Homework #3

Oregon State University

ECE 478 Network Security

Spring 2016

Student:
Sam Quinn
Quinnsa@Oregonstate.edu

Professor:
Dr. Attila A Yavuz
Attila.Yavuz@oregonstate.edu

May 23, 2016

Contents

1 Impact of the PRGN Quality over the Security of DLP-based Primitives **2**

2 Basic security models for authentication primitives **2**

3 Synergy between Elgamal and DH **2**

4 RSA digital signatures and their properties **3**

5 PKI Concepts **3**

1 Impact of the PRGN Quality over the Security of DLP-based Primitives

[30] 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.

2 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 Bellares Lecture Notes as a source. Also, the book of Prof. Dr. Jonathan Katz referred in the Syllabus is a good resource for this question.

3 Synergy between Elgamal and DH

[20] Do you see any synergy between Elgamal encryption scheme and DH key exchange

Elgamal encryption scheme is very similar to the Diffie Hellman key echange.

Elgamal Encryption:

Keygen:	ENC(A,M)	DEC(a,(B,C)):
$a \leftarrow \mathbb{Z}_n$	$b \leftarrow \mathbb{Z}_n$	$K = B^a$
$pk = A = g^a$	$B = g^b$	$M = C * K^{-1}$
$sk = a$	$K = A^b$	Return M
	$C = K * M$	
	Return (B, C)	

Diffie Hellman Key Agreement:

Alice	Transfer	*Bob*
$a \leftarrow \mathbb{Z}_n$		$b \leftarrow \mathbb{Z}_n$
$A = g^a$	$A \rightarrow$	
	$\leftarrow B$	$B = g^b$
$K = B^a$		$K = A^b$

4 RSA digital signatures and their properties

[20] Aggregate signatures enable O(L) protocol? Explain how one implicitly uses another to achieve its objective. 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.

5 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?**