Informatica- Prof. Cristina Gena

Alessandro Lucci

2023

1. Web Usability

L'usabilità riguarda seguire una serie di principi che ci permettono di evitare degli errori di progettazione. L'idea è che quando un sistema è generato bene dalla parte dell'usabilità l'utente non deve porsi molte domande(l'utente capisce tutto al volo).

Le componenti dell'usabilità sono:

1. **Appredabilità** Quanto è semplice usare il prodotto per la prima volta.

2. **Efficienza**: Quanto velocemente l'utente puo raggiungere gli obiettivi?

3. **Soddisfazione**: Quanto positiva è l'esperienza?

2. Accessibilità

3. Crittografia

La crittografia è la tecnica di nascondere informazioni ne esistono di 2 tipi:

1. **Simmetrica**, quando la chiave è la stessa usata da mittente e destinatario (cifrario mnoalfabetico)

2. **Asimmetrica**, ogni utente usa due chiavi diverse ma corrispondenti: una pubblica e una privata (smartcarrd)

Tipicamente la cifratura assiemtrica è più lenta della cifratura simmetrica.Dato che la cifratura asimmetrica è più lenta della cifratura simmetrica, di solito vengono abbinate: si usa la cifratura asimmetrica per scambiarsi la chiave simmetrica

RSA

L'Rsa è un sistema a chiave pubblica basato sui numeri primi, che si usa per autenticazione e per garantire integrità.

Funzioni di Hash

Sono funzioni matematiche che a partire da una sequenza di bit restituiscono un riassunto di una sequenza di bit, le funzioni di cash godono di due proprietà:

1. Complicato trovare due oggetti che abbiano lo stesso riassunto

2. Complicato trovare un oggetto che produca quel riassunto

HTTPS

Basa il suo funzionamento sulla cifratura simmetrica, asimmetrica ei certificati; ha vari livelli di sicurezza come il server autenticato con comunicazione diretta.

Il funzionamento del HTTPS è come segue:

1. Il server si autentica inviando il proprio certificato di chiave pubblica

2. Il browser verifica che l'URL del server coincida con l'identità contenuta nel certificato

3. Il browser usando la chiave pubblica del server condivide una chiave simmetrica temporanea

Questo garantisce **autenticazione** del server e **confidenzialità** della comunicazione. Non fornisce altre garanzie.

4. Sicurezza nelle reti locali

4.1 Intranet

Con intranet s'intende l'uso delle tecnologie internet per riorganizzare il modo di comunicare e lavorare interno all'azienda. Si tratta di una rete privata, limitata agli elaboratori interni all'azienda, cui spesso i dipendenti possono connettersi anche dall'esterno.

4.2. Extranet

Con questo termine si indica una rete virtuale con un insieme di servizi accessibili non soltanto all'interno di un'azienda ma anche da parte di aziende partner. (Evoluzione dei sistemi EDI con cui le aziende partner possono scambiarsi richieste e altre informazioni)

4.3. Caratteristiche della comunicazione sicura

1. **Disponibilità del servizio:** il messaggio arriva a destinazione
2. **Privatezza**: le informazioni del messaggio sono disponibili solo al destinatario
3. **Autenticazione e integrità:** il messaggio proviene dal mittente dichiarato e non contiene alterazioni
4. **Non disconiscibilità** : il mittente non può negare di avere trasmesso il messaggio

4.3. Firewall

É un componente passivo di difesa che garantisce una protezione in termini di sicurezza informatica della rete stessa. La rete viene divisa in 3 sottoreti:

1. Quella esterna che comprende internet
2. LAN: che comprende una sezione di computer locali.
3. DMZ: ovvero un segmento isolato di LAN collegati a server pubblici, raggiungibile sia da reti interni sia da reti esterne e caratterizzate dal fatto che gli host attestati sulla DMZ hanno possibilità limitate di connessione verso host specifici della rete interna

Esistono diversi tipi di firewall

1. Firewall basato su router
2. Firewall a livello applicativo