UNIVERSITÀ DEGLI STUDI DI SALERNO

Corso di Laurea Magistrale in Informatica, prof. ssa Rita Francese

a.a 2024/2025

ENTERPRISE MOBILE APPLICATION DEVELOPMENT

DefNet

RAD

Studenti:

Marta Coiro matr. 0522501611

Katia Buonocore matr 0522501744

Gabriele Coralluzzo matr 0522501784

Umberto Della Monica 0522501617

Coach Aziendale:

Gabriele Ciliberti

LinearIT

INDICE

1. Introduzione

1.1. Contesto del progetto

Con l'aumento della diffusione di dispositivi smart e sistemi IoT nelle case moderne, la sicurezza delle reti domestiche è diventata una questione cruciale. Dispositivi come telecamere di sicurezza, elettrodomestici intelligenti e sistemi di automazione offrono comodità e funzionalità, ma comportano anche rischi significativi per la privacy e la sicurezza. Ogni dispositivo connesso rappresenta un potenziale punto di accesso per attacchi informatici, e le violazioni della sicurezza sono in costante aumento. È quindi essenziale fornire soluzioni di sicurezza efficaci e accessibili per gli utenti domestici e le piccole aziende.

1.2. Descrizione del Progetto

Questo progetto mira a sviluppare un dispositivo hardware di sicurezza dedicato alle reti domestiche. Il dispositivo fungerà da punto di controllo per tutti i dispositivi connessi, operando come un sistema di rilevamento delle intrusioni (IDS) e di prevenzione delle intrusioni (IPS). Sarà in grado di monitorare e analizzare il traffico di rete in tempo reale, identificando e prevenendo attività sospette e pericolose. Inoltre, un'applicazione mobile intuitiva accompagnerà il dispositivo, consentendo agli utenti di gestire facilmente le impostazioni di sicurezza e ricevere notifiche in caso di eventi di sicurezza.

1.3. Obiettivi del Progetto

Il progetto ha come obiettivo primario quello di fornire agli utenti domestici uno strumento semplice ed efficace per monitorare la sicurezza della rete e proteggere i dispositivi connessi. Gli obiettivi specifici includono:

- **Rilevamento e prevenzione di minacce informatiche.**
- **Archiviazione storica degli eventi di sicurezza per analisi future.**
- **Personalizzazione delle impostazioni di sicurezza tramite un'interfaccia user-friendly.**

1.4. Target del Progetto

Il progetto si rivolge a un'ampia gamma di utenti, dalle famiglie agli utenti domestici, passando per piccole aziende e professionisti. Ogni gruppo ha esigenze specifiche e livelli di competenza variabili in materia di sicurezza informatica, ma condividono tutti l'interesse per una protezione semplice, affidabile e personalizzabile delle loro reti domestiche e dei dispositivi connessi.

2. Requisiti del sistema

2.1. Requisiti funzionali

2.1.1. **Monitoraggio della Sicurezza di Rete**: Il sistema deve monitorare in tempo reale il traffico di rete, identificando e segnalando attività sospette o anomale.

2.1.2. **Rilevamento e Prevenzione delle Minacce**: Utilizzando un sistema IDS/IPS, il dispositivo deve rilevare e prevenire attacchi informatici come accessi non autorizzati, malware e tentativi di phishing.

2.1.3. **Archiviazione Storica degli Eventi**: Il sistema deve memorizzare gli eventi di sicurezza in un'infrastruttura cloud, consentendo l'accesso a uno storico dettagliato per analisi retrospettive e ottimizzazione delle impostazioni.

2.1.4. **Personalizzazione delle Impostazioni di Sicurezza**: Gli utenti devono poter configurare facilmente le impostazioni di sicurezza tramite un'app mobile, consentendo un alto grado di personalizzazione in base alle loro esigenze specifiche.

2.1.5. **Estensibilità per Future Funzionalità**:La piattaforma deve essere progettata per supportare l'aggiunta di nuove funzionalità in futuro, come un ad-blocker o controlli parentali, per migliorare la sicurezza e la gestione della rete.

2.2. Requisiti non funzionali

2.2.1. **Usabilità e Accessibilità**:L'interfaccia utente dell'app mobile deve essere intuitiva e facile da navigare, consentendo anche agli utenti con competenze tecniche limitate di configurare e monitorare la sicurezza della rete senza difficoltà.

2.2.2. **Scalabilità del Sistema**: Il sistema deve essere in grado di gestire un aumento del numero di dispositivi connessi e dell'intensità del traffico di rete senza compromettere le prestazioni. Inoltre, deve supportare l'aggiunta di nuove funzionalità senza necessità di ristrutturazioni significative.

2.2.3. **Sicurezza dei Dati e Privacy**: Tutti i dati trasmessi e memorizzati devono essere protetti tramite protocolli di crittografia adeguati per garantire la privacy degli utenti e la sicurezza delle informazioni sensibili.

2.2.4. **Affidabilità e Continuità Operativa**: Il sistema deve garantire un'elevata disponibilità, operando senza interruzioni e con un tempo di inattività minimo. Deve inoltre essere in grado di riprendersi rapidamente in caso di guasti o malfunzionamenti.

2.2.5. **Performance**: Il dispositivo deve gestire un elevato volume di traffico in tempo reale, fornendo notifiche e report senza ritardi significativi. Il tempo di risposta dell'app deve essere rapido, permettendo agli utenti di ottenere informazioni tempestive sulle minacce.

2.2.6. **Manutenibilità**: Il sistema deve essere progettato per facilitare la manutenzione e l'aggiornamento. Ciò include l'implementazione di procedure per la gestione delle versioni e la risoluzione dei problemi, consentendo aggiornamenti software e patch di sicurezza senza interruzioni per l'utente finale.

2.2.7. **Interoperabilità**: Il sistema deve essere compatibile con una varietà di dispositivi e protocolli di rete esistenti, garantendo che possa integrarsi facilmente in ambienti di rete eterogenei e supportare diversi standard di comunicazione.

3. Architettura del sistema

3.1. Panoramica dell'architettura

L'architettura del sistema si basa su un modello client-server distribuito, composto da diversi componenti chiave che lavorano insieme per garantire la sicurezza della rete domestica. Di seguito sono descritti i principali elementi architettonici:

1. **Dispositivo di Sicurezza Hardware (IDS/IPS)**:
   - **Funzione**: Questo dispositivo è il cuore del sistema e opera come un punto di controllo per il traffico di rete. Implementa funzionalità di Intrusion Detection System (IDS) e Intrusion Prevention System (IPS) utilizzando software open-source come Suricata.
   - **Caratteristiche**: È dotato di capacità di monitoraggio in tempo reale, analisi del traffico, rilevamento di minacce e prevenzione di accessi non autorizzati. Inoltre, è in grado di registrare eventi di sicurezza per l'analisi retrospettiva.
2. **Infrastruttura Cloud**:
   - **Funzione**: L'infrastruttura cloud è utilizzata per l'archiviazione storica degli eventi di sicurezza, garantendo accesso e disponibilità a lungo termine dei dati. Supporta anche l'analisi avanzata dei dati e l'implementazione di funzionalità predittive.
   - **Caratteristiche**: Include servizi di storage, database e analisi, permettendo di gestire grandi volumi di dati e facilitando l'accesso remoto da parte degli utenti attraverso l'app mobile.
3. **Applicazione Mobile**:
   - **Funzione**: L'app mobile funge da interfaccia utente principale, consentendo agli utenti di monitorare e gestire la sicurezza della loro rete domestica. Gli utenti possono ricevere notifiche in tempo reale, visualizzare report di sicurezza e configurare le impostazioni di sicurezza.
   - **Caratteristiche**: Deve presentare un design intuitivo e reattivo, adattandosi a diversi dispositivi e dimensioni dello schermo. Supporta l'autenticazione sicura e la comunicazione con il dispositivo di sicurezza hardware e l'infrastruttura cloud.
4. **Rete Domestica**:
   - **Funzione**: Comprende tutti i dispositivi connessi (smartphone, tablet, elettrodomestici intelligenti, telecamere di sicurezza, etc.) che interagiscono attraverso il router di rete.
   - **Caratteristiche**: Il sistema deve monitorare tutto il traffico generato da questi dispositivi, identificando comportamenti sospetti e garantendo la protezione della privacy degli utenti.

3.2 Componente hardware

3.2.1 Raspberry PI 4 B

Il Raspberry Pi 4 Model B è una delle versioni più recenti e potenti della popolare serie di microcomputer Raspberry Pi. È stato lanciato nel giugno 2019 e offre una serie di miglioramenti significativi rispetto ai modelli precedenti. Ecco una panoramica delle sue caratteristiche principali e delle applicazioni comuni:

Processore:

- **Tipo**: Quad-core Cortex-A72 (ARM v8) a 1.5 GHz.
- **Prestazioni**: Offre un notevole incremento delle prestazioni rispetto ai modelli precedenti, rendendo il Raspberry Pi 4 adatto per applicazioni più intensive.

Memoria RAM:

- **Opzioni di RAM**: Disponibile in versioni con 2 GB, 4 GB e 8 GB di LPDDR4-3200.
- **Impatto**: Maggiore capacità di RAM consente una migliore gestione di applicazioni multitasking e più complesse, come server e desktop.

Interfacce di I/O:

- **USB**: Due porte USB 3.0 e due porte USB 2.0, che offrono una connettività veloce per dispositivi esterni.
- **GPIO**: 40 pin GPIO (General Purpose Input/Output) per connessioni a sensori, attuatori e altri componenti elettronici.
- **Display**: Supporto per due monitor tramite due porte micro HDMI, fino a 4K a 60 fps.

Connettività:

- **Ethernet**: Porta Ethernet Gigabit per connessioni di rete ad alta velocità.
- **Wi-Fi e Bluetooth**: Supporto per Wi-Fi 802.11ac e Bluetooth 5.0, che garantisce una connettività wireless efficiente.

Alimentazione:

- **Alimentazione**: Utilizza un connettore USB-C per alimentazione, richiedendo un alimentatore da 5V/3A.
- **Consumo Energetico**: Maggiore efficienza energetica rispetto ai modelli precedenti.

Archiviazione:

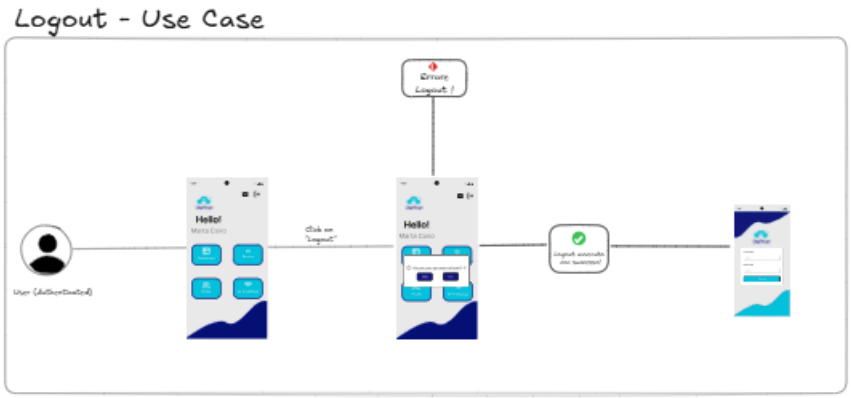
- **Schede microSD**: Utilizza schede microSD per il sistema operativo e l'archiviazione dei dati, con la possibilità di avvio da USB.
- **Opzioni di Archiviazione Esterna**: Supporto per dischi rigidi e unità flash USB per ulteriore archiviazione.

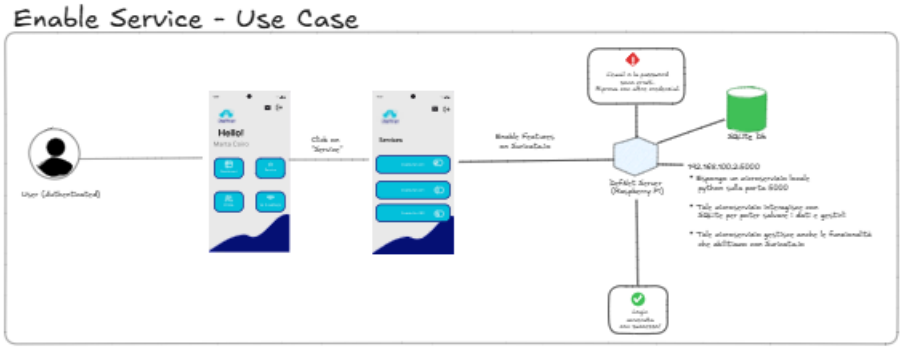
Applicazioni Comuni

- **Progetti Domotici**: Può essere utilizzato come hub per la gestione di dispositivi smart home e sistemi IoT.
- **Media Center**: Grazie alla sua potenza e supporto 4K, è popolare per costruire media center domestici utilizzando software come Kodi.
- **Server Leggeri**: Può funzionare come server web, server di file o server di gioco per applicazioni a bassa intensità.
- **Educazione e Sviluppo**: Ottimo strumento per imparare a programmare e sviluppare progetti di elettronica, data la sua comunità attiva e la vasta documentazione disponibile.
- **Sistemi Embedded**: Utilizzato in progetti industriali e di automazione, dove la compattezza e la versatilità sono fondamentali.

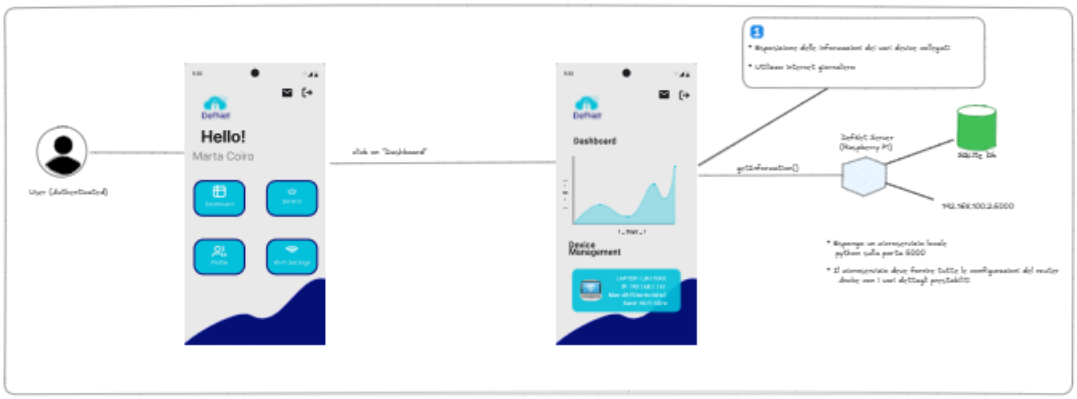
Il Raspberry Pi 4 Model B rappresenta un grande passo avanti nella tecnologia dei microcomputer, combinando potenza, flessibilità e una vasta gamma di possibilità di utilizzo. Grazie alla sua comunità attiva e al supporto per una varietà di sistemi operativi e applicazioni, è una scelta popolare sia per hobbisti che per professionisti.

3.3 Casi d'uso



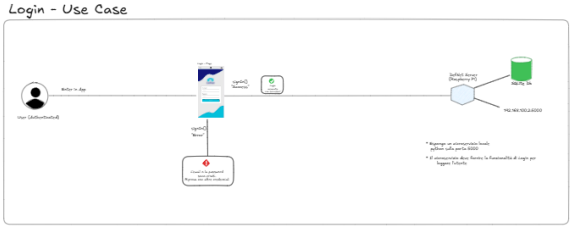


Dashboards - Use Case

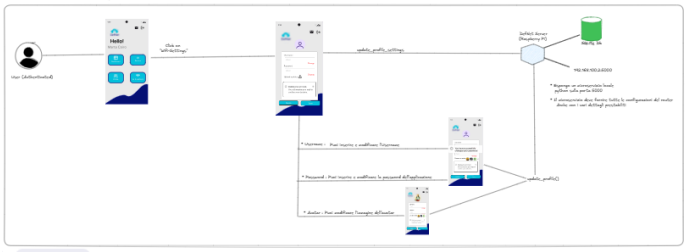


WiFi Settings - Use Case

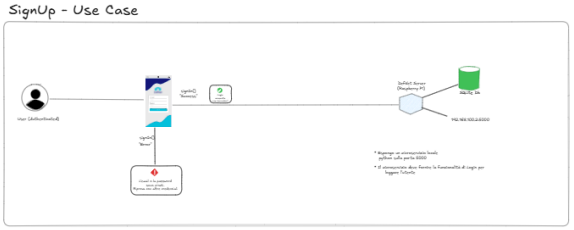
Login - Use Case



Profile Settings - Use Case



SignUp - Use Case



4 Tecnologie utilizzate

Siamo riusciti ad implementare vari attacchi che possono alterare lo stato del dispositivo (**ICMP Flooding**, **Smurf**, **SYN Flooding** e **UDP Flooding**) .

Implementazione di regole di Suricata.io per poter abilitare i servizi sviluppati.

- AdBlocking .
- Identificazione Attacchi effettuati.

Flutter per la realizzazione dell'interfaccia grafica.

Python combinato con FastAPI per realizzare un piccolo microservizio locale.

SQLite per la memorizzazione dei dati su database locale.