UNIVERSITÀ DEGLI STUDI DELL'INSUBRIA

DIPARTIMENTO DI SCIENZE TEORICHE E APPLICATE

CORSO DI STUDIO TRIENNALE IN
INFORMATICA

"Analisi dei modelli di minaccia per sistemi ibridi IoT in scenari smart home"

Relatore:
Prof.ssa Sabrina Sicari

Correlatore:
Dr. Fulvio Valenza

Riassunto Tesi di Laurea di:
Gabriele Sassi
Matricola 745081

Anno accademico:
2022/2023

L'avanzamento delle nuove tecnologie ha portato ad un'enorme diffusione dei dispositivi *smart*, i quali sono diventati più accessibili e convenienti per l'utilizzo quotidiano, in qualsiasi contesto e momento. L'IoT (*"Internet of Things"*), punto di congiunzione tra il mondo fisico e digitale si è affermato come concetto chiave alla base dei sistemi smart. Attualmente non si è ancora riusciti a dare una definizione concreta di IoT, ma generalmente si tratta di una rete in rapida crescita di dispositivi connessi a Internet e in grado di agire nell'ambiente circostante su base collaborativa, acquisire dati e comunicare tra loro per raggiungere un obiettivo comune. Questi dispositivi possono essere utilizzati in una varietà di scenari di diverso dominio applicativo. L'aumento di questi dispositivi connessi in rete ha conseguito un incremento significativo delle **minacce** alla sicurezza e delle **vulnerabilità** dei dati personali. Questo è principalmente attribuibile alle limitate risorse energetiche, alla complessità dei dispositivi IoT, alla natura delle componenti e all'eterogeneità dei dati raccolti e degli standard di comunicazione utilizzati. Inoltre, va evidenziato che il fattore umano costituisce un altro aspetto di rilievo nell'ambito della sicurezza all'interno dei sistemi IoT. Diventa fondamentale quindi assicurare integrità e confidenzialità dei dati trasmessi tra le varie componenti, autenticare ed autorizzare solo ed esclusivamente le entità coinvolte e proteggere in maniera continuativa il sistema da eventuali danni. La sicurezza rappresenta quindi un elemento indispensabile 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 approcci proattivi e reattivi. L'analisi di sicurezza rappresenta quindi un concetto di fondamentale importanza, valutando sistematicamente i rischi associati e l'impatto di determinate o inattese minacce. Queste rappresentano l'obiettivo dell'attaccante, e può essere definita come una qualsiasi situazione potenzialmente in grado di danneggiare un sistema. L'identificazione delle minacce è uno degli *step* fondamentali dell'approccio strutturato alla valutazione della sicurezza, ma spesso è necessario interrogarsi anche sulle relazioni dirette e indirette che intercorrono tra le componenti coinvolte, al fine di individuare percorsi d'attacco che non emergerebbero altrimenti.

Il ***"threat modeling"*** rappresenta una possibile soluzione alle problematiche precedentemente elencate. Si tratta di un processo strutturato, comunemente suddiviso in quattro fasi, che studia le potenziali minacce che possono compromettere gli *assets* di un sistema, identificando le fonti, le cause e le conseguenze previste. Le principali informazioni ottenute da un processo di threat modeling includono:

- **Risorse:** identificazione delle risorse critiche che il sistema cerca di proteggere.
- **Minacce:** introdotte dalle risorse.
- **Vulnerabilità:** individuazione dei punti deboli all'interno del sistema che potrebbero essere sfruttate dagli attaccanti per perpetrare le minacce.

La ***"threat analysis"*** è un concetto cooperante al threat modeling, ma si differenzia in quanto rappresenta un processo più ampio e continuo. Nel dettaglio si concentra sull'identificazione e l'analisi continua dei rischi specifici associati al sistema. L'obiettivo principale è fonire un insieme di informazioni mirate circa lo stato di sicurezza del sistema che possono essere constantemente consultate e valutate. In tal modo, "imparando" dai risultati ottenuti, si può procedere adottando decisioni e strategie utili a proteggere le componenti, i dati e le operazioni del sistema da minacce future.

Lo scopo di questa tesi è condurre un'analisi di sicurezza applicando tale approccio ad uno scenario IoT in ambito smart home, come ampiamente analizzato nel capitolo 4. In dettaglio, viene definito uno scenario smart home composto da due unità abitative, che include diverse sorgenti dati per il monitoraggio dei consumi e delle presenze all'interno delle abitazioni. Alla luce delle iterazioni e delle autorizzazioni tra sensori che forniscono i dati e utenti che li visualizzano, si definisce un threat model volto ad individuare eventuali vulnerabilità ed attacchi al sistema a seguito di compromissione di uno o più dispositivi e/o dell' identità degli utenti. L'*output* previsto consiste in una threat analysis derivante dal threat model. Si cercherà attraverso **TAMELESS**, un *tool* di valutazione delle vulnerabilità per sistemi ibridi, di identificare le minacce alla sicurezza associate all'uso di dispositivi IoT in una casa domotica. Prima d'illustrare il lavoro svolto è fondamentale chiarire due concetti ampiamente citati nella tesi. Data la complessità dei sistemi odierni, la continua espansione di minacce, la molteplicità di componenti connessi ed il grande numero di percorsi e *pattern* d'attacco, si è reso infattibile condurre un'analisi di sicurezza completa in modo manuale. TAMELESS è uno strumento automatico che definisce un modello e un'analisi delle minacce destinata a sistemi ibridi come edifici intelligenti. Lo strumento è utile per supportare l'analisi di sicurezza ispirandosi alla logica del primo ordine. Riceve in *input* le specifiche del sistema e le relazioni tra le entità, espresse sotto forma di proprietà di base e di alto livello e le varie assunzioni di sicurezza. Una volta forniti questi elementi, l'utente può eseguire la threat analysis attraverso *query*. Dopo aver esaminato lo scenario, viene fornita una visione completa e comprensiva dello stato di sicurezza del sistema, inclusi tutti i possibili rischi. Per determinare gli *output* vengono introdotte un set di regole (regole di derivazione) che consentono al tool di lavorare su un qualunque sistema descritto. TAMELESS è stato progettato per condurre un'analisi su **sistemi ibridi**, che includono entità di natura fisica, digitale ed informatica. Lo strumento si basa su **Prolog**, un linguaggio di programmazione logico costruito su fatti e regole, e utilizza **SWI-Prolog** come ambiente di sviluppo.

Il lavoro è stato suddiviso in diverse fasi. Inizialmente si è reso necessario definire degli *use cases* che includono requisiti, infrastrutture ed entità coinvolte. Successivamente, dopo aver definito gli obiettivi di sicurezza, individuato le iterazioni all'interno del sistema, le possibili vulnerabilità ed il *data flow* si è proceduto con l'implementazione, attraverso query, dell'analisi di sicurezza dello scenario descritto. Questo ha incluso l'esame di attacchi che coinvolgono:

- **integrità e confidenzialità delle informazioni**;
- **identità degli utenti**;
- **rete e dispositivi**.

L'analisi ha delineato, come riassunto nel capitolo 5, i possibili attacchi, fornendo una rappresentazione visuale delle entità vulnerabili o sicure. I risultati dimostrano inequivocabilmente che la sicurezza di un sistema non può essere considerata in modo isolato. Dipende da una serie di fattori, tra cui l'ambiente specifico, le entità coinvolte e le relazioni tra esse. Questi fattori insieme determinano se un sistema è vulnerabile a determinati attacchi, se risulta compromesso o malfunzionante oppure se è dotato di adeguate misure di protezione in grado di prevenire o mitigare le minacce affrontate.