ABC di Crittografia

Andrea Pasquinucci
UCCI.IT

Crittografia ... questa sconosciuta

- Cos' è la crittografia oggi ?
- Perché se ne parla tanto ?
- Perché dovrei saperne qualche cosa ?

Crittografia oggi in IT

- La crittografia è ormai pervasiva, compare in quasi tutte le applicazioni, dai sistemi operativi ai giochi
- E' implementata sia in HW che in SW
- Chi gestisce sistemi IT oggi si trova spesso a dover gestire anche protocolli crittografici

Principi di Crittografia

- Confidenzialità
- Integrità
- Autenticità

- La crittografia è una disciplina matematica difficile!

Classi di Algoritmi

- Algoritmi Simmetrici: stessa o (semplicemente deducibile una dall'altra) chiave per cifrare e decifrare (DES, AES)
- Algoritmi Asimmetrici o a Chiave Pubblica: è in pratica impossibile ottenere la chiave Privata dalla chiave Pubblica in un tempo ragionevole (RSA)
- Algoritmi di Hash o Digest: data una stringa di lunghezza arbitraria generano una stringa praticamente unica di lunghezza fissa (MD5, SHA1)

Attacchi

- Nessun algoritmo è matematicamente sicuro (eccetto il One-Time-Pad)
- Se si scopre una vulnerabilità (es. MD5) l'algoritmo cessa di essere sicuro anche praticamente
- Se la chiave (per gli algoritmi simmetrici/a-simmetrici) è troppo corta, si possono provare tutte le chiavi e decifrare il messaggio senza aver bisogno di rompere l'algoritmo

Protocolli Crittografici

Gli algoritmi vengono combinati in protocolli crittografici per ottenere:

- Confidenzialità cifrando i dati con chiavi segrete scambiate automaticamente
- Integrità dei dati con la verifica delle impronte (hash)
- Autenticità dei dati con firma digitale (algoritmi a-simmetrici) o Message-Authentication-Code MAC (hash)

Uso della crittografia

- Per usare correttamente i protocolli crittografici bisogna comprendere i principi di funzionamento degli algoritmi crittografici
- Non è sempre semplice scegliere le opzioni giuste per configurare una applicazione che usa protocolli crittografici
- Se si fa un errore, tutta la protezione offerta dalla crittografia può essere persa

Grazie

Per corsi in crittografia a vari livelli

www.ucci.it/it/corsi/

Andrea Pasquinucci

pasquinucci-At-ucci.it www.ucci.it

Riferimenti Introduttivi

- Simon Singh, *Codici e segreti*, Rizzoli, Milano, 1999
- A.P., *Aspetti di Crittografia Moderna*, Quaderno Clusit, http://www.clusit.it/
- A.P., "*Gestire Certificati Digitali con openssl*", "*Una Introduzione a TLSv1.0*", "*Certificati Digitali e sicurezza di SSL/TLS*", "*OpenVPN, come fare VPN con SSL/TLS*", "*Creare connessioni cifrate con stunnel*", "*File Encryption: Come e Perché*", articoli apparsi su ICTSecurity scaricabili da http://www.ucci.it/

Copyright e Licenza