Subject: Sicurezza Gmail SSL
Posted by Lurkos on Wed, 18 Feb 2009 14:52:53 GMT
View Forum Message <> Reply to Message

La coppia cipher/hash di Gmail Ã¨ ancora considerabile sicura, specie
guardando la dimensione della chiave?
A occhio direi di sÃ¬, ma personalmente non mi sembra sia una bella idea
usare oggi per sistema cosÃ¬ importante MD5 e una chiave pubblica a
soli 1024 bit.

$ openssl s_client -connect imap.gmail.com:993

New, TLSv1/SSLv3, Cipher is RC4-MD5
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol : TLSv1
    Cipher   : RC4-MD5
    Session-ID: **********
    Session-ID-ctx:
    Master-Key: **********
    Key-Arg   : None
    Start Time: 12349*****
    Timeout   : 300 (sec)
    Verify return code: 21 (unable to verify the first certificate)

$ openssl s_client -connect imap.aol.com:993

New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol : TLSv1
    Cipher   : AES256-SHA
    Session-ID: **********
    Session-ID-ctx:
    Master-Key: **********
    Key-Arg   : None
    Start Time: 12349*****
    Timeout   : 300 (sec)
    Verify return code: 20 (unable to get local issuer certificate)

--
Lurkos