Certificazione di sicurezza per una rete wireless

La certificazione con Verisign è molto costosa e complessa nei piccoli ambienti aziendali. Ecco come utilizzare in alternativa CACert: una certification authority free che consente di operare con certificati digitali nella massima sicurezza

di Giuseppe Paternò

Per rendere più sicura la mia rete Wireless, ho deciso di implementare l'autenticazione del client in modo da generare le chiavi WEP per ogni singolo utente. Per fare questo, ho dovuto installare un RADIUS server ed assegnargli un certificato digitale: solo così, infatti, il RADIUS server è in grado di generare una chiave WEP dinamicamente. Ho creato così una piccola Certification Authority per gestire i miei certificati digitali. In poco tempo però mi sono reso conto che gestire una piccola CA è oneroso e non si giustificava per pochi certificati digitali.

L'alternativa sarebbe stata di farsi assegnare dei certificati digitali da una CA ufficialmente riconosciuta, ad esempio Verisign, ma sarebbe stato costoso. Avrebbe avuto senso se avessi avuto dei siti Web pubblici in SSL, ma non per un uso interno (ad esempio per le VPN, Wireless, LDAP, ...).

Ho trovato in Internet una Certification Authority che rilascia certificati digitali gratuitamente sia per e-mail che per server. Questa CA si chiama CACert (http://www.cacert.org) ed è una organizzazione non-profit con sede in Australia, ma con volontari in tutto il mondo, anche in Italia. La sua missione è rilasciare certificati digitali sia per le persone (per usi come email e autenticazione della persona), sia per i server.

Registrarsi a CACert non costa nulla, ma richiede una verifica dell'identità. Per quanto riguarda i certificati digitali per i server, anche se il certificato viene usato solo all'interno dell'azienda, è necessario avere un dominio su Internet (ad es: azienda.it) ed essere la persona o l'amministratore tecnico che lo ha registrato: questo perchè in automatico CACert deve verificare l'identità dell'ente/persona richiedente mandando in automatico una mail di conferma all'amministratore del dominio Internet. Per avere un certificato digitale per una persona, ad esempio per criptare la posta o per l'identificazione dell'utente (es: VPN, Wireless, ...), basta solamente avere una mail e registrarsi on-line. Se invece si vuole che nel proprio certificato digitale venga indicata la prova della propria identità (ovvero inserire nome e cognome nel certificato), è necessario avviare una procedura apposita, chiamata "Web of Trust". Questa procedura prevede di incontrare personalmente un "notaio incaricato" da CACert (chiamato Assurer) che verifichi l'identità della persona richiedente attraverso due documenti. Qualora un "notaio" non sia vicino, è possibile o contattare l'assurer più vicino e accordarsi (mandando i documenti via fax per esempio) o avviare una seconda procedura descritta sul sito e chiamata TTP. La procedura non è perfetta perchè è possibile rubare o falsificare un documento, ma - come sottolineato da un volontario- sarebbe un problema maggiore rispetto ad avere un certificato da CACert, in quanto punibile penalmente. Altre Certification Authorities ufficiali richiedono di mandare copia dei documenti via fax, pertanto suscettibili di andare incontro alle stesse problematiche.

Vista la crescente popolarità, ci sono discussioni per includere in Mozilla e Konqueror la Certification Authority di CACert, facendo della CA australiana una vera e propria alternativa alle CA tradizionali.

Grazie a CACert, con poco sforzo e senza portare in casa complesse infrastrutture, è possibile per chiunque (privati, piccole e medie aziende) raggiungere un ottimo *livello di sicurezza fino ad oggi raggiunto solo dalle medie* e grandi aziende, sia nell'ambito dell'accesso Wireless, ma anche di privacy sulle e-mail e sui web server interni.

L'Autore
Giuseppe Paternò - gpaterno@gpaterno.com