Progetto di Algoritmi e Protocolli per la Sicurezza

Davide D'Acunto Noemi Biancamano

Gruppo 9

Indice

1 WP 1: Modello **1**
- 1.1 Attori & Obiettivi . . . 2
  - 1.1.1 Studente Erasmus . . . 2
  - 1.1.2 Università Ospitante . . . 2
  - 1.1.3 Università di Origine . . . 2
  - 1.1.4 Ente di accreditamento (CA?) . . . 3
- 1.2 Threat Model . . . 3
  - 1.2.1 Ascoltatore comunicazioni credenziali . . . 3
  - 1.2.2 Intercettatore comunicazioni credenziali . . . 3

2 WP 2 **3**

3 WP 3 **3**

4 WP 4 **3**

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

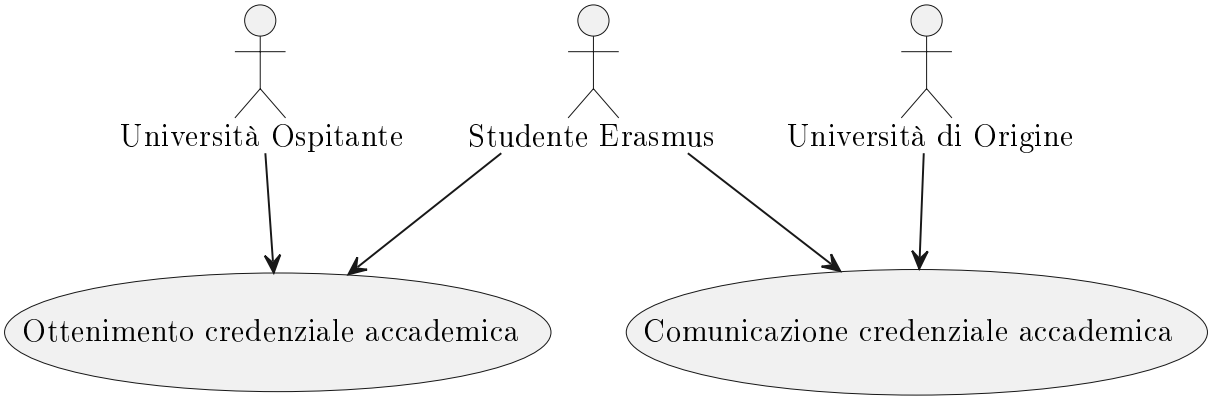

Figura 1: Use Case degli attori onesti

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; per cui necessita dall'università ospitante una credenziale accademica, che attesti le attività da egli effettuate all'interno dell'università ospitante durante il periodo di mobilità.
Tale credenziale dev'essere successivamente fornita all'università di origine per certificare le attività svolte dallo studente in sede ospitante. 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.

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.
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.
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.

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 di soddisfare per validare il suo periodo di mobilità.
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.

1.1.4 Ente di accreditamento (CA?)

1.2 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.

1.2.1 Ascoltatore comunicazioni credenziali

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.
In questo caso, 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.

1.2.2 Intercettatore comunicazioni credenziali

Si considera un attaccante in grado di compromettere le comunicazioni tra gli attori, alterando le credenziali durante la loro trasmissione. In questo caso, 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.

2 WP 2

Describe your methodology here.

3 WP 3

Describe your methodology here.

4 WP 4

Describe your methodology here.