Metodi di autenticazione

Per un qualsiasi soggetto, l'autenticazione rappresenta l'atto di dimostrare la propria identità. I metodi a disposizione ricadono all'interno di queste tre casistiche:

- **Il soggetto possiede qualcosa**: chiavi elettroniche, chiavi hardware o smart card;
- **Il soggetto conosce qualcosa**: password o PIN;
- **Il soggetto ha una determinata caratteristica o comportamento**: biometria.

E' bene chiarire che, visto le differenze sostanziali esistenti fra i vari metodi, utilizzare l'uno o l'altro dovrebbe sempre derivare da un'attenta analisi del bene da proteggere.

Vediamo brevemente quali sono le caratteristiche principali dei diversi metodi:

- **Kerberos**:
  - La password non viene mai inviata;
- **NTLM v2** (NT Lan Manager Versione 2):
  - Versione migliorata dell'NTLM v1;
  - L'autenticazione avviene utilizzando la password elaborata in modo irreversibile ed uno schema challenge-response;
  - Chiavi di 128 bits.
- **NTLM v1** (NT Lan Manager Versione 1):
  - La password non viene mai inviata;
  - L'autenticazione avviene utilizzando la password elaborata in modo irreversibile ed uno schema challenge-response;
  - Chiavi di 56 bits.
- **LM** (Lan Manager) :
  - La password non viene mai inviata;
  - Utilizza l'algoritmo crittografico DES;
  - Invia i dati in chiaro.
- **EAP** (Extensible Authentication Protocol):
  - E' un'estensione del protocollo PPP (Point-to-Point Protocol) ed è stato sviluppato per permettere l'utilizzo con quest'ultimo di metodi di autenticazione addizionali come, per esempio, token card, one time password e crittografia a chiave pubblica con smart cards e certificati digitali.
- **MS-CHAP v2** (Microsoft Challenge Handshake Authentication Protocol Versione 2):
  - Versione migliorata, dal punto di vista crittografico e della sicurezza, del MS-CHAP;
  - Supporta la mutua autenticazione;
  - Utilizza esclusivamente lo schema di autenticazione NTLM;
  - Invia i dati cifrati utilizzando il protocollo MPPE (Microsoft Point-to-Point Encryption).
  - Permette di cambiare la password se quest'ultima scade durante la procedura di autenticazione.
- **MS-CHAP v1** (Microsoft Challenge Handshake Authentication Protocol Versione 1):
  - E' una versione proprietaria del protocollo CHAP sviluppata da Microsoft;
  - Supporta esclusivamente l'autenticazione del client verso il server;
  - Utilizza lo schema di autenticazione Lan Manager (LM);
  - Invia i dati cifrati utilizzando il protocollo MPPE (Microsoft Point-to-Point Encryption).
  - Permette di cambiare la password se quest'ultima scade durante la procedura di autenticazione.
- **CHAP** (Challenge Handshake Authentication Protocol):
  - La password non viene mai inviata;
  - L'autenticazione avviene utilizzando la password elaborata in modo irreversibile mediante l'algoritmo di hash MD5 ed uno schema challenge-response a triplice handshake.

- **SPAP** (Shiva Password Authentication Protocol):
  - E' una versione proprietaria del protocollo PAP sviluppata da Shiva (società acquisita da Intel nel Febbraio 1999);
  - Durante il processo di autenticazione, la password viene inviata cifrata con un algoritmo crittografico di tipo reversibile;
  - Invia i dati in chiaro;
  - Non permette di cambiare la password se quest'ultima scade durante la procedura di autenticazione.
- **PAP** (Password Authentication Protocol):
  - Trasferisce la password in chiaro;
  - Invia i dati in chiaro;
  - Non permette di cambiare la password se quest'ultima scade durante la procedura di autenticazione.