Academic Year: Winter Semester 2021/22

6090: Security of Computer and Embedded Systems

Problem Sheet 9

Security Protocols

In this problem sheet, we will

- deepen our knowledge of security protocols and in particular authentication protocols,
- design and analyse security protocols as well as try to find attacks.

1. Security Protocols

Exercise 1: *Security Protocols*

1- What properties should a nonce satisfy (at the generation time)?

- ☐ a) freshness
- ☐ b) known to all participants
- ☐ c) secret
- ☐ d) easy to compute

2- Which of the following can be used to make replay attacks in authentication protocols harder?

- ☐ a) Nonce
- ☐ b) Monotonically increasing sequence number
- ☐ c) Time stamp
- ☐ d) Random number used no more than once

3- Which notation are we using for symmetric encryption?

- ☐ a) $\{M\}_{\mathrm{inv}K}$
- ☐ b) $\{M\}_K$
- ☐ c) $\{|M|\}_K$
- ☐ d) none of the mentioned

4- On which assumption is the security of the Diffie-Hellmann Key Exchange based?

- ☐ a) Computing discrete logarithms
- ☐ b) Computing prime factorization
- ☐ c) Computing cubic roots
- ☐ d) Exponentiation

2. Designing and Analysing Security Protocols

The following exercise will deepen your knowledge on various security goals that we might want to achieve when designing security protocols as well as deepen your knowledge in designing and/or extending security protocols.

Exercise 2: *Electronic Voting*

To simplify the process of organizing an upcoming referendum, a government plans to automate the process, i.e., to introduce online voting. The company that was hired to implement the online referendum system designed the following protocol:

1. $A \rightarrow S: A$
2. $S \rightarrow A: \{Q, \mathrm{N}_S\}_{\mathrm{pk}(A)}$
3. $A \rightarrow S: \{Ans_Q, \mathrm{N}_S\}_{\mathrm{pk}(S)}$

where A is a voter, S is the voting server, N_S is a nonce sent by the server to ensure freshness, Q is a referendum question, and Ans_Q is A's answer to the questions Q. Assume that A and S share their public keys in advance.

You are hired as a security consultant. Your main task is to compare the proposed electronic voting protocol with the physical voting method (which we assume to be secure). In your analysis, you should make the following assumptions with respect to the capabilities of the attacker, i.e., the attacker can (i) create new messages, (ii) block messages, and (iii) compose new messages.

1. Does this protocol provide anonymity? Can an attacker tell who has voted?
2. Does it provide confidentiality? Can an attacker find out, for a given A, how he or she voted?
3. Does the protocol provide authentication? Can S be sure that the answer came from A?
4. Can each voter vote at most once?
5. Is availability guaranteed? Can A be sure that she can vote if she wants to?
6. Is integrity provided? Does S know that a given answer has not been modified?

3. Attacking Security Protocols

In the following exercise, you will deepen your knowledge in finding security problems in security protocols or their actual use.

Exercise 3: *Interleaving Attack*

Consider the following mutual authentication protocol with pre-shared symmetric keys:

1. $A \rightarrow B: A, Seq$
2. $B \rightarrow A: \{|Seq + 1, A|\}_{\mathrm{sk}(A,B)}$
3. $A \rightarrow B: \{|Seq + 2, B|\}_{\mathrm{sk}(A,B)}$

where Seq is a 32-bit monotonically increasing sequence number and maintained by both A and B.
A and B reject the authentication if Seq in the first step is less than or equal to their maintained value.
Does an interleaving attack (similar to the discussed Lowe's attack on NSPK) work? If so, write down how to attack the protocol and how to fix it. Otherwise, explain why the attack will not work.

References

1. Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, Inc., New York, NY, USA, 1st edition, 2001. The complete book is available at: http://www.cl.cam.ac.uk/~rja14/book.html
2. Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. Handbook of Applied Cryptography. CRC Press, Inc., Boca Raton, FL, USA, 5th edition, 2001. The complete book is available at: http://cacr.uwaterloo.ca/hac/
3. Bruce Schneier. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.
4. Chris Karlof, Naveen Sastry, and David Wagner. Cryptographic Voting Protocols: A Systems Perspective. In Proceedings of the 14th Conference on USENIX Security Symposium - Volume 14 (SSYM'05), 2005. Available at: https://www.usenix.org/legacy/event/sec05/tech/full_papers/karlof/karlof.pdf