Confronto Ragionato tra HPKE e la Crittografia Tradizionale

Lorenzo Cappetti Matricola:7165929

October 2024

1 Introduzione al problema e contesto

La sicurezza nelle comunicazioni digitali è un aspetto cruciale nel mondo moderno, in particolare quando due o più utenti devono scambiarsi informazioni in modo riservato. Una delle prime soluzioni per garantire la riservatezza di una comunicazione è stata l'algoritmo di **Diffie-Hellman (DH)**, sviluppato nel 1976. Questo algoritmo permette a due parti di stabilire una chiave segreta condivisa su un canale pubblico, senza dover trasmettere direttamente la chiave stessa.[1]

Tuttavia, il protocollo Diffie-Hellman presenta alcune vulnerabilità, in particolare contro attacchi come:

- **Man-in-the-Middle (MitM)**: Qui un aggressore può intercettare e modificare lo scambio delle chiavi tra due parti, rendendo di fatto il protocollo insicuro se non è adeguatamente protetto.
- **Replay Attack**: In questo tipo di attacco, un aggressore può registrare un'interazione legittima e ripeterla in seguito per ottenere accesso non autorizzato.

La ragione principale di queste vulnerabilità è che il protocollo Diffie-Hellman non autentica le due parti che stanno scambiando le chiavi. Non garantisce che la chiave scambiata provenga effettivamente dal destinatario previsto, aprendo la porta a questi tipi di attacchi. [4]

1.1 Necessità di combinare tecniche di crittografia

Per superare i limiti del Diffie-Hellman e garantire uno scambio sicuro delle chiavi, è necessario combinare più tecniche di crittografia. Questo è il motivo per cui vengono utilizzati insieme tre blocchi fondamentali:

- **Diffie-Hellman**: viene utilizzato per stabilire una chiave condivisa tra due parti. [5]

- **Crittografia asimmetrica** (pubblico-privato): serve per garantire la sicurezza della distribuzione delle chiavi e per autenticare le parti, risolvendo i problemi di autenticazione che affliggono Diffie-Hellman.
- **Crittografia simmetrica**: offre efficienza computazionale, viene utilizzata per proteggere il traffico di dati una volta che la chiave è stata condivisa. [2]

1.2 Introduzione alla crittografia ibrida

Combinando questi tre blocchi, si possono sviluppare protocolli di crittografia più robusti, come quelli utilizzati nei moderni sistemi di comunicazione sicura. Uno degli approcci più diffusi è la crittografia ibrida (Hybrid Public Key Encryption - HPKE), che unisce i vantaggi della crittografia asimmetrica e simmetrica per fornire sia sicurezza che efficienza.

2 Combinazione tradizionale di crittografia

La combinazione tradizionale di crittografia asimmetrica e simmetrica ha origine dalla necessità di sfruttare i punti di forza di entrambe le tecnologie crittografiche, superando i limiti di ciascuna. La crittografia asimmetrica, pur offrendo un modo sicuro per distribuire le chiavi pubbliche e private, è computazionalmente più lenta e inefficiente per la crittografia di grandi volumi di dati. La crittografia simmetrica, invece, è estremamente efficiente, ma richiede che la chiave segreta sia scambiata in modo sicuro, cosa che può essere complicata senza l'ausilio di un sistema di gestione delle chiavi.

Nella combinazione tradizionale di crittografia ibrida, questi due approcci vengono uniti per ottenere i vantaggi di entrambi i sistemi. Questo avviene tramite questi passaggi:

1. **Generazione della chiave simmetrica:** Il mittente genera una chiave simmetrica (detta anche chiave di sessione). Questa chiave sarà utilizzata per crittografare il contenuto del messaggio poiché la crittografia simmetrica è molto più veloce per cifrare grandi quantità di dati rispetto alla crittografia asimmetrica.
2. **Cifratura della chiave simmetrica con crittografia asimmetrica:** Una volta generata la chiave di sessione, il mittente utilizza la chiave pubblica del destinatario per cifrare questa chiave simmetrica. La crittografia asimmetrica permette di garantire che solo il destinatario legittimo, che possiede la corrispondente chiave privata, sarà in grado di decifrare la chiave simmetrica.
3. **Invio della chiave crittografata e del messaggio cifrato:** Il mittente invia al destinatario due elementi: la **chiave simmetrica crittografata** e il **messaggio cifrato** utilizzando la chiave simmetrica.

4. **Decifratura da parte del destinatario:** Il destinatario utilizza la propria chiave privata per decifrare la chiave simmetrica inviata e una volta ottenuta la chiave simmetrica, il destinatario può utilizzarla per decrittare il messaggio cifrato. [4]

2.1 Vantaggi della combinazione tradizionale

Sul piano dell'efficienza, la crittografia simmetrica è molto più veloce di quella asimmetrica per cifrare e decifrare grandi quantità di dati. Questo rende il processo di crittografia e decrittografia più rapido ed efficiente una volta che la chiave di sessione è stata scambiata.

Inoltre, la crittografia asimmetrica viene utilizzata solo per cifrare la chiave di sessione, che è molto più piccola rispetto al messaggio stesso. Questo riduce il carico computazionale derivante dall'uso di algoritmi asimmetrici, mantenendo comunque la sicurezza dello scambio di chiavi. Questa facilita lo scambio sicuro della chiave simmetrica senza la necessità di un canale sicuro preesistente per il trasferimento delle chiavi.

3 Benefici di HPKE

Il modello di crittografia ibrida descritto nel documento RFC 9180 [3], noto come Hybrid Public Key Encryption (HPKE), rappresenta un'evoluzione rispetto alla combinazione tradizionale di crittografia simmetrica e asimmetrica. HPKE introduce un nuovo metodo per generare e incapsulare la chiave simmetrica durante il processo di crittografia, portando con sé una serie di vantaggi significativi.

In particolare, HPKE utilizza uno schema a 3 blocchi per essere implementato.

1. **Diffie-Hellman:** viene utilizzato per stabilire il materiale di base che servirà per derivare la chiave simmetrica. Questo avviene durante il processo di incapsulamento della chiave, dove il mittente utilizza la chiave pubblica del destinatario insieme alla propria chiave privata per generare una chiave condivisa.

2. **Crittografia Asimmetrica (chiavi pubblica/privata):** viene utilizzata per incapsulare la chiave simmetrica generata. Il mittente utilizza la chiave pubblica del destinatario per cifrare la chiave simmetrica in modo che solo il destinatario, usando la sua chiave privata, possa decapsulare la chiave e utilizzarla per decifrare i dati.

3. **Crittografia Simmetrica:** Una volta incapsulata la chiave simmetrica, HPKE utilizza la crittografia simmetrica per cifrare i dati effettivi. Questa parte del processo è identica alla crittografia combinata tradizionale: una chiave simmetrica (detta chiave di sessione) viene utilizzata per cifrare il messaggio perché è più veloce e più efficiente nel trattare grandi volumi di dati.

Uno dei principali vantaggi nell'utilizzo di HPKE è il miglioramento della sicurezza rispetto agli attacchi più sofisticati, inclusi gli attacchi **man-in-the-middle** e **replay attack**, ma diminuisce anche la **latenza**.

- **Protezione contro MitM:** HPKE utilizza la crittografia asimmetrica per garantire che la chiave simmetrica generata e incapsulata sia condivisa solo con il destinatario legittimo. La chiave pubblica del destinatario viene usata per incapsulare la chiave simmetrica, rendendo estremamente difficile per un attaccante intercettare o modificare la comunicazione senza essere rilevato.
- **Riduzione del rischio di replay attack:** HPKE può essere integrato con altre tecniche crittografiche, come l'inclusione di un nonce o un contatore, per rendere ogni trasmissione unica e non riutilizzabile.
- **Riduzione della latenza:** Poiché la chiave simmetrica e il messaggio cifrato possono essere trasmessi simultaneamente, HPKE riduce il tempo necessario per stabilire una connessione sicura, migliorando così le prestazioni in contesti come messaggistica sicura o connessioni web sicure.

4 Differenze chiave dei due approcci

La differenza principale tra HPKE e la crittografia tradizionale sta, come abbiamo detto in precedenza, nel modo in cui viene gestito lo scambio di chiavi e l'efficienza del processo di crittografia.

HPKE utilizza un approccio ibrido in cui la crittografia asimmetrica viene utilizzata solo per incapsulare una chiave simmetrica, che a sua volta è usata per cifrare i dati reali.

4.1 Efficienza

La crittografia simmetrica è più efficiente rispetto a quella asimmetrica per cifrare grandi quantità di dati. HPKE ottimizza questo processo, riducendo il numero di operazioni computazionalmente costose legate alla crittografia asimmetrica, utilizzata solo per incapsulare la chiave di sessione. Nella crittografia tradizionale, questo processo può essere più frammentato, con la chiave simmetrica generata e cifrata in passaggi separati.

4.2 Sicurezza

Nella crittografia ibrida tradizionale il rischio di attacchi MitM (Man-in-the-Middle) può essere mitigato con protocolli aggiuntivi, HPKE integra direttamente la protezione contro tali attacchi. La chiave pubblica del destinatario è utilizzata per incapsulare la chiave simmetrica, il che garantisce che solo il legittimo destinatario possa decifrarla, riducendo le possibilità di intercettazioni o modifiche fraudolente.

4.3 Latenza

HPKE riduce la latenza complessiva grazie alla generazione simultanea e all'incapsulamento della chiave simmetrica. Nella crittografia tradizionale, il processo può richiedere più tempo a causa della necessità di scambiare le chiavi in passaggi separati.

5 Conclusioni

HPKE rappresenta un'evoluzione importante, fornendo una maggiore protezione contro gli attacchi avanzati e riducendo al contempo la latenza operativa. Questo protocollo, grazie all'incapsulamento simultaneo delle chiavi simmetriche, si distingue per la sua capacità di mantenere elevati standard di sicurezza senza sacrificare le prestazioni, rendendolo particolarmente adatto per applicazioni ad alta intensità di dati e comunicazioni in tempo reale.

Le future direzioni di ricerca potrebbero concentrarsi sull'integrazione di HPKE con altre tecnologie di sicurezza emergenti. La continua evoluzione della crittografia sarà essenziale per mantenere la sicurezza nelle comunicazioni digitali in un panorama tecnologico in costante mutamento.

References

[1] Wikipedia, *Scambio di chiavi Diffie-Hellman*, `https://it.wikipedia.org/wiki/Scambio_di_chiavi_Diffie-Hellman`, Accesso il 21 ottobre 2024.

[2] NamirialFocus, *Crittografia asimmetrica: come, quando e perché*, `https://focus.namirial.it/crittografia-asimmetrica-come-quando-perche/`

[3] RFC9180, *Documento RFC9180*, `https://www.rfc-editor.org/rfc/rfc9180.html`

[4] ChatGPT, OpenAI, *Conversazione con ChatGPT*, 21 ottobre 2024.

[5] ComputerSec, *Algoritmo di Diffie-Hellman*, `https://www.computersec.it/2018/12/26/algoritmo-di-crittografia-diffie-hellman/`