare il proprio payoff, ma non può semplicemente annullare quello dell'avversario. Quindi la strategia ottima non è cercare di ridurre al minimo il payoff dell'attaccante, ma massimizzare il proprio, tenendo conto della risposta dell'attaccante. La soluzione del gioco resta un equilibrio di Stackelberg, ma la funzione obiettivo del difensore non coincide con il minimo del guadagno dell'attaccante e inoltre serve un modello di ottimizzazione più generale, spesso formulato come un problema bilevel oppure come un

Mixed-Integer Linear Program (MILP). Nello specifico, l'**ottimizzazione a due livelli** (**bilevel optimization**) è un tipo di problema di ottimizzazione gerarchica in cui esistono due problemi annidati. Il primo è il problema di livello superiore (upper-level problem), in cui un decisore principale ottimizza una funzione obiettivo, ma le sue decisioni dipendono dalla soluzione di un altro problema. Quest'ultimo consiste nel problema di livello inferiore (lower-level problem), ovvero un sotto-problema che deve essere risolto per determinare la soluzione ottimale del livello superiore.

Nel contesto di un Stackelberg Security Game, il problema di ottimizzazione bi-livello consiste nel leader, ovvero il difensore, che decide una strategia di protezione ottimale per minimizzare i danni, sapendo che l'attaccante osserverà questa scelta. Mentre, dall'altra parte, il follower, ovvero l'attaccante, osserva la strategia del difensore e sceglie il miglior attacco per massimizzare il proprio guadagno.

La soluzione di un SSG consiste in una condizione di equilibrio detta **Strong Stackelberg Equilibrium** (**SSE**), la quale è un concetto di equilibrio nei giochi Stackelberg, che sono giochi gerarchici in cui un giocatore (leader) sceglie la sua strategia per primo, e l'altro giocatore (follower) risponde ottimizzando la propria strategia dopo aver osservato la decisione del leader.

Il SSE assume che:

- Il leader sceglie la sua strategia per massimizzare il proprio payoff, assumendo che il follower reagirà in modo ottimale.
- Se il follower ha più strategie ottimali, sceglie quella che favorisce il leader (questo è ciò che lo rende "strong"). Questo avviene per indurre una conclusione al gioco, evitando loop nella ricerca di una condizione di equilibrio.

Categorie di SSG

Con i progressi nella ricerca sui security games e l'ampliamento delle applicazioni, è utile considerare la categorizzazione di questo lavoro in tre aree distinte a seconda dell'ambito di applicazione. Di seguito si illustrano le categorie individuabili in letteratura, facendo riferimento a [2].

1. Giochi di Sicurezza per le Infrastrutture (**Infrastructure Security Games**): questi giochi sono focalizzati sulla protezione delle infrastrutture critiche, come porti, aeroporti, treni e voli, spesso con

l'obiettivo di assistere le agenzie impegnate nell'antiterrorismo. Le infrastrutture protette sono generalmente statiche e i bersagli hanno una struttura discreta, come i terminal di un aeroporto o i singoli voli.

Sono considerati giochi a "colpo singolo" (single-shot games). La strategia mista del difensore può essere utilizzata per mesi, ma un singolo attacco da parte di un avversario conclude il gioco. Si assume che gli avversari siano altamente strategici, pianifichino attentamente gli attacchi con sorveglianza e che tali attacchi abbiano gravi conseguenze.

Tradizionalmente, il difensore non aggiorna ripetutamente le proprie strategie, e l'apprendimento automatico non è stato utilizzato, dato che gli attacchi tendono ad essere rari.

Un esempio significativo è ARMOR (Assistant for Randomized Monitoring over Routes), schierato all'Aeroporto Internazionale di Los Angeles (LAX) dal 2007 per randomizzare i posti di blocco sulle strade di accesso e i percorsi delle pattuglie canine all'interno dei terminal.

2. Giochi di Sicurezza Ambientale (**Green Security Games**): questi giochi si concentrano sulla protezione dell'ambiente, inclusi foreste, pesce e fauna selvatica, contro bracconieri, pescatori illegali o coloro che tagliano alberi illegalmente. A differenza dei giochi per le infrastrutture, gli animali o il pesce da proteggere possono spostarsi nello spazio geografico, e i bersagli sono distribuiti su vaste aree aperte.

   Non sono giochi a "colpo singolo", quindi l'avversario conduce spesso molteplici "attacchi" ripetuti, come il bracconaggio, e una singola attività illegale non pone fine al gioco. Il difensore pianifica nuovamente le sue attività di sicurezza dopo aver ricevuto rapporti sulle attività illegali, rendendoli giochi di sicurezza ripetuti. Possono esserci anche più avversari attivi.

   Gli avversari sono impegnati in attività illegali ripetute, e le conseguenze del fallimento o del successo non sono così gravi come nell'antiterrorismo. Di conseguenza, mostrano razionalità e sorveglianza più limitate. Tuttavia, non agiscono in modo completamente opportunistico a causa dei pericoli (ad es. nelle foreste profonde).

   Dato che è un ambiente di gioco ripetuto, il difensore aggiorna ripetutamente le proprie strategie, e l'apprendimento automatico

può essere utilizzato, sfruttando la disponibilità di grandi quantità di dati sugli attacchi.

Un esempio è PAWS (Protection Assistant for Wildlife Security), che mira ad assistere le agenzie di conservazione nella creazione di pattuglie ottimizzate per prevedere dove i bracconieri attaccheranno e per coprire quelle aree al fine di proteggere la fauna selvatica. Si menziona anche la protezione delle risorse ittiche sostenibili con la Guardia Costiera degli Stati Uniti.

3. Giochi di Sicurezza per la Criminalità Opportunistica (**Opportunistic Crime Security Games**): questi giochi sono mirati a contrastare la criminalità opportunistica, come i furti di cellulari nelle metropolitane o i furti di laptop nelle biblioteche universitarie. L'attenzione si concentra sulla protezione della proprietà pubblica in aree geografiche specifiche e limitate.

   Anche se non sono esplicitamente formulati come giochi ripetuti, l'avversario può tentare o condurre molteplici "attacchi" (furti) in un singolo round del gioco. Nonostante il difensore si impegni in una strategia mista, un singolo attacco non conclude il gioco, e più aggressori possono essere attivi contemporaneamente.

   Come nei giochi di sicurezza ambientale, le conseguenze non sono così severe come nell'antiterrorismo, e gli avversari possono agire in modo meno strategico, mostrando maggiore razionalità e sorveglianza limitate. Sono più flessibili nell'esecuzione dei loro piani, cogliendo le opportunità.

   I dati disponibili sulla criminalità possono essere utilizzati per aiutare il difensore a pianificare e adattare la strategia di difesa, e le tecniche di machine learning sono particolarmente applicabili in questi scenari.

   Il modello OCSG (Opportunistic Crime Security Game) è stato convalidato tramite prove sul sistema Los Angeles Metro, con buoni risultati nel contrastare reati come lo scippo di telefoni. Il sistema TRUSTS (Tactical Randomization for Urban Security in Transit Systems) si concentra anche sul contrasto all'evasione tariffaria e alla soppressione della criminalità urbana nel sistema della metropolitana di Los Angeles

Applicazioni degli SSGs

Gli Stackleberg Security Games costituiscono un modello della teoria dei giochi scalabile e con la possibilità di essere impiegato in molteplici occasioni.

Come è osservabile in [6], una possibile applicazione degli SSG risiede nella strutturazione di strategie di pattugliamento ad opera di aeromobili a pilotaggio remoto (unmanned aerial vehicles, UAVs), per la difesa di target esposti. In tale caso di studio vengono tenute in considerazione anche la limitata autonomia dei droni e la capacità dell'attaccante di apprendere e adattare le proprie strategie. Le attuali strategie di pattugliamento, come quelle fisse o completamente casuali, risultano insufficienti: le prime perdono efficacia di fronte a un attaccante che apprende, mentre le seconde non garantiscono protezione sufficiente ai target strategicamente importanti.

Per ovviare a tali problematiche, è possibile proporre un modello di SSG composto da due distinti gruppi di droni, uno per ogni agente all'interno del gioco. Il primo rappresenta i droni a disposizione del difensore per la protezione di un insieme di target fissi, applicando strategie di pattugliamento ottimizzate. Il secondo gruppo, invece, è costituito dagli UAVs suicidi dell'attaccante che sorpassano in numero il primo gruppo e hanno come obiettivo quello di infliggere danni ai target. Per quanto riguarda i payoff, se un drone difensore pattuglia un target durante un attacco, l'attacco è considerato fallito e il difensore guadagna il valore del target. Viceversa, se la difesa fallisce, l'attaccante guadagna il valore del target.

In tale situazione si ottiene un modello di SSG in cui: l'attaccante osserva la strategia del difensore e la considera costante, la massimizzazione del payoff dell'attaccante non dipende più dalla strategia del difensore, l'attaccante sceglie una strategia pura. Inoltre, il difensore affronta un problema di ottimizzazione a due livelli:

- Problema di livello superiore: ottimizzazione del payoff del difensore.
- Problema di livello inferiore: ottimizzazione del payoff dell'attaccante.

Sperimentalmente è stato provato che la strategia di pattugliamento derivata dal modello di Stackelberg offre un payoff significativamente più alto per il difensore (e un payoff inferiore per l'attaccante) rispetto

alla strategia di copertura media (dove i droni difensori pattugliano ogni target con uguale probabilità). Tale risultato vale sia che i valori dei target siano uguali o diseguali.

Inoltre, è stato osservato che una diminuzione del numero di droni difensori porta a un notevole aumento del payoff per l'attaccante, e la strategia proposta mantiene comunque la sua superiorità rispetto a un approccio casuale.

Un' ulteriore possibile applicazione degli SSGs, come descritto in [8], consiste nell'analisi e nella previsione di attacchi malevoli in una rete.

In base ai diversi obiettivi specifici della previsione della situazione di sicurezza della rete, la ricerca esistente può essere suddivisa in attack prediction e attack forewarning. La prima consiste nel prevedere il passo successivo nel momento in cui si verifica una minaccia, ovvero in seguito a un attacco già avvenuto. Il secondo, invece, consiste nel prevedere i possibili tipi di attacco sulla rete target, nonché i possibili eventi e le posizioni specifiche dei corrispondenti attacchi quando gli eventi di minaccia non si sono ancora verificati.

Il modello leader-follower degli SSG si adatta bene al processo di attacco/difesa di una rete, ed è interessante osservare come in questa analisi i ruoli di leader e follower all'interno del gioco siano invertiti rispetto alla consuetudine. Infatti, nel modello proposto è l'attaccante del sistema a svolgere il ruolo di leader, mentre il difensore della rete viene definito come follower.

Gli esperimenti sono stati condotti simulando un ambiente di rete specifico. Questa struttura è composta da una zona demilitarizzata (DMZ) e una rete locale (LAN), interconnesse tramite firewall e router. Lo scenario di attacco simulato prevedeva che un attaccante entrasse nell'area DMZ per ottenere la password del router, prendesse poi il controllo del router e, infine, scoprisse e sfruttasse vulnerabilità nella LAN per assumerne il controllo. Le strategie di attacco considerate erano basate su un elenco di vulnerabilità specifiche, con associati vari livelli di complessità e punteggio di minaccia. Le corrispondenti strategie di difesa consistevano nell'applicazione di patch. Inoltre, una matrice di payoff di attacco e difesa è stata costruita per rappresentare i benefici per entrambe le parti, considerando i guadagni in caso di successo della patch o l'impatto dell'attacco.

I risultati sperimentali hanno dimostrato che l'algoritmo basato sul SSG è capace di generare una strategia di attacco ottimale, evidenziando come la metodologia proposta possa fornire un riferimento concreto ed efficace per gli attacchi in un ambiente di rete. Conclusione Nel futuro l'obiettivo

consisterà nel migliorare ulteriormente il modello, per adattarlo meglio alle caratteristiche di cambiamento in tempo reale negli ambienti di rete.

Purché ci siano altri settori, oltre a quelli proposti precedentemente, in cui modelli di SSGs possono essere sviluppati per risolvere le più svariate problematiche, l'ambiente tra i più prolifici per l'applicazione degli Stackelberg Security Games è quello della cybersecurity. Infatti, sarà proprio in tale direzione che continuerà la trattazione della tesi.

In particolare, sono già stati ideati modelli di SSG finalizzati alla cloud security, come è osservabile nelle fonti [1] e [4].

Generalmente, i modelli di SSG utilizzati in cloud security hanno una tipica struttura leader-follower, in cui il cloud provider, o l'amministratore del cloud, svolge il ruolo di difensore e quindi di leader all'interno del gioco. Il compito dell'attaccante, invece, viene compiuto da un hacker, o, più in generale, da una qualsiasi minaccia per il cloud.

L'obiettivo dei cloud provider è applicare gli SSGs nell'individuazione e nella previsione delle minacce per il servizio e nella modellazione di una strategia contro di esse.

Il difensore intende individuare la funzione di payoff dell'attaccante, affinché, risolvendo il problema inverso, sia possibile prevedere i comportamenti futuri del suo avversario.

Poiché il cloud provider non è direttamente in grado di osservare la strategia degli attaccanti, è necessario strutturare il SSG in due stadi:

1. **Stadio Passivo**: dedicato alla raccolta di informazioni da parte del difensore sulla strategia dell'attaccante, a tale proposito il gioco viene ripetuto molteplici volte.

2. **Stadio Attivo**: il difensore è in grado di prevedere i comportamenti dell'attaccante grazie alla stima della funzione di payoff ricavata dallo stadio passivo.

Il gioco si basa sulla risoluzione di problemi di massimizzazione della funzione di payoff, sia per il difensore che per l'attaccante. La soluzione di uno SSG risiede nell'individuazione di un SSE.

Per ottenere modelli più realistici, in ambito cloud, si possono considerare anche attaccanti non completamente razionali. In tal caso possono essere introdotti altri due tipi di equilibrio:

- **Quantal Response Equilibrium** (**QRE**): concetto di equilibrio nei giochi strategici che generalizza il Nash Equilibrium, tenendo conto di scelte non perfettamente razionali da parte dei giocatori. Mentre

nel Nash Equilibrium si assume che i giocatori scelgano sempre l'azione con il miglior payoff deterministico, nel QRE i giocatori prendono decisioni in modo probabilistico, con una maggiore probabilità di scegliere azioni che danno payoff più alti, ma senza escludere del tutto le azioni peggiori. L'idea centrale è che i giocatori commettano errori nel prendere decisioni e che la probabilità di scegliere una certa strategia dipenda dal payoff associato. Questo errore è modellato matematicamente da una funzione chiamata quantal response function, che trasforma i payoff in probabilità di scelta. Il QRE è quindi un equilibrio in cui le strategie probabilistiche dei giocatori sono coerenti con la quantal response function, ovvero ogni giocatore sceglie strategie in modo stocastico, e le strategie di tutti sono in equilibrio tra loro.

- **QRE con Preferenze**: consiste in un'estensione dell'Equilibrio di Nash, che tiene conto della razionalità limitata dei giocatori. Invece di scegliere sempre la strategia ottimale, i giocatori rispondono in modo probabilistico in base ai payoff attesi. QRE con preferenze introduce il concetto di bias o pesi soggettivi sulle strategie, modellando scenari in cui i giocatori hanno preferenze individuali che influenzano le loro decisioni.

Quindi, il problema di ottimizzazione della funzione di payoff per il cloud provider diventa più complesso a causa della razionalità limitata dell'attaccante.

2.2 CYBERSECURITY RISK ASSESSMENT

Nel momento in cui si entra nell'ambito del CRA si può fare riferimento all'articolo [3]. Tale lavoro, nello specifico, tratta il processo di CRA in relazione alla serie di standard ISA/IEC 62443, che definiscono i requisiti e i processi per la progettazione, lo sviluppo e la manutenzione di sistemi di automazione e controllo industriale (IACS) elettronicamente sicuri.

2.3 ATTACK GRAPH

Per gli attack graph citare [7].

3

APPLICAZIONE DEGLI SSG NEL PROCESSO DI CRA

DA SCRIVERE

4

MODELLAZIONE DEL CASO DI STUDIO

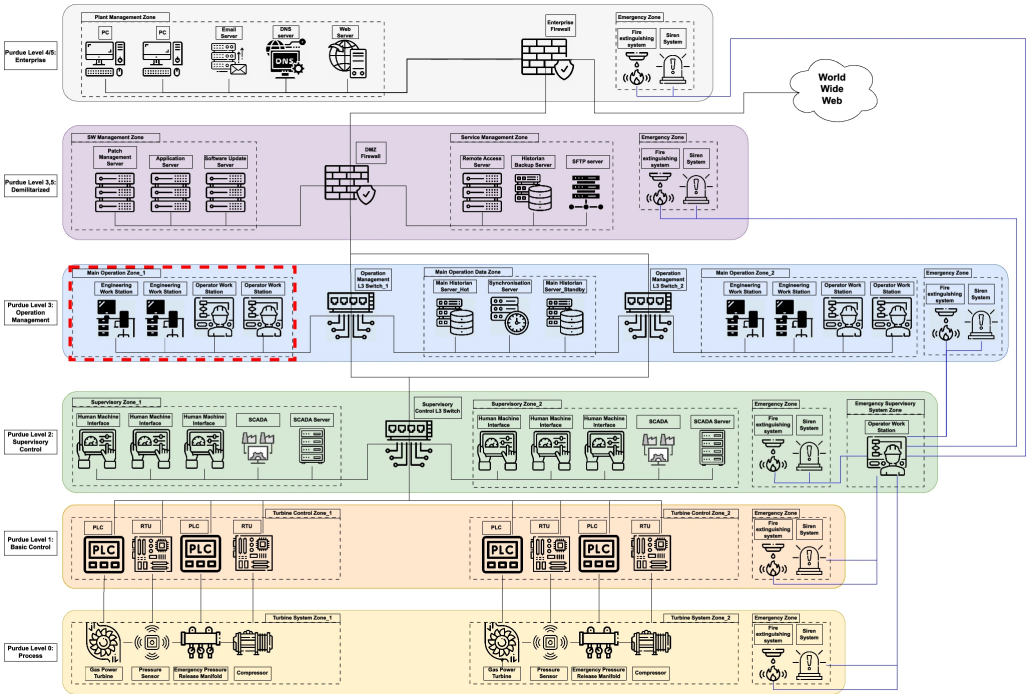

Figure 1: Schema SUC

SUC per esempio per creazione attack graph (Purdue level 3 e 3.5 del file Brancat et al)

- Patch Management Server (PMS): sistema che automatizza il processo di distribuzione degli aggiornamenti software (patch) ai dispositivi in una rete, inclusi server e workstation.
- Application Server (AS): server che fornisce l'infrastruttura e le funzionalità logiche di supporto, sviluppo ed esecuzione di applicazioni nonché altri componenti server in un contesto distribuito.

- Software Update Server (SUS): server centrale che distribuisce aggiornamenti software (patch, nuove versioni, fix di sicurezza) ai dispositivi di una rete, evitando che ogni dispositivo scarichi gli aggiornamenti direttamente da Internet.
- Remote Access Server (RAS): è un server che consente agli utenti di connettersi da remoto a una rete privata o aziendale tramite una connessione sicura, come una VPN, un desktop remoto o un protocollo di accesso remoto (es. RDP, SSH).
- SFTP Server (SFTPS): un server che utilizza il protocollo SFTP per il trasferimento sicuro di file su una rete.
- DMZ Firewall (F): separa la rete interna di un'organizzazione da una zona demilitarizzata (DMZ), che ospita servizi accessibili da Internet. Questo crea un ulteriore livello di sicurezza, impedendo che eventuali compromissioni nella DMZ si propaghino alla rete interna.
- Synchronization Server (SS): è un sistema o componente di rete che ha il compito di mantenere dati o stati coerenti tra più dispositivi, server o applicazioni. In altre parole, assicura che le informazioni siano uguali e aggiornate su tutti i nodi coinvolti.
- Main Historian Server (MHS): è un tipo speciale di server utilizzato per raccogliere, archiviare, gestire e analizzare dati di processo nel tempo (dati storici), tipicamente in contesti industriali, di automazione o impianti SCADA (Supervisory Control and Data Acquisition).
- Operation Management L3 Switch (S3):
- Operator Workstation (OWS): è una postazione di lavoro (computer) usata dagli operatori di impianto per monitorare e controllare in tempo reale i processi industriali o di automazione
- Engineering Workstation (EWS): è un computer utilizzato in ambienti industriali o di automazione che serve per configurare, gestire e manutenere i sistemi di controllo.

Archi grafo $\rightarrow$ AFR (rappresentata in un intervallo da 0 a 1)
STRIDE model:

- Spoofing: Pretending to be something or someone other than yourself
- Tampering: Modifying something on disk, network, memory, or elsewhere
- Repudiation: Claiming that you didn't do something or were not responsible; can be honest or false (non considerata nell'esempio)
- Information disclosure: Someone obtaining information they are not authorized to access
- Denial of service: Exhausting resources needed to provide service
- Elevation of privilege: Allowing someone to do something they are not authorized to do

Analisi senza contromisure iniziale.

Si chiede all'owner quali contromisure del Fundamental Requirement sono già state implementate (guarda std 62443-3-3 annex B) per ogni minaccia STRIDE. (giustifica il perché delle probabilità assegnate) Non si esclude totalmente la minaccia, ma a seconda delle contromisure implementate si diminuisce la probabilità che quella minaccia avvenga.

Mappatura delle probabilità sugli archi da qualitativo a quantitativo (si considerano tutte le minacce del modello STRIDE, ad esclusione della Repudiation e, per ogni minaccia per la quale è già presente una contromisura, la probabilità si abbassa alla fascia inferiore):

- high (H): $[0.8, 1]$ (1 minaccia risolta)
- medium-high (MH): $[0.6, 0.8)$ (2 minacce risolte)
- medium (M): $[0.4, 0.6)$ (3 minacce risolte)
- medium-low (ML):$[0.2, 0.4)$ (4 minacce risolte)
- low: $[0, 0.2)$ (5 minacce risolte)

Archi e probabilità associate (accanto ad ogni arco viene messa la lettera della minaccia per la quale, nel nodo iniziale, sono state implementate le contromisure):

- EWS $\rightarrow$ OWS (S, E): 0.69
- OWS $\rightarrow$ EWS (D, T): 0.77

- EWS → S3 (S): 0.92
- OWS → S3 (S, T, I): 0.57
- S3 → MHS (T): 0.93
- S3 → SS (I, D): 0.71
- S3 → F (E): 0.89
- MHS → SS (T, D, E): 0.40
- SS → MHS (S, I): 0.74
- F → PMS (D): 0.90
- F → AS (T): 0.82
- F → SUS (T, I, D, E): 0.38
- F → SFTPS (E): 0.86
- F → RAS (T, D, E): 0.44
- PMS → AS (S, I, E): 0.46
- AS → PMS (S): 0.80
- AS → SUS (D, E): 0.72
- SUS → AS (S, T, I, D): 0.26
- SFTPS → RAS (T, I, D, E): 0.30
- RAS → SFTPS (S, T, I, E): 0.24

Ad ogni nodo viene inoltre associato un impatto (il valore sarà rilevante nel momento in cui il nodo diventerà l'obiettivo di un determinato attaccante; l'impatto assume un valore da 0 a 10, dove 10 indica un danno molto ampio in caso di raggiungimento):

- EWS: 2
- OWS: 1
- S3: 3
- MHS: 4

- SS: 4
- F: 5
- PMS: 9
- AS: 10
- SUS: 7
- SFTPS: 6
- RAS: 8

Dato che abbiamo l'impatto e l'AFR, non rimane che mappare tali valori per ottenere il rischio ("risk") associato a una determinata. Considerando un path dell'attack graph, poiché ad ogni nodo si associa un determinato impatto e ad ogni arco si associa l'AFR. Quindi si calcola il rischio, usando la tabella del paper [3], considerando l'impatto del nodo da cui esce l'arco e la probabilità associata all'arco stesso. Quindi si ottiene un rischio per ogni arco del path (il rischio in questo caso corrisponde a "il rischio legato ad ogni asset da cui l'attaccante passa per arrivare al suo obiettivo") e per determinare il rischio associato al raggiungimento del nodo finale del path stesso, si prende il maggiore dei rischi trovati.

5

CONCLUSIONI E SVILUPPI FUTURI

DA SCRIVERE

BIBLIOGRAPHY

[1] Abdelkarim Ait Temghart and Mbarek Marwan. Stackelberg security game for optimizing cybersecurity decisions in cloud computing. *Security and Communication Networks*, 2023:1–13, 12 2023.

[2] Bo An and Milind Tambe. *Stackelberg Security Games (SSG) Basics and Application Overview*, pages 485–507. 11 2017.

[3] Francesco Brancati, Diamantea Mongelli, Francesco Mariotti, and Paolo Lollini. A cybersecurity risk assessment methodology for industrial automation control systems. *International Journal of Information Security*, 24(2):76, Feb 2025.

[4] Agnieszka Jakóbik, Francesco Palmieri, and Joanna Kołodziej. Stackelberg games for modeling defense scenarios against cloud security threats. *Journal of Network and Computer Applications*, 110, 03 2018.

[5] Arunesh Sinha, Fei Fang, Bo An, Christopher Kiekintveld, and Milind Tambe. Stackelberg security games: Looking beyond a decade of success. In *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence, IJCAI-18*, pages 5494–5501. International Joint Conferences on Artificial Intelligence Organization, 7 2018.

[6] Hongliang Wang, Yuan Zuo, and Qiang Chang. Target protection using multiple unmanned aerial vehicles based on stackelberg security game. pages 169–174, 10 2023.

[7] Yunxiao Zhang and Pasquale Malacaria. Bayesian stackelberg games for cyber-security decision support. *Decision Support Systems*, 148:113599, 05 2021.

[8] Tianyang Zhou, Xiaoyue Ge, Yichao Zang, and Qingxian Wang. Prediction method of attack behavior based on stackelberg security game. pages 1649–1654, 12 2019.