Security models
1st Semester 2009/2010

F. Autreau
P. Lafourcade
JL. Roch

Final Exam 1h30
Date: 3.12.2009
TOTAL: 80 points

Notice: the number of points corresponds approximatively to the number of minutes needed for solving an exercise.

Exercise 1
(15 points) Given the security levels TOP SECRET, SECRET, CONFIDENTIAL and UNCLASSIFIED (ordered from highest to lowest) and two categories: Nuclear and Army. We consider four subjects:

- the president has a TOP SECRET clearance for Nuclear and Army,
- the colonel has SECRET clearance for Army and Nuclear,
- the major has only CONFIDENTIAL clearance for Army, and
- the soldier has only UNCLASSIFIED clearance for Nuclear.

We also have some objects (documents):

- the army position at security level SECRET,
- the number of army units at security level CONFIDENTIAL,
- the number of nuclear units at security level CONFIDENTIAL,
- the costs of the nuclear program at security level UNCLASSIFIED,
- the costs of the army at security level UNCLASSIFIED, and
- the nuclear code at security level TOP SECRET.

1. (3 points) Recall Bell-LaPadula and Biba security models and explain the difference between the two models.

2. (1 points) Draw the lattice associated with this scenario.

3. (5 points) Place on the lattice all the objects and subjects.
4. (6 points) Answer with justifications the following questions based on the Bell-LaPadula model:

(a) Can the president compute the overall defense costs (army + nuclear)?
(b) Can the major compute the total number of nuclear and army units?
(c) Can the colonel compute the total number of nuclear and army units?
(d) Can the colonel change the army position?
(e) Can the major change the nuclear code?
(f) Can the soldier change the nuclear code?

Exercise 2
(10 points) Consider the following control access in a bank, where users are Alice, Bob, Charlie and John:

<table>
<thead>
<tr>
<th>User</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>read account of Mr X</td>
</tr>
<tr>
<td>Alice</td>
<td>read account of Mr Y</td>
</tr>
<tr>
<td>Alice</td>
<td>write in project New Bank</td>
</tr>
<tr>
<td>Alice</td>
<td>start application Money</td>
</tr>
<tr>
<td>Alice</td>
<td>start application Create New client</td>
</tr>
<tr>
<td>Bob</td>
<td>read account of Mr Y</td>
</tr>
<tr>
<td>Bob</td>
<td>write in project New Bank</td>
</tr>
<tr>
<td>Bob</td>
<td>start application Create New client</td>
</tr>
<tr>
<td>Bob</td>
<td>read account of Mr X</td>
</tr>
<tr>
<td>Charlie</td>
<td>read account of Mr X</td>
</tr>
<tr>
<td>Charlie</td>
<td>read account of Mr Y</td>
</tr>
<tr>
<td>Charlie</td>
<td>write in project New Bank</td>
</tr>
<tr>
<td>Charlie</td>
<td>start application Create New client</td>
</tr>
<tr>
<td>John</td>
<td>read account of Mr Y</td>
</tr>
<tr>
<td>John</td>
<td>start application Money</td>
</tr>
<tr>
<td>John</td>
<td>start application Create New client</td>
</tr>
</tbody>
</table>

Propose a RBAC model for improving this situation.

Exercise 3
(10 points) Let $\mathcal{E}$ be an IND-CCA2 secure encryption scheme. We modify this scheme into $\mathcal{E}'(m) = \mathcal{E}(m)||h(m)$, where $h$ is an hash function. This should help the user to detect some errors in the transmission of the messages. Prove that the new scheme $\mathcal{E}'$ is not IND-CPA. It means give an attack against IND-CPA for $\mathcal{E}'$.

Exercise 4
(10 points)
We recall Dolev-Yao intruder deduction system:
Consider the following protocol

\begin{align*}
A \to S : & \langle A \rangle_{Ks}, \{B\}_{Ks} >, \{A \oplus N_A\}_{Ks} > \\
A \to S : & \langle N_A \oplus B \rangle_{Ks}, \{N_A \oplus c\}_{Ks} > \\
B \to S : & \langle B \rangle_{Ks}, \{A\}_{Ks} >, \{B \oplus N_B\}_{Ks} > \\
B \to S : & \langle N_B \oplus A \rangle_{Ks}, \{N_B \oplus c\}_{Ks} > \\
S \to A : & K \oplus \{N_A\}_{Ks} \\
S \to B : & K \oplus \{N_B\}_{Ks}
\end{align*}

Where $c$ is a weak shared secret between $A$ and $B$, $\oplus$ is the exclusive-or and $K$ is a new fresh symmetric key between $A$ and $B$ which has been generated by $S$.

1. (3 points) Modify the protocol in order to model the following property
   \[ \{x \oplus y\}_{Ks} = \{x\}_{Ks} \oplus \{y\}_{Ks} \]

2. (2 points) Extend the Dolev-Yao deduction system by adding an extra rule called (XOR) which models the intruder’s ability to use the xor.

3. (5 points) In the extended deduction system, prove or disprove that $K$ is a secret for a passive Dolev-Yao intruder?

Exercise 5

(20 points) We recall the Yahalom protocol, where $Kas$, $Kbs$ and $Kab$ are symmetric keys.

1. $A \to B: A, N_A$
2. $B \to S: B, \{A, N_A, N_B\}_{Kbs}$
3. $S \to A: \{B, Kab, N_A, N_B\}_{Kas}, \{A, Kab\}_{Kbs}$
4. $A \to B: \{A, Kab\}_{Kbs}, \{N_B\}_{Kab}$

1. (5 points) Give a role description of this protocol.
2. (5 points) Give a constraint system associated to your role description.
3. (10 points) Propose a type flaw attack on this protocol.
   Hint: message 3 is not used in the attack.
Exercise 6
(15 points) Zheng & Seberry in 1993 proposed the following encryption scheme:

\[ f(r)||G(r) \oplus (x||H(x)) \]

where \( x \) is the plain text, \( f \) is a one way trap-door function (like RSA), \( G \) and \( H \) are two public hash functions, || denotes the concatenation of bitstrings and \( \oplus \) is the exclusive-or operator.

- (5 points) Give the associated decryption algorithm.
- (10 points) Give an IND-CCA2 attack against this scheme.
  
  Hint: you cannot ask the cipher of \( m_b \) to the decryption oracle, but a cipher of \( m_{\overline{b}} \) is not forbidden...