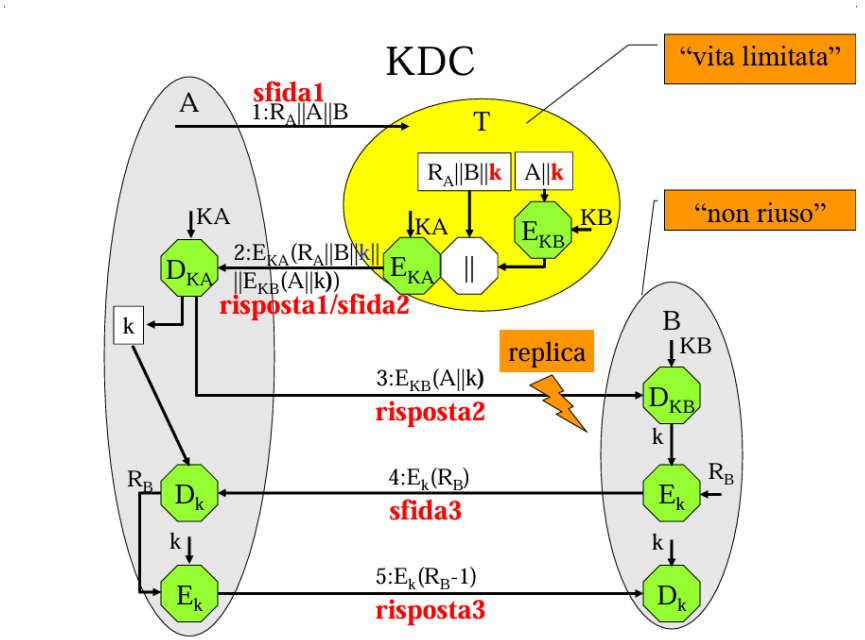
Potenziale Vulnerabilità KDC

Attacco alla Autenticità

Autore Pietro Bertozzi
Docente Rebecca Montanari
Anno Accademico 2024/2025
Giovedì, 13.03.2025

Contesto e Vulnerabilità

Il meccanismo di distribuzione delle chiavi centralizzato (KDC) è utilizzato per consentire a due entità, A e B, di stabilire una chiave segreta condivisa attraverso un'autorità fidata. In figura il protocollo di autenticazione tra A e B, che coinvolge il KDC nella generazione e distribuzione della chiave di sessione k. Da notare che la sfida dei messaggi 4 e 5 genera una possibile vulnerabilità perchè R_B è molto simile a R_{B-1}



Ipotesi e Precondizioni e Obiettivo dell'Attacco

Precondizioni necessarie affinchè la vunerabilità sia attaccabile:

- La modalità di cifratura del cifrario a blocchi è ECB, quindi le modifiche su un blocco non influenzano gli altri.
- La lunghezza di R_B eccede di poco un multiplo della lunghezza di un blocco.
- Lo schema di padding utilizzato è semplice

Obbiettivo

L'obiettivo dell'attacco è quindi quello di compromettere l'autenticazione, facendo sì che B accetti un interlocutore non legittimo come se fosse A.

Procedimento

- L'attaccante osserva il cifrato $E_K(R_B)$ inviato nel messaggio 4.
- Forse è possibile per l'attaccante, sfruttando lo schema di padding, riuscire a generare il cifrato di R_{B-1} senza conoscerne direttamente né il valore in chiaro, né la chiave, cambiando solo l'ultimo blocco, il cui messaggio è principalemnte padding.
- Poiché il valore $E_K(R_{B-1})$ è esattamente ciò che B si aspetta come risposta da A nel messaggio 5, l'attaccante può riprodurre il messaggio corretto senza avere accesso alla chiave k.
- B accetta la risposta e considera l'attaccante come un interlocutore valido; l'autenticazione è quindi comromessa.

Considerazioni Finali

Conclusione

Se si progetta un sistema che utilizza la modalità di cifratura ECB con cifrari a blocchi, è importante:

- Prestare attenzione a non generare messaggi la cui lunghezza ecceda di poco un multiplo della lunghezza dei blocchi, per evitare problematiche con il padding e la gestione dei blocchi.
- Evitare di sfidare gli interlocutori a cifrare messaggi che modificano pochi bit, per evitare che un solo blocco venga modificato.