Security models

1st Semester 2011/2012

F.Autreau
P.Lafourcade
M. Gagné
JL. Roch

P. Lafourcade
M. Gagné

Final Exam
90 minutes

Date: 1.12.2011
TOTAL: 90 points

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

Exercise 1 (Security Proof (15 points))

- (3 points) Give the definition of the notion of OW-CPA security in the form of a security game.
- (12 points) We remind the definition of a one-way function: a function f is a one-way function if, for a randomly chosen x in the domain of f, no polynomial-time algorithm can compute x when given only the description of f and $f(x)$.

  We define the encryption algorithm E, which has a one-way function as its public key, as follows:

  - sample a random x in the domain of f.
  - output $\langle f(x), x \oplus m \rangle$

  Prove that this is a OW-CPA secure encryption scheme if f is a one-way function.

Exercise 2 (Exercise of the SET: Recoverable Set of Keys (15 points))
Compute the recovrable set of keys F_{kr} and the pattern of the following expressions:

- $E_1 = \langle \{k_1\}_{k_2}, \{k_2\}_{k_1} \rangle$
- $E_2 = \langle \{\langle k_2, k_4 \rangle\}_{k_1}, \{\{k_1\}_{k_2}\}_{k_4} \rangle, k_4$
- $E_3 = \{\{\langle k_3, 0 \rangle\}_{k_2}\}_{k_1}, \langle \{0\}_{k_3}, k_1 \rangle, k_5$

Exercise 3 (Access Control (14 points))
In a hospital we have 4 kind of users: Doctor, Nurse, Secretary, Patient. In this hierarchy, Doctors are superior to Nurse, Secretary and Patient, Nurse and Secretary are superior to Patient, but Nurse is neither superior nor inferior to Secretary. Medical information have several security levels for files, in decreasing order: Operating room, Emergency and Personal.

1. (3 points) Draw a lattice of all the security clearances.

Suppose that **Dave** the surgeon has clearance (Doctor,Operating room), **Nancy** the nurse has clearance (Nurse, Emergency), **Shari** the secretary has clearance (Secretary, Emergency) and **Paul** the patient has clearance (Patient, Personal). A **Receipt** containing payment information has clearance (Secretary, Personal), a **Prescription** for antibiotics has clearance (Doctor, Emergency), the **List** of medical tools necessary for an operation has clearance (Nurse, Operating room) and the **File** containing the home address of patients in the hospital has clearance (Secretary, Emergency).

2. (3 points) Place all these actors and documents (in bold in the paragraph above) on the preceeding lattice.

In the Bell-Lapadula model, say if the following actions are allowed, explaining each time why that is:

3. (1 point) Dave writes on the List.
4. (1 point) Nancy reads the File.
5. (1 point) Paul writes on the Prescription
6. (1 point) Shari reads the receipt.

In the BIBA model, say if the following actions are allowed, explaining each time why that is:

7. (1 point) Dave writes on the List
8. (1 point) Nancy reads the File
9. (1 point) Dave writes on the File
10. (1 point) Shari reads the prescription.

Exercise 4 (Proof protocol (25 points))
We recall the rules for solving a constraint system.

R_1	$C \cup \{T \Vdash u\}$	$\rightsquigarrow$	C	if $T \cup \{x \mid T' \Vdash x \in C, T' \subset T\} \vdash u$
R_2	$C \cup \{T \Vdash u\}$	$\rightsquigarrow_\sigma$	$C\sigma \cup \{T\sigma \Vdash u\sigma\}$	$\sigma = mgu(t,u), t \in st(T)$, t, u not both variables
R_3	$C \cup \{T \Vdash u\}$	$\rightsquigarrow_\sigma$	$C\sigma \cup \{T\sigma \Vdash u\sigma\}$	$\sigma = mgu(t_1,t_2), t_1, t_2 \in st(T)$, t_1, t_2 not both variables
R_4	$C \cup \{T \Vdash \{u\}_v\}$	$\rightsquigarrow$	$C \cup \{T \Vdash u, T \Vdash v\}$	
R_5	$C \cup \{T \Vdash \langle u, v\rangle\}$	$\rightsquigarrow$	$C \cup \{T \Vdash u, T \Vdash v\}$	
R_6	$C \cup \{T \Vdash u\}$	$\rightsquigarrow$	$\bot$	if $T = \emptyset$ or $var(T) = var(u) = \emptyset$ and $T \not\vdash u$

We consider the following naïve protocol.

1. $I \to R : \{I, N_I\}_{pk(R)}$
2. $R \to I : \{N_R, N_I\}_{pk(I)}, \{R\}_{pk(I)}$
3. $I \to R : \{N_R\}_{pk(R)}$

1. (5 points) Give an (active) attack that would allow an adversary to recover the secret N_R of this protocol.
2. (5 points) Give the role specification of the protocol.
3. (5 points) Give the constraint system associated with the interleaving $(u_{I_1} \to v_{I_1}), (u_{R_1} \to v_{R_1}), (u_{I_2} \to v_{I_2})$, assuming that the adversary knows only the participants to the protocol, their public key, and his own public/private key pair.
4. (10 points) Resolve the constraint system in a way that shows the existence of an attack.

Exercise 5 (E-Voting (21 points) ONLY M2P)
We modify the ElGamal encryption as follows to encrypt small integers:

- Compute $h = g^x$ where $g, h \in \mathbb{Z}_p^\star$ for a large prime p and g is a generator of $\mathbb{Z}_p^\star$.
- Public key is (p, g, h) and the private key is x.
- Encryption of $n \in \mathbb{Z}_p^\star$ is $c = (g^k, g^n \cdot h^k)$, where k is a random number between 0 and $p - 1$.

1. (2 points) Give the decryption algorithm associated to ElGamal. *Hint:* since we assume that the encrypted integer n is small, it is ok to use up to n operations to recover n.
2. (2 points) If $\{m\}_k = (a, b)$ and $\{n\}_k = (c, d)$ are two ciphertexts, we define $\{m\}_k \cdot \{n\}_k = (a \cdot c, b \cdot d)$. Prove that, under this operation, ElGamal is a homomorphic encryption ($\{m\}_k \cdot \{n\}_k$ will be a ciphertext for $m + n$).
3. (5 points) Explain 5 security properties that an e-voting system should satify.
4. (3 points) Naïve voting system: We consider that 1 and 0 are the two possible ballots for an elections. A server publishes his public RSA key (N, e). Each voter encrypt his vote, 0 or 1, as $RSA_{(N,e)}(0)$ or $RSA_{(N,e)}(1)$ respectively. At the end of the election the server decrypt all received messages and counts the votes. Show how an attacker eavesdropping on the network can learn everybody's vote.
5. We improve this scheme by replacing RSA by the variant of ELGamal above. At the end, instead of decrypting all the votes, the server uses the homomorphic property to sum all the ciphertexts, and decrypts only this final ciphertext to obtain the tally.

- (2 points) Exlpain why this IND-CPA encryption can prevent the previous attack.

(∗) (2 points) Find how a voter (who does not have a decryption oracle at any point of the attack) could cheat in this protocol to favor his candidate.

- (2 points) Suppose that an attacker A wants to force a voter V to vote for candidate 0. If A intercepts the ciphertext containing V's vote, how could he ask V to prove that he voted for candidate 0?
- (3 points) Propose a solution in order to avoid this attack found at question (∗).

Exercise 6 (IND-XXX Attack (21 points) ONLY M2R)
We consider the following encryption function that uses the RSA function with public key (N, e) and secret key d, and a public hash function G:

- sample a random $x \in \{0, \ldots, N-1\}$
- output $\mathcal{E}_{(N,e)}(m) = \langle RSA_{(N,e)}(x),\ G(x) \oplus m \rangle$

1. (3 points) Recall the defintion of IND-CCA2 in the form of a security game.
2. (3 points) Give the decryption function corresponding to the encryption function above.
3. (5 points) Show that this scheme is not IND-CCA2 secure by giving an adversary that breaks the IND-CCA2 security of the scheme.

Consider now the following modification to to the encryption function above, which uses one more hash function (H):

- sample a random $x \in \{0, \ldots, N-1\}$
- output $\mathcal{E}'_{(N,e)}(m) = \langle RSA_{(N,e)}(x),\ G(x) \oplus m,\ H(m) \oplus x \rangle$

in which decryption of $C = \langle a, b, c \rangle$ proceeds as for the preceeding scheme, except that after the message m is computed, the decryption algorithm also verifies that $c = RSA_d^{-1}(a) \oplus H(m)$; if it is, it outputs m, otherwise it outputs $\perp$.

4. (10 points) Show that this new scheme is not even IND-CPA by giving an adversary that breaks the IND-CPA security of the scheme.