ASSIGNMENT № 1

Jiageng Chen, CCNU Wollongong Joint Institute Due: 03/19/2020

Problem 1

Besides the password-based identification scheme, we have also seen one-time password SecureID system (time-based security token), S/Key system, as well as the challenge response protocol. Currently, most of the industrial solutions like to apply one of these techniques as a second identification factor as a complementary guarantee to the password-based method.

You are required to investigate the industrial solutions (from domestic or international organizations) regarding the identification techniques. Please provide 3 use cases of the following methods:

1. One-time password SecureID system
2. S/Key system
3. Challenge response protocol

You should describe: 1). the industrial application; 2). how the technique is applied in the solution; 3). related figures and algorithms.

Problem 2

Implement Schnorr signature scheme (both the original and the optimized versions) satisfying the following criteria. Please refer to the implementation of ECDSA for the program structure and necessary utility functions.

1. Use P256 curve.
2. Apply SHA256 for the Hash function.
3. Design "Key generation", "Sign", and "Verify" APIs.
4. Message to be signed: "CSCI468/968 Advanced Network Security, Spring 2020"

Problem 3

(Bad randomness attack on Schnorr signatures). Let (sk, pk) be a key pair for the Schnorr signature scheme (Section 19.2). Suppose the signing algorithm is faulty and chooses dependent values for α_t in consecutively issued signatures. In particular, when signing a message m_0 the signing algorithm chooses a uniformly random α_{t0} in $\mathbb{Z}_q$, as required. However, when signing

m_1 it choose α_{t1} as $\alpha_{t1} \leftarrow a \cdot \alpha_{t0} + b$ for some known $a, b \in \mathbb{Z}_q$. Show that if the adversary obtains the corresponding Schnorr message-signature pairs (m_0, σ_0) and (m_1, σ_1) and knows a, b and pk, it can learn the secret signing key sk, with high probability.

Problem 4

(Batch Schnorr verification). Consider the unoptimized Schnorr signature scheme $\mathcal{S}_{sch}$. Let $\{(m_i, \sigma_i)\}_{i=1}^n$ be n message/signature pairs, signed relative to a public key u. In this exercise we show that verifying these n signatures as a batch may be faster than verifying them one by one. Recall that a signature $\sigma = (u_{ti}, \alpha_{zi})$ on message m_i is valid if $g^{\alpha_{zi}} = u_{ti} \cdot u^{c_i}$, where $c_i = H(m_i, u_{ti})$. To batch verify n signatures, the verifier does:

1. Choose random $\beta_1, ..., \beta_n \xleftarrow{R} \mathcal{C}$,
2. Compute $\bar{\alpha} \leftarrow \Sigma_{i=1}^n \beta_i \alpha_{zi} \in \mathbb{Z}_q$ and $\bar{c} \leftarrow \Sigma_{i=1}^n \beta_i c_i \in \mathbb{Z}_q$,
3. Accept all n signatures if $g^{\bar{\alpha}} = u^{\bar{c}} \cdot \Pi_{i=1}^n u_{ti}^{\beta_i}$.

Explain why β values are required, and what would happen if they are not applied in the scheme. Please demonstrate with concrete security evaluation with the related advantages.