Security by Design: Progetto Sistemi Autenticazione

Oggigiorno la quasi totalità delle soluzioni IT si basano su architetture web.

Nella maggior parte dei casi tali soluzioni prevedono l'autenticazione di utenti su un Front-End di presentazione che interagisce con un sistema Back-End sul quale sono memorizzati database e procedure/algoritmi.

Nel corso di questo progetto verranno applicate le tecnologie di autenticazione e di identificazione in due ambiti:

a. un piccolo progetto dimostrativo dei sistemi di autenticazione di utenti a diversi livelli (password, multi-factor authentication);
b. un piccolo progetto che mostri l'applicazione dei sistemi di autenticazione per rendere sicure le API (Application Programmin Interface).

Particolari aspetti da considerare valutando i rischi delle diverse architetture:

- Quali informazioni vengono utilizate.
- Dove vengono salvate queste informazioni (file sul Back-End, file sul Front-End, cookies, tokens, …).
- Quali verifiche vengono effettuate e a quale stadio di autenticazione.

1. Studiare casi distinti d'applicazione per autenticazione di utenti che fanno uso di multi-factor authentication quali ad esempio:

   - l'architettura PostFinance Mobile ID,
   - un'architettura che faccia uso di autenticazione mTAN,
   - un'architettura Photo-TAN,
   - un'architettura che faccia uso di biometria per il mobile banking.

   Descrivere il flusso di informazione di queste architetture nelle fasi di user authentication (non di user registration).

   Spiegare vantaggi e svantaggi a livello di costi di implementazione di architetture del genere.

© A. Consoli
SUPSI DTI
Riproduzione vietata
Viganello, 2022

2. Comunicazione tra applicazione e infrastrutture eterogenee: come rendere sicura una API. A differenza del punto precedente questa soluzione prevede un progetto pratico di sviluppo di una applicazione delle tecniche da studiare.

   Cercare e documentare le principali alternative di autenticazione (JWT, OAUTH, SAML). Una buona base per iniziare può essere il link seguente: https://www.kelltontech.com/kellton-tech-blog/api-security-design-patterns

3. Realizzare un piccolo progetto che faccia uso di JWT, JWE, JWS o JWK quali access token (esempio di riferimento: RFC 7518).

   Il linguaggio e l'ambiente di sviluppo possono essere scelti liberamente dal gruppo di lavoro (2 studenti).

   L'applicazione deve essere in grado di dimostrare tutte le fasi di registrazione, autenticazione e uso dei token.

4. Studiare il framework di autorizzazion OAUTH2 partendo dai seguenti link https://auth0.com/docs/authorization/protocols/protocol-oauth2

   https://auth0.com/docs/authorization/flows/call-your-api-using-the-authorization-code-flow

   Spiegare le differenze principali tra OAUTH2 e JWT.

5. Per i sistemi JWT usati in questa esercitazione teorica e di laboratorio, quali rischi per la privacy si possono identificare?
   Sarebbe possibile implementare una contromisura che garantisca una migliore privacy?

© A. Consoli
SUPSI DTI
Riproduzione vietata
Viganello, 2022