UNIVERSITÀ DEGLI STUDI DI SALERNO

Dipartimento di Ingegneria dell'Informazione ed Elettrica e Matematica Applicata

Cybersecurity Mini-Project:

Implementation of a Notification Counter for a Decentralized Contact Tracing DP3T System

Febbraio 2021

Barbella Michele **0622701341**

Ventre Salvatore **0622701343**

ANNO ACCADEMICO 2020-2021

INDICE

1. Proposta di Progetto

Il nostro progetto vuole implementare un contatore che monitori il numero di utenti che sono stati informati di un'esposizione rischiosa dopo l'ultimo rilevamento dell'esposizione (ovvero, dopo che il dispositivo ha scaricato nuove chiavi di esposizione temporanea dal server e ha rilevato se l'utente è stato esposto a utenti SARS-CoV-2 positivi). Questa funzionalità, integrata su un sistema di contact tracing decentralizzato di tipo DP3T, è resa possibile da un'applicazione di contact tracing che, scaricando le chiavi degli infetti da un Server gestito dalle autorità sanitarie, è in grado di verificare se l'utente è stato in contatto con individui risultati positivi e di inviare allo stesso server un incremento del contatore di notifiche generate dal sistema.

1.1 Titolo del progetto

Implementazione di un Contatore di Notifiche per un Sistema di Contact Tracing Decentralizzato di tipo DP3T.

1.2 Entità Coinvolte

- **Cittadino**: utente che usa l'applicazione e che interagisce quotidianamente con il sistema.
- **Servizio Sanitario Nazionale**: ente che ha il compito di gestire un Server di Analisi sul quale sono presenti le chiavi di tutti i cittadini infetti in quel periodo ed un contatore che permetta di conoscere quante notifiche di esposizione ha generato il sistema.
- **Autorità di controllo**: ente che ha il compito di gestire un Server che garantisca al SSN (Servizio Sanitario Nazionale) che l'utente che vuole interagire con esso sia un cittadino in possesso di un'applicazione originale.

1.3 Obiettivi del progetto

Il nostro progetto tratta i seguenti obiettivi:

1. Individuazione delle proprietà di Privacy e di Integrità.
2. Progettazione di un meccanismo per realizzare il contatore.
3. Analisi della progettazione rispetto alle proprietà di Privacy e Integrità.
4. Implementazione di un piccolo modulo che simuli il meccanismo progettato.

2. Descrizione delle Proprietà e degli Avversari

2.1 Proprietà

Quando si parla di sicurezza informatica ci si riferisce allo sviluppo di tre elementi base: Confidenzialità, Integrità e Disponibilità, conosciuti anche con l'acronimo CIA (Confidentiality, Integrity, Availability).

Si vuole impedire che i dati e le informazioni scambiate tra le entità siano manomessi e utilizzati per generare false segnalazioni e di conseguenza inquinare il valore del contatore presente sul Server di Analisi.

Confidenzialità: si intende la protezione dei dati e delle informazioni scambiate tra mittente e destinatario rispetto a individui di terze parti. Questa deve essere realizzata a prescindere dal sistema di comunicazione utilizzato.
Nel progetto, tutti i messaggi inviati dai dispositivi non contengono dati sensibili dell'utente. Inoltre, un avversario che entra in possesso delle informazioni conservate sul server autoritativo non deve essere in grado di ricavarne alcun contenuto informativo comprensibile sull'identità del soggetto.

Integrità: si intende l'abilità di impedire che i dati vengano modificati in modo non autorizzato o indesiderato. Ciò vuol dire che i dati devono essere protetti da modifiche o cancellazioni non approvate.
Nel nostro caso, un avversario non deve essere in grado di fingersi il backend, in quanto questo causerebbe una sottrazione impropria di dati, con la conseguente alterazione non autorizzata del valore del contatore. Inoltre un utente non deve essere in grado di generare una falsa notifica di esposizione, in quanto avremmo inquinamento sulla raccolta dei dati del contatore. Su questo, nel nostro lavoro prevediamo due scenari possibili:

1. Un avversario che utilizza una versione manomessa del software applicativo, che risulta essere differente dall'originale.
2. Un avversario in grado di manomettere l'hardware del dispositivo e di modificare l'applicazione originale.

Disponibilità: fa riferimento alla capacità di avere a disposizione i dati quando se ne ha bisogno. La perdita di disponibilità del servizio può essere riferita ad una grande varietà di errori o malfunzionamenti all'interno di un sistema, che non ci permettono di accedere ai dati.
In questo progetto, quando parliamo di dati, facciamo riferimento a:

1. il valore del contatore presente sul Server di Analisi, utilizzato per monitorare il livello di utilizzo dell'applicazione da parte degli utenti che l'hanno scaricata;
2. le informazioni presenti sul Server dell'Autorità di controllo, che forniscono un modo per autenticare ogni dispositivo che debba interfacciarsi con il Server di Analisi.

La manomissione del contatore di notifiche di esposizione inviate potrebbe causare problemi solo a livello organizzativo. Poiché questi dati sono utilizzati solo a fini statistici, non ci sono rischi diretti nei confronti del cittadino che utilizza questo sistema.
La violazione del Server dell'Autorità di controllo, a sua volta, non potrebbe portare all'individuazione del cittadino, dal momento che le informazioni qui conservate non sono riconducibili all'identità dello stesso.

2.2 Avversari e possibili attacchi

- **Backend Impersonation**: l'attaccante potrebbe impersonificare un backend server ed inviare false informazioni di risposta al dispositivo.
- **Avversario che si impossessa di un ID valido appartenente ad un altro dispositivo**: Un attaccante che, in maniera impropria, entra in possesso del cellulare di un utente che è stato a contatto con un individuo risultato positivo, otterrà un ID valido e utilizzabile per caricare.
- **Utente che spegne il dispositivo o la connessione**: Un avversario potrebbe avere l'obiettivo di impedire l'invio delle informazioni del contatore al Server di Analisi, dopo aver ricevuto la notifica di potenziale esposizione.
- **Utente esperto di tecnologia** (Ghost Attack):
  Un utente malintenzionato può inoltrare più richieste di autorizzazione al Server nell'arco di un tempo relativamente ristretto.
- **Man in the Middle**:
  - Un attaccante potrebbe intercettare i pacchetti sul canale di comunicazione Dispositivo-Server autoritativo.
  - Un attaccante potrebbe intercettare i pacchetti sul canale di comunicazione Dispositivo-Server di Analisi.
  - Un attaccante potrebbe intercettare i pacchetti sul canale di comunicazione Server autoritativo-Server di Analisi.
- **Sybil attack** (False Report attack): un avversario, particolarmente capace, potrebbe essere in grado di manomettere l'App e cambiare le informazioni relative al dispositivo (informazioni hardware del dispositivo che vengono raccolte durante la fase di richiesta di autorizzazione). Dunque, potrebbe emulare la generazione di una notifica di avvenuta esposizione ed esigere una

approvazione di richiesta di autorizzazione dal Server.
Come conseguenza, l’avversario potrebbe inquinare i dati relativi al counter delle notifiche di esposizione.

3. Progettazione del Sistema

3.1 Introduzione

Per realizzare le funzionalità necessarie a far operare l'intero sistema, è stato analizzato, come punto di partenza, il protocollo DP-3T. In particolar modo, dall'analisi del protocollo, sono emersi degli aspetti fondamentali che si è ritenuto opportuno tenere in considerazione nella proposta della soluzione finale:

1. Le informazioni relative all'aggiornamento del contatore vengono caricate senza richiedere all'utente di autenticarsi in alcun modo (inclusa la verifica di un numero di telefono o di un'e-mail).
   L'invio delle informazioni relative al contatore (aggiornamento del contatore sul Server di Analisi) viene effettuato automaticamente appena viene rilevata un'esposizione di rischio. Inoltre, questo garantisce che l'incremento del contatore sul Server di Analisi sia unitario.
   Va sottolineato che lo scaricamento delle nuove chiavi di esposizione, e il rilevamento, viene eseguito ad intervalli regolari di 24 ore.
2. Le richieste di incremento del contatore da parte del dispositivo vengono indirizzate al Server di Analisi, che tramite questi dati può adattare in maniera adeguata le sue capacità di prevenzione.
3. La richiesta di autorizzazione a poter caricare dati sul Server di Analisi viene generata se il Dispositivo in questione è onesto (ovvero che non sia stato manomesso). Infatti, affinché ciò avvenga, la richiesta contiene informazioni relative al dispositivo (codice unico che dipende da fattori hardware e software), ma non relative all'identità della persona.
4. Una volta che il dispositivo incrementa il valore del counter sul Server di Analisi, il meccanismo in locale dovrebbe essere azzerato e dovrebbe ripartire dall'inizio se viene rilevata una nuova esposizione.

3.2 Utilità dei dati

Potrebbe essere necessario chiarire i motivi dell'importanza di raccogliere questi dati: oltre a stimare il livello di adozione del sistema in tutto il paese, favorirebbe il processo di ottimizzazione nell'allocazione delle risorse del SSN in modo efficiente. Inoltre, conoscere la data in cui si è verificata l'ultima esposizione al rischio aiuterebbe a stimare quando possono comparire i sintomi. Tali fattori consentono al Servizio Sanitario Nazionale di adeguare la propria risposta in modo ancora più accurato.

Le Informazioni raccolte dal dispositivo sono:

- data e ora dell'avviso di rischio
- Provincia: costituisce un'informazione utile nello studio sulla misura di diffusione del virus in una determinata area geografica.

3.3 Meccanismo

Al fine di permettere alle autorità sanitarie di avere sentore di come stia progredendo la curva dei contagi, e di quanti utenti effettivamente stiano utilizzando il sistema, prevediamo tale funzionamento:

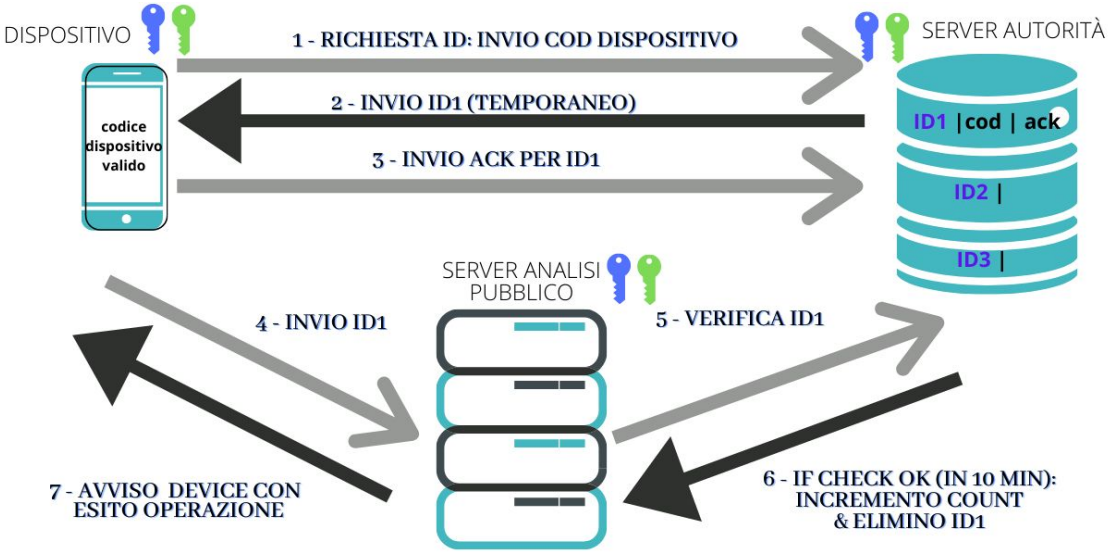

Figura 1: schema delle entità del sistema e delle loro relazioni.

1. Un Dispositivo onesto (che non sia stato manomesso) genera una richiesta di autorizzazione a poter caricare dati sul Server di Analisi. Dunque, invia ad un Server, gestito dall' autorità di controllo, una richiesta di un ID (codice), che servirà per validare il processo di caricamento delle informazioni. Questa richiesta è firmata attraverso la chiave privata del Dispositivo che la invia, in quanto quest'ultimo ha stabilito col Server una connessione sicura attraverso la crittografia asimmetrica.
   Nello specifico, è utile definire le informazioni scambiate tra le due entità:
   - **Richiesta ID**: Il dispositivo invia un codice cifrato che è ottenuto a partire da informazioni relative al dispositivo. Questo codice dipende da fattori hardware, ma non dall'identità della persona. Questo garantisce l'anonimato della persona.

- **ID**: è un codice temporaneo generato dal server, qualsiasi tentativo di convalida dopo la sua scadenza, fallirà. Questo garantisce che l'ID non possa essere utilizzato per identificare in modo univoco un dispositivo.

2. Dopo che la richiesta di autorizzazione (Richiesta ID) ha raggiunto il Server, questo memorizza il codice cifrato del dispositivo e associa a quest'ultimo un ID temporaneo, opportunamente generato, ottenendo dunque un'associazione ID-Cod.

3. Questo ID viene inviato al dispositivo che l'ha richiesto, il quale risponderà al Server dell'avvenuta ricezione, attraverso un ACK. Sul Server, la ricezione dell'ACK, fa partire un timer che contrassegna la validità di quell'ID. Allo scadere del timer, l'ID in questione sarà eliminato.

ID1	COD	ack
XX	COD	ack
-	-	-

4. Il Dispositivo effettuerà una richiesta di aggiornamento al Server di Analisi, attraverso l'invio dell'ID ricevuto. Siccome il sistema prevede l'invio dell'incremento del counter sul Server di Analisi, ogni qual volta venga generata una notifica di esposizione sul dispositivo, il solo invio dell'ID sarà indice di incremento unitario del contatore.

5. Il Server di Analisi, prima di poter accettare la richiesta di incremento in arrivo, ha bisogno di verificare la validità dell'ID. Questo avviene inoltrando l'ID ricevuto in entrata al Server autoritativo e affidando a quest'ultimo il compito della verifica. Infatti, questo Server, dopo aver ricevuto il pacchetto contenente l'ID, effettuerà la seguente verifica: confronta l'ID ricevuto con ogni ID generato (autorizzato) presente all'interno del suo database.
   Ogni associazione ID-Cod presente all'interno del Server è temporanea. Infatti, il Server dopo aver generato e autorizzato un ID, si aspetta di ricevere un riscontro positivo all'interno di una finestra di tempo limitato (es. 10 minuti).

6. Il Server dell'Autorità risponderà al Server di Analisi con:
   a. ***ACK***: se la verifica ha avuto successo.
   b. ***NACK***: se la verifica non ha prodotto riscontro.

Se viene generato un Ack viene rimosso l'ID relativo alla voce ID-Cod, ma non il Cod che persisterà per le successive 24 ore, in modo da garantire che non vengano effettuati caricamenti multipli da un stesso dispositivo nell'arco di tale finestra. Questo è dovuto alla conseguente scelta di eseguire lo scaricamento delle chiavi SK e la rilevazione di esposizione allo scadere di una finestra temporale di 24 ore.
Di conseguenza, il Server di Analisi, in seguito alla risposta affermativa del Server, accetta la richiesta di incremento del contatore.
Viceversa, se il Server risponde con un Nack, il Server di Analisi scarterà il pacchetto, con la richiesta di incremento, ricevuto a sua volta dal dispositivo.
La ricezione di un Nack è dovuta all'assenza di una corrispondenza di un ID sul Server. Questo dipende da due motivi:

- l'ID ricevuto dal Dispositivo non è mai stato generato dal Server.
- l'ID è stato generato dal Server, ma non è stato utilizzato entro i limiti temporali previsti dal sistema e quindi è stato rimossa la relativa voce ID-Cod sul Server, alla scadenza del timer.

In entrambi i casi, il meccanismo prevede di riprovare la richiesta di incremento del contatore con un nuovo tentativo, partendo da una nuova richiesta di un ID.
La rimozione dell'ID in entrambe le circostanze garantisce che il Server abbia un minor carico computazionale nel confrontare le diverse voci all'interno del suo database.

7. In caso di incremento avvenuto con successo, il Server di Analisi comunicherà al dispositivo che tutto il processo è andato a buon fine. Questo fa sì che il dispositivo non riprovi con un nuovo tentativo. Inoltre, le informazioni relative al dispositivo (Cod) presenti sul Server saranno valide per 24 ore dall'avvenuto incremento, questo impedisce caricamenti multipli durante la stessa giornata.
   In caso contrario, il Server di Analisi comunica al dispositivo che il processo non è andato a buon fine. Come conseguenza, il Dispositivo proverà ad effettuare l'incremento del contatore con un nuovo tentativo, ripetendo il processo dall'inizio.

3.4 Canali di Comunicazione

Per una migliore comprensione sulle comunicazioni che intercorrono tra le varie entità coinvolte nel sistema, in questo paragrafo, vengono descritte le principali caratteristiche dei canali di comunicazione.
In particolar modo, definiamo:

- ➢ Canale Sicuro: le informazioni che vengono trasmesse e ricevute su questo canale sono cifrate. Almeno una tra le due identità in comunicazione (Sender, Receiver) non viene determinata, ovvero non è riconosciuta da un certificato digitale.
- ➢ Canale Autenticato: è un canale sicuro, in quanto le informazioni in transito sono cifrate ed inoltre, entrambe le entità (Sender, Receiver) attestano la loro identità attraverso un certificato digitale.

Tutte le entità presenti all'interno del sistema sono dotate di una coppia di chiavi Pubblica-Privata. Questo permette di attuare tutti i concetti di crittografia asimmetrica.

- Dispositivo - Server Autorità di controllo: canale Sicuro
    a. Le informazioni che viaggiano dal dispositivo al server sono cifrate in quanto il dispositivo usa la chiave pubblica del Server per inviare le informazioni.
    b. Le informazioni di ritorno (Server-dispositivo) sono cifrate. Il Server cifra le informazioni attraverso la chiave pubblica del dispositivo. Inoltre, il Dispositivo può fidarsi del Server in quanto quest'ultimo dispone di un Certificato (chiave PubK-PriK con relativa firma).

- Dispositivo - Server Analisi: canale Sicuro
    a. Le informazioni che viaggiano dal Dispositivo al Server di Analisi sono cifrate in quanto il dispositivo usa la chiave pubblica del Server di Analisi per inviare le informazioni.
    b. Le informazioni di ritorno (Server di Analisi - Dispositivo) sono cifrate. Il Server di Analisi cifra le informazioni attraverso la chiave pubblica del Dispositivo. Inoltre, il dispositivo può fidarsi del Server di Analisi in quanto quest'ultimo dispone di un Certificato (chiave PubK-PriK con relativa firma).

- Server Analisi - Server Autorità di controllo: canale Autenticato (e dunque Sicuro)
    a. Entrambi i server dispongono di Certificati Digitali validi che attestano la loro identità. Le comunicazioni attraverso il canale avvengono in modo sicuro e cifrato, garantendo autenticazione, integrità dei dati e confidenzialità.

4. Analisi del Sistema Proposto

In questa sezione, vengono descritte nel dettaglio le soluzioni ai possibili attacchi che sono stati introdotti nel capitolo 2 del documento. Per ciascuno di essi analizziamo il tipo di rischio che rappresentano per il sistema e come è possibile mitigare o annullare tale minaccia.

4.1 Proprietà

- **Confidenzialità**:
  Tutte le comunicazioni tra:
  - dispositivo e Server dell'Autorità,
  - dispositivo e Server di Analisi,
  - Server dell'Autorità e Server di Analisi,

  sono protette dal protocollo TLS 1.2 o superiori. Ciò rende impossibile leggere o modificare le informazioni contenute nei messaggi scambiati, dal momento che TLS fornisce un canale cifrato e autenticato. Quindi la privacy riguardante il contenuto dei messaggi è garantita.
  In particolare, i due attori della comunicazione scelgono quindi una cipher suite ed effettuano uno scambio di chiavi per renderla cifrata e autenticata.

  L'anonimato degli utenti del sistema è garantito creando sul Server dell'Autorità di controllo una corrispondenza tra l'ID temporaneo assegnato da quest'ultimo e la cifratura del codice che individua un particolare dispositivo valido per 24 ore.
  L'unico modo per ottenere i dati relativi ai codici dei singoli dispositivi sarebbe realizzabile compiendo un attacco di forza bruta di complessità computazionale nell'ordine di 2^n, con *n* la lunghezza in bit della chiave di cifratura utilizzata dal server autoritativo oppure rompendo lo schema di cifratura usato dal server dell'autorità medica.

  Un'autorità malevola o un qualsiasi avversario che può accedere in lettura ai Database presenti sui due server potrebbe voler capire a quali utenti appartengono queste informazioni, ma anche ottenendo tutto ciò che è memorizzato su queste basi di dati, è impossibile estrapolare da tali dati informazioni sull'identità dei cittadini.

- **Integrità**:
  Questa proprietà è garantita affidando al Server autoritativo il ruolo di root CA in

grado di fornire certificati. Il Server di Analisi è in possesso di un certificato rilasciato dalla root CA. Questo garantisce che la connessione da parte di un dispositivo verso ciascun Server coinvolto nel sistema, avvenga attraverso uno scambio di messaggi, assoggettato all'utilizzo di un certificato valido.
Inoltre, per garantire questa proprietà, è opportuno introdurre dei meccanismi che assicurino che non vi sia nessun tipo di manomissione, lato hardware e software del dispositivo. Infatti, si fa affidamento a sistemi come SafetyNet (Dispositivi Android su cui è presente Google Play Services v13.0 e superiori) che permettono una verifica sulla correttezza e sicurezza del dispositivo.

- **Disponibilità**:
  il corretto funzionamento del sistema deve essere garantito anche per l'operazione di invio degli ID, da parte del Server dell'autorità di controllo, sul dispositivo che voglia incrementare il contatore, interagendo con il sistema. Nonostante l'operazione da eseguire non sia particolarmente difficile, è comunque opportuno che il Server sia in grado di gestire una grande quantità di richieste in ingresso, in modo da gestire situazioni che prevedano ondate di contagi molto vaste (e dunque molte notifiche di esposizione).
  La disponibilità e la correttezza del valore del contatore sul Server di Analisi, viene garantita dal momento che è possibile effettuare incrementi del counter solo attraverso un ID valido, che viene verificato in ogni caso dal Server dell'autorità. La sua manomissione potrebbe causare problemi limitati al solo livello organizzativo. Inoltre, va anche sottolineato che la disponibilità del dato sarebbe compromessa se una buona percentuale degli utenti spegnesse il dispositivo, il che significherebbe avere anche il sistema di tracciamento della prossimità non funzionante.

4.2 Avversari e possibili contromisure

- **Backend Impersonation**: i Server sono dotati di certificati, rilasciati da una rootCA e pertanto possono dimostrare la loro identità.
- **Avversario che si impossessa di un ID valido appartenente ad un altro dispositivo**: questo attacco è parzialmente mitigabile in quanto l'attaccante avrebbe a disposizione solamente un periodo di tempo limitato per effettuare la sottrazione dell'ID in questione. Questo è dovuto al fatto che la validità di un ID generato sul Server è limitata ad un intervallo di tempo ristretto (ad esempio come menzionato precedentemente: 10 minuti). Dopo la scadenza di tale

intervallo, l'ID, seppur generato in maniera attendibile, non viene considerato più valido.

- **Utente che evita l'invio della notifica di incremento**: questo attacco non è contrastabile ed è equivalente ad un utente che spegne il dispositivo o che disabilita la connessione. Poiché il meccanismo da noi progettato prevede che il processo parta non appena l'utente del sistema abbia letto e accettato la notifica di esposizione, se questo spegne il telefono o disabilita la connessione non darà modo al sistema di iniziare il suo processo.
- **Utente esperto di tecnologia (Ghost Attack)**: il Server memorizza le informazioni del dispositivo che sono presenti nella richiesta di autorizzazione (codice univoco). Inoltre, tutti i pacchetti provenienti da uno stesso Dispositivo, presenteranno sempre lo stesso Codice, in quanto questo dipende da fattori puramente hardware. Dunque, il Server non effettuerà più di un'associazione ID con quella specifica richiesta nell'arco di tempo che intercorre tra un rilevamento dell'esposizione ed il successivo (24h). Questo controllo è implementato solo per bloccare potenziali avversari, infatti, il sistema prevede lo scaricamento degli SK infetti solo una volta al giorno, di conseguenza anche l'incremento del contatore può avvenire solo dopo che saranno trascorse 24 ore dall'ultimo match.
- **Man in the Middle**: un utente malintenzionato, pur intercettando le informazioni in transito sul canale, non potrebbe leggerle in nessun modo in quanto crittografate attraverso un sistema a crittografia asimmetrica. (Il Sender cifra le informazioni utilizzando la chiave pubblica del Receiver).
- **Sybil attack (False Report attack)**: in questo caso è opportuno considerare due scenari:
    - ➢ Controllo solo hardware: l'avversario che ottiene la manomissione della sola generazione delle notifiche (software), ma non quella relativa alla modifica delle informazioni hardware del dispositivo, avrebbe come conseguenza quella di inviare una richiesta di incremento del contatore al Server di Analisi, solo una volta al giorno, tutti i giorni. Questo perchè il Server dell'autorità conserva il Codice (che ha dipendenze hardware del Dispositivo) al suo interno per 24 ore dall'avvenuto incremento.
      Questo comporterebbe, comunque un inquinamento dei dati, ma sarebbe limitato. (avversario limitato)
    - ➢ SafetyNet (controllo hardware e software): il sistema operativo del dispositivo usa delle misure anti-abuso progettate per valutare l'integrità del meccanismo del contatore, e del dispositivo su cui viene eseguito tale meccanismo. Queste misure anti-abuso possono prevedere dei controlli basati sull'hardware e sul software (applicazione in uso), in modo da impedire tecniche di aggiramento o contraffazione dell'hardware del

dispositivo o che prevedano la manomissione dell’applicazione originale. Questo permette di mitigare totalmente l’attacco.

5. Implementazione

In questa sezione si vuole descrivere la realizzazione di un modulo crittografico e la simulazione di una parte del funzionamento del sistema, che è stato realizzato al fine di presentare quanto precedentemente discusso.

Si è scelto di implementare tutta la comunicazione che avviene a partire da quando il dispositivo riceve un ID dal Server dell'autorità ed ha, quindi, i requisiti per effettuare l'invio dell'incremento del contatore al Server di Analisi.
In particolar modo, il progetto ha visto come implementazione la comunicazione rappresentata in questo schema:

- **Dispositivo**: simula la generazione di una notifica in locale e, dopo aver richiesto ed ottenuto un ID valido (processo omesso in questa dimostrazione), invia la richiesta di incremento del contatore attraverso l'invio dell'ID al Server di Analisi (*passo 1*). Successivamente, attende il riscontro della sua richiesta (*passo 4*).

- **Server di Analisi**: gestisce la ricezione dell'ID inviato dal dispositivo. Prima di effettuare l'aggiornamento del contatore, inoltra tale ID al Server gestito dall'autorità per verificare se è un ID assegnato da quest'ultima e se è valido (*passo 2*). In seguito, attende la risposta (ACK o NACK) da parte del Server dell'autorità, in modo da aggiornare o scartare l'incremento del contatore delle notifiche. Infine, risponde al dispositivo con l'esito dell'operazione eseguita (*passo 4*).

- **Server dell'Autorità**: gestisce la ricezione dell'ID inviato dal Server di Analisi e controlla la validità dello stesso in base alle informazioni ad esso associate contenute nel suo database. In seguito, risponde attraverso un ACK o un NACK

al Server di Analisi (*passo 3*), a seconda se l'operazione ha avuto successo o meno. Inoltre, si occupa di eliminare eventuali voci non più valide, presenti all'interno del database.

5.1 Configurazione

Per garantire una trasmissione di informazioni in modo criptato e sicuro tra le entità in gioco si è deciso di utilizzare i certificati SSL.
Per automatizzarne la creazione, utilizziamo lo script ***configurationScript.sh***. Questo file permette di creare un certificato autofirmato utilizzato dal Server dell'autorità (Root CA) ed un certificato rilasciato ad un Server intermedio (Intermediate CA). Questi certificati garantiscono la comunicazione sicura delle entità protagoniste nel nostro progetto, poichè ognuna di loro prima di stabilire una connessione, ne verifica la validità.

Sono stati prodotti due file di configurazione OpenSSL. Questi file, forniscono delle impostazioni predefinite per elementi come i nomi relativi all'entità del certificato, i parametri relativi alla sicurezza, la posizione dei file del certificato, ed altro. In particolare, i due file sono:

- *configCA.cnf*
- *configAnalyticsServer.cnf*

ed hanno il compito di configurare il Server delle autorità (*configCA*) e il Server di Analisi (*configAnalyticsServer*). Ognuno è stato creato partendo dal file di configurazione di default, che mette a disposizione OpenSSL, e adattandolo alle specifiche del nostro sistema. Infatti, sono stati ritoccati i parametri di sicurezza e quelli relativi all'identità.

5.2 Simulazione

Per la simulazione del sistema è necessario utilizzare un sistema Linux, in quanto è necessario eseguire dei comandi da terminale.
Come già precedentemente menzionato, è stato realizzato uno script di configurazione ***configurationScript.sh***, che ha lo scopo di inizializzare l'ambiente di lavoro per una nuova esecuzione della simulazione. In particolare, l'azione di questo script è quella di installare le librerie necessarie (nel caso non siano già presenti nel sistema), rimuovere i file vecchi relativi a configurazioni precedenti, creare un nuovo albero delle directory,

creare nuovi certificati per le entità e firmarli, azzerare il contatore delle notifiche di esposizione, infine creare un nuovo database e popolarlo.

Dunque per prima cosa, è opportuno posizionarsi all'interno della directory del progetto ed eseguire questo comando: ***./configurationScript.sh***
Dopo l'esecuzione dello script iniziale, per simulare l'intero funzionamento del sistema è necessario lanciare tre istanze di terminale. L'azione da fare è quella racchiusa nei seguenti comandi:

- Terminale 1:
  cd authorityServer/
  python3 authorityServer.py

- Terminale 2:
  cd analyticsServer/
  python3 analyticsServer.py

- Terminale 3:
  cd client/
  python3 client.py

Lo scopo è quello di lanciare tre terminali, ognuno dei quali preposto ad eseguire lo script relativo ad una entità. Abbiamo, dunque, una prima istanza che eseguirà il codice relativo al Server delle autorità, una seconda che simulerà il comportamento del Server di Analisi ed, infine, una terza che eseguirà lo script che simula il comportamento dei dispositivi di più cittadini.
Lo script è stato pensato in modo da simulare diversi casi:

- cittadino avente un ID valido, questo implica il conseguente incremento del contatore delle notifiche di esposizione.
- cittadino avente un ID non valido in quanto scaduto, con conseguente scarto del pacchetto da parte del Server di Analisi.
- avversario avente un ID non presente sul Server, anche in questo caso la richiesta di incremento sarà ignorata dal Server di Analisi.

Gli script *python* contengono anche un controllo sul certificato (generato da *configurationScript.sh*) che viene ricevuto dalle varie entità. In caso di certificato non valido, verrà mostrato nell'output del terminale un messaggio di warning che attesta la non validità del certificato.
Inoltre, durante tutta la simulazione, i due Server, mostrano come output i parametri di

connessione che sono stati stabiliti durante la fase di *handshaking*, eventuali messaggi di ACK o NACK ricevuti e i messaggi che mostrano la verifica della ID.

Va sottolineato che è stato implementato un altro script che automatizza il processo di lancio della demo nel caso si stia lavorando con un *sistema operativo Linux Ubuntu*. Quindi invece di lanciare i tre terminali con i rispettivi comandi, dopo lo script iniziale, l'unico comando da lanciare è il seguente: ***./runSimulation.sh***