

Crittografia e Sicurezza delle reti Impianti, esame parte Crittografia

22 settembre 2006 100 minuti

Una proposta (preliminare ma non realizzata) per aumentare la sicurezza di DES da parte dei laboratori RSA è stata la seguente DESV (dove k è una chiave DES di 56 bit e K_1 è una chiave di 64 bit (lunghezza del blocco DES); pertanto la chiave complessiva kk_1 è di 110 bit.

$$DES_{V_{kk_1}}(M) = DES_k(M) \text{ EXOR } k_1$$

Mostrare che questo metodo non aumenta la sicurezza di DES: per rompere DESV sono sufficienti molto meno codifiche di 2^{110} codifiche/decodifiche

(si assume che siano a disposizione un numero adeguato di coppie testo/codifica $M_i / C_i = DES_{kk_1}(M_i)$).

(Intr.: ricordare le proprietà per cui il codice ONE TIME può essere utilizzato per codificare un solo messaggio.)

Con riferimento ai firewall fornire una figura che mostri lo schema di un'architettura e spiegare brevemente cosa è una zona demilitarizzata in un'architettura che utilizza firewall motivando i motivi per la sua realizzazione. Discutere inoltre anche con esempi le modalità operative dei firewall nel filtraggio dei pacchetti.

Illustrare e discutere i seguenti protocolli di MUTUA autenticazione, IN CIASCUN CASO DISCUTERNE BREVEMENTE LA CORRETTEZZA:

- a) proporre un protocollo per la mutua autenticazione con l'assunzione che Alice e Biagio abbiano orologi sincronizzati e condividano un segreto comune K ; utilizzare crittografia simmetrica e minimizzare il numero di messaggi scambiati;
- b) proporre un protocollo per la mutua autenticazione con l'assunzione che Alice e Biagio abbiano orologi sincronizzati e condividano un segreto comune K ; utilizzare funzioni hash invece della codifica crittografica e minimizzare il numero di messaggi scambiati;

Descrivere la fase di autenticazione in SSL. In particolare in essa si utilizza nella fase di autenticazione una funzione hash (in particolare HMAC) tra il cliente e il server. Quale è lo scopo di questo scambio?

Abbiamo discusso in classe come il paradigma "prima hash dopo firma" è sicuro se si utilizza una funzione hash e uno schema crittografico sicuro. In particolare si chiede di discutere brevemente (max 4 righe per ciascuna domanda)

- a) come la firma di un messaggio m come $RSA_{KS}(m)$ (per firmare m codifica m con la chiave segreta) non sia sicuro; mostrare un attacco
- b) discutere la sicurezza di $RSA_{KS}(\text{hash}(m))$; inoltre discutere sotto quali condizioni lo schema si utilizza in pratica (fornendo le ulteriori modifiche presentate in uno standard di firma)