Sicurezza nelle reti e nei sistemi informatici – 16/5/2011
Tempo: 100 minuti. N.B.: le domande potrebbero avere pesi differenti!

1. Autenticazione

a. Illustrare le idee fondamentali dell'autenticazione basata su challenge/response e su chiave pubblica, mostrando almeno un esempio per ciascuno dei due casi.
b. Descrivere almeno un esempio di attacco a uno schema di autenticazione, mostrando anche le modifiche da effettuare sullo schema per rendere vano l'attacco descritto.

2. Firma digitale

a. Descrivere lo schema di firma digitale DSS.
b. Descrivere lo schema di firma digitale ElGamal e confrontarlo con DSS.

3. Firewall

a. Alice deve configurare un firewall aziendale, consentendo agli utenti solo la navigazione Web esterna (connessioni http – porta 80 – e https – porta 443). Illustrare, attraverso un formalismo scelto a piacere, un insieme di regole che consentano quanto stabilito, distinguendo fra i due casi "filtraggio stateless di pacchetti" e "filtraggio stateful di pacchetti".
b. Introdurre, nello scenario aziendale con filtraggio stateful, la presenza di un Web server (connessioni http e https) e di un e-mail server (gli utenti possono leggere/spedire e-mail solo mentre si trovano all'interno del perimetro aziendale), aggiungendo opportune regole che ne consentano il funzionamento.

4. Controllo degli accessi

a. Descrivere il modello di Bell-LaPadula (BLP), spiegando in dettaglio in cosa consistano le regole "no read-up" e "no write-down", discutendo anche le ragioni della loro esistenza.
b. Descrivere uno scenario applicativo immaginario in cui il modello BLP sia una buona soluzione al problema del controllo degli accessi e illustrarne un altro in cui BLP sia una soluzione non adeguata alle esigenze.

5. Domande brevi (al più 8 linee e una figura per risposta)

a. Descrivere una tecnologia utilizzabile per consentire a un utente domestico di ottenere un collegamento sicuro, attraverso Internet, alla rete aziendale, usufruendone di tutti i servizi.
b. Nella rete aziendale dove lavora Alice viene utilizzata l'infrastruttura di sicurezza "Kerberos". Alice, mentre si reca al lavoro, riflette sul numero minimo di messaggi che la sua workstation dovrà scambiare con altri host della rete per stampare un certo file, memorizzato sull'hard disk della workstation. Qual è questo numero? Spiegare.