Soluzione dello scritto del 7 giugno 2023

Crittografia

1. Fornire la definizione di One Time Pad e di Sicurezza Perfetta di Shannon, provare che OTP è sicuro.

Le risposte sono nel pacco di lucidi `crittografia/02-stream-ciphrs.pdf`.

2. Cos'è e cosa gestisce un Trusted 3rd Party TTP? Descrivere il Puzzle di Markle.

Le risposte sono nel pacco di lucidi `crittografia/05-key-exchange.pdf`.

Sicurezza

1. DB S.R.L. sviluppa un sistema di accesso basato su un software compilato e offuscato (l'eseguibile viene dato in pasto a Ghidra per vedere se si riesce ad analizzare e vengono messe in atto politiche di anti-debug). Questo è un buon metodo per garantire la sicurezza di un sistema? Perché o perché no?

No, questo non è un buon modo per garantire la sicurezza di un sistema, perché è un'istanza di *"security by obscurity"* e come tale ne eredita tutte le criticità. Se questo è l'unico sistema di sicurezza messo in atto, allora è sufficiente analizzare il comportamento dell'applicativo dall'esterno durante l'esecuzione (per esempio, il traffico con il server nel processo di autenticazione), per poter sviluppare un nuovo client che autentichi senza il bisogno di inserire credenziali. Quello che DB S.R.L. dovrebbe fare sarebbe invece applicare i principi della crittografia per proteggere ogni tipo di comunicazione che l'applicativo effettua con la rete o sul disco.

2. Supponiamo di disporre di un sistema che prevede una password e la ricezione di un codice (OTP) via SMS, come si potrebbe aumentare la sicurezza dal punto di vista teorico? È sufficiente una seconda password? Perché?

No, perché le due password sono entrambe "qualcosa che si sa", e più meccanismi dello stesso tipo non aumentano la sicurezza. Sarebbe necessario invece aggiungere un meccanismo di un tipo nuovo, e cioè "quello che si è", che fa riferimento ai dati biometrici come l'impronta digitale, la scansione della retina o il riconoscimento facciale.

Laboratorio

1. Spiegare brevemente l'obiettivo e che strategia di attacco utilizzi `aircrack-ng`, specificando se è un attacco di tipo online o offline.

Le risposte sono nel pacco di lucidi `prove/esercitazioni/parziale3-2023-04-03-testo.pdf`.