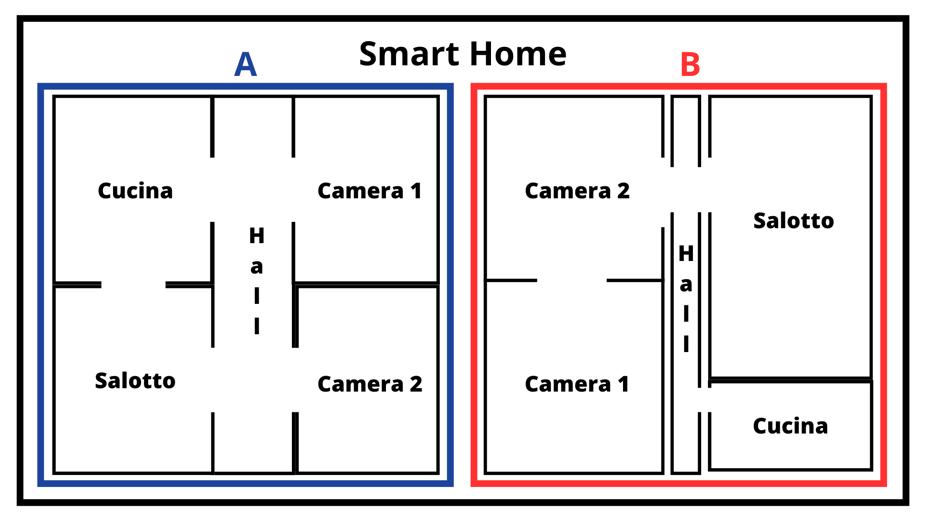
**Descrizione** lavoro proposto:

* definizione di uno scenario smart home, che comprende diverse sorgenti di dati per il monitoraggio dei consumi e delle presenze 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.

**FASE 1:** **Definizione dei casi d’uso, in particolare**:

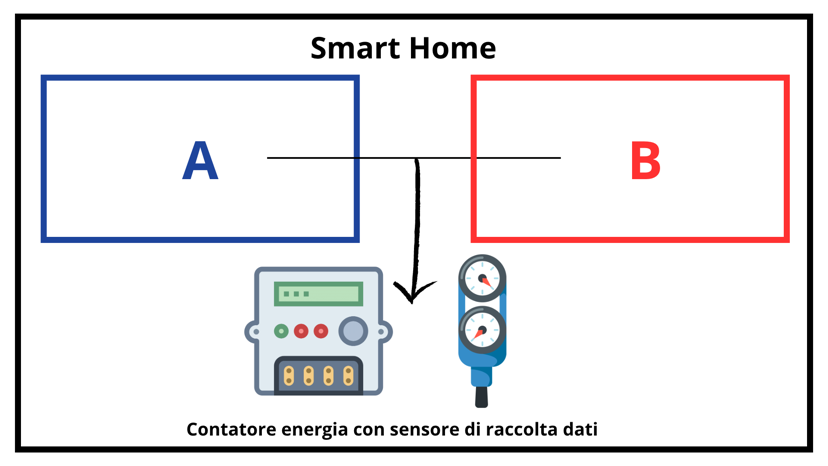
* **requisiti**.
* **infrastrutture**.
* **entità coinvolte**.

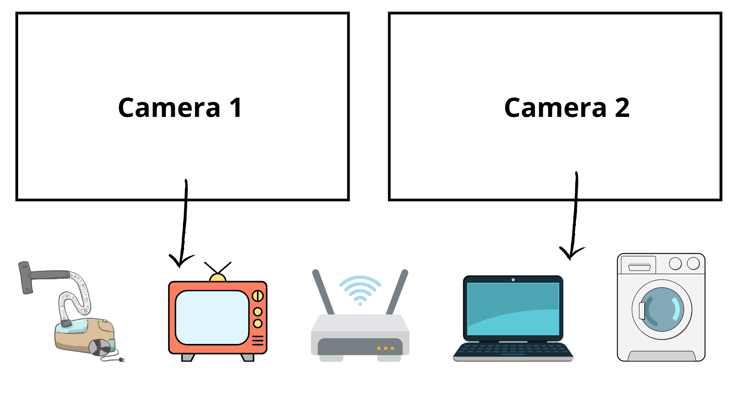
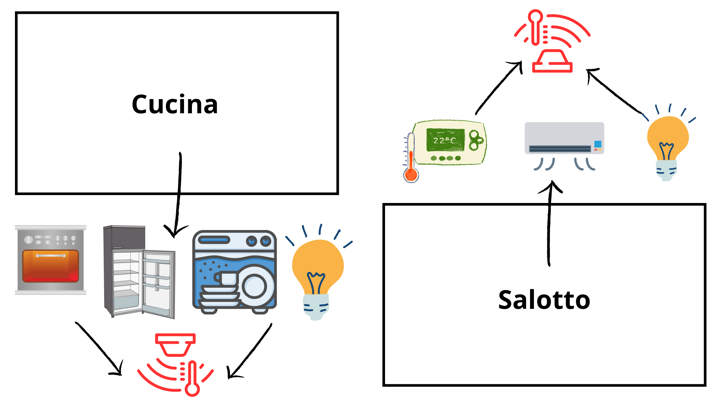
**SCENARIO:** Una Smart home divisa in due appartamenti (CASA A e CASA B) entrambi dotati di sistemi di **monitoraggio dei consumi** e **delle presenze** all’interno delle singole abitazioni. Gli utenti possono accedere ai dati elaborati e visualizzarne il contenuto.



**INFRASTRUTTURA**

Per quanto riguarda il **monitoraggio dei consumi energetici** vengono utilizzati dei sensori installati sui contatori elettrici o sui singoli elettrodomestici (microonde, frigorifero, lavatrice, luci cucina, luci stanza da letto ecc..).

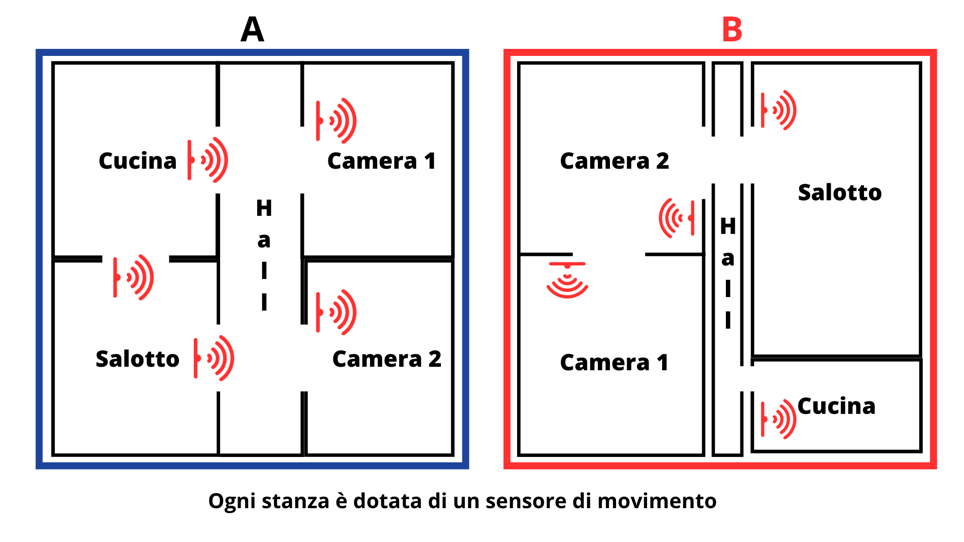




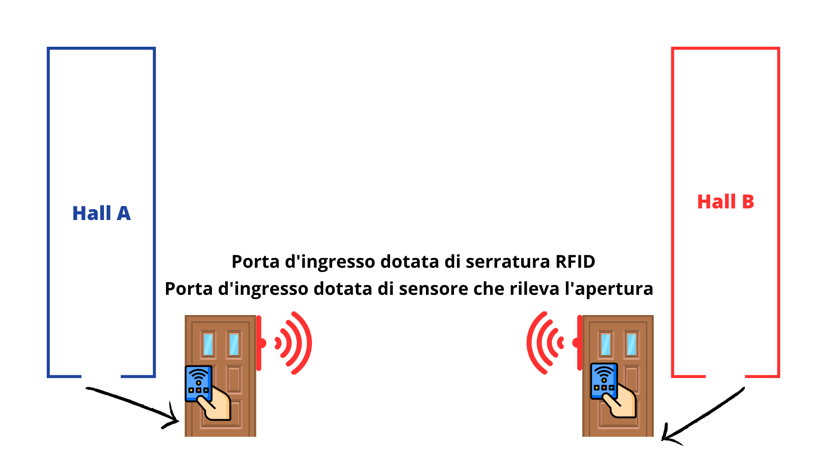
I sensori rilevano il consumo energetico e lo inviano ad un sistema centrale di raccolta dati ogni mezz’ora.

L’utente, attraverso un’interfaccia grafica, ha la possibilità di accedere a tutte le rilevazioni di ogni singolo sensore della propria abitazione.

Per quanto riguarda il **monitoraggio delle presenze** vengono utilizzati dei sensori di movimento installati in ciascuna stanza (soggiorno, cucina, camere da letto, ingresso).



Inoltre, è presente un sensore che rileva l’apertura della porta di ingresso. L’utente, attraverso un’interfaccia grafica, ha la possibilità di accedere a tutti i movimenti rilevati e all’informazione di apertura della porta. La porta è dotata di una serratura basata su tecnologia RFID, per accedere all’abitazione gli utenti dispongono di una tessera.

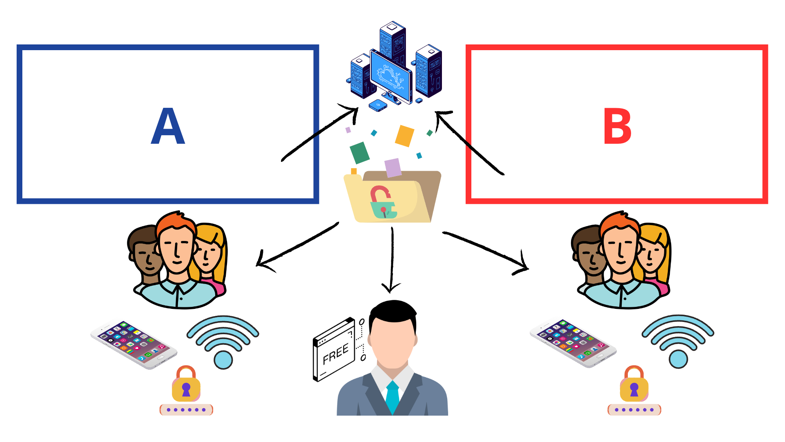


**REQUISITI**

I requisiti necessari alla funzione di **monitoraggio dei consumi energetici** sono dei sensori programmati in modo da rilevare i dati correttamente ed una connessione a internet per permettere il monitoraggio e la conseguente visualizzazione delle rilevazioni. Inoltre, un server deve ospitare il sistema centrale di raccolta dei dati, quest’ultimi devono essere elaborati e mostrati attraverso appositi algoritmi ed interfacce (web o app).

L’utente potrà accedere alle proprie informazioni solamente dopo aver eseguito l’autenticazione.

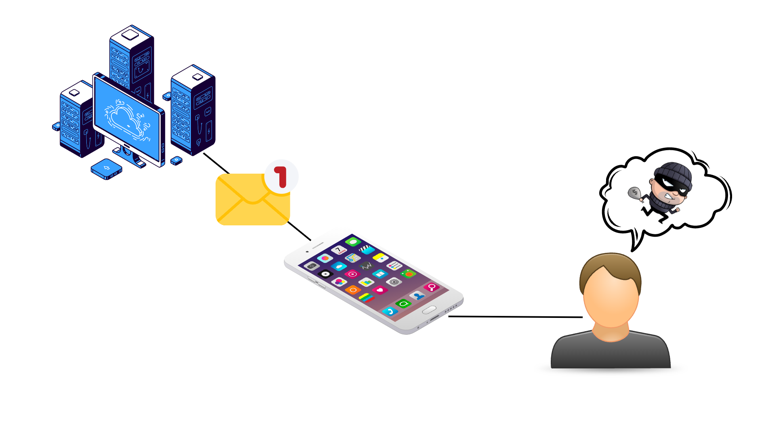
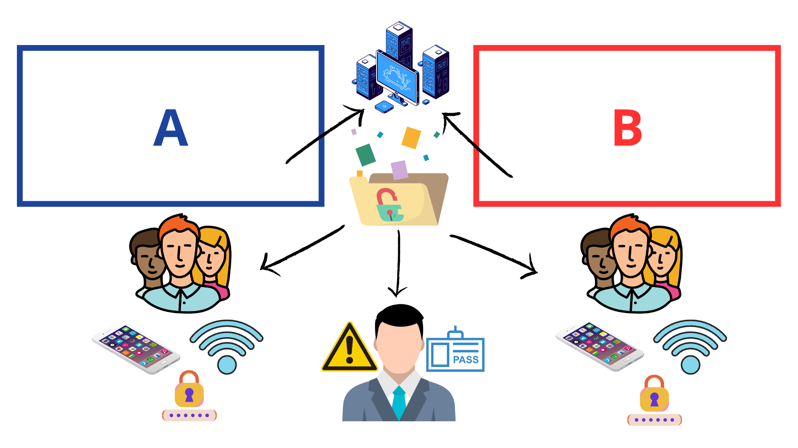
L’amministratore ha la possibilità di accedere liberamente alle complete informazioni di consumo della smart home (entrambi gli appartamenti), dopo aver verificato la propria identità.



Per garantire il **monitoraggio delle presenze** sono richiesti dei sensori che rilevano i movimenti posizionati in punti strategici della casa. Il sistema centrale di raccolta dati riceve le informazioni necessarie in modo da poter avvertire l’utente di eventuali presenze non autorizzate attraverso un sistema di notifica. I dati devono essere elaborati tramite appositi algoritmi e mostrati attraverso un’interfaccia (web o app).

L’utente potrà accedere alle informazioni inviate attraverso un sistema d’autenticazione.

L’amministratore invece potrà accedere alle informazioni di movimento raccolte dai sensori delle due abitazioni solamente dopo aver ricevuto appositi permessi da parte degli utenti coinvolti, in modo da preservare la privacy.



**ENTITA’**

Le entità coinvolte nel **monitoraggio dei consumi elettrici** sono gli utenti della casa, l’amministratore, i sensori, il sistema centrale di raccolta dati e autenticazione e l’interfaccia per permettere all’utente la visualizzazione dei dati, come ad esempio un semplice smartphone o un pc.

Le entità coinvolte nel **monitoraggio delle presenze** sono gli utenti della casa, l’amministratore, i sensori di movimento, il sistema centrale di monitoraggio e autenticazione, il sistema di notifica e l’interfaccia utente per permettere la visualizzazione dei dati.

**FASE 2: Definizione degli obiettivi di sicurezza:**

* **Threat model**
* **Threat analysis**

**THREAT MODEL**

In questa sezione, considerano lo scenario precedentemente descritto, **andremo a realizzare un modello di minaccia identificando le possibili minacce per il sistema**. Lo scopo è quello di **creare una rappresentazione astratta del sistema e delle sue vulnerabilità** esaminando i componenti hardware e software, i dati e le iterazioni con l’ambiente interno ed esterno.

Il Threat model comprende differenti entità: fisiche, umane e cyber.

Le **entità** nel nostro sistema rappresentano i componenti, invece i **threat** sono una o più sequenze di azioni che cambiano direttamente o indirettamente lo stato delle entità.

Ricordando lo scenario descritto, le principali **entità** che compongono il nostro sistema sono:

* ABITAZIONE A e B
* UTENTI divisi in:
  + AMMINISTRATORE
  + CONDOMINI
* SENSORI suddivisi in:
  + DI MOVIMENTO
  + DI MONITORAGGIO CONSUMI
  + DI RILEVAZIONE APERTURA PORTA
* SISTEMA CENTRALE DI RACCOLTA DATI E MONITORAGGIO
* SISTEMA DI AUTENTICAZIONE
* SISTEMA DI NOTIFICA
* TESSERA RFID
* DEVICE DI MONITORAGGIO come:
  + SMARTPHONE
  + PC

Gli **stati** delle entità nel nostro sistema sono le seguenti:

* **COMPROMESSO** 🡪 L’entità viene compromessa da una minaccia.
* **MALFUNZIONAMENTO** 🡪 l’entità non funziona correttamente o come previsto.
* **VULNERABILE** 🡪 l’entità ha una vulnerabilità che può essere sfruttata dalla minaccia.

**Altri stati** che il componente del sistema può assumere sono:

* **RILEVAZIONE** 🡪 viene rilevato che l’entità è stata compromessa a causa della minaccia.
* **RIPRISTINO** 🡪 indica che è stato ripristinato il controllo sull’entità precedentemente attaccata.
* **FIXED** 🡪 descrive che l’entità è stata riparata dopo il malfunzionamento causato.

Esistono inoltre alcune **relazioni** **che legano le nostre entità** all’interno del sistema, creando delle dipendenze, queste possono essere sfruttate per prevenire o controllare una possibile minaccia, ma possono indurre effetti negativi a più componenti del sistema se opportunamente sfruttate dall’attaccante. Le principali sono:

* **CONTROLLO** 🡪 l’entità A controlla l’entità B.
  + Esempio: Il device di monitoraggio controlla il sensore permettendo di spegnerlo e accenderlo.
  + Esempio: il computer verifica che il sensore di monitoraggio dei consumi funziona correttamente.

Immagine che contiene lavagna

Descrizione generata automaticamente

* **CONNETTORE** 🡪 L’entità A connette l’entità B.
  + Esempio: La rete connette il sistema centrale di raccolta dati con i sensori.

Immagine che contiene diagramma

Descrizione generata automaticamente

* **CONTENIMENTO** 🡪 L’entità A contiene l’entità B.
  + Esempio: La porta d’ingresso contiene il sensore di rilevazione dell’apertura della stessa.
  + Esempio: Il sistema di raccolta dati contiene il sistema di autenticazione per la verifica dell’identità.

Immagine che contiene testo

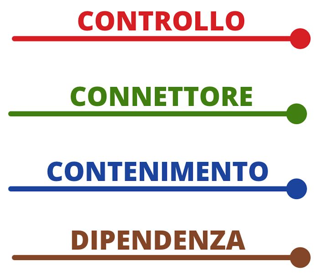
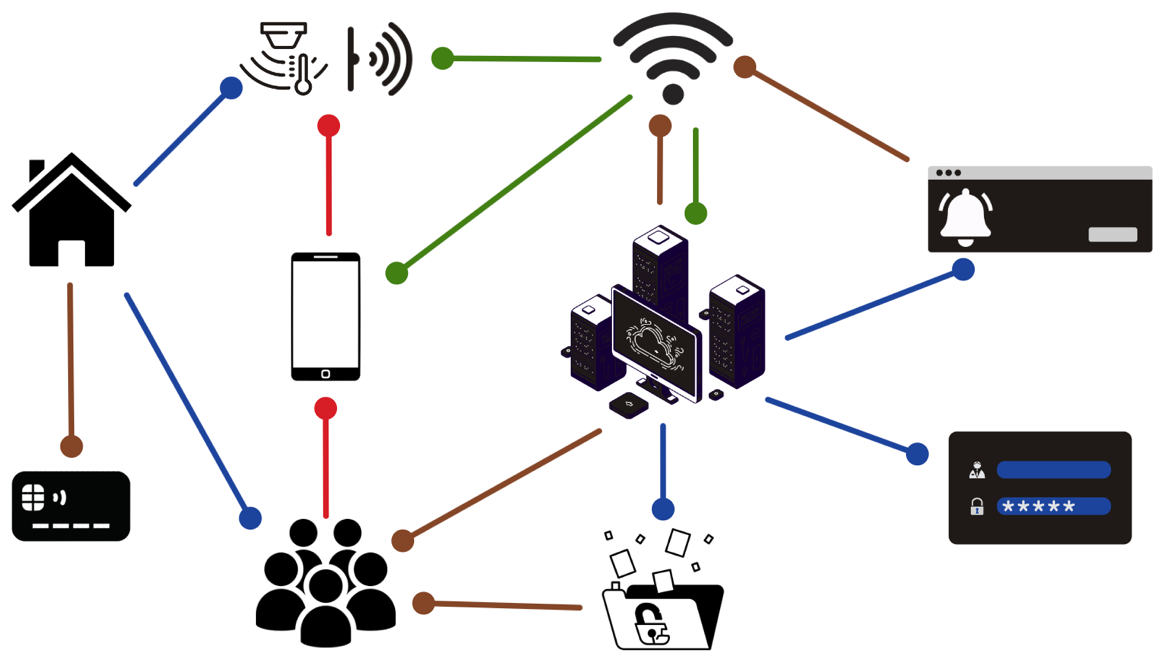
Descrizione generata automaticamente

* **DIPENDENZA** 🡪 Il funzionamento dell’entità A dipende dal funzionamento dell’entità B.
  + Esempio: Il sistema di raccolta dati e notifica dipende dal funzionamento della rete, una sua compromissione comporta uno spegnimento dei sistemi.
  + Esempio: Il sistema di raccolta dati e i dati effettivi dipendono dagli utenti, una compromissione sfruttando quest’ultimi comporta un punto d’accesso al sistema e alle informazioni.

Immagine che contiene diagramma

Descrizione generata automaticamente

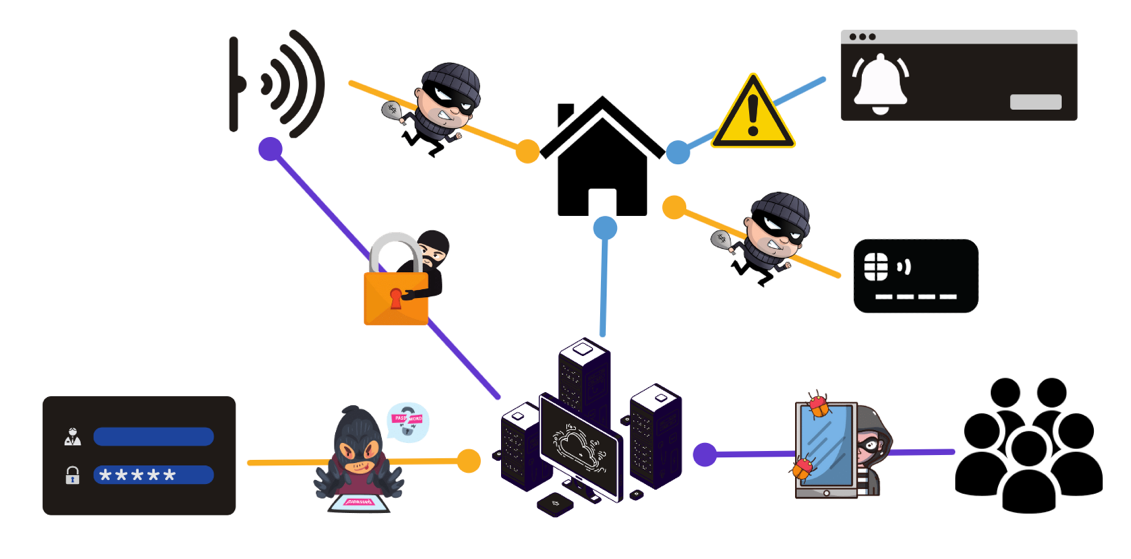
Nel **diagramma** seguente verranno rappresentati i principali componenti del sistema e le loro relazioni:



Tuttavia, possono essere create **relazioni anche tra entità e possibili minacce**, come ad esempio:

* **PROTEZIONE** 🡪 L’entità A protegge l’entità B da una potenziale minaccia.
  + Esempio: Il sistema d’autenticazione protegge il sistema di raccolta dati da un accesso non autorizzato.
  + I sensori di rilevazione proteggono l’abitazione da una possibile minaccia, se questa viene evitata in tempo.
* **MONITORAGGIO** 🡪 l’entità A monitora l’entità B, ma non può evitarla.
  + Esempio: il sistema di notifica monitora una possibile minaccia per l’abitazione A e B.
* **DIFFUSIONE** 🡪 l’entità A può propagare la minaccia ad un’entità B.
  + Esempio: un’e-mail di phishing viene usata per propagare la minaccia al sistema di raccolta dati.
  + Esempio: il sistema d’autenticazione può propagare la minaccia ai danni dei controlli sensori, per esempio un accesso non autorizzato può comportare il pieno controllo di questi, permettendo di spegnerli o effettuare comportamenti illeciti.

Nel diagramma seguente verranno rappresentati i principali componenti del sistema e le loro relazioni con le possibili minacce:

Immagine che contiene diagramma

Descrizione generata automaticamente

Seguendo lo schema di definizione di Threat Model, viene identificato:

* **OBIETTIVO** del sistema “Smart Home”🡪 Lo scopo del sistema è quello di monitorare i consumi energetici delle singole abitazioni, e rilevare la presenza di persone all’interno dell’edificio in modo da poter monitorare e prevenire l’accesso di eventuali soggetti non autorizzati. Vengono quindi raccolti dati sensibili come il progressivo consumo in termini energetici degli elettrodomestici, inoltre viene controllata la presenza continua dei soggetti anche attraverso un sensore che rileva lo stato di apertura della porta d’ingresso. I dati vengono salvati all’interno di un centro di raccolta ed è possibile accedervi solamente con autenticazione; pertanto, un possibile attacco a questo sistema permette di avere una visione completa a tutte le informazioni raccolte e successivamente utilizzare queste ultime illecitamente.
* **POSSIBILI VULNERABILITA’ E MINACCE** 🡪 il sistema così definito può essere vulnerabile a differenti attacchi, un esempio può essere un attacco informatico di phishing, dove viene sfruttata la vulnerabilità umana per rubare dati sensibili. Sfruttando la natura informatica, la rete può essere fonte di un attacco Man-In-The-Middle. Grazie alle caratteristiche hardware e software dei sensori un malintenzionato potrebbe infiltrarsi nel firmware per modificarlo o controllarlo a distanza, in modo da alterare il comportamento. Può anche essere eseguito un attacco Dos, sovraccaricando la rete con richieste di dati o elaborazione, bloccando l’intero sistema IoT.
* **VALUTAZIONE DELL’IMPATTO DELLE MINACCE** 🡪 Tutte le possibili minacce precedentemente elencate impattano in maniera negativa su aspetti fondamentali del sistema: l’identità dell’utente, il comportamento del dispositivo fisico e i dati elaborati. Quest’ultimi, se compromessi, hanno un impatto più significativo sulla vita del sistema; tuttavia, con un sistema d’autenticazione si aggiunge un livello di sicurezza che però può essere “raggirato” sfruttando ad esempio un attacco phishing. Consideriamo quindi tutti i possibili attacchi come “critici”, focalizzando l’attenzione sia sui dati raccolti in particolare modo sull’ integrità e confidenzialità, che sulla compromissione dei dispositivi e della rete, le quali implicano conseguenze dannose all’intero sistema interconnesso.

**THREAT ANALYSIS**

In questa sezione **entreremo in un processo più specifico e mirato di valutazione delle minacce**, concentrandoci sull’analisi dei rischi al sistema, **definendo possibili scenari d’attacco** all’integrità/ confidenzialità delle informazioni, all’identità degli individui e alla rete, esaminando le vulnerabilità specifiche, sia ai dati che al sistema stesso, che agli utenti coinvolti e le possibili contromisure per mitigare i rischi identificati.

Prima di introdurre i casi effettivi, vengono analizzate le definizioni dei possibili attacchi, che coinvolgono il sistema IoT descritto, in modo da avere una panoramica completa sulla natura teorica delle compromissioni:

* PHISHING 🡪 tipo di attacco informatico che mira a rubare informazioni sensibili, come password, numeri di carte di credito o altri dati personali, ingannando le persone attraverso l'uso di tecniche ingannevoli.

In un attacco phishing, l'attaccante crea un falso sito web o invia un falso messaggio di posta elettronica che sembra provenire da una fonte affidabile, come una banca, un'azienda o un'organizzazione governativa. Il messaggio o il sito web invita la vittima a fornire informazioni personali o a fare clic su un link che porta ad un sito web dannoso.

* MAN IN THE MIDDLE 🡪 in cui l'attaccante intercetta la connessione Wi-Fi tra il dispositivo della vittima e il punto di accesso Wi-Fi (AP).

In questo tipo di attacco, l'attaccante può creare una rete Wi-Fi fittizia con un nome simile a quello del punto di accesso reale, in modo che la vittima si connetta alla rete Wi-Fi falsa invece di quella reale o intercettare direttamente il traffico della rete. Una volta connessi alla rete Wi-Fi falsa, l'attaccante può intercettare il traffico di rete, inclusi dati sensibili come le password, i numeri di carta di credito o altre informazioni personali.

* DENIAL OF SERVICE 🡪 tipo di attacco informatico in cui l'attaccante tenta di sovraccaricare un sistema o una rete con una quantità eccessiva di traffico, pacchetti o richieste, allo scopo di impedire agli utenti legittimi di accedere ai servizi o alle risorse disponibili. L’obiettivo principale di un attacco DoS è quello di rendere inutilizzabile il sistema o la rete colpita, causando la disconnessione o il blocco degli utenti che cercano di accedere alle risorse. Questo tipo di attacco può essere realizzato attraverso varie tecniche, come l'invio di pacchetti falsi, la generazione di traffico di rete anomalo, il saturamento delle risorse del sistema con richieste di elaborazione e altri metodi. può essere utilizzato anche come diversivo per nascondere altri tipi di attacchi informatici più sofisticati, come quelli mirati a rubare dati sensibili o a infiltrarsi nella rete.

Per facilitare l’analisi specifica al sistema, vengono definiti esempi di possibili scenari d’attacco concreti che compromettono differenti entità delle Smart Home, combinando fasi di:

* Attacco fisico 🡪 come ad esempio scassinare serratura.
* Attacco Informatico 🡪 come, ad esempio, una compromissione della rete domestica.
* Attacco Umano 🡪 come rubare la password.

CASO 1: **FURTO D’IDENTITA’ CON ATTACCO PHISING**

Studiando questo caso mostreremo come **l’attaccante potrà sottrarre le credenziali d’accesso dell’utente coinvolto al sistema centrale**.

Ricordiamo come il **sistema** è formato:

L’accesso al sistema centrale di raccolta dati e monitoraggio è consentito solo dopo aver inserito le credenziali sul sistema d’autenticazione. Ogni utente è responsabile del salvataggio dei propri dati sensibili.

Quindi:

* Le credenziali d’accesso possono essere salvate su un dispositivo digitale come pc o smartphone.
* La **password** può essere compromessa in quanto rubata tramite un attacco di phishing, sfruttando la vulnerabilità umana, l’utente può essere indirizzato, attraverso una e-mail, ad un sito dannoso creato dall’attaccante stesso, questo può essere una replica del sistema d’autenticazione che mira a sottrarre i dati sensibili inseriti dall’utente.
* Il **sistema d’autenticazione** può essere compromesso, in quanto l’attaccante conosce la password appena rubata, ed il sistema d’autenticazione stesso non è difeso da controlli di sicurezza avanzati.
* L’attaccante ha quindi accesso al server, e sfruttando la natura digitale, può controllare l’intero sistema.
* Avendo accesso al sistema, la **confidenzialità delle informazioni** può essere compromessa, con la possibilità di monitorare i consumi e le attività degli utenti.

Per compromettere l’identità dell’utente è necessario:

* Sfruttare vulnerabilità umane, per portare ad una compromissione dell’ambiente digitale.
* La compromissione dell’ambiente digitale consente di sfruttare ulteriori vulnerabilità digitali per accedere ai dispositivi degli utenti per ottenere la password.
* Per accedere al sistema vengono sfruttate ulteriori vulnerabilità digitali per compromettere il sistema d’autenticazione.

Dopo aver analizzato l’impatto dell’attacco al sistema, questo può essere prevenuto educando gli utenti a riconoscere tentativi di phishing e inserendo opportuni controlli al sistema d’autenticazione, come ad esempio auth a due fattori, inoltre può essere aggiunta una misura di sicurezza avanzata al sistema centrale, con controlli di monitoraggio dei device che eseguono l’accesso, come ad esempio inserendo la verifica dell’ indirizzo IP, e informazioni generali sul dispositivo che sta tentando di accedere.

CASO 1.1: **FURTO D’IDENTITA’ CON ATTACCO A FORZA BRUTA**

Studiando questo caso mostreremo come **l’attaccante potrà sottrarre le credenziali d’accesso al sistema centrale utilizzando un altro tipo d’attacco**.

Ricordiamo come il **sistema** è formato:

L’accesso al sistema centrale è consentito solo dopo aver inserito le credenziali sul sistema d’autenticazione, in questo scenario d’attacco la premessa è che l’attacco di phishing non sia andato a buon fine, e quindi l’attaccante non conosce la password.

Quindi:

* L’attaccante potrebbe tentare di forzare l’accesso all’interfaccia d’autenticazione mediante un attacco di forza bruta, ovvero provando una serie di password diverse fino a trovare quella giusta.
* Il **sistema d’autenticazione** può essere compromesso, in quanto l’attaccante conosce la password appena generata, ed il sistema d’autenticazione stesso non è difeso da controlli di sicurezza avanzati.
* L’attaccante ha quindi accesso al server, e sfruttando la natura digitale, può controllare l’intero sistema.

Questo tipo di attacco può essere prevenuto innanzitutto migliorando il comportamento dell’entità umana coinvolta: l’utente dovrà utilizzare delle password complesse.

Inoltre, il sistema d’autenticazione deve implementare opportuni controlli al sistema d’autenticazione, come ad esempio un sistema di blocco automatico dopo un certo numero di tentativi ed un sistema di notifica periodica di cambio della password.

**CASO 2**: **ACCESSO NON AUTORIZZATO ALL’ABITAZIONE**.

Studiando questo caso **mostreremo come l’attaccante potrà accedere fisicamente a una delle due abitazioni**, mostrando i passaggi dell’attacco riuscito:

Ricordiamo come il **sistema** è formato:

L’abitazione è protetta da una porta con serratura dotata di tecnologia RFID. Si suppone che le tessere RFID per aprire la porta possano essere lette e clonate a una distanza moderata. Inoltre, la porta stessa è monitorata da sensore di rilevamento apertura. All’interno dell’abitazione, in ogni stanza è presente un sensore di rilevamento delle presenze, i sensori possono essere controllati attraverso il sistema di monitoraggio dopo aver inserito la password nel sistema d’accesso.

Quindi:

* La **tessera RFID** che protegge la serratura della porta può essere duplicata, quindi compromessa, in quanto vulnerabile a letture e clonazione da una distanza moderata poiché priva di opportuni controlli di sicurezza.
* Il **sistema d’autenticazione** può essere compromesso: l’attaccante conosce la password grazie ad un precedente attacco, ed il sistema d’autenticazione stesso non è difeso da controlli di sicurezza avanzati.
* Il **sistema di monitoraggio** è protetto dal sistema d’autenticazione, di conseguenza la minaccia può essere diffusa. Questo viene protetto dall’entità compromessa e chiunque conosce la password può accedervi.
* L’attaccante ha quindi accesso al sistema, e sfruttando la natura digitale, può causare un malfunzionamento al **sensore**, spegnendolo.
* Il malfunzionamento del sensore può diffondersi ai restanti, siccome questi non sono difesi da sistemi di controlli d’autenticazione e quindi vulnerabili a manipolazioni da parte di qualsiasi utente connesso.
* **L’abitazione** è quindi vulnerabile ad un accesso da parte di un utente non autorizzato, siccome questa non è più difesa dalla porta e monitorata dai sensori.
* L’attaccante, quindi è riuscito a **modificare il normale comportamento del sistema** e di conseguenza potrà rubare e compromettere qualsiasi elemento all’interno della smart home.

Per accedere all’abitazione è necessario:

* Sfruttare le vulnerabilità digitali della tessera RFID per compromettere l’ambiente fisico.
* La compromissione dell’ambiente fisico consente di sfruttare ulteriori vulnerabilità digitali per accedere al sistema.
* Le vulnerabilità digitali consentono di sfruttare le ulteriori vulnerabilità digitali e vulnerabilità fisiche dei sensori per manipolarli.
* L’insieme delle vulnerabilità digitali e umane dell’intero sistema vengono utilizzate per sfruttare ulteriori vulnerabilità fisiche per accedere all’abitazione.

Analizzando questo possibile scenario, per mitigare questi rischi sarebbe opportuno introdurre dei controlli specifici che impongano l’impossibilità di duplicare la tessera dotata di tecnologia RFID, verificando ogni qualvolta la sua unicità. Inoltre, i sensori di rilevamento delle presenze possono essere sostituti fisicamente con dei sensori multimediali che catturano le immagini, disaccoppiando il loro singolo funzionamento, in tal modo che una compromissione di un sensore non comporta il malfunzionamento dell’intera rete e quindi attraverso sistemi di backup è possibile ripristinarli.

Può essere sfruttato il sistema di notifica per implementare controlli sui singoli sensori in modo da informare l’utente di comportamenti anomali, come ad esempio lo spegnimento improvviso.

CASO 3: **MANIPOLAZIONE DELLE INFORMAZIONI RACCOLTE**

Analizzando questo possibile attacco, mostreremo **come l’attaccante intercetta e modifica le informazioni che i sensori raccolgono ed inviano al sistema centrale di raccolta dati**, con lo scopo di danneggiare l’integrità delle stesse, alterando valori dei consumi e delle presenze.

Il **sistema** è così formato:

La rete connette i diversi sensori che monitorano i consumi dei singoli elettrodomestici all’interno della smart home e il sistema centrale di raccolta dati che memorizza le informazioni raccolte ed elaborate.

Quindi:

* La **rete**, non essendo protetta da un sistema di autenticazione è vulnerabile ad un accesso fisico da parte di un eventuale attaccante.
* Un attaccante sfrutta questa vulnerabilità attraverso un attacco man-in-the-middle ponendosi “in mezzo” alla comunicazione tra sensori e sistema di raccolta dei dati.
* Il sistema di raccolta dati dipende dalla rete, quindi la compromissione della rete si può diffondere anche sul **sistema di raccolta dei dati**.
* In questo modo l’attaccante intercetta i dati elaborati che, partendo dai sensori, “viaggiano” verso il sistema di raccolta dati. Anche questo è quindi compromesso.
* L’attaccante, avendo accesso al traffico della rete, può generare false informazioni o modificare dati esistenti, compromettendo le **informazioni** che vengono raccolte dai sensori e inviati al sistema centrale.

**NOTA BENE**: in questo scenario d’attacco, l’attaccante potrebbe essere l’utente stesso della casa, che effettua la modifica delle informazioni raccolte dai sensori o ne genera nuove, con il solo scopo di diminuire i valori dei consumi registrati dai sensori in modo da avere un successivo abbassamento dei costi energetici di utilizzo dei componenti.

Per compromettere l’integrità delle informazioni è necessario:

* Sfruttare le vulnerabilità informatiche della rete per accedere fisicamente alla stessa.
* Queste vulnerabilità consentono all’attaccante di accedere alla comunicazione compromettendo la natura digitale ed il comportamento fisico del sistema.

IoT si basa su tecnologie wireless molto soggette a violazioni: l’immissione di pacchetti falsi nella rete contenente dati non validi o manipolati, descritti in questo possibile scenario d’attacco, prende il nome di “**Packet Injection**”. Questa tecnica è utilizzata al fine di causare una variazione non prevista nel comportamento del sistema.

Questo possibile scenario d’attacco può essere mitigato riducendo i rischi: un essenziale misura di sicurezza è limitare l’accesso alla rete solo ai dispositivi autorizzati. Ciò può essere fatto introducendo un sistema d’autenticazione basato su protocolli di sicurezza moderni come WPA3 per la connessione wi-fi. Un ulteriore funzionalità di sicurezza che può essere aggiunta è la “Guest Network”: per separare i dispositivi degli ospiti dalla rete principale, limitando alcune funzionalità. Per quanto riguarda il flusso di informazioni è necessario aggiungere protocolli crittografici più robusti e protocolli di sicurezza aggiornati per il traffico in rete.

CASO 4: **ATTACCO ALLA RETE DEL SISTEMA**

Analizzando questo scenario d’attacco mostreremo come, tramite un attacco di Denial of Service (DoS), sia possibile **interrompere il normale funzionamento della rete**. L’obbiettivo di questo attacco è quello di andare a saturare la rete, rendendo molto difficili le comunicazioni tra i sensori ed il sistema centrale e la conseguente visualizzazione delle informazioni da parte degli utenti.

Il sistema è composto da un insieme di sensori che comunicano con il sistema centrale tramite la rete, l’obiettivo principale è quello di compromettere la rete, la quale comporta una possibil compromissione dell’intero sistema.

* Come nell’attacco mostrato nello scenario 3, la **rete** è vulnerabile in quanto non è composta di adeguati controlli di accesso e di autenticazione.
* Sfruttando la vulnerabilità della rete l’attaccante installa del software dannoso sui **sensori**, andando a comprometterli, siccome anch’essi non sono protetti da opportuni controlli d’accesso.
* La compromissione viene “sfruttata” per causare un malfunzionamento stesso dei **sensori**: questi inviano una grande quantità di richieste o dati al **sistema centrale di raccolta**, sovraccaricando la rete e quindi compromettendola.
* Il **sistema centrale di raccolta dei dati** dipende dalla rete: la mole di traffico in rete indirizzato al sistema ne impedisce il corretto funzionamento.
* Questo potrebbe impedire agli **utenti** di accedere ai dati dei propri sensori di monitoraggio dei consumi energetici e di presenza, impedendo di fatto la funzionalità della rete.
* Arrivati a questo punto **tutto il sistema è compromesso** in quanto, fino ad un ipotetico ripristino, l’intero sistema IoT è inutilizzabile.

Per attaccare e compromettere la rete del sistema è necessario:

* Sfruttare le vulnerabilità informatiche della rete domestica per accedere.
* Modificare il corretto funzionamento delle componenti fisiche della smarthome sfruttando vulnerabilità di natura digitale e fisica.
* Impedire all’utente di eseguire qualsiasi operazione di natura digitale, attraverso vulnerabilità digitali e fisiche (comportamento) dei sensori stessi e dei sistemi di raccolta delle informazioni.

Per effettuare questo attacco si può, come nello scenario 3, introdurre la tecnica di “**Packet Injection**”, inviando un gran numero di pacchetto malevoli a dispositivi al fine di sovraccaricarli e renderli inutilizzabili. Questi attacchi descritti possono essere particolarmente pericolosi poiché molti dispositivi IoT sono progettati per essere accessibili da remoto e spesso hanno vulnerabilità di sicurezza significative.

Analizzando questo tipo di attacco è possibile prevenire e mitigare alcuni rischi connessi. Oltre al sistema d’autenticazione alla rete domestica ampiamente discusso nel caso 3, un’altra soluzione rilevante può essere quella di utilizzare un firewall per monitorare il traffico di rete e bloccare quello sospetto o eccessivo. L’utente inoltre potrebbe limitare il numero di connessioni simultanee ed impostare limiti di banda sulla connessione per evitare che uno o pochi utenti monopolizzino tutta la larghezza di banda.

**NOTA BENE**: Negli scenari analizzati, in particolare 1 e 3, gli scopi d’attacco sono ben definiti, nel caso 1 si ha l’obiettivo di rubare l’identità dell’utente mentre nel terzo il fine è quello di manipolare le informazioni che viaggiano in rete, dai sensori al sistema centrale di raccolta dati. Tuttavia, è fondamentale sottolineare che:

* Se l’attacco descritto nello scenario 1 dovesse andare a buon fine, si avrebbe completo accesso alle informazioni sensibili raccolte dai sensori, sfruttando le capacità informatiche l’attaccante potrà utilizzare la tecnica di “**Packet Injection**”, che consiste nel tracciamento dei pacchetti e nella conseguente perdita o diffusione di eventuali dati sensibili.
* Nello scenario 3 l’attaccante, anche se non esplicitamente, utilizza la tecnica di “**Packet Injection**”, poiché intercettando il traffico che viaggia in rete, può avere completo accesso a tutte le informazioni sensibili, compromettendo anche la confidenzialità dei dati e non la sola integrità.

Nel contesto degli attacchi ai sistemi IoT, il packet sniffing viene spesso utilizzato per raccogliere informazioni sulle comunicazioni tra dispositivi IoT e la rete a cui sono collegati. Gli attaccanti possono utilizzare questa tecnica per raccogliere informazioni sensibili che vengono trasmesse.