Esecurity: secure internet & e-passports, summer 2011

MICHAEL NÜSKEN, RAOUL BLANKERTZ

14. Exam preparation sheet
No handin

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 14.1 (Security notion). (0 points)

Prove or disprove the following statements:

(i) Existential Unforgeability implies Universal Unforgeability.

(ii) Security under a Chosen Ciphertext Attack implies security under a 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 factorization of integers is easy then RSA encryption scheme is UB-KOA insecure.

(vi) 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 14.2. (0 points)

Describe the role of randomness in cryptographic schemes. What happens if we use a predictable pseudo random number generator?

Exercise 14.3. (0 points)

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

(ii) Assume a given public key encryption scheme gives n bit security and a given private 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?

(iii) What are the pros and cons for hybrid encryption schemes.

Exercise 14.4. (0 points)

Assume an attacker can guess the least bit of a secret RSA key e form a chipher-/plaintext pair (x, y) with probability of 0.51. How can he proceed to compute the complete key?

Exercise 14.5. (0 points)

Describe the public key infrastructure of X.509.

Exercise 14.6. (0 points)

Describe the public key infrastructure of GnuPG (web of trust).

Exercise 14.7. (0 points)

(i) Is the Diffie-Hellman key exchange vulnerable to man-in-the-middle attacks? Explain.

(ii) How could one modify the protocol to prevent man-in-the-middle attacks?

Exercise 14.8. (0 points)

Consider the following modified Diffie-Hellman protocol. It makes use of a secure signature scheme.

Protocol DH+sign+ack. Signed and acknowledged Diffie-Hellman key exchange.

1. Alice chooses $a \in \mathbb{N}_{<d}$, computes aP and signs $['\text{Alice}', aP]$. $\xrightarrow{['\text{Alice}', aP]_{\text{Alice}}}$
2. Bob chooses $b \in \mathbb{N}_{<d}$, computes bP and signs $['\text{Bob}', bP]$. $\xleftarrow{['\text{Bob}', bP]_{\text{Bob}}}$
3. Alice computes $a(bP) = abP$ and a hash. $\xrightarrow{\text{hash}(0, abP)}$
4. Bob computes $b(aP) = abP$ and a hash. $\xleftarrow{\text{hash}(1, abP)}$

(i) Is this protocol secure against man-in-the-middle attacks?

(ii) Does it provide perfect forward security?

(iii) Is it secure against replay attacks?

Exercise 14.9 (Right or Wrong). (0 points)

Are the following statements right or wrong?

(i) ElGamal encryption scheme with $(\mathbb{Z}_n, +)$ is UB-KOA secure.

(ii) ElGamal encryption scheme with $(\mathbb{Z}_p^\times, \cdot)$ and p being an appropriate 160 bit number gives 80 bit security.

(iii) Combining ECDSA over $\mathbb{F}_{2^{512}}$ with SHA-256 gives 256 bit security.

(iv) If factoring integers is hard, then RSA is UB-KOA secure.

(v) The cryptographic schemes used in IPsec are negotiated between the client and the host.

(vi) After communicating to Bob via IPsec, Alice can proof that Bob has actually said what he had said.

(vii) Encryption provides integrity.

(viii) Encryption provides authenticity.

(ix) Encryption provides confidentiality.

(x) A terminal can access an e-Passport only if it knows the MRZ (or at least certain parts of the MRZ).

Exercise 14.10. (0 points)

Assume we have a database with 1000 entries. There are different users who have limited access to this database. We want to provide integrity by a cryptographic signature scheme.

(i) If we sign each possible combination of entries, how many signatures do we produce? Does this introduce some security concerns?

(ii) How can we provide integrity by producing only one signature?

Note. *The following questions are given by students as solution of 13.4.*

Exercise 14.11 (e-mail). (0 points)

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

Exercise 14.12. (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 14.13. (0 points)

How is the "not clonable" property brought into todays e-passports. How does it work?

Exercise 14.14. (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 14.15. (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 14.16. (0 points)

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

Exercise 14.17. (0 points)

Explain the idea of a "challenge semantic attack".

Exercise 14.18. (0 points)

What are challenges and difficulties of the concept of recovation lists within a PKI?

Exercise 14.19. (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?