Ingegneria della sicurezza

Problemi comuni nelle propostеWS 2022/23

Elisabetta Oswald

Panoramica

La valutazione è molto specifica e ti incarica di evidenziare problemi specifici con una specifica di sistema fornita. Citando da Moodle:

> Il mini progetto ti mette nei panni di un consulente indipendente a cui vengono fornite una specifica iniziale/progetto di sistema e l'implementazione AES incorporata associata per un sistema di controllo degli accessi sicuro, chiamato SuperSAM.
>
> Il tuo compito è fornire una valutazione di ciò che ti viene fornito: la “nota di implementazione” descrive il sistema complessivo in modo semi-formale e fornisce alcune motivazioni per alcune scelte progettuali. Esiste anche un'implementazione AES associata pensata per essere eseguita su un token hardware che sarà una parte essenziale del sistema complessivo. Dovresti evidenziare i difetti e offrire soluzioni.

Il motivo principale per cui gli studenti hanno perso punti è che hanno fornito discussioni generiche su questioni di sicurezza, che non è ciò che richiede la valutazione. Richiede una valutazione esatta del sistema fornito, e quindi di evidenziare problemi specifici nelle specifiche e nel codice sorgente associato. Non viene assegnato alcun punto per una discussione generica, ad esempio sui tipici problemi di sicurezza RFID. Non si possono assegnare punti nemmeno per la discussione di soluzioni generiche: il compito è aggiustare il sistema specifico, non aggiustare qualche sistema.

Un altro problema importante sembra essere stato il fatto che le specifiche non sono state sufficientemente studiate e quindi sono state tratte conclusioni/interpretazioni strane/errate, che apparentemente si sono diffuse tra il corpo studentesco e sono state adottate (apparentemente) da molti senza una valutazione critica. Menzionerò alcuni frequenti “malintesi” di seguito.

Un terzo problema importante è stato che, a differenza degli anni precedenti, molti studenti non hanno partecipato agli incontri e non mi hanno consegnato le bozze perché potessi commentarle.

AES come “suggerimento”: AES è una specifica e, sebbene esistano funzioni circolari equivalenti, lo schema di crittografia AES non è aperto a interpretazioni.

Problemi di sicurezza RFID: le comunicazioni wireless in generale non sono sicure se non crittografate. Gli attacchi specifici RFID sono problematici quando le comunicazioni non sono crittografate e non viene fornita alcuna autenticazione. La specifica è chiara che vengono comunicati solo messaggi crittografati ed è prevista l'autenticazione dei token. Se

vuoi sostenere che cose come lo sniffing e lo skimming sono ancora una minaccia, devi dimostrare un attacco che funzioni per il sistema fornito.

Errore umano: infatti è sempre importante tenerne conto. Ma elencare questioni generiche relative all'usabilità senza descrivere uno specifico vettore di attacco al sistema in questione non è sufficiente.

DPA: richiede di avere ingressi conosciuti con chiave fissa. Bisogna pensare se questo può essere applicato o meno ai diversi protocolli nella specifica data.

Dimensione degli ID: sembra esserci l'idea che se un valore ID può trovarsi al di fuori di uno spazio di 232 valori, è necessario memorizzare da qualche parte 232 valori. Questo non ha senso; Sarebbe necessario memorizzare 32 bit sul token per l'ID. I suggerimenti di x bit sufficienti dovrebbero essere considerati attentamente: se x non è un multiplo di un tipo di dati nativo del processore, il caricamento di x sarà costoso. Inoltre, se x è troppo piccolo, ciò potrebbe causare problemi se, ad esempio, gli ID edificio devono essere revocati regolarmente.

Modalità BCE: chiaramente non è una buona scelta, ma come sarebbe realmente un attacco in questo sistema concreto?

Fattorizzazione: non è un problema quando si lavora con i numeri primi (se si pensa ancora che i numeri primi più grandi siano più difficili da fattorizzare, si dovrebbe considerare di riprendere la Crittografia).

Diversi studenti ritengono che la decisione progettuale del sistema centrale di mantenere i lettori il più possibile offline, tramite gettoni con biglietti, sia sbagliata. Abbastanza giusto: ma allora la tua analisi dovrebbe considerare quali sarebbero i potenziali problemi quando i token venissero utilizzati solo per l'autenticazione? Cosa succede se i lettori vanno offline? Ciò sarebbe possibile per tutte le aziende/allestimenti/luoghi di costruzione?

Diversi studenti hanno estratto immagini da fonti e utilizzato testi da articoli pubblicati. Questo è un tipo di plagio chiamato "cattiva pratica accademica". Non farlo. A qualsiasi passaggio che conteneva testo rimosso o figure copiate venivano assegnati 0 punti.