# A HYBRID THREAT MODEL FOR SMART SYSTEM

**Descrizione** lavoro proposto:

- definizione di uno scenario smart home, che comprende diverse sorgenti di dati per il monitoraggio dei consumi e del presente all'interno delle abitazioni.
- alla luce delle interazioni e delle autorizzazioni tra sensori che forniscono i dati e utenti che li visualizzano, definizione di un threat model, volto a individuare eventuali vulnerabilità e attacchi al sistema a seguito di compromissione di uno o più dispositivi e/o delle identità degli utenti.
- **output previsto**: una threat analysis derivante dal threat model.

## TEORIA E CONCETTI SU THREAT MODEL E THREAT ANALYSIS

**THREAT MODEL** —> processo di sicurezza con il quale vengono **identificate, classificate e analizzate potenziali minacce**, valutando successivamente il rischio (ANALYSIS) fornendo le necessarie misure, permettendo di comprendere soprattutto:

- **Risorse** che il prodotto sta cercando di proteggere.
- **Minacce** e vulnerabilità introdotte dalle risorse.
- **Vulnerabilità** ovvero tutti i punti deboli che vengono sfruttati
- dettagli su come vengono mitigate tali minacce.

**DOMANDE** PIU RILEVANTI PER LA **MODELLAZIONE**:

1. **Dove sono più vulnerabile agli attacchi?**
2. **Quali sono le minacce più rilevanti?**
3. **Cosa devo fare per proteggermi da tali minacce?**

✅**SCOPO**: fornire una visione completa dello stato attuale delle minacce informatiche, **valutando il potenziale danno** in modo da fornire successivamente una contromisura.

La sicurezza è un elemento che deve essere considerato e gestito in maniera attiva, sin dalle prime fasi della progettazione di un prodotto e per tutto il suo ciclo di vita, adottando approccio:

- **proattivo** —> minacce previste durante la progettazione.
- **reattivo** —> permettono di affrontare problemi inizialmente non previsti.

MODELLO PIU UTILIZZATO: **STRIDE**, che suddivide le minacce in sei classi.

**APPROFONDIMENTO:** https://www.cybersecurity360.it/soluzioni-aziendali/threat-modeling-cose-e-quali-metodologie-usare-per-lidentificazione-delle-minacce/

**APPROFONDIMENTO 2**: https://rislab.it/threat-modeling-cose-e-come-aiuta-lethical-hacking/

**APPROFONDIMENTO 3**: https://en.wikipedia.org/wiki/Threat_model

**THREAT ANALYSIS** —> processo derivante dal threat model, consiste in una **strategia di analisi delle minacce** che mira a valutare:

- **protocolli**.
- **processi e procedure di sicurezza** di un'organizzazione per identificare:
  - **Minacce**.
  - **Vulnerabilità**.
  - **Raccolta info su un potenziale attacco** prima che si verifichi.

Sfruttando le varie minacce messe in scena contro la propria organizzazione, le squadre di sicurezza possono ottenere una migliore comprensione del livello di sofisticazione delle minacce e identificare le aree di sicurezza dell'organizzazione che potrebbero essere vulnerabili a tali minacce.

✅Le **strategie** adottate mediante Analisi delle minacce, possono **prevenire l'attacco stesso o ridurre i danni subiti da un attacco imprevisto**.

È importante **stare un passo avanti rispetto alle entità dannose**.

***QUALI SONO I BENENFICI?***

1. **Aggiornamento continui alla modellazione delle minacce (THREAT MODEL)** → costruire modelli di minaccia efficaci e aggiornati, poiché con ogni nuova tecnologia o servizio che viene introdotto sul mercato arriva un potenziale rischio per la sicurezza o una nuova superficie di attacco che i. criminali informatici stanno cercando di sfruttare.

2. **Riduce la superficie di attacco** → Quando le organizzazioni **investono in una solida strategia di analisi, beneficiano di una drastica riduzione della loro superficie di attacco**, perché appunto le organizzazioni di analisi delle minacce aggiornano in modo continuo il loro elenco di minacce identificate, rafforzando così il perimetro di sicurezza delle organizzazioni.

3. **Profilo di rischio aggiornato** → la **valutazione continua delle minacce e la loro classificazione** tramite un repository o un sistema di gestione interno si tradurrà in un **profilo di rischio aggiornato**, che migliora notevolmente la posizione di sicurezza di un'organizzazione.

***COME ESEGUIRE UN THREAT ANALYSIS?***

Può assumere **varie forme a seconda dei requisiti di sicurezza delineati da un'organizzazione**, ci sono pero quattro passaggi comuni per eseguire un'analisi delle minacce:

1. **DEFINIRE L'AMBITO DELLE VALUTAZIONI DELLE MINACCE** → iniziare con la **definizione dell'ambito, che pone le basi delineando gli obiettivi**:
   - Cosa deve essere coperto?
   - Cosa è necessario per seguire una valutazione di successo?

   Questa fase dovrebbe **fornire una chiara tabella di marcia per l'aspetto di un'analisi delle minacce e cosa è coinvolto in ogni fase**.

2. **CREA PROCESSI E PROCEDURE NECESSARI PER ESEGUIRE LA VALUTAZIONE DELLE MINACCE** → se l'ambito è stato delineato correttamente definendo gli obiettivi, in questa fase vengono **creati processi e procedure necessari per eseguire la valutazione delle minacce**.

3. **DEFINIRE UN SISTEMA DI CLASSIFICAZIONE PER LE MINACCE (RATING SYSTEM)** —> può **aiutare a comunicare la gravità delle minacce, dei rischi e delle vulnerabilità** a tutte le principali parti interessate in un formato accessibile e di facile comprensione. Inoltre, può **aiutare una organizzazione a classificare, segnalare e monitorare le minacce molto tempo dopo l'analisi**.

4. **ESECUZIONE DEL THREAT ANALYSIS** —> le organizzazioni possono sfruttare l'esperienza della squadra o del personale di sicurezza interno per **eseguire l'analisi delle minacce** o impiegare una terza parte.

**APPROFONDIMENTO:** https://www.vmware.com/topics/glossary/content/threat-analysis.html

## ANALISI DEL DOCUMENTO

✅**SCOPO:** Lo scopo principale del nostro lavoro è **progettare un approccio di modellazione delle minacce che tenga conto degli aspetti umani, informatici e fisici dei sistemi ibridi, delle loro interdipendenze** e che possa analizzare le loro debolezze e aiutare a ragionare sulla correzione.

### 1. INTRODUZIONE:

I sistemi intelligenti sono quelli che comprendono il mondo fisico e sulla base delle informazioni ricavate attuano delle decisioni in risposta.
Il documento analizzerà le minacce e possibili vulnerabilità dei sistemi smart **considerando però tre aspetti fondamentali**:

- **Fisico.**
- **Umano**.
- **Informatico (cyber)**.

Questo modello prende il nome di "**Ibrido**".

**Determinare le possibili minacce (threat) in questi smart system e trovare una soluzione di protezione efficace è più impegnativo** che in sistemi tradizionali (ad esempio pc) per molte ragioni come:

- bassa capacità computazionale.
- inadeguata qualità del software

Ma anche, cosa più importante, **il fatto che tali ambienti combinano aspetti umani, fisici e digitali** (cyber) alla progettazione e all'implementazione del sistema. In questi scenari, la **superficie di attacco è più ampia** e si estende oltre il dominio "cyber" fino agli aspetti fisici e umani del sistema.

**HYBRID SYSTEM** —> riferito ad un **sistema** che tiene conto di aspetti umani, fisici e informatici.

**HYBRID ATTACK** —> riferito ad un **multi-step attack** che comprende attacchi di genere fisico, umano e informatico in combinazione.

**SECURITY ANALYSIS** —> considera:
- il **contesto fisico** del sistema.
- **risorse digitali** e connessioni.
- gli **esseri umani** che lo usano e lo gestiscono.

**THREAT MODELS** —> rappresenta **scenari d'attacco che sfruttano le iterazioni tra i tre aspetti**.
- ex. Jackpot Attack ATM machine.

**L'output finale prodotto** e descritto dal documento sarà:
- **HYBRID THREAT MODEL** —> in grado di **rappresentare le relazioni e le proprietà di sicurezza dei componenti del sistema**.

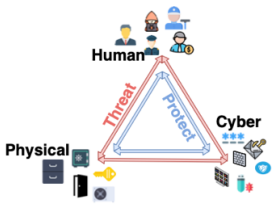
- **THREAT ANALYSIS METHOD** —> insieme di **regole di derivazione che permettono di comprendere le proprietà dei componenti del sistema e lo stato di sicurezza complessivo**.

- **TOOL (TEAMLESS)** —> che rappresenta le proprietà e le relazioni di sicurezza dei componenti del sistema. Questo strumento **analizza automaticamente le minacce al sistema e può generare automaticamente una rappresentazione grafica corrispondente**.

## 2. PROBLEM STATEMENT AND APPROACH:

✅**MAIN GOAL**: identificare e costruire un **threat model** (modello di possibili minacce), per **sistemi ibridi**, che combina i tre differenti aspetti.
Per fare ciò è **necessario una rappresentazione delle relazioni tra i differenti aspetti del sistema**.
- **FISICO**.
- **CYBER**.
- **UMANO**.

Una particolarità rilevante è anche quella di **capire come questi tre aspetti si influenzano** tra loro ovvero:
- Come un aspetto **introduce una minaccia/vulnerabilità** verso l'altro.
  - **Se viene compromesso un aspetto, può compromettere anche l'altro?**
- Come un aspetto può **proteggere da minacce o vulnerabilità** verso l'altro.
  - **Come possono proteggersi a vicenda?**
  - **Può un aspetto aiutare a proteggere un altro?**



## ESEMPI DI POSSIBILI MINACCE CONNESSE

- Avere un accesso a una stanza non protetta cui è possibile connettersi a una rete cablata, permette all'attaccante di compromettere i componenti software/network del sistema.
- Avere l'accesso fisico ad un sensore permette all'attaccante di disturbare cosa il sensore misura.

**In questi esempi, UNA VULNERABILITA' FISICA PERMETTE UN ATTACCO INFORMATICO AL SISTEMA IBRIDO**.

- Compromettere una serratura digitale o un sistema di controllo per permettere di aprire la porta di un'area protetta o di un edificio.

**In questo esempio, UNA VULNERABILITA' CYBER PERMETTE UN ATTACCO FISICO AL SISTEMA**.

- Ingannare l'utente per rubare i dettagli d'accesso o rubare le chiavi d'accesso.

**In questo esempio, UNA VULNERABILITA' UMANA PERMETTE UN ATTACCO INFORMATICO AL SISTEMA IBRIDO**

## ESEMPI DI POSSIBILI PROTEZIONI A VICENDA

- Un essere umano può ispezionare o monitorare la sicurezza fisica di un'area, edificio intelligente o di un dispositivo → **UMANO – FISICO – DIGITALE**.
- Un involucro fisicamente sicuro può proteggere componenti umani o digitali: PC o Server protetti in apposite aree → **FISICO – UMANO – DIGITALE**.
- I sistemi digitali vengono utilizzati per monitorare la sicurezza di spazi fisici e il comportamento delle persone per proteggerci da minacce interne → **DIGITALE – FISICO – UMANO**.

**DESCRIZIONE SCENARIO → ILLUSTRAZIONE ESEMPIO SU CUI VIENE UTILIZZATO L'APPROCIO.**

**CASO**: edificio intelligente che può essere **soggetto ad attacchi che combinano fasi** di:
- Attacco **FISICO**: rompere una porta, scassinare serratura.
- Attacco **INFORMATICO**: compromissione rete, serrature digitali.
- Attacco **UMANO**: rubare password o perdere chiave.

L'edificio **comprende**:
- **HALL** → con sistema di monitoraggio dove le immagini delle telecamere sono controllate da una persona per impedire accesso non autorizzato.
- **AREA UFFICI** → dotate di serrature nelle porte per impedire l'accesso non autorizzato.
- **TETTO**.

**È presente una stanza dove si trova la cassetta di sicurezza:**

- Protetta da misure di **sicurezza fisica** → accessibile solo attraverso una **porta chiusa a chiave** che per essere aperta, viene **utilizzata una chiave che si basa su RFID**, fornita solo ai dipendenti autorizzati.

⚠**NOTA BENE:** per accedere alla cassetta di sicurezza **l'attaccante deve sia entrare nella porta sia conoscere la password di sicurezza per aprire la cassaforte**.

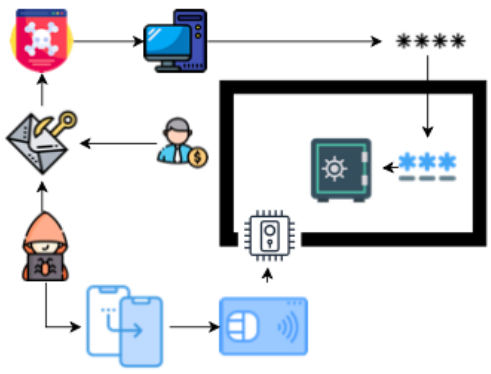
**Supponiamo** che:

- Attacco fisico alla cassaforte non sia possibile.
- La password d'accesso alla cassaforte è memorizzata nella macchina del dipendente d'ufficio.
- Le carte RFID per leggere la porta possono essere lette e clonate a una distanza moderata, dando la possibilità di creare una carta duplicata.

Quindi, per **accedere ai contenuti della cassaforte è necessario**:

- ✅Sfruttare **vulnerabilità umane** (phishing) per portare ad una **compromissione dell'ambiente digitale**.
- ✅La compromissione dell'ambiente digitale consente di **sfruttare ulteriori vulnerabilità digitali per accedere alla macchina del dipendente per ottenere la password**.
- ✅Sfruttare **ulteriori vulnerabilità digitale** per **compromettere sistemi di sicurezza** per poter accedere all'edificio
- ✅Sfruttare **vulnerabilità fisiche** per **entrare nell'edificio** passando dal tetto.
- ✅Sfruttare **vulnerabilità umane** per **compromettere l'ambiente fisico e digitale**.

**SCENARIO**



## TAMELESS (strumento automatizzato di implementazione del modello e analisi minacce)

**Def:** Modello delle analisi delle minacce in grado di ricavare lo stato di sicurezza corrente del sistema e dei suoi componenti, fornendo:

- Info di input sui componenti.
- Proprietà di sicurezza dei componenti.

**INPUT PROGRAMMA** → **specifica del sistema** da analizzare:

- **Componenti** e **minacce**.
- **Relazioni** tra componenti.
- **Relazioni** tra componenti e minacce.
- **Ipotesi** di sicurezza.

L'utente può **eseguire quindi l'analisi delle minacce interrogando TAMELESS** per visualizzare un insieme di proprietà di sicurezza predefinire dei componenti del sistema:

- **Come può cambiare lo stato di sicurezza dei componenti**.

✅**SCOPO**: **CONTROLLO DI CONSISTENZA** → determinare se gli **stati attesi dei componenti differiscono da quelli derivati**, aspetto **importante considerando le differenti caratteristiche** dei sistemi smart:

- In alcuni fondamentale che componenti non vengano compromessi.
- In altri fondamentali che componenti funzionino correttamente.

**OUTPUT PROGRAMMA**: dopo analisi **visualizza graficamente le possibili minacce e come sono state derivate**, **identificando le contromisure**, fornendo **un insieme di possibili entità che possono essere utilizzate per prevenire o mitigare la minaccia**.

### CARATTERISTICHE TAMELESS

1. Consente agli **utenti di avere una visione completa della sicurezza del sistema e dei suoi rischi** attraverso gli aspetti **umani**, **fisici**, **informatici**.

2. Fornisce una **rappresentazione grafica della propagazione dell'attacco**:
   a. Consente di **aggiungere nuovi componenti di protezione e monitoraggio**.
   b. Consente quindi di **ripetere le operazioni di analisi in modo continuo** fino a quando non è convinto che il modello sia accettabile.

3. **Può aiutare gli architetti di sicurezza a considerare gli aspetti economici** per garantire la sicurezza del sistema se la protezione è associata ad un costo.
   a. Consente di **confrontare i costi con i vari approcci**.

⚠️⚠️**ASPETTO FONDAMENTALE OMESSO NEGLI STUDI FINO A OGGI**: ci **concentriamo sulla rappresentazione delle relazioni tra le minacce agli aspetti fisici, informatici e umani del sistema e su come si combinano con le relazioni tra i componenti del sistema**.

**LAVORO IPOTETICO DA SVOLGERE SOTTOLINEANDO LIMITI:**

Le **tecniche per la gestione del rischio e le contromisure, in particolare**:

1. ❌**ANALISI STATICA**: quando il sistema cambia l'analisi deve essere eseguita di nuovo:
   a. ✅Estendere quindi TAMELESS **con condizioni monitorate che rilevano tali cambiamenti e attivano una rivalutazione dell'analisi.**

2. ❌**ANALISI DETERMINISTICA:** le relazioni e i fatti derivati sono veri o no generando un grafico di attacco logico**:**
   a. ✅Estendere il grafico di attacco con **informazioni probabilistiche per ragione su rischi e contromisure**.
      i. Esprimere **probabilità di successo di ciascuna vulnerabilità e utilizzare analisi baysiana per lavorare sul rischio**.
      ii. Ipotizzando una **certa distribuzione di attacchi è possibile condurre un'analisi del rischio ed esaminare contromisure per ridurre il rischio**.
      iii. Condurre **analisi basata su costi** per indentificare **contromisure più convenienti o per valutare efficacia in termini di costi di diverse strategie**.

3. ❌**NON VENGONO CONSIDERATI ASPETTI E VENTI TEMPORALI**:
   a. ✅Sarebbe possibile **estendere il modello al ragionamento su proprietà temporali e relazioni temporali** (utilizzando Event Calculus/Situation Calculus).

3. **HYBRID THREAT MODEL**:

Il Threat model comprende **differenti entità**: fisiche, umane e cyber.
**ENTITA'** → sistema o componente del sistema di differente natura, rappresentato con **E** l'insieme di tutte le entità.

**THREAT** → una o più sequenze di azioni che cambiano direttamente o indirettamente le proprietà che possono alterare lo stato delle entità, rappresentate con **T**, l'insieme delle minacce.

**PROPRIETA DELLE ENTITA'**
assunte come vere o derivate come vere applicando le regole:

- **Basic Proprieties** → descrivono la **conoscenza primaria della sicurezza** sui componenti.
  - **Compromessa:** L'entità A è stata compromessa da una minaccia T.
  - **Malfunzionamento:** L'entità A non funziona correttamente o come previsto.
  - **Vulnerabile:** A ha una vulnerabilità nota che lo rende vulnerabile alla minaccia T.
- **Auxiliary Proprieties** → descrivono **gli stati dell'entità**, quando è compromessa o non funziona a causa di una minaccia.
  - **Detected:** descrive che è stato rilevato che A è stata compromessa da una minaccia T.
  - **Restored:** descrive che controllo su A è stato ripristinato dopo una minaccia.
  - **Fixed:** descrive che la funzionalità di A viene riparata dopo un malfunzionamento.

- **Assumed Proprieties** → fanno parte delle **ipotesi di sicurezza**:
  - Denotano conoscenza iniziale
  - Esplicitamente dichiarate

- **Derived Proprieties** → si ottengono **applicando le regole di derivazione** alla proprietà note
  - Indicano proprietà di sicurezza che possono diventare vere quando un utente malintenzionato sfrutta le vulnerabilità.

## RELAZIONI DELLE ENTITA'

Le entità del sistema hanno **differenti relazioni con altre entità o con le minacce**.

**RELAZIONI TRA ENTITA'** → rappresentate dall'insieme **R**, si basano su una **relazione binaria**.

- **Contain** → A contiene B e rappresenta come il sistema è composto.
  - Stanza A contiene Server B.

- **Control** → A controlla B.
  - Controller A controlla sensore B.

- **Connect** →A connette B a C.
  - La rete A connette Server B con Server C

- **Depend** → A dipende da B, A funziona solo se B funziona, viene usata per identificare la diffusione delle vulnerabilità o misure di protezione.
  - L'aria condizionata dipende dalle ventole.

- **Check** → A controlla che B stia funzionando normalmente e quindi rileva i malfunzionamenti.

- **Replicate** → A è una replica di B, rende possibile riparare un'entità.

**RELAZIONI TRA ENTITA' E MINACCE** → permettono di **rappresentare quale entità è vulnerabile da una particolare minaccia** o **come le entità si possono proteggere a vicenda**, si basano su una **relazione ternaria**.

- **Protect** → A protegge B dalla minaccia T.
  - Un lucchetto protegge una cassaforte da un determinato accesso.

- **Monitor** → A monitora B per un eventuale minaccia T, gli attacchi possono essere rilevati ma non prevenuti.
  - Una telecamera monitora la sala contro un ladro.

- **Spread** → A può propagare la minaccia T ad altre entità.
  - Phishing e-mail usata per propagare il malware.

- **Potentially Vulnerable** → A può essere potenzialmente vulnerabile ad una minaccia T, magari a causa di un malfunzionamento.
  - Un utente è vulnerabile a phishing.

## PROPRIETA' DI ALTO LIVELLO

- Permettono all'utente di **capire più facilmente lo stato di sicurezza del sistema**.
- Permettono di **rappresentare lo stato complessivo di un'entità** inclusi i suoi componenti, dipendenze e connessioni.

- **Valid** → A è valida quando **non è stata compromessa** e **non ha avuto malfunzionamenti**.

- **Defended** → A difesa da una minaccia T quando **entità B esistente protegge A ed è valida**.

- **Safe** → A è sicura da una minaccia T, quando **non è vulnerabile a una minaccia T o può essere difeso**.

- **Monitored** → A è monitorata da una minaccia T quando un'entità **B monitora A ed è valida**.

- **Checked** → A è controllata quando **un'entità B verifica che la funzionalità di A e B sia valida**.

- **Replicated** → A replicato quando **esiste un'entità B che replica A ed è valida**.

## 4. THREAT ANALYSIS:

Vengono introdotte le **regole di derivazione** utilizzate per l'analisi delle minacce:

- Vengono **applicate alla proprietà precedenti** e possono essere **utilizzate per proteggere il sistema**.
- Vengono derivate quali entità possono essere vulnerabili, compromesse o non funzionare correttamente.
- Aiutano a costruire il **GRAFICO DI ATTACCO** → rappresenta graficamente i risultati dell'analisi delle minacce e i percorsi di attacco attraverso il sistema.

### REGOLE DI DERIVAZIONE

Vengono introdotte due tipi di regole di derivazione:

- **BASIC DERIVATION RULES** → affermano che **se una proprietà è vera, allora naturalmente può essere derivata come vera**.

- **SPECIFIC DERIVATION RULES** → per **determinare quando un'entità è compromessa, malfunzionante, vulnerabile, ripristinata o riparata**.
    - **Compromissione**: per ragionare su **come le minacce possono compromettere** diverse attività e propagarsi nel sistema. (guarda regole su pdf).

⚠ **Esempio**: Il dipendente controlla il pc dove è memorizzata la password per aprire la cassaforte, esso può accedere alla mail su un server che connette il dipendente alla mail. Il dipendente è **vulnerabile** a phishing, e il pc a malware, la password a essere rubata.
**Non ci sono misure protettive** a queste vulnerabilità.

L'attacco phishing può essere **diffuso** via mail, il dipendente può diffondere accidentalmente il codice malware e le info in esso memorizzate.

Con le **proprietà di alto livello**:
- Dipendente, pc, password **non protetti e non sicuri**.
- Il Server **non è protetto**.

Con le **regole di derivazione** deduciamo che:
- ❌L'impiegato può essere **compromesso** con attacco phishing.
- ❌Il pc dell'impiegato può essere **compromesso**.
- ❌La password può essere **compromessa**.

    - **Malfunzionamento:** (guarda regole su pdf).

⚠️**Esempio**: Un server fisico hosta un sito web. La funzionalità del sito web dipende pesantemente dal suo server:

Con le **regole di derivazione** deduciamo che:
- ❌Se il server viene compromesso da una minaccia, causa un **malfunzionamento**.
- ❌Il sito web a sua volta ha un **malfunzionamento**.

    - **Vulnerabile:** un malfunzionamento può causare una vulnerabilità sfruttata da una minaccia T.

⚠️**Esempio**:
- ❌Un lucchetto rotto può essere **vulnerabile** all'apertura da parte di un utente malintenzionato.

    - **Rilevamento di una minaccia:** minaccia T può essere rilevata da un'entità che monitora A e non è compromessa.

⚠️**Esempio**:
- ✅Un sistema monitora intrusione, questa può essere **rilevata**.

    - **Servizi di riprisitino:** quando la minaccia T può essere rilevata da A e A è duplicata, allora A può essere ripristinata.

⚠️**Esempio**:
- ✅**Riprisitino** di un backup.

    - **Servizi di riparazione:** quando A funziona male e il suo funzionamento può essere rilevato allora A può essere riparato.

⚠️**Esempio**:
- ✅**Riparazione** dell'aria condizionata se non funziona e se viene rilevato

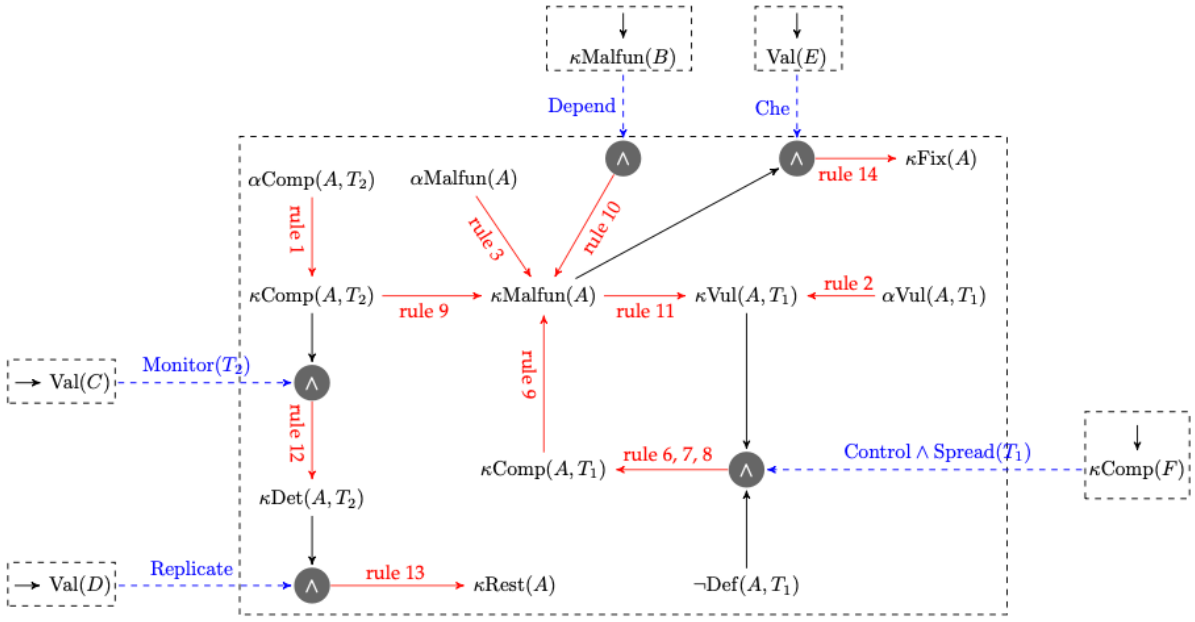
Le **regole sopra introdotte vengono automaticamente utilizzate per derivare nuove proprietà di sicurezza per le entità del sistema**. Date quindi le proprietà iniziali, l'analisi delle minacce rileverà nuove proprietà di sicurezza che verranno utilizzate per analizzare il modello di analisi delle minacce.

- Se meccanismi di sicurezza ASSUNTI **NON VULNERABILI**, TAMELESS identifica **POSSIBILI ATTACCHI**.
- Se meccanismi di sicurezza ASSUNTI **VULNERABILI**, TAMELESS identifica **ATTACCHI CHE POSSONO ESSERE ESEGUITI.**

## GRAFO DEGLI ATTACCHI

Le **regole di derivazione ci permettono di costruire un grafo di attacco** come, ad esempio, quello della compromissione di un server web o al malfunzionamento di una porta.

- Offre una **rappresentazione** grafica e semplice **dell'analisi delle minacce**.
- **Strumento potente per la valutazione della sicurezza** analizzando vulnerabilità della rete e i percorsi che possono utilizzare per compromettere sistema.
- **Con info probabilistiche**, si possono ricavare **misure di rischio** ovvero la **probabilità che le parti del sistema possono essere compromesse.**
- **Le probabilità di compromissione possono essere utilizzate per scegliere contromisure**.



## 5. CASE STUDY EVALUATION:

Applichiamo quindi la nostra analisi a **due casi d'uso**.

**TAMELESS**:

- **Analizza automaticamente** le informazioni fornite.
- Fornisce all'utente le **proprietà di sicurezza** derivate.
- Fornisce una **rappresentazione grafica** delle proprietà derivate e delle relazioni.

**CASO 1: ACCESSO NON AUTORIZZATO ALLA CASSAFORTE** (Scenario della sezione 2)

Mostreremo **come l'aggressore può accedere alla cassetta di sicurezza**, compresi i **passaggi dell'attacco riuscito**, nel dettaglio:

- **Cambiamento delle proprietà di sicurezza** delle varie entità.

Ricordiamo come è formato il **sistema**:

- Contenuto della cassetta protetto attraverso una combinazione che richiede una **password**.
- Cassetta si trova in una stanza a cui si accede attraverso una porta, apribile solo con **tessera RFID**.

Quindi:

- ❌**Password** può essere **compromessa** in quanto rubata tramite **attacco phishing**.
- ❌La **serratura** della porta può essere **compromessa**: siccome la porta non è protetta da una persona fisica, la tessera **RFID può essere duplicata** ed utilizzata da un utente non autorizzato.

$$\begin{array}{ll} \mathrm{Control}(\mathrm{key}, \mathrm{lock}), & \alpha\mathrm{Vul}(\mathrm{lock}, \mathrm{unAuthUser}), \\ \neg\mathrm{Def}(\mathrm{lock}, \mathrm{unAuthUser}), & \nexists P.\ \mathrm{Protect}(P, \mathrm{lock}, \mathrm{unAuthUser}), \\ \neg\mathrm{Safe}(\mathrm{lock}, \mathrm{unAuthUser}) & \end{array}$$

- ❌La **tessera RFID** può essere **duplicata** e non ci sono prevenzioni a questo; quindi, **non è sicura** se la carta viene compromessa, può **diffondere** la minaccia di un **accesso non autorizzato**.

$$\begin{array}{ll} \mathrm{Vul}(\mathrm{key}, \mathrm{copy}), & \neg\mathrm{Def}(\mathrm{key}, \mathrm{copy}), \\ \neg\mathrm{Safe}(\mathrm{key}, \mathrm{copy}), & \mathrm{Spread}(\mathrm{key}, \mathrm{unAuthUser}) \end{array}$$

- ❌Le info della carta collega l'aggressore alla scheda RFID, possiamo quindi considerare **compromesse** le **info sulla carta**.
- ❌La **scheda RFID**, quindi, **non è sicura** per un **attacco di copia**.
- ❌L'aggressore può **diffondere** l'attacco di copia.

$$\begin{array}{l} \mathrm{Connect}(CardInfo, \mathrm{Att}, \mathrm{key}) \wedge \kappa\mathrm{Comp}(\mathrm{Att}) \wedge \\ \mathrm{Spread}(\mathrm{Att}, \mathrm{copy}) \wedge \neg\mathrm{Safe}(\mathrm{key}, \mathrm{copy}) \wedge \\ \kappa\mathrm{Comp}(CardInfo) \rightarrow \kappa\mathrm{Comp}(\mathrm{key}, \mathrm{copy}) \end{array}$$

- ❌Con la **regola 6 di derivazione**, anche la **serratura della porta** può essere **compromessa** siccome la carta non è sicura e può diffondere la minaccia.

$$\begin{aligned}&\mathrm{Control}(\mathrm{key},\mathrm{lock}) \wedge \kappa\mathrm{Comp}(\mathrm{key},\mathrm{copy}) \wedge \\ &\mathrm{Spread}(\mathrm{key},\mathrm{unAuthUser}) \wedge \neg\mathrm{Safe}(\mathrm{lock},\mathrm{unAuthUser}) \\ &\rightarrow \kappa\mathrm{Comp}(\mathrm{lock},\mathrm{unAuthUser})\end{aligned}$$

- ❌Se la **serratura** è compromessa, questa **non è valida**.
- ❌La **stanza** protetta dalla serratura **non è difesa** da **accessi non autorizzati**.

$$\begin{aligned}&\mathrm{Protect}(\mathrm{lock},\mathrm{room},\mathrm{unAuthAccess}), \quad \neg\mathrm{Val}(\mathrm{lock}), \\ &\neg\mathrm{Def}(\mathrm{room},\mathrm{unAuthAccess})\end{aligned}$$

- ❌La password può essere compromessa in quanto può essere rubata **tramite phishing**; quindi, seguendo le proprietà di alto livello: la **password** **non è valida** e quindi **compromessa**.

$$(\neg\mathrm{Val}(\mathrm{Pw}) = \mathrm{Comp}(\mathrm{Pw})).$$

- ❌Si deduce quindi che se la password proteggeva la cassaforte da accessi non autorizzati ma non è più valida, anche la **cassaforte** **non è difendibile**.

$$\begin{aligned}&\neg\mathrm{Def}(\mathrm{sbox},\mathrm{unAuthAccess}) = \\ &\mathrm{Protect}(\mathrm{Pw},\mathrm{sbox},\mathrm{unAuthAccess}) \wedge \neg\mathrm{Val}(\mathrm{Pw})\end{aligned}$$

- ❌Quindi la **cassaforte** **non è sicura**, **vulnerabile** ad un attacco da parte di una **persona non autorizzata**.

$$\begin{aligned}&\neg\mathrm{Safe}(\mathrm{sbox},\mathrm{unAuthAccess}) = \\ &\mathrm{Vul}(\mathrm{sbox},\mathrm{unAuthAccess}) \wedge \neg\mathrm{Def}(\mathrm{sbox},\mathrm{unAuthAccess})\end{aligned}$$

Quindi:

- **La stanza collega l'aggressore alla cassaforte**.
- L'aggressore può **diffondere l'accesso non autorizzato**.
- **La cassetta non è sicura** per un accesso non autorizzato.
- La **stanza non è difendibile**.
- **La cassetta di sicurezza può essere compromessa attraverso un accesso autorizzato**, in quanto **l'aggressore può accedere fisicamente alla stanza** compromettendo le misure di sicurezza.

$$\begin{aligned}&\mathrm{Connect}(\mathrm{room},\mathrm{Att},\mathrm{sbox}) \wedge \kappa\mathrm{Comp}(\mathrm{Att}) \wedge \\ &\mathrm{Spread}(\mathrm{Att},\mathrm{unAuthAccess}) \wedge \neg\mathrm{Safe}(\mathrm{sbox},\mathrm{unAuthAccess}) \wedge \\ &\neg\mathrm{Def}(\mathrm{room},\mathrm{unAuthAccess}) \rightarrow \kappa\mathrm{Comp}(\mathrm{sbox},\mathrm{unAuthAccess})\end{aligned}$$

**SISTEMA IBRIDO** PERCHE:

- L'aggressore deve sfruttare vulnerabilità **UMANA** del sistema (phishing).
- L'aggressore deve sfruttare la vulnerabilità **INFORMATICA** del sistema (pc).
- L'aggressore deve sfruttare la vulnerabilità **FISICA** del sistema. (scheda RFID).

Grazie all' **ANALISI DELLE MINACCE**, si può capire:

- ✅**Quale parte del sistema può essere compromessa**, sfruttando le differenti vulnerabilità.
- ✅Il **posto migliore dove mettere in atto un nuovo meccanismo di sicurezza** per interrompere la propagazione dell'attacco, come ad esempio:
  - Installazione sistema antiphising.
  - Serratura cui tessere non possono essere copiate.
  - Aggiunta di una guardia nella stanza e telecamere.
- ✅Può considerare **ogni soluzione** sugli aspetti:
  - D'efficacia.
  - Logistica.
  - Economici.
  - Etici.

⚠️Per **altri esempi** guarda pagina 10-11 PDF (**WEB SERVER-WIND FARM**)

## 6. RELATED WORK:

Negli ultimi anni **l'analisi delle minacce per i sistemi cyber-fisici** sta diventando un **argomento popolare** nella sicurezza informatica.

Gli autori hanno presentato **diversi modelli di minaccia** **ma nessuno modella i tre aspetti**: fisici, umani e informatici.

Inoltre diversi autori hanno **sviluppato analisi che si concentrano sull'iterazione tra spazi fisici e cyber** ma con **obiettivi diversi**: **mirano ad identificare potenziali violazione dei requisiti di sicurezza**, a differenza del nostro **obiettivo**: **identificare gli elementi non attendibili del nostro sistema**.

**MulVal** → utilizzato per la generazione del grafo.

## 7. CONCLUSIONI:

- **MODELLO** E **ANALISI** implementato in uno strumento basato su **PROLOG** (linguaggio logico).
- Il modello è stato implementato sugli esempi precedentemente descritti.
- Vengono identificati **minacce** e **vulnerabilità** del sistema, e può essere utilizzato per adottare **contromisure efficaci**.

**DIREZIONE INTERESSANTE PER LAVORO FUTURO**:

- **Estrazione automatica delle relazioni e delle proprietà** di sicurezza dei componenti.
- Integrazione con **database di vulnerabilità esistenti** (CVE) per automatizzare ulteriormente la creazione del modello.
- Cosi facendo è **possibile ragionare sulla gestione del rischio** sia **staticamente** che **in fase di progettazione** che **durante un attacco**.
- **Arricchire l'espressività e le capacità di ragionamento** del nostro modello **aggiungendo vincoli temporali e ipotesi probabilistiche** sulle relazioni e regole, per modellare sistemi più complessi.
    - **In modo da essere esteso a sistemi dinamici in cui nuovi componenti possono entrare o uscire dal sistema.**