Università Politecnica delle Marche
Dipartimento Ingegneria dell'informazione

Analisi e valutazione sperimentale di varianti basate su primitive crittografiche postquantum del protocollo IKEv2 per lo scambio di chiavi crittografiche nelle comunicazioni satellitari

Relatori:
Prof. Marco Baldi

Candidato:
De Zuane Davide

"Over the Air Cryptographic Keys Exchang for Secure Governmental Satellite Communications"

Amcona - 15/05/24

Relazione

La seguente relazione riporta il lavoro effettuato per l'incarico di "Analisi e valutazione sperimentale di varianti basate su primitive crittografiche postquantum del protocollo IKEv2 per lo scambio di chiavi crittografiche nelle comunicazioni satellitari".

Attraverso una serie di test mirati, si sono esaminate le prestazioni di IKEv2 con StrongSwan mediante utilizzo di diverse primitive crittografiche. In particolare nel corso di questo studio ci si è concentrati su quelle che sono le principali problematiche riguardanti il post-quantum, per tali motivi abbiamo considerato come metriche:

- la dimensione dei pacchetti;
- il tempo necessario ad effettuare gli scambi.

Tutte le caratteristiche che si sono prese in consierazioni sono descritte in maniera dettagliata nei seguenti RFC:

- RFC7296
- RFC7383
- RFC9370
- RFC9242

Post Quantum

Il presente rapporto si propone di esplorare in dettaglio le prestazioni dell'implementazione di IKEv2 tramite StrongSwan, mediante uno studio approfondito e un'analisi dettagliata. Tuttavia, ciò che lo distingue è l'obiettivo specifico di valutare come il comportamento di StrongSwan si modifica durante il passaggio dall'utilizzo di primitive crittografiche classiche a primitive post-quantum.

La necessità del post-quantum è fondamentale per quanto riguarda gli scambi nelle fasi: INIT e AUTH. Entrambi questi scambi sono suscettibili ad attacchi quantistici. Per quanto riguarda i certificati chiave pubblici, sarebbe sufficiente utilizzare firme post-quantum, poiché questo garantirebbe che gli attaccanti, anche quelli dotati di un potente computer quantistico, non possano falsificare i certificati. Per lo scambio di chiavi impiegato nella fase di INIT, invece, la situazione è piuttosto diversa.

Dato che lo scambio DH è vulnerabile ad attacchi quantum, la comunità crittografica ha esaminato metodi per ottenere protocolli post-quantum diversi da "ideare uno scambio di chiavi DH post-quantum". Per quanto riguarda IKEv2, i metodi più comuni sono:

- utilizzare **pre-shared key**;
- utilizzare molteplici **key-exchange**;
- utilizzare **KEM PQ**.

Nel nostro studio abbiamo confrontanto le varie metologie.

PSK

Il processo di utilizzo delle PSK classiche in IKEv2 è piuttosto semplice ma efficace. Prima di tutto, sia il client che il server devono essere configurati con la stessa PSK, che può essere stabilita manualmente o tramite un sistema di gestione delle chiavi. Durante la fase di negoziazione `IKE_SA_INIT`, il client invia al server la sua proposta di sicurezza, che include l'indicazione dell'utilizzo della PSK per l'autenticazione. Il server, a sua volta, verifica se la PSK ricevuta corrisponde a quella configurata e, in caso affermativo, accetta la connessione.

Multiple Key Exchange

RFC9242 introduce un nuovo scambio per IKEv2 chiamato `IKE_INTERMEDIATE`, che deve essere utilizzato per trasferire grandi quantità di dati che, altrimenti, causerebbero frammentazione IP se inviati attraverso lo scambio `IKE_SA_INIT`. Lo scambio `IKE_INTERMEDIATE` avviene subito dopo lo scambio `IKE_SA_INIT` e prima dello scambio `IKE_AUTH`.

`IKE_INTERMEDIATE` può essere impiegato per eseguire scambi di chiavi o KEM (Key Encapsulation Mechanism) post-quantum. RFC9370 propone il cosiddetto metodo dei "multipli scambi di chiavi". L'idea è quella di eseguire più di uno scambio di chiavi/KEM e di derivare le chiavi simmetriche come una funzione pseudo-casuale e unidirezionale di tutto il materiale chiave che è stato scambiato.

Ad ogni KEM le chiavi vengono aggiornate con il materiale appena scambiato.

PQ-KEM

La procedura descritta nella descrizione precedente può ovviamente essere modificata in modo che lo scambio DH classico non venga eseguito e venga impiegato solo un KEM post-quantum. In tal caso, le modifiche a IKEv2 sono minime poiché, in pratica, l'unica differenza è che il materiale chiave condiviso è derivato utilizzando solo il KEM post-quantum. Tra le soluzioni basate su PQC, questa è quella con il minor impatto poiché viene impiegato solo un KEM. Tuttavia, potrebbe essere la più rischiosa, poiché richiede di fare affidamento su un singolo KEM: la sicurezza dell'intero protocollo dipende dal KEM impiegato.

Results

Per determinare l'impatto del post-quantum sul protocollo sono state effettuate diverse simulazioni utilizzando la versione 6.0beta4 di Strongswan, il quale supporta solo alcune primitive crittografiche PQ e alcuni algoritmi di firma digitale PQ.

Le simulazioni sono state eseguite su un laptop che utilizza Arch Linux con Kernel 6.8.5-arch1-1, con un processore AMD Ryzen 7 5825U con 8 core di

grafica Radeon e 24 GB di RAM. Gli endpoint comunicanti sono stati implementati utilizzando Docker Versione 26.0.1. Il protocollo IKEv2 è stato eseguito utilizzando Strongswan versione 6.0beta4, utilizzando Lliboqs Versione 0.9.2 per gli algoritmi post-quantum. Le configurazioni considerate sono riportate nella seguente tabella.

	ID	A	B	C	D	E	F	G
INIT	Request	294B	1062B	1446B	662B	342B	1078B	310B
	Response	367B	1038B	1358B	670B	350B	1054B	318B
	Time	0.7 ms	0.7 ms	3.8 ms	6.2 ms	0.1 ms	0.9 ms	1.1 ms
INTER	Request	-	-	-	927B	2394B	1686B	-
	Response	-	-	-	895B	4694B	1718B	-
	Time	-	-	-	11.3 ms	1.3 ms	1.8 ms	-
AUTH	Request	630B	6665B	2638B	2640B	2622B	2624B	238B
	Response	571B	6631B	2615B	2610B	2594B	2595B	190B
	Time	1.4 ms	1.2 ms	1.3 ms	1.3 ms	1.1 ms	1.2 ms	0.7 ms

Quando vengono impiegati algoritmi asimmetrici post-quantum, le dimensioni dei messaggi tendono ad aumentare tipicamente. Inoltre, quando vengono impiegati più scambi di chiavi, il modello dei messaggi diventa più complicato in quanto richiede lo scambio `IKE_INTERMEDIATE`.

L'aumento del costo della comunicazione diventa più evidente quando vengono impiegati certificati di chiave pubblica. Infatti, per le configurazioni da B a G, le dimensioni dei messaggi `IKE_AUTH` sono molto più grandi rispetto a quella della configurazione A, che è l'unica a utilizzare firme classiche. La configurazione G è ovviamente eccezionale, poiché l'autenticazione viene ottenuta senza certificati.

Per ottenere tali risultati è stato necessario una prima fase di progettazione e di sviluppo di un software di simulazione. Questo ha permesso di generare ed analizzare in maniera completamente automatizzata i risultati numerici di interesse, i quali sono stati successivamente resi disponibili per il progetto intitolato "Over the Air Cryptographic Keys Exchange for Secure Governmental Satellite Communications". Questo progetto si occupa dello scambio sicuro di chiavi crittografiche tramite comunicazioni satellitari governative. Il presente lavoro si inserisce e contribuisce in modo significativo a tale progetto, fornendo dati e analisi fondamentali per il suo avanzamento e successo. Oltre al software di simulazione è stata predisposta tutta una configurazione automatica per favorire la portabilità del lavoro anche in altri ambienti e lo sviluppo di altri tool ausiliari al conseguimento degli obiettivi.

Il software realizzato è disponibile al seguente link.