

Crittografia e sicurezza delle reti domande di esame 2003-2004

Spiegare cosa è una zona demilitarizzata in un'architettura che utilizza firewall e motivando i motivi per la sua realizzazione. Inoltre usando la notazione del libro (o una notazione tipo pseudocodice scrivere le regole che permettono ad un firewall di

- permettere tutte le connessioni TCP per il WWW e di posta sulla macchina server.
- permettere tutto il traffico in uscita
- non permettere altro traffico

PGP usa il seguente approccio per generare chiavi di sessione che sono usate per codificare il testo di un messaggio di posta.

Il mittente genera una chiave segreta K , codifica il testo del messaggio e invia al mittente il testo codificato con K e la chiave K codificata con la chiave pubblica del ricevente.

Un diverso approccio consiste nell'utilizzare un metodo come lo scambio di chiavi di Diffie-Hellman per generare una chiave di sessione. Spiegare in una frase perché questo secondo approccio non è adatto in applicazioni di posta.

Nella firma di un documento con DSS l'utente utilizza un numero casuale che viene mantenuto segreto. Spiegare come la firma di due diversi messaggi con DSS utilizzando la medesima chiave sia una cattiva idea.

Si discuta la sicurezza di uso di password in ciascuno dei seguenti scenari e si confrontino fra loro i vantaggi e gli svantaggi.

- Alice utilizza l'ufficio del suo amico Biagio per utilizzare il suo PC e leggere la posta elettronica utilizzando un sistema di WebMail (sistema che usa SSL per l'invio di password durante la fase di autenticazione: Alice inserisce il suo username e la sua password).
- Carlo usa il suo laptop per collegarsi in un nuovo internet cafe' che è dotato di una rete wireless (802.11) e che offre il servizio in modo gratuito. Carlo usa telnet per collegarsi al computer del suo ufficio.
- Daria è a casa e si collega telefonicamente al suo ISP con un modem analogico. Il modem si collega tramite una rete Ethernet ad un server di autenticazione presso l'ISP che memorizza username e password: Daria inserisce username e password in una finestra di dialogo windows, il modem chiama l'ISP e l'ISP autentica.

Stimare la probabilità che ci siano due file in qualche parte del pianeta che abbiano la stessa impronta MD5; ripetere il calcolo per SHA.

NB una valutazione esatta è difficile; una stima può essere calcolata assumendo che ci siano 1 miliardo di computer e server e che ciascuno di essi memorizzi 100000 file (in media). Discutere eventuali altre ipotesi necessarie.

Spiegare cosa si intende per proprietà moltiplicativa di RSA e spiegare in che modo questa proprietà possa essere utilizzata per condurre attacchi. Illustrare infine come sia possibile evitare questi attacchi.

Illustrare e discutere il protocollo di autenticazione di Kerberos versione 4; in particolare motivare l'uso di timestamp e di tempo di vita dei certificati e spiegare come la sicurezza offerta da Kerberos è minore se si usano solo una o due chiavi.