PROGETTI

Istruzioni

1. Ogni gruppo è costituito da due persone al massimo.
2. Ogni gruppo comunica al docente sia la composizione del gruppo (nome, cognome e numero di matricola) sia il progetto prescelto. Nell'oggetto della email utilizzare "snr: progetto"
3. Si possono apportare delle modifiche alla formulazione dei progetti ma queste devono essere concordate con il docente.
4. Il progetto può essere realizzato con il linguaggio C, C++ o Java.
5. Si consiglia di utilizzare la libreria OpenSSL.

Progetto n. 1

Si consideri un sistema distribuito di tipo cliente-servitore in cui ciascun cliente A condivide una chiave segreta K_{ab} 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, K_{ab}' , tra A e B;
- al termine dell'esecuzione del protocollo, il cliente A ritiene che il server B ha la chiave di sessione K_{ab}';
- al termine dell'esecuzione del protocollo, il server B ritiene che il cliente A ha la chiave di sessione K_{ab}';
- la chiave di sessione K_{ab}' viene generata dal server B.

La specifica del protocollo deve mettere chiaramente in evidenza le ipotesi sotto le quali il protocollo funziona correttamente.
Nel progetto può essere utilizzato un qualunque formalismo visto nell'insegnamento di Ingegneria dei Sistemi Software.
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 K_{ab}'.
Le attività di specifica, analisi e progetto dovranno essere documentate da una concisa relazione scritta.

Progetto n. 2

Si consideri un sistema distribuito 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 ha la chiave di sessione;
- al termine dell'esecuzione del protocollo, il servitore ritiene che il cliente ha la chiave di sessione.

La specifica del protocollo deve mettere chiaramente in evidenza le ipotesi sotto le quali il protocollo funziona correttamente.
Nel progetto può essere utilizzato un qualunque formalismo visto nell'insegnamento di Ingegneria dei Sistemi Software.
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.

Progetto n. 3

Si consideri un sistema distribuito 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 il cliente ed il server;
- al termine dell'esecuzione del protocollo, il cliente ritiene che il server ha la chiave di sessione;
- al termine dell'esecuzione del protocollo, il server ritiene che il cliente ha la chiave di sessione.

La specifica del protocollo deve mettere chiaramente in evidenza le ipotesi sotto le quali il protocollo funziona correttamente.
Nel progetto può essere utilizzato un qualunque formalismo visto nell'insegnamento di Ingegneria dei Sistemi Software.
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.

Progetto n. 4

Si consideri un sistema distribuito 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 il cliente ed il server;

- al termine dell’esecuzione del protocollo, il cliente ritiene che il server ha la chiave di sessione;
- al termine dell’esecuzione del protocollo, il server ritiene che il cliente ha la chiave di sessione.

La specifica del protocollo deve mettere chiaramente in evidenza le ipotesi sotto le quali il protocollo funziona correttamente.
Nel progetto può essere utilizzato un qualunque formalismo visto nell’insegnamento di Ingegneria dei Sistemi Software.
L’implementazione deve comprende la realizzazione di un prototipo in cui due partecipanti 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.