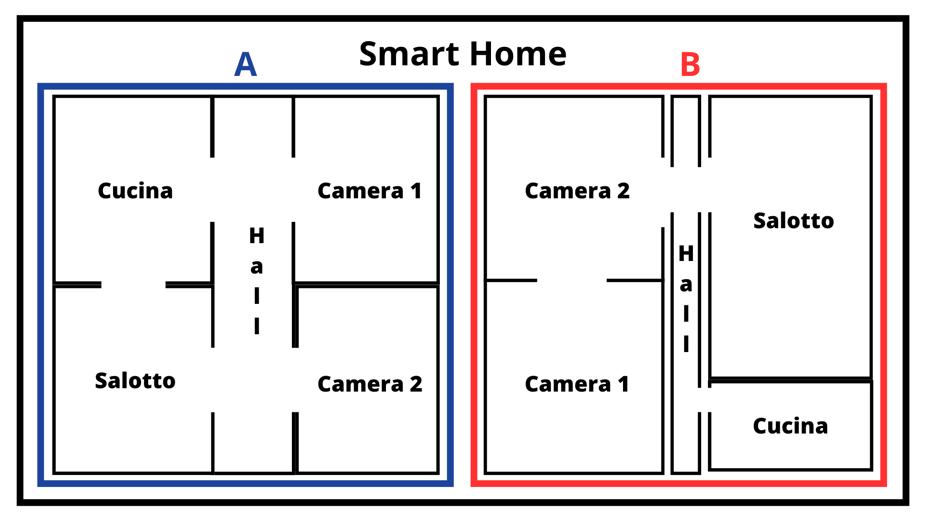
**Descrizione** lavoro proposto:

* 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**:

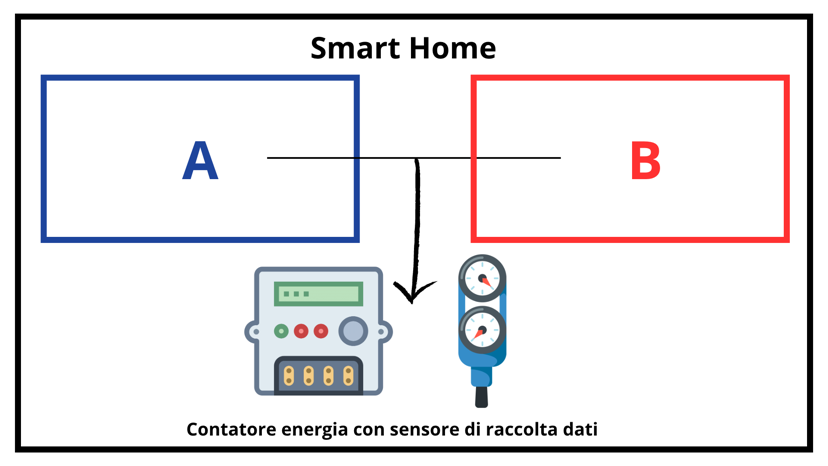
* **requisiti**.
* **infrastrutture**.
* **entità coinvolte**.

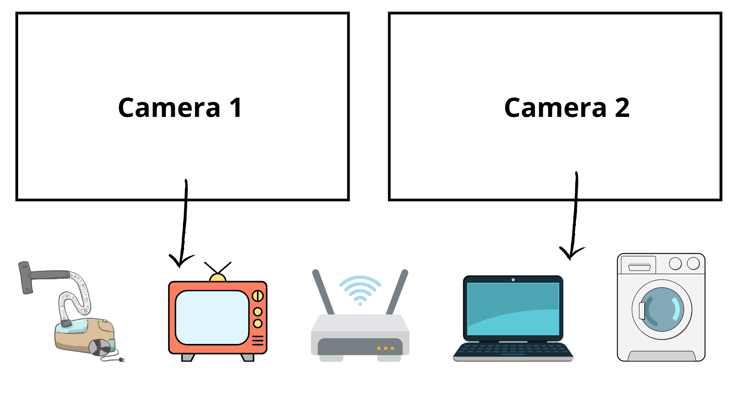
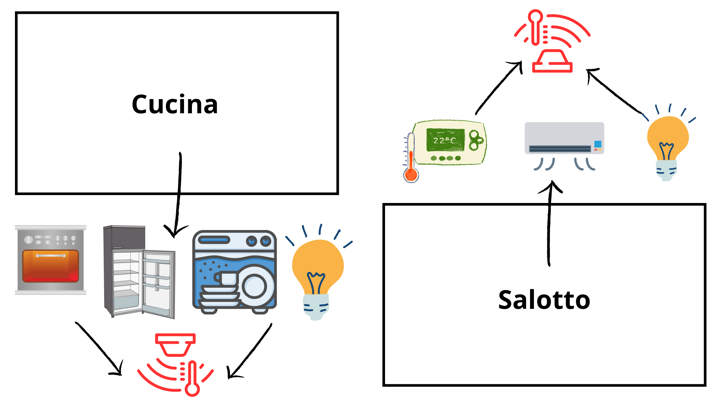
**SCENARIO:** Una Smart home divisa in due appartamenti (CASA A e CASA B) entrambi dotati di sistemi di **monitoraggio dei consumi** e **delle presenze** all’interno delle singole abitazioni. Gli utenti possono accedere ai dati elaborati e visualizzarne il contenuto.



**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..).

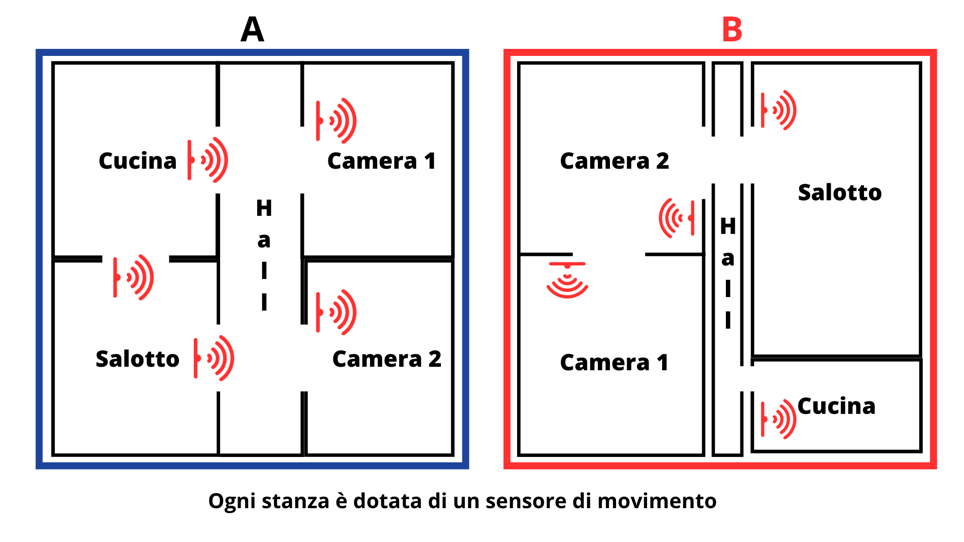




I sensori rilevano il consumo energetico e lo inviano ad un sistema centrale di raccolta dati ogni mezz’ora.

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.

Immagine che contiene testo

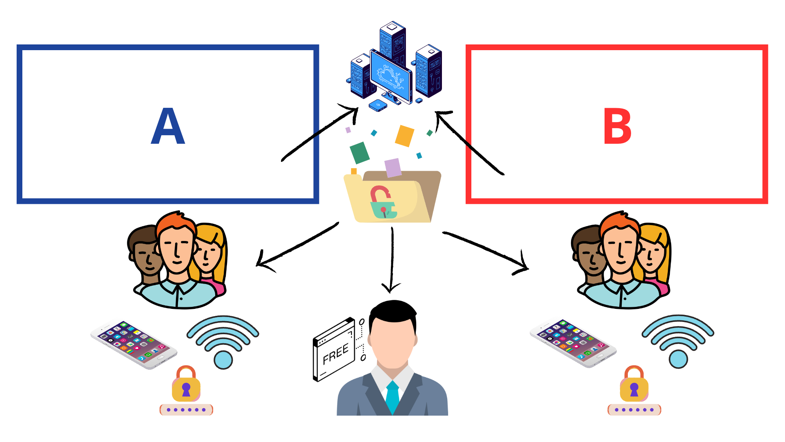
Descrizione generata automaticamente

**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 un visualizzatore dati.

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

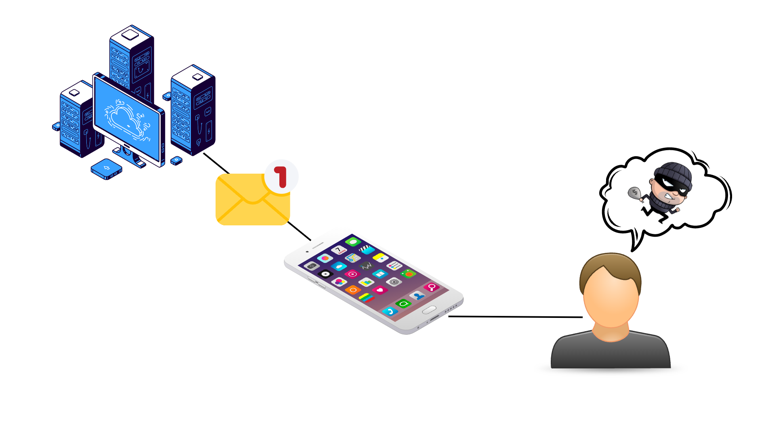
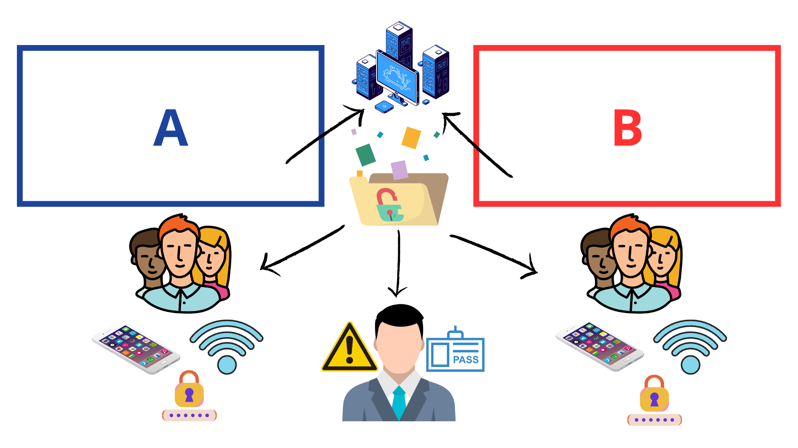
L’amministratore ha la possibilità di accedere liberamente alle complete informazioni di consumo della smart home (entrambi gli appartamenti), dopo aver verificato la propria identità.



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 visualizzatore dati.

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 raccolta dati 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
* SISTEMA DI AUTENTICAZIONE
* SISTEMA DI NOTIFICA
* 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

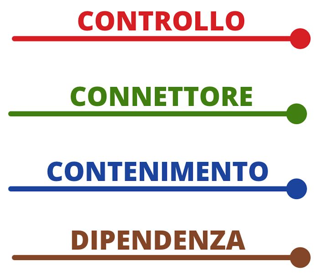
* **DIPENDENZA** 🡪 Il funzionamento dell’entità A dipende dal funzionamento dell’entità B.
  + Esempio: Il sistema di raccolta dati e notifica dipende dal funzionamento della rete, una sua compromissione comporta uno spegnimento dei sistemi.
  + Esempio: Il sistema di raccolta dati e i dati effettivi 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:

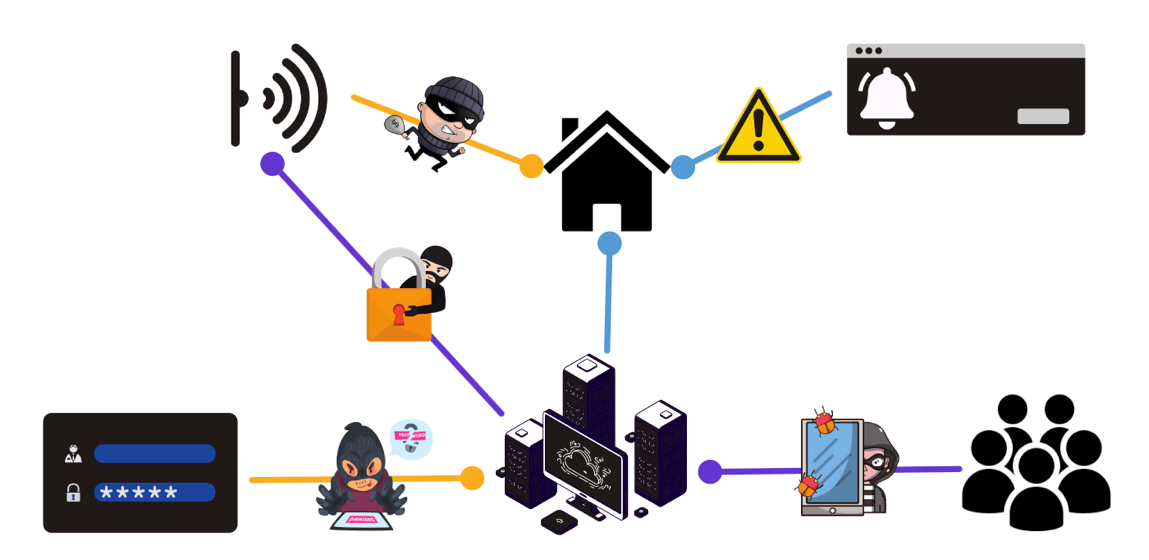
Immagine che contiene diagramma

Descrizione generata automaticamente

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 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 accedere a dati sensibili. Sfruttando la natura informatica, la rete wi-fi 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, questo può anche essere eseguito con un attacco di denial of service, sovraccaricando il sensore con richieste di dati o elaborazione. Infine, una possibile minaccia può essere un attacco spoofing dove l’attaccante può creare un segnale falso per simulare una situazione diversa da quella effettiva per ingannare il sensore.
* **VALUTAZIONE DELL’IMPATTO DELLE MINACCE** 🡪 Tutte le possibili minacce precedentemente elencate impattano in maniera negativa su due aspetti fondamentali del sistema: 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 gli attacchi elencati come “critici”, focalizzando l’attenzione sia sui dati raccolti in particolare modo sull’ identità e confidenzialità, che sulla compromissione dei dispositivi e della rete, le quali implicano conseguenze dannose.

**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.

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 crea 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. Una volta che la vittima si è connessa 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.

SPOOFING 🡪 è un tipo di attacco informatico in cui l'attaccante utilizza una tecnica di falsificazione dell'identità per mascherare la sua vera identità e impersonare un'altra persona, un dispositivo o una rete. In pratica, l'attaccante si finge qualcun altro per ingannare le vittime e ottenere informazioni o accesso a sistemi o dati sensibili. In particolare, modo può essere utilizzato un DNS Spoofing modificando le informazioni di DNS per associare un nome di dominio a un indirizzo IP diverso da quello corretto, al fine di indirizzare le vittime ad un sito web falso e impossessarsi di dati come credenziali d’accesso o un IP Spoofing dove l’attaccante falsifica l’indirizzo IP di origine di un pacchetto di rete per mascherare la sua vera identità e ingannare la destinazione.

**PHISHING**

ENTITA’ COINVOLTE: UTENTI.

VULNERABILITA’: vulnerabilità di tipo umano, viene sfruttata la persona per ottenere dati sensibili compromettendo anche l’ambiente digitale.

MINACCIA: Attacco di phishing

DESCRIZIONE: un attaccante potrebbe sfruttare la vulnerabilità umana con un attacco di phishing, come ad esempio l’indirizzamento su un sito web ingannevole inviato tramite e-mail. Lo scopo di questo attacco è sottrarre informazioni sensibili come credenziali d’autenticazione, compromettendo l’identità dell’utente.

**MAN-IN-THE-MIDDLE**

ENTITA’ COINVOLTE: RETE, SENSORI DI RILEVAZIONI E DI CONSUMI, SISTEMA CENTRALE DI RACCOLTA DATI

VULNERABILITA’: Rete, Accesso fisico

MINACCIA: Attacco Man-In-The-Middle

DESCRIZIONE: L’attaccante può intercettare il traffico tra il sensore e la smart home sfruttando la rete tramite appositi software oppure attraverso l’accesso fisico al router della smart home (nel caso in cui password sia conosciuta grazie ad un attacco precedente oppure il router non richiede alcuna autenticazione).

L’attaccante può quindi intercettare i dati trasmessi dal sensore o inviare dati falsificati con valori dei consumi alterati, compromettendo l’integrità delle informazioni.

Questo attacco può essere effettuato anche sui sensori di rilevamento delle presenze, cancellando gli avvisi di rilevazione dei movimenti in un certo momento all’interno dell’abitazione, in modo che, successivamente, l’attaccante avrà modo di accedere fisicamente all’abitazione.

**(D)DoS**

ENTITA’ COINVOLTE: SENSORI, RETE

MINACCIA: Attacco DoS (Denial Of Service)

VULNERABILITA’: mancanza di controlli di accesso: l'assenza di controlli di accesso adeguati può consentire ad un attaccante di accedere ai dispositivi della smart home. Questo può permettere all'attaccante di installare software dannoso sui dispositivi e di utilizzarli per attaccare la rete.   
Protocolli d’autenticazioni deboli: La mancanza di autenticazione forte può rendere i dispositivi smart home vulnerabili ad attacchi DoS. Senza autenticazione adeguata, un attaccante può facilmente impersonare un dispositivo e inviare pacchetti di dati dannosi.

DESCRIZIONE: Questo tipo di attacco è ampiamente utilizzato nei sistemi IoT: L’attaccante dopo aver eseguito l’accesso ad uno dei dispositivi connessi alla rete della smart home, può effettuare questo attacco tramite la saturazione della rete: l’attaccante invia una grande quantità di dati alla rete, sovraccaricandola ed impedendo ai sensori di rilevare correttamente i dati.

**SPOOFING D’IDENTITA’**

ENTITA’ COINVOLTE: SISTEMA CENTRALE DI RACCOLTA DATI, SENSORI

VULNERABILITA’: Identità Utente

MINACCIA: Attacco Spoofing

DESCRIZIONE: L’utente autorizzato ha accesso a tutti i dati a disposizione del proprio appartamento, mentre l’amministratore ha accesso a tutti i dati relativi ai consumi e in alternativa, se concesso, anche alle rilevazioni delle presenze di entrambe le smart home. L’attaccante, una volta ottenuto le credenziali tramite un precedente attacco di phishing potrebbe accedere al sistema IoT, utilizzando l’identità dell’utente legittimo. In questo modo potrebbe visualizzare e rubare informazioni sensibili, disattivare sensori di sicurezza, alterare la configurazione dei dispositivi.   
Così facendo oltre a compromettere la confidenzialità dell’informazione, viene danneggiata anche l’integrità del dato tramite una manipolazione di natura digitale al sensore.

CASO 1: 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:

Abitazione protetta da porta con sensore di rilevamento d’apertura,all’interno di ogni stanza è presente un sensore di rilevamento delle presenze, questi possono essere monitorati attraverso il sistema di raccolta dati, dopo aver inserito password nel sistema d’autenticazione.

Quindi:

* La password può essere compromessa in quanto rubata tramite un attacco di phising.
* Il sistema d’autenticazione può essere compromesso, in quanto l’attaccante conosce la password appena rubata.
* L’attacco al sistema d’autenticazione può diffondere la minaccia al sistema di monitoraggio, in quanto questo viene protetto dall’entità compromessa.
* L’attaccante ha quindi accesso al sistema, può causare un malfunzionamento al sensore, spegnendolo.
* Il malfunzionamento del sensore può\ diffondersi ai restanti, siccome questi sono privi di sistemi di controlli d’autenticazione e quindi vulnerabili a manipolazioni da parte di qualsiasi utente.
* L’attaccante, quindi sfruttando le vulnerabilità fisiche della porta potrà accedere all’abitazione, poiché i sensori che monitoravano l’abitazione sono disattivati.
* l’abitazione è quindi vulnerabile ad un accesso da parte di un utente non autorizzato.

CASO 2: ATTACCO ALL’INTEGRITA’ DELLE INFORMAZIONI

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.

Il sistema è cosi 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.

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 attraverso un attacco man-in-the-middle si pone “in mezzo” alla comunicazione tra sensori e sistema di raccolta dei dati compromettendo la rete.
* Il sistema di raccolta dati dipende dalla rete, quindi la compromissione delle rete si diffonde anche sul sistema di raccolta dei dati.
* Viene utilizzata la rete per inviare al sistema di raccolta dati alterati, quindi anche questo viene 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.

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 con il solo scopo di diminuire i valori dei consumi registrati dai sensori in modo da avere un successivo abbassamento dei costi di utilizzo dei componenti.

CASO 3: ATTACCO ALLA CONFIDENZIALITA’ DELLE INFORMAZIONI

In questo caso si mostra come l’attaccante, previo precedente furto delle credenziali, acceda al intero sistema IoT, utilizzando l’identità del utente legittimo.

Nel sistema tutte le rilevazioni effettuate dai sensori vengono registrate nel sistema centrale di raccolta dati (i sensori di monitoraggio inviano dati ogni mezz’ora mentre i sensori di rilevamento delle presenze inviano i dati ogni volta che viene rilevata una presenza).

Quindi:

* La password può essere compromessa in quanto l’attaccante ne è a conoscenza (phishing)
* Il sistema di autenticazione può essere compromesso
* Il sistema di monitoraggio viene compromesso in quanto questo è protetto da un’entità compromessa
* La confidenzialità è compromessa in quanto un soggetto esterno ha libero accesso al sistema di monitoraggio
* L’identità del utente viene compromessa

CASO 4: ATTACCO ALLA RETE DEL SISTEMA

Analizzando questo attacco mostreremo come, tramite un attacco di Denial of Service, 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.

Il sistema è composto da un insieme di sensori che comunicano con il sistema centrale tramite la rete.

* La rete è vulnerabile in quanto non è composta di adeguati controlli di accesso
* Sfruttando la vulnerabilità della rete l’attaccante installa del software dannoso sui sensori, andando a comprometterli.
* La rete dipende dai sensori. I sensori compromessi inviano una grande quantità di informazioni sulla rete, sovraccaricandola e quindi compromettendola.
* Arrivati a questo punto tutto il sistema è compromesso in quanto, fino a quando l’attacco non termina, l’intero sistema IoT è inutilizzabile.