Alcuni scenari per il progetto

In questo documento proponiamo alcuni scenari utilizzabili per il progetto. Altri scenari posso essere adottati purché concordati con il docente.

Scenario n. 1
Si consideri un'applicazione distribuita di tipo cliente-servitore in cui ciascun cliente A condivide una chiave segreta a lungo termine con il servitore B. Supponendo di essere in una situazione di mutual-trust, si specifichi, si analizzi, si progetti ed, infine, si implementi un protocollo crittografico che soddisfa i seguenti requisiti:

- al termine dell'esecuzione del protocollo, viene stabilita una chiave di sessione tra A e B;
- al termine dell'esecuzione del protocollo, il cliente A ritiene che il server B dispone della chiave di sessione e viceversa;
- la chiave di sessione viene generata dal server B.

La specifica del protocollo deve mettere chiaramente in evidenza le ipotesi sotto le quali il protocollo funziona correttamente.
L'implementazione deve comprendere la realizzazione di un prototipo in cui il server ed il cliente si scambiano del materiale (testo o binario) cifrato con la chiave di sessione.

Le attività di specifica, analisi e progetto dovranno essere documentate da una concisa relazione scritta.

Scenario n. 2

Si consideri un'applicazione distribuita di tipo cliente-servitore in cui ciascun processo possiede una coppia di chiavi pubblica e privata. Si assuma che il servitore conosca la chiave pubblica di ogni suo cliente (i certificati non sono necessari). Si specifichi, si analizzi, si progetti ed, infine, si implementi un protocollo crittografico che soddisfa i seguenti requisiti:

- al termine dell'esecuzione del protocollo, viene stabilita una chiave di sessione tra cliente e servitore;
- al termine dell'esecuzione del protocollo, il cliente ritiene che il servitore dispone della chiave di sessione e viceversa;

La specifica del protocollo deve mettere chiaramente in evidenza le ipotesi sotto le quali il protocollo funziona correttamente.
L'implementazione deve comprende la realizzazione di un prototipo in cui il server ed il cliente si scambiano del materiale (testo o binario) cifrato con la chiave si sessione .
Le attività di specifica, analisi e progetto dovranno essere documentate da una concisa relazione scritta.

Scenario n. 3

Si consideri un'applicazione distribuita di tipo cliente-servitore in cui il server ha una coppia di la chiavi pubblica e privata e la chiave pubblica è nota ai clienti (il certificato non è necessario). Ciascun cliente condivide una password segreta con il server. Si specifichi, si analizzi, si progetti ed, infine, si implementi un protocollo crittografico che soddisfa i seguenti requisiti:

- al termine dell'esecuzione del protocollo, viene stabilita una chiave di sessione tra cliente e servitore;
- al termine dell'esecuzione del protocollo, il cliente ritiene che il servitore dispone della chiave di sessione e viceversa;

La specifica del protocollo deve mettere chiaramente in evidenza le ipotesi sotto le quali il protocollo funziona correttamente.
L'implementazione deve comprende la realizzazione di un prototipo in cui il server ed il cliente si scambiano del materiale (testo o binario) cifrato con la chiave si sessione .
Le attività di specifica, analisi e progetto dovranno essere documentate da una concisa relazione scritta.

Scenario 4

Si consideri un'applicazione distribuita di tipo peer-to-peer in cui ciascun membro del sistema dispone di una coppia di chiavi pubblica e privata opportunamente certificata. Si specifichi, si analizzi, si progetti ed, infine, si implementi un protocollo crittografico che soddisfa i seguenti requisiti:
al termine dell'esecuzione del protocollo, viene stabilita una chiave di sessione tra cliente e servitore;

- al termine dell'esecuzione del protocollo, il cliente ritiene che il servitore dispone della chiave di sessione e viceversa;

La specifica del protocollo deve mettere chiaramente in evidenza le ipotesi sotto le quali il protocollo funziona correttamente.
L'implementazione deve comprende la realizzazione di un prototipo in cui il server ed il cliente si scambiano del materiale (testo o binario) cifrato con la chiave si sessione .
Le attività di specifica, analisi e progetto dovranno essere documentate da una concisa relazione scritta.