IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2017

MEng Honours Degrees in Computing Part IV
MSc in Advanced Computing
MSc in Computing Science (Specialist)
for Internal Students of the Imperial College of Science, Technology and Medicine

This paper is also taken for the relevant examinations for the Associateship of the City and Guilds of London Institute

PAPER C408H

PRIVACY ENHANCING TECHNIQUES

Thursday 15 December 2016, 11:40
Duration: 70 minutes

Answer TWO questions

Paper contains 3 questions
Calculators not required

1a Consider the following *1*-from-*2* oblivious transfer protocol based on the well-known Diffie-Hellman key-exchange protocol in an honest-but-curious setting.

1. Alice generates a random number a (from $\mathbb{Z}p$). Similarly, Bob generates a random number b. Bob's message selection bit is m.

2. Alice sends $A=g^a$ to Bob. g is a suitable generator for the group.

3. If $m=0$ Bob sends $B=g^b$ to Alice.
   If $m=1$ Bob sends $B= Ag^b$ to Alice.

4. Alice computes $k_0=Hash(B^a)$, $k_1=Hash((B/A)^a)$,
   $C_0 = E_{k_0}(M_0)$, $C_1 = E_{k_1}(M_1)$
   Alice sends C_0 and C_1 to Bob.

5. Bob computes $k = Hash(A^b)$, $M_m = D_m(C_m)$,

For this protocol:

i) Explain why Bob's output equals M_m.

ii) Explain why Alice learns nothing about m and why Bob learns nothing about M_z for $z \neq m$. What assumptions do you have to make about the two cryptosystems for this to be true?

iii) Explain what, if any, issues arise if Alice sets a to 0. What if Bob sets b to 0 (with Alice generating a random number a as normal)?

b Complete the following oblivious transfer protocol that uses a trusted third party Trent. Alice's messages M_0 and M_1 are binary values of length k. Bob's message selection bit is m.

1. Trent → Alice: R_0, R_1 Random binary values each of length k

2. Trent → Bob: t, R_t Random bit t

3. Bob → Alice: b $b = t \oplus m$

4. Alice → Bob: C_0, C_1

How should Alice compute C_0 and C_1? How should Bob compute M_m?

The four parts a(i), a(ii), a(iii), b carry 50%, 15%, 15%, 20% of the marks.

2 Write S4P specifications for the following hospital patient record system. Label your S4P assertions and queries. Underline S4P keywords *says*, *may*, *will*, *can say*, *exists*. State any assumptions that you make.

a Imperial Hospital Privacy Policy

(i) Doctors of the hospital are permitted to access the records of patients under their care. Any doctor is permitted to access the record of a patient they treat in a medical emergency – however an audit of the access will be carried out within 3 days.

(ii) Doctors are able to delegate access to their patient's record to a nurse of the hospital.

(iii) Doctors must be registered with the British Medical Association (BMA). Nurses must be registered with the Nursing and Midwifery Council (NMC).

(iv) Doctors cannot be nurses.

(v) Doctors and nurses cannot access their own record.

b Patient Pat's Privacy Preferences

(i) Doctors and nurses of a hospital can access Pat's hospital record if Pat is a patient at the hospital and he gives his consent.

(ii) If Pat is unable to give consent, for example, if Pat is unconscious, then consent can be given by his next of kin, Mary.

(iii) In an emergency, any doctor treating Pat can access Pat's patient record, but accesses must be subject to a follow up audit within 7 days.

c How would we check that Imperial's privacy policy (part a) would be satisfied by Pat's privacy preferences (part b)?

Which assertions would need to be satisfied to enable nurse Nancy to access Pat's record? You can add new assertions for Principals.

The three parts carry, respectively, 50%, 30%, and 20% of the marks.

3a In the released Netflix dataset would removing the names of columns have prevented de-anonymisation while allowing an effective competition? Explain you answer.

b Prove that the Laplace Mechanism is ε-differentially private.

c In IPv6 networking every device can have several globally unique addresses.

IPv6 addresses are 128-bit and have a 64-bit network prefix and a 64-bit device interface identifier.

ISPs typically assign customers their own network prefix.

Device interface identifiers are typically generated by devices and/or by routers. One technique even includes the device's MAC address in the generated identifier.

Discuss the privacy implications of using IPv6 and what mechanisms are needed to support privacy.

The three parts carry, respectively, 20%, 30%, and 50% of the marks.