Esecurity: secure internet & e-cash, summer 2012

MICHAEL NÜSKEN, RAOUL BLANKERTZ

12. Exercise sheet
Hand in solutions until Sunday, 1 July 2012, 23:59

The following is a loose collection of exercises, which you can solve to prepare for the exam. Note that this is not an example of how the exam could look like. In particular the exam will differ in length.

Exercise 12.1 (Multiple choice). (0 points)

Decide which of the following statements are right and which are wrong. Write "R" in the box for right and "W" for wrong. In any subquestion you achieve the points only if you have filled in all boxes correctly.

(i) Encryption provides ...

(a) ... confidence. ☐

(b) ... fun. ☐

(c) ... integrity. ☐

(d) ... confidentiality. ☐

(e) ... authenticity. ☐

(ii) The Diffie-Hellman key exchange based on the group G is ...

(a) ... insecure if the discrete logarithm in G is easy compute. ☐

(b) ... secure against passive attackers if the computational Diffie-Hellman problem in G is hard. ☐

(c) ... vulnerable against man-in-the-middle attacks. ☐

(iii) Consider a protocol which uses a Diffie-Hellman key exchange to provide keys for encryption and message authentication.

(a) To safe resources the key for encryption and the key for authentication should be the same. ☐

(b) Since encryption is most important the encryption scheme used in the protocol should be much harder to break than the key exchange and the authentication scheme. ☐

(c) Since the Diffie-Hellman key exchange is vulnerable against man-in-the-middle attacks, the protocol is insecure. ☐

(d) Since the protocol does not provide more security than the weakest scheme in the chain, increasing the security of the encryption scheme does not increase the overall security of the protocol. ☐

(iv) The public key infrastructure of X.509 is ...

(a) ...a hierarchical public key infrastructure. ☐

(b) ...the key infrastructure used in GnuPG. ☐

(c) ...a large physical network, that ensures the security of electronic locks. ☐

(d) ...a key infrastructure that can be used for SSL/TLS. ☐

Exercise 12.2 (Security notion). (0 points)

Prove or disprove:

(i) Existential Unforgeability implies Universal Unforgeability.

(ii) Security under Chosen Ciphertext Attack implies security under Key Only Attack.

(iii) If factorization of integers is hard then the RSA signature scheme (without hashing) is EUF-CMA secure.

(iv) If factorization of integers is hard then RSA encryption scheme is IND-KOA secure.

(v) If the discrete logarithm problem for a group G is hard then the ElGamal encryption scheme with underlying group G is UB-KOA secure.

Exercise 12.3 (Combination of encryption schemes). (0 points)

(i) What does it mean if an encryption scheme provides n-bit security.

(ii) Assume a given symmetric key encryption scheme gives n-bit security and a given public key encryption scheme gives m-bit security. How many bits security does a hybrid scheme, which makes use of these both encryption schemes, provide at most. Is this upper bound always achieved?

Exercise 12.4. (0 points)

Make up your own protocols and consider for them the questions from exercise 6.2.

Exercise 12.5 (secure Internet?). (0 points)

(i) What is a hybrid encryption scheme? What are its advantages?

(ii) Briefly say what IKE is and how it works in IPsec?

(iii) Discuss the advantages and disadvantages of protocols, where the parameters (Diffie-Hellman group, block encryption algorithm, etc.) are negotiated.

(iv) Discuss a man-in-the-middle attack against SSH.

Exercise 12.6 (Blind signature schemes). (10 points)

(i) What is a blind signature scheme. 2

(ii) Describe a particular blind signature scheme (of your choice) in detail. 3

(iii) Explain why and how blind signature schemes are employed in ecash protocols. 3

(iv) If the bank signs a blinded message, how can she be sure that the original message is of the required form? 2

Exercise 12.7 (Coin flipping via hash functions). (0 points)

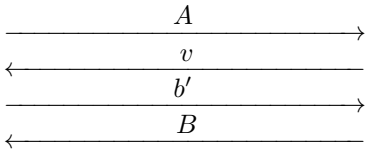
Let $h\colon \{0,1\}^{2n} \to \{0,1\}^m$ with $n > m$. A chosen-prefix collision (CPC) of h with respect to the prefix $A\{0,1\}^k$ with $2n > k > 0$ is a pair $(B, B^*) \in (\{0,1\}^{2n-k})^2$ such that $B \neq B^*$ and $h(A\|B) = h(A\|B^*)$. We say h is chosen-prefix collision resistant (CPC resistant) if for any given prefix A it is hard to compute a chosen-prefix collision of h with respect to A.

(i) Prove: If h is collision resistant then h is CPC resistant.

Now consider the following coin flipping protocol.

Coin flipping protocol.

1. Alice chooses $A \in \{0,1\}^n$.
2. Bob chooses $b \in \{0,1\}^n$ and $v = h(A\|B)$.
3. Alice makes a guess b' to the first bit of B.
4. Bob acknowledges Alice of B.
5. Alice wins if her guess was right; else Bob wins.



Prove the following statements.

(ii) If Bob is honest, then Alice wins with probability $1/2$.

(iii) If Bob can compute CPCs with respect to any A, then he can win each coin flip.

(iv) If h is collision resistant and Alice chooses b' randomly, then Bob wins with probability $1/2$.

Note. *The following questions are suggested by students as solution of 11.4 and from the course of the last year.*

Exercise 12.8. (0 points)

What are the eight different criteria to judge a protocol? Explain them (optional: explain one way to solve the issues).

Exercise 12.9. (0 points)

Name possible attacks on e-mail traffic and countermeasures that can be taken to prevent these attacks.

Exercise 12.10. (0 points)

(i) Explain by means of an example how a so called replay attack works.

(ii) Give at least one concrete countermeasure against replay attacks used in technologies discussed during the semester.

Exercise 12.11. (0 points)

(i) How does SSL provide authenticity, how does SSH?

(ii) Give a concrete example on where and how SSL is introduced in other technologies/protocols.

Exercise 12.12. (0 points)

(i) What is the difference between tunnel mode and transport mode in IPSec?

(ii) Is it possible to establish an IPSec tunnel within a different IPSec tunnel? Explain why/why not.

Exercise 12.13. (0 points)

Why does encrypting an email not implicitly provide authentication of the sender?

Exercise 12.14. (0 points)

How does the Diffie-Hellmann key change perform under a man in the middle attack? And how to prevent a man in the middle attack?