VPN mobili con IPsec

Antonio Forzieri, Davide Cerri, Alessandro Ghioni

La possibilità di connettersi alla propria rete aziendale mentre si è in viaggio o ci si trova nella sede di partner, clienti e fornitori è una richiesta costante del mondo delle imprese. Per rispondere a questa esigenza di mobilità dei lavoratori, fin dai primi anni novanta sono state sviluppate diverse soluzioni di accesso remoto, in genere basate su connessioni PSTN terminanti direttamente sul NAS aziendale. Questo tipo di accesso è sempre stato considerato relativamente sicuro, poiché è molto complesso (anche se non impossibile) violare l'integrità o la riservatezza di una connessione effettuata attraverso la rete PSTN. Per questo motivo i servizi di sicurezza offerti erano limitati alla sola autenticazione utente e all'autorizzazione che ne consegue.

Dalla VPN alla Mobile VPN Nel corso degli anni la gestione dell'accesso remoto alla rete aziendale ha tuttavia subito una indubbia accelerazione tecnologica: la necessità di abbattere i costi di connessione e la grande diffusione di Internet (con crescenti ampiezze di banda) hanno portato allo studio di protocolli per l'accesso remoto attraverso reti IP, con la conseguente ben nota crescita dei problemi legati alla sicurezza delle connessioni e delle comunicazioni. Diverse società commercializzano già oggi soluzioni che permettono una connessione sicura che provenga da un punto fisso, o, in altre parole, che abbia origine da un host che non possa cambiare il proprio indirizzo IP durante la comunicazione con la propria rete aziendale.

Ma nell'ultimo decennio abbiamo assistito a una nuova rivoluzione delle comunicazioni: la diffusione della comunicazione mobile. Con lo sviluppo delle reti GPRS, UMTS e Wi-Fi ci troviamo oggi di fronte a un nuovo scenario che promette di rivoluzionare ancora una volta la qualità e la quantità degli accessi sicuri alle reti aziendali. L'evoluzione dei telefoni cellulari, dei computer portatili e dei PDA, unita alla sempre maggiore disponibilità di interfacce di rete dual-standard, spingono infatti a studiare sistemi di comunicazione che permettano lo sviluppo di MVPN (Mobile Virtual Private Network): si tratta di un particolare scenario di accesso remoto sicuro in cui il dispositivo deve essere in grado di cambiare il proprio indirizzo IP senza perdere la connettività con la propria rete aziendale. Quello che stiamo considerando è lo sviluppo di sistemi che permettano, ad esempio, di accedere alla rete aziendale mediante una connessione Wi-Fi, disponibile presso un albergo o in aeroporto e, senza mai disconnettersi, mantenere l'accesso attraverso la rete UMTS o la rete GPRS (per esempio viaggiando in taxi).

La sicurezza delle MVPN Lo sviluppo di Mobile VPN genera una serie di nuove sfide tecnologiche che derivano dal fatto che gli utenti sono fisicamente e logicamente mobili:

siamo cioè di fronte a utenti (e dispositivi) che si muovono nello spazio e contemporaneamente possono cambiare rete e/o indirizzo IP. Il problema da risolvere può quindi essere così sintetizzato: ottenere un accesso alla propria rete aziendale, trovandosi all'esterno, attraverso un canale sicuro in Internet, in modo da mantenere la connessione con la propria rete aziendale anche qualora ci si sposti attraverso reti o sottoreti differenti, senza essere costretti a dover rinegoziare l'accesso ad ogni spostamento.

È chiaro che lo scenario descritto riunisce insieme sia le problematiche connesse all'accesso remoto sicuro attraverso Internet sia quelle della mobilità IP. I requisiti che impone sono molteplici e complessi: si va dalla gestione dinamica dell'autenticazione dei due interlocutori (l'utente che richiede l'accesso e il gateway della rete aziendale) all'instaurazione di un canale sicuro, dalla configurazione di politiche di sicurezza alla gestione automatica ed efficiente della mobilità. Utilizzando IPsec per la connessione sicura, un cambiamento dell'indirizzo IP dell'utente remoto, causato da un suo spostamento, provoca un "disallineamento" tra le security association (nelle due direzioni della comunicazione) presenti tra l'host remoto e il gateway, impedendo la corretta comunicazione tra i due.

Lo stato dell'arte Per permettere la mobilità dell'utente remoto senza compromettere la comunicazione si possono seguire approcci differenti. La soluzione più semplice al problema consiste nel rinegoziare il tunnel IPsec ad ogni cambiamento di indirizzo IP. Poiché ogni host remoto deve contattare il proprio security gateway al fine di negoziare le security association necessarie (deve cioè essere avviato un handshake IKE al fine di negoziare sia una IKE SA per rendere sicura la negoziazione successiva, che una coppia di IPsec SA per la protezione del traffico dati), sarà sufficiente avviare un nuovo handshake IKE ogni volta che il terminale si sposta da una rete all'altra. Questa soluzione comporta tuttavia un elevato ritardo (per la necessità di portare a termine un intero handshake IKE, eventualmente comprese anche alcune estensioni per l'autenticazione utente o altro) e un considerevole overhead computazionale (per via delle operazioni crittografiche asimmetriche necessarie per lo svolgimento dell'handshake), il che potrebbe essere particolarmente problematico nel caso di dispositivi (quali PDA o smartphone) dotati di capacità di calcolo non elevate.

Un'altra soluzione consiste allora nel combinare un protocollo che gestisca la sicurezza (IPsec) con uno che gestisca la mobilità (Mobile IP), tuttavia in questo caso si ha un overhead elevato sui pacchetti dati, dovuto alla presenza di due tunnel (il tunnel IPsec e il tunnel Mobile IP) anziché di uno solo. Questa soluzione lascia inoltre esposte alcune informazioni sull'identità del nodo (home address) che sarebbe invece opportuno proteggere.

Verso una possibile soluzione Il tentativo di creare una Mobile VPN mostra diverse carenze dell'attuale architettura di IPsec e, in particolare, del protocollo IKE: con lo standard attuale non è infatti possibile gestire un'autenticazione asimmetrica (a livello utente per l'host remoto e a livello macchina per il security gateway), configurare il dispositivo che accede, attraversare sistemi intermedi (NAT), permettere la mobilità dell'host remoto. Questi problemi, ad eccezione di quello della mobilità, sono tuttavia risolti da IKEv2,

nuova versione del protocollo IKE il cui processo di standardizzazione presso l'IETF appare ormai in dirittura d'arrivo.

Il problema della mobilità rimane quindi comunque aperto: una possibile soluzione, su cui si sta lavorando anche al Cefriel (Politecnico di Milano), consiste nell'integrare la gestione della mobilità all'interno del protocollo IKE. Si vuole cioè permettere ad IKE di traslare il punto terminale del tunnel sicuro (cioè della security association), in modo da mantenere la connessione sicura anche dopo un cambiamento di indirizzo IP. Tale funzionalità potrebbe inoltre essere sfruttata in altri contesti, ad esempio per permettere una comunicazione sicura (utilizzando IPsec) tra due host entrambi mobili. È importante notare che una soluzione di questo tipo è limitata al solo protocollo di scambio delle chiavi (IKE) e non intacca l'architettura IPsec; è quindi poco "invasiva" e sufficientemente semplice da essere realizzabile e utilizzabile in tempi brevi.