Intuizioni Progetto Cybersecurity

Immagine che contiene testo, lavagnabianca

Descrizione generata automaticamente

Il problema è definito nella richiesta di dati da parte del laboratorio analisi, che può essere performata anche da un avversario che può attaccare in due modi: overflow attack e approccio ad oracolo (Vedi MAC e CPA-sicurezza). L’idea è di utilizzare due funzioni separate, in ingresso abbiamo l’autenticazione (il punto interrogativo), e in uscita abbiamo la definizione del logaritmo discreto, che contiene i codici da assegnare ai pazienti infetti, (pensa all’approccio di El Gamal). L’idea è di utilizzare una cifratura a chiave pubblica dove il server contiene la chiave segreta per la sicurezza dei dati.

Pensiero 2.0

Si suppone che il ministero della salute, sia una rootCA la quale può rilasciare certificati client ai laboratori analisi; in questo caso il laboratorio esegue l’accesso al server backend del ministero, il quale rilascerà una nuova inf list contenente i codici (generati in modo randomico) che verranno dati alle persone infettate (assegnandoli ad esempio su di un foglio bianco oppure mediante altri meccanismi definiti in seguito), tali codici sono ritenuti validi dal server perchè saranno salvati sul database contenuto sul backend. In questo caso può essere utilizzato lo schema con firma digitale (Gen, Sign, Vrfy) con particolare attenzione a come sviluppare la Sign (parte critica da approcciare con i codici presentati dall’OpenSSL). Per avere una comunicazione sicura, si frutta il protocollo TLS 1.3 (semplice supposizione).

# MIM attack, come gestirlo e in particolare, come attenderlo su un canale del genere.

I codici verranno generati con l’utilizzo di una codifica a 32 bit, dobbiamo utilizzare un secondo canale per fare le verifiche del MIM attack, un consiglio: pensa alla procedura del MAC sicuro.

Per generare la inf list utilizziamo l’algoritmo con il logaritmo discreto di Diffie-Hellman, con un’aggiunta di una funzione hash per evitare il mim attack.

La funzione hash contiene lo SHA2 come codifica dei messaggi inf-code generati.