La Sicurezza nelle reti Wireless

Laurea in Ing. delle TLC presso la Facoltà di Ingegneria di Napoli "Federico II"
Seduta di Luglio 2005

Ing. Giampiero Longo

La Wireless LAN rappresenta una delle tecnologie più diffuse per le comunicazioni private, e il suo utilizzo nel mondo è in rapida crescita. Tuttavia se nelle reti wired il binomio trasmissione dati ed accesso alla rete è stato reso fisicamente sicuro e facilmente controllabile nelle reti wireless, invece, questa esigenza per molto tempo non ha trovato una soluzione concreta e solo con la pubblicazione nel Luglio 2004 dello Standard IEEE 802.11i si è posta in essere la piattaforma che meglio di tutte risolve le oramai note problematiche sulla sicurezza quali l'Autenticazione Client/Server; la Protezione Dati; il Controllo di Integrità ed il Non Disconoscimento.
Per comodità di esposizione questo lavoro di tesi è stato articolato in due tempi distinti ma non disgiunti fra loro. Nella "prima parte" sono state analiticamente e criticamente descritte soluzioni *adattabili* ed *innovative* in grado di "proteggere" una Wi-Fi da intrusioni non controllabili. Fra le soluzioni *adattabili* sono state dettagliatamente illustrate: **VPN; WEP; WPAv1; PPPoE; Proxy; IEEE 802.1x** e tra quelle *innovative*: **WPAv2; PKI; SSL; Honey-Net; IDS**, evidenziando per entrambe gli attacchi informatici più comunemente in uso (*Man in the middle; Replay Attack; Brute Force; Bit-Flipping; Weak Keys; Reflex Attack; Spoofing; Sniffing e Spamming).* Sulla base della esperienza maturata dall'autore, è stato effettuato un confronto tra le varie tecnologie elencate, utilizzando come termine di paragone "il livello di riservatezza strategico dei dati" e classificando le possibili realtà wireless in 4 categorie: SOHO; PMI; Corporate; Operatori Mobili/ISP. Infine per quanto concerne l'Autenticazione, con particolare riferimento al Certificato Digitale che ne è la massima espressione, sono stati descritti i meccanismi attraverso i quali è possibile effettuare un controllo d'accesso al network con un Centro di Autenticazione delle Chiavi; Kerberos V4; Autenticazione a Chiave Segreta Condivisa; Autenticazione con Crittografia a chiave pubblica; Firme Digitali (a chiave pubblica e privata) e Certificato Digitale. In questa sede è parso opportuno affrontare la questione relativa alle tecniche di *hashing* con l'algoritmo MD5 ed all'uso diffuso che se ne fa attualmente tramite i certificati digitali X-509. Per completezza infine si è dissertato su problematiche quali il funzionamento; le caratteristiche; la tipologia; i requisiti di protezione ed il livello di sicurezza dei certificati digitali; i compiti delle Certification Authority (CA) e la loro struttura gerarchica, illustrando tecniche di creazione di certificati Self-Signed e fasulli attraverso l'impiego di *openssl* ed *ssl_mode*.
Nella "seconda parte" si è proceduto ad affrontare, in modo sperimentale, due aspetti significativi: *La Validità di una soluzione di sicurezza economica e la Realizzazione di una piattaforma software "veloce" per la crittoanalisi con l'algoritmo RSA.* Nel primo caso abbiamo dimostrato empiricamente sia l'inefficacia del protocollo di sicurezza WEP in ambienti Enterprise o PMI, sia la possibilità di utilizzare questa soluzione come valido deterrente, nei confronti di attacchi informatici, in piccole reti domestiche con volumi di traffico limitato. Per il raggiungimento di tale obiettivo si è realizzata, in primo luogo, una rete wireless Ethernet con una protezione WEP con chiave a 128 bit, sulla quale è stato opportunamente configurato un generatore di traffico costante (2000 pkt/sec di 2600 byte ciascuno), e poi si è provveduto ad attuare un attacco di tipo *brute force* che consiste in una ricerca esaustiva della chiave di autenticazione/crittografia WEP con i software: NetStumbler (per consentire all'attacker di acquisire informazioni utili sulla rete da attaccare quali: canale di trasmissione, tipo di protezione, SSID ed altro ancora), AiroPeek 2.1 SE Demo e Sniffer Wireless AirDump 2.1 (per ottenere i pacchetti trasmessi sul link radio) ed AiroCrack 2.1 (per recuperare la chiave WEP di 128 bit). Il risultati tabellati hanno evidenziato che con 7200000 pkts acquisiti dall'attacker un completo crack del sistema di sicurezza è possibile in 36 secondi, e scendendo di 500000 pkts per volta abbiamo iterato la simulazione fino al raggiungimento di 4800000 pkts per i quali il WEP risulta "inviolabile".
Nel secondo caso abbiamo lavorato esclusivamente sull'*algoritmo di crittografia asimmetrico RSA* per creare un software in grado di generare una chiave privata per la crittoanalisi dei testi cifrati spingendoci fino al limite fisico previsto dallo standard IEEE 754, a cui fanno riferimento i compilatori stessi. Siamo, dunque, partiti dall'ipotesi che i due numeri primi (alla base dell'RSA) e la chiave privata fossero noti ed abbiamo realizzato un software in linguaggio **MatLab** in grado di accertare la validità dei dati di ingresso, trovare la

prima chiave privata utile, di interpretare un testo criptato e di cifrarne uno in chiaro. Inoltre, con altre procedure software abbiamo dimostrato le debolezze *Modulo Comune, Esponente privato piccolo, Esponente pubblico piccolo*, che l'RSA presenta per valori di output "piccoli" ossia minori di 768 bit. I tempi di calcolo elevati, impiegati dal codice MatLab (circa 25 minuti per chiavi di 90 bit) hanno reso necessari alcuni interventi per migliorare le prestazioni. A tale proposito si sono realizzati un file eseguibile, direttamente dal codice MatLab, ed una versione in **C++** con DEV v4. Le prestazioni con la versione eseguibile hanno avuto un miglioramento medio di circa 3 minuti rispetto al codice MatLab, invece con la versione in C++ abbiamo ridotto i tempi di calcolo di un ordine di grandezza, attestando il tempo stesso di calcolo per chiavi di 90 bit intorno a 3 minuti circa. L'utilizzazione di tali software ha consentito un opportuno dimensionamento del numero minimo di bit della chiave pubblica descritta in certificati temporanei di autenticazione, basati sull'algoritmo RSA, autonomamente generati dai nodi di una rete wireless al fine di garantire la sicurezza durante orizzonti temporali limitati.