Security Methods and Verification

1 Introduction

1. Which are the three main Information Security properties? Please list and briefly describe them.
   (Quali sono le tre principali proprietà per la sicurezza dell'informazione? Elencarle e fornirne una breve descrizione.)
2. Which are the capabilities of an active attacker?
   (Quali sono le capacità di un attaccante attivo?)
3. What is the meaning of *brute force* attack?
   (Che cosa si intende per attacco *brute force*?)

2 Language-based Security and Runtime Verification

1. What does a *Safe Programming Language* provide?
   (Cosa offre un *linguaggio di programmazione safe*?)
2. What is *type safety*?
   (Che cosa si intende per *type safety*?)
3. Which is the difference between *safety* and *security*?
   (Qual è la differenza tra *safety* and *security*?
4. Which are the advantages and the limitations of *Run Time Verification*?
   (Quali sono i vantaggi e i limiti della *Run Time Verification*?)

3 Cryptography

1. DES is block cipher: it takes ...-bit block of plaintext as input, uses a ...-bit key and has ... rounds.
   (DES è un cifrario a blocchi, i cui blocchi sono di ... bit e la cui chiave è di ... bit e in cui i *round* sono ...)
2. Which is the difference between substitution ciphers and transposition ciphers?
   (Quale differenza c'è tra i cifrari a sostituzione e i cifrari a trasposizione?)
3. What is a *message authentication code*?
   (Che cosa è un *message authentication code*?)
4. Which are the three fields of application of the public-key systems?
   (Quali sono le tre categorie di applicazione dei sistemi a chiave pubblica?)

4 Key Management

1. What are the Certification Authorities?
   (Che cosa sono le Autorità di Certificazione?)
2. What is *cross-certification*?
   (Che cosa si intende con *cross-certification*?)

5 Protocols

1. Which is the potential problem with the following protocol?
   (Qual è il problema che si può creare con il seguente protocollo?)

$$\begin{array}{lll} 1 & A \rightarrow S & A, B \\ 2 & A \rightarrow S & \{K_{AB}, B\}_{K_{AS}}, \{K_{AB}, A\}_{K_{BS}} \\ 3 & B \rightarrow A: & \{K_{AB}, A\}_{K_{BS}} \end{array}$$

2. Given the following protocol, describe a possible *type flaw* attack.
   (Dato il seguente protocollo, descrivere un possibile attacco di tipo *type flaw*.)

$$\begin{array}{lll} 1 & A \rightarrow B: & A, \{N_A\}_{K_{AB}} \\ 2 & B \rightarrow A: & \{N_A + 1, N_B\}_{K_{AB}} \\ 3 & A \rightarrow B: & \{N_B + 1\}_{K_{AB}} \\ 4 & B \rightarrow A: & \{K_{AB}, N'_B\}_{K_{AB}} \end{array}$$

3. Given the asymmetric-key Needham-Schroeder protocol, describe the *replay attack* found by Gavin Lowe.
   (Dato il protocollo di Needham-Schroeder a chiave asimmetrica, descrivere il *replay attack* trovato da Gavin Lowe.)

$$\begin{array}{lll} 1 & A \rightarrow B: & \{N_A, A\}_{K_B} \\ 2 & B \rightarrow A: & \{N_A, N_B\}_{K_A} \\ 3 & A \rightarrow B: & \{N_B\}_{K_B} \end{array}$$

6 BAN logic

1. What is BAN logic and which are its aims?
   (Quali sono i limiti di questo approccio?)
2. Write the following formula in BAN logic terms. (Scrivere nella BAN logic questa formula.)

   A believes that B believes they share a secret key.

3. How the protocol messages are transformed in *idealized* messages?
   (Come si trasformano i messaggi dei protocolli e quella dei protocolli *idealizzati*?)

7 Paulson Inductive Method

1. Which are the events that occur in traces?
   (Che tipo di eventi compongono le tracce?)
2. Is the accidental loss of information modelled in this approach?
   (Viene modellata la perdita accidentale di informazione in questo approccio?)
3. What are the operators `parts`, `analz` and `synth` supposed to do?
   (Che cosa fanno gli operatori `parts`, `analz` e `synth`?)
4. How the attacker is taken into account?
   (Come si tiene conto dell'attaccante?)

8 Process algebras and security.

1. Which are the main primitives in the Pi Calculus?
   (Quali sono le primitive principali del Pi Calcolo?)
2. Which are the main differences among Spi-calculus, Pi calculus and LySa?
   (Quali sono le principali differenze tra Spi-calcolo, Pi calcolo e LySa?)

9 CFA and its application to Security

1. What is static analysis and which are its advantages?

   (Cosa si intende per analisi statica e quali sono i suoi vantaggi?)

2. How must the over-approximation be interpreted concerning the prediction of events or violations?

   (Come deve essere interpretata la sovrapprossimazione per quanto riguarda la predizione degli eventi o delle violazioni?)

3. What kind of information the components ρ e κ in the CFA applied to the pi calculus collect?

   (Che cosa raccolgono le componenti ρ e κ nella CFA vista del Pi calcolo?)

4. $$P \mid Q \mid R = (\underbrace{\overline{c}d.P' | c(y).y(z)P''}_{P} \mid R \mid \underbrace{c(w).\overline{w}c.Q'}_{Q})$$

   - Which could be the result (in terms of the ρ e κ components) of the analysis in the above example?
     (Quale potrebbe essere il risultato dell'analisi nell'esempio sopra nelle componenti ρ e κ?)

5. Which is the aim of the component Ψ in the CFA for LySa? (A cosa serve la componente Ψ nella CFA per LySa?)