CS 419 / ECE 478: Introduction to Network Security (Spring 2016)

Instructor: Dr. Attila A Yavuz

Homework 3
(Assigned 05/17/16, Due 5/27/16)

Requirements: HW will be completed by each student **individually (no collaboration)**.

Directly borrowing (e.g., copy-paste) from any material and putting in solutions (e.g, from online solutions, Wikipedia, or research papers) is **plagiarism** (see Syllabus for its corresponding actions). Please cite very carefully each resource you use, but citing a solution does not give a license to directly put it as an answer**. All of your answers must be in your in own words and interpretations.**

HW should be prepared by LaTeX or Word. Handwritten submissions **are *not* accepted.**

----

1) [30] Impact of the PRGN Quality over the Security of DLP-based Primitives

During the class, we have discussed Meta-Elgamal signature families. DSS and Schnorr signatures are some of the most well-known examples of such digital signatures. In all these schemes, during the signature generation phase, the signer invokes a PRNG. For instance, in Schnorr signature scheme [see the slides of ETA paper in the webpage], randomness *r* is generated and used together with the message as *H(M||r)*. Despite its advantages for the formal proof process, this approach may also create vulnerabilities for such cryptosystems. Consider the following attack:

The server computes a Schnorr signature under private key *y* (here we follow the notation of ETA slide/paper) periodically such that for every message M to be signed, it adds current time stamp *ts_i* and involve randomness *r_i* as H(M||ts_i||r_i) and follows the Schnorr signature algorithm as required. Here, r_i is the output of a PRNG, which derives randomness from certain Operating System (OS) parameters.

Assume that an attacker managed infiltrating a virus into the OS of the server, which is capable of resetting OS parameters that PRGN relies on, meaning the seed of PRNG is set to its initial values.

Show that by observing small-constant number of signatures, the attacker can totally break the Schnorr signature scheme under these circumstances (remark that it does not mean the Schnorr signature scheme is flawed, it is about how it is used with certain PRNGs).

You must show how the attack works step by step, by illustrating algebraic recovery step, and explain how *ts_i* and *r_i* play a role in this attack.

3) [20] Basic security models for authentication primitives

- (3) Explain EU-CMA experiment for a MAC scheme.
- (4) Explain EU-CMA experiment for a digital signature scheme.
- (3) Why adaptability is important, and what are non-triviality and validity conditions?

Please describe the formal experiments with cryptographic games, providing the related probability equation, and then give a brief explanation what these probabilities means. You may refer Mihir Bellare's Lecture Notes as a source. Also, the book of Prof. Dr. Jonathan Katz referred in the Syllabus is a good resource for this question.

4) [20] Do you see any synergy between Elgamal encryption scheme and DH key exchange protocol? Explain how one implicitly uses another to achieve its objective.

5) [20] RSA digital signatures and their properties: Aggregate signatures enable *O(L)* signatures to be compressed into a single, compact (i.e., constant-size) verifiable signature.

- In RSA, it is easy to aggregate signatures computed under the same private key. What is the name of this scheme, and how this aggregation is performed?
- In cloud computing environment, especially in outsourced databases, several tuples belonging to different users are stored together. Therefore, it is desirable to aggregate signatures computed with different keys belonging different users. Is it possible to use the RSA aggregation strategy discussed above for this purpose? If it is possible, show how it can be done. If it is not possible, explain the reason in detail.

  Hint: The paper "Practical immutable signature bouquets (PISB) for authentication and integrity in outsourced databases" might give you clues for both questions.

6) [10] PKI Concepts:

- (4) What are the core components of a PKI? Briefly describe each component.
- (3) Discuss the trustworthiness of root certificates provided by browsers.
- (3) What is the purpose of the X.509 standard and what is a certificate chain? How is an X.509 certificate revoked?