Progetto di Algoritmi e Protocolli per la Sicurezza

Davide D'Acunto Noemi Biancamano

Gruppo 9

Indice

1 WP 1: Modello

La seguente sezione si occupa di descrivere gli attori onesti presenti nel sistema, evidenziando le attività che sono interessati a svolgere.
Successivamente, si procede alla discussione degli avversari e del threat model considerato, andando a specificare le capacità e le risorse da essi possedute. Infine, si presentano le proprietà che devono essere possedute dal sistema al fine di essere resiliente agli attacchi considerati.

1.1 Attori & Obiettivi

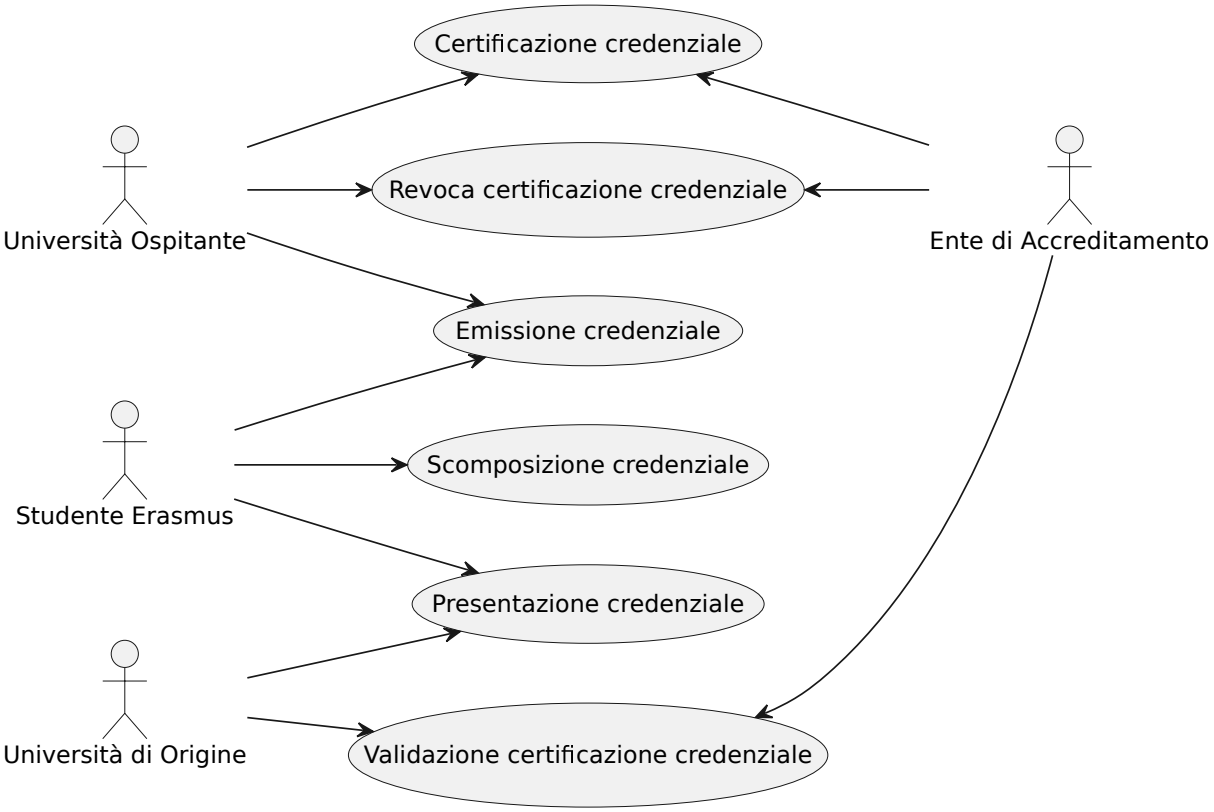

Figura 1: Use Case degli attori onesti

1.1.1 Studente Erasmus

Lo studente Erasmus è interessato a sostenere attività accademiche all'interno della sede ospitante, le quali devono essere poi certificate e dimostrate all'università di origine.

Richiesta credenziale Per cui lo studente necessita dall'università ospitante una credenziale accademica, che attesti le attività da egli effettuate all'interno dell'università ospitante durante il periodo di mobilità.

Trasmissione credenziale Tale credenziale dev'essere successivamente fornita all'università di origine per certificare le attività svolte dallo studente in sede ospitante.

Condivisione selettiva Tuttavia, lo studente potrebbe desiderare di comunicare solamente un sottoinsieme delle informazioni contenute all'interno della credenziale, in maniera tale da dimostrare il rispetto dei criteri dell'accordo di mobilità e non rivelare informazioni personali superflue.
Si suppone che le risorse computazionali dello studente siano limitate.

1.1.2 Università Ospitante

L'università ospitante, accordatasi con l'università di origine, permette a vari studenti erasmus di poter usufruire di un periodo di mobilità all'interno della sua sede, nel quale gli studenti hanno la possibilità di effettuare varie atttività accademiche.

Emissione credenziale La sede è interessata a certificare, per ogni studente in mobilità da essa, le attività svolte da questo attraverso una credenziale, cosicché egli sia in grado di comunicarle successivamente alla sua sede d'origine.

Interoperabilità credenziale Siccome l'università ospitante non conosce i criteri definiti dall'accordo di mobilità per ciascuno degli studenti, inserisce nelle credenziali tutte le informazioni relative alle attività accademiche dallo studente, sicché sia poi in grado di poterle comunicare all'università di origine.

Certificazione credenziale L'ateneo inoltre desidera dimostrare che la credenziale è stata effettivamente emessa da sé, per cui richiede all'ente di accrediamento la certificazione dell'avvenuta emissione, che fornisce allo studente congiuntamente alla credenziale.

Revoca certificazione Infine, in particolari casi laddove si verifichino errori amministrativi, oppure lo studente fornisca dati fraudolenti e/o cometta plagio o frode, l'università ospitante deve essere in grado di invalidare la credenziale revocando il certificato, attraverso l'ente di accreditamento.

1.1.3 Università di Origine

L'università di origine è accordata con l'università ospitante, mentre con lo studente attraverso un accordo di mobilità. All'interno di questo vengono definite tutte le attività accademiche che lo studente è richiesto soddisfare per validare il suo periodo di mobilità.

Presentazione credenziale Per cui si aspetta di ricevere, da ciascuno studente che ha terminato il proprio periodo di mobilità, una credenziale nella quale sono presenti almeno le attività definite dall'accordo di mobilità.

Validazione credenziale Inoltre, la credenziale deve essere certificata da un ente di accreditamento, cosicché si abbia la certezza della validità di questa. Qualora la credenziale non fosse certificata, oppure la certificazione è invalida o revocata, l'ateneo è in grado di rifiutare la credenziale.

1.1.4 Ente di accreditamento

L'ente di accreditamento è un'autorità esterna, che si occupa di certificare le credenziali emesse dalle università, in modo tale da garantirne validità e autenticità.

Archiviazione certificati Non solo, si occupa anche dell'archiviazione delle certificazioni associate alle credenziali, conservandole sino ad una determinata data, ed eventualmente si rende disponibile ad informare gli atenei della revoca di una certificazione.

Definizione formato Infine, l'ente stabilisce, congiuntamente con le università, il formato delle credenziali, a cui gli atenei devono attenersi per essere in grado di emettere credenziali universali.
Si suppone che l'ente di accreditamento sia affidabile e che possieda alte risorse computazionali.

1.2 Credenziale

La credenziale è un documento contenente le informazioni relative alle attività accademiche che lo studente in mobilità ha svolto nella sede ospitante.
Le informazioni contenute all'interno della credenziale sono le seguenti:

- Matricola interna dello studente
- Nome e cognome dello studente
- Matricola esterna dello studente
- Codice e nome dell'università ospitante
- Nome e cognome del referente dell'università ospitante
- Nome e cognome del referente dell'università di origine
- Periodo di mobilità
- Per ciascun esame sostenuto:
    - Nome e codice dell'esame
    - Eventuale voto espresso in trentesimi, oppure esito
    - Eventuale lode
    - CFU conseguiti
    - Data di superamento dell'esame
    - Nome e cognome del docente
    - Nome e codice del corso di laurea
- Per ciascuna attività svolta:
    - Nome e codice dell'attività
    - Periodo di inizio e fine dell'attività

- Eventuali CFU dell'attività
- Nome e cognome del docente o del referente

Le università devono attenersi a questo formato per assicurare l'interoperabilità delle credenziali emesse.

1.3 Threat Model

Come threat model si considerano avversari in grado di compromettere il sistema in un determinato attacco, dipendente dalle risorse e capacità da essi possedute, andando a definire quale sia la proprietà che viene meno laddove il sistema non sia resiliente a tale attacco.
Ciascun attaccante viene considerato efficiente e probabilistico, ovvero con una determinata probabilità di avere successo nell'intento in tempo polinomiale.

1.3.1 Ascoltatore tra studente e università

Si considera un attaccante in grado di ascoltare le comunicazioni che avvengono tra le università e lo studente, cercando di carpire le credenziali scambiate tra gli attori, cosicché da avere accesso a informazioni riservate dello studente.
A questo punto, la proprietà compromessa è la confidenzialità delle credenziali, in quanto, sebbene possedere la credenziale di per sé non rappresenti un pericolo, l'attaccante è in grado di leggere informazioni sensibili dello studente contenute in questa.

1.3.2 Intercettatore tra studente e università

Si considera un attaccante in grado di compromettere le comunicazioni tra gli attori, alterando le credenziali durante la loro trasmissione. L'attaccante potrebbe manipolare le informazioni contenute nelle credenziali, invalidandole o cambiando i dati in esse contenuti.
In questo caso, la proprietà violata è l'integrità delle credenziali, siccome si perde la garanzia che il contenuto sia originale, ovvero che non sia stato alterato durante la trasmissione.
In questo modello si aggiunge anche il caso di uno studente malevolo che tenta di fornire una credenziale alterata, non originale, o che venga impersonato dall'attaccante. In queste circostante, l'attaccante potrebbe fornire credenziali errate o alterate, per tentare di validarle.
Sebbene non rappresenti una minaccia importante, vi è comunque la perdita della proprietà di autenticita dei messaggi dello studente.

1.3.3 Intercettatore tra università e ente di accreditamento

Si considera un attaccante in grado di compromettere le comunicazioni tra l'università e l'ente di accreditamento, alterando le credenziali durante la loro trasmissione. Nel seguente caso, l'attaccante potrebbe manipolare le informazioni contenute nelle credenziali, invalidandole o cambiando i dati in esse contenuti, portando l'ente di accreditamento a rigettare il messaggio, o peggio a certificare credenziali false o alterate.
La proprietà infranta è l'integrità delle credenziali, siccome si perde la garanzia che il contenuto sia originale, ovvero che non sia stato alterato durante la trasmissione.

Infine, in questo modello si considera anche il caso di un attaccante che si frapponga nella comunicazione, assumento le parti dell'università dal punto di vista dell'ente di accreditamento, e viceversa. In queste circostanze, l'attaccante che assume le sembianze dell'università ospitante è in grado di:

- Alterare la credenziale, per ottenere una certificazione valida di una credenziale alterata
- Bloccare la comunicazione, per evitare che l'università possa certificare una credenziale valida o revocare una certificazione
- Revocare una certificazione valida

Riguardo invece l'università di origine, l'attaccante potrebbe:

- Validare una certificazione invalida
- Invalidare una certificazione valida
- Bloccare una richiesta di validazione, per evitare che l'università possa validare una credenziale

Per cui si aggiunge anche una perdita della proprietà di autenticità delle credenziali, in quanto non si ha la certezza che la credenziale sia stata emessa da un'autorità competente.

1.4 Definizioni formali

In questa sezione riportiamo le definizioni formali delle proprietà predentemente citate.
Lo schema di cifratura di riferimento utilizzato per le formalizzazione delle proprietà successive è $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, dove:

- Gen è l'algoritmo di generazione di un determinato numero di chiavi, necessario alla cifratura e decifratura dei messaggi, la cui sicurezza dipende dal parametro di sicurezza n.
- Enc è l'algoritmo di cifratura, che produce un messaggio cifrato, detto cyphertext c, a partire da un messaggio in chiaro, detto plaintext m.
- Dec è l'algoritmo di decifratura, che produce un messaggio in chiaro, a partire da un messaggio cifrato.

Con $\mathcal{A}$ indichiamo un attaccante

1.4.1 Confidenzialità

La confidenzialità è la proprietà che assicura l'accesso alle informazioni solamente a chi autorizzato. Un individuo non autorizzatto non deve essere in grado di accedere ad alcuna informazione, neanche parziale.
Si esprime la proprietà di confidenzialità tramite l'esperimento $\mathsf{Exp}^{\mathsf{conf}}_{\mathcal{A},\Pi}(n)$,

1.4.2 Integrità

1.4.3 Autenticità

2 WP 2

Describe your methodology here.

3 WP 3

Describe your methodology here.

4 WP 4

Describe your methodology here.