CHAPTER 1

THE PROBLEM

This chapter discusses the research rationale which consists of the background and followed with the overview of several previous methods of dynamic identity based remote user authentication using smart card. The discussion continues with the theoretical framework, the conceptual framework, the statement of problem, hypothesis, assumption, scope and delimitation, and importance of the studies.

1.1 Rationale

The use of smart cards began in the 1980s and since then the use of its technology was increasing. Since the smart card is used for securing transaction, then security issue in the smart card becomes important.

However, there are problems with smart card security such as smart card forging, smart card user impersonating, user's identity theft, and the use of smart card extracted data for breaking the scheme, etc. There are several mechanisms to mitigate the smart card's authentication problem. To overcome the smart card's problem, dynamic identity based authentication scheme is introduced. Dynamic identity based scheme allows the users to choose and change their password. The scheme protects the smart card against ID-theft and other attacks during authentication process based on a one-way hash function [2].

There are many dynamic identity based mechanism that has been proposed, but each of them is still vulnerable against some attacks such as Lee et al [6] that claims their proposed scheme is secured against impersonation attack and server spoong. However, Li et al [7] claims that Lees scheme still has vulnerabilities against some attacks such as improper authentication, forgery attack and server spoofing attack. Li et al [7] proposes an improvement to overcome Lee's scheme vulnerability and claims that his scheme is secured against replay attack, forgery attack, server spoofing and registration center spoofing attack, and stolen smart card attack. Wang et al [9] claims that Li's scheme is vulnerable against offline password guessing attack, denial of service attack. Wang proposed a new scheme which is secured against offline password guessing attack, stolen verifier attack, user impersonation attack, server masquerading attack, replay attack, parallel session attack, and denial of service attack. However, Zhai et al [11] claims that Wang's scheme still has vulnerability to offline password guessing attack. This attack is conducted by assumption that the attacker is equipped with a machine which has infinite capacity. It has been proven that the password can be guessed using messages exchanged between the user and the server.

1.2 Theoretical Framework

Dynamic identity based scheme allows the users to choose and change their password. The scheme protects the smart card against ID-theft and others attacks in authentication process based on a one-way hash function [2]. Authentication is a method for verifying a person's/unit's identity when he/she would like to access confidential data stored in a server. Before the server gives access to a user, the server has to check whether the user is a legitimate one or not. If the user is not a legitimate one, then the server has to deny it.

In general, the dynamic identity based remote user authentication using smart card can be described as follow: Suppose Alice wants to access resources from a server. Then, Alice has to register as a legitimate user of the server. Alice then come to an authorized administrator to register. This authorized administrator asks Alice to select her username and password, processes these values and sends them to the server to issue a smart card including the security parameter. Furthermore, the server sends the security parameter that has to be saved in the smart card and give the smart card to Alice.

When Alice wants to access resources from the server, then Alice inserts the smart card into a smart card reader, inputs her username and password which is used in the registration process. The smart card checks whether Alice is a legitimate user or not. The smart card and the server will authenticate each other to verify each other that both of them are legitimate. After the smart card and the server have successfully authenticated each other, then they use a common session key to communicate with each other. Finally, Alice can access the resources in the server.

There are several types of dynamic identity based remote user authentication scheme using smart card, but most of them are not flawless. One of the vulnerabilities is that it is not secured against offline password guessing attack. When a smart card is stolen and an attacker get the smart card, then the attacker can attempt to guess the user's password and uses the password to access the server. Using the guessed password, the attacker can successfully obtain the permission to access the server.

This research attempts to improve Wang's scheme especially to decrease the successful probability of the attacker in offline password guessing attack.

1.3 Conceptual Framework

In order to decrease the probability of success in offline password guessing by the attacker, then the proposed scheme has to use a secret value to secure the password such that it is harder to be guessed than the previous scheme. This research uses Diffie-Helman key exchange to strengthen the mutual authentication scheme between the user and the server. The proposed scheme uses the Diffie-Helman key exchange because it is based on the discrete logarithm problem which is classified as hard problem.

Dynamic identity based authentication using smart card consists of three phases, registration phase, login phase and verification phase. When the new user wants to access resources from the server, then the user has to be registered as the legitimate one. After the user has been registered to the server, then the user receives a smart card including the security parameter. When the user wants to access the server, the user has to insert the smart card into a smart card reader and inputs the user's identity and password. Then, the smart card creates a login message and sends it to the server. If the authentication succeeds, the user is allowed to access the server.

In the registration phase, user has to select his/her identity and password. The smart card computes all values needed for registration and sends them to the server. After receiving the registration message from the smart card, the server computes the message and sends the security parameter to the smart card.

When the user wants to access the server, then the user inserts the smart card into the smart card reader and inputs the user's identity and password. The smart card computes all values needed for creating the login message and sends it to the server. After receiving the login message from the smart card, the server computes it to check whether the smart card is a legitimate one or not. After proving that the smart card is legitimate, then the server computes a verification message and sends it to the smart card.

After receiving a verification message from the server, then the smart card computes the message and checks whether the server is legitimate or not. If the server is legitimate, then the smart card computes a verification response message and sends it to the server. This message is used to prove that the smart card has received the verification message. After receiving the verification response message from the smart card, the server computes the message to verify whether the smart card has the same shared secret key or not. If the smart card has the same shared secret key, it means that the server and the smart card has successfully conducted mutual authentication and they agree to use the same secret key for securing the communication.

1.4 Statement of the Problem

Wang's scheme is still vulnerable against offline password guessing attack. Based on Zhai et al [11], with the recorded authentication messages and the extracted data of smart card, the attacker can obtain the user's password by guessing it without knowing the user's identity. The weakness of Wang's scheme is the use of the secret variable in creating the dynamic variable of user's identity. That dynamic variable is then used for securing the user's password and sent it to the server. The attacker that eavesdrops the communication channel and gets the login message can use it with the extracted data of smart card for guessing the user's password. The probability of success in guessing the password in Wang's scheme is only $\frac{1}{2^{128}}$. In other word, the security of Wang's scheme against offline password

guessing attack only depends on the strong of the user's password itself. If the security only depends on the user's password, then the attacker will use dictionary attack rather than brute force attack. The dictionary attack tries some common password combination instead of all combination. Therefore, dictionary attack is faster than brute force attack.

1.5 Objective and Hypotheses

This research proposes a new scheme that attempts to improve or strengthen the security of Wang's scheme against offline password guessing attack while still preserving the scheme against user impersonation attack. To strengthen Wang's scheme against offline password guessing attack, the proposed scheme has to use a secret variable only for securing the user's password in the login phase. It means that the secret variable for securing the user's password is not used for securing the user's identity. Therefore, for securing the user's identity a new variable is proposed. The proposed scheme uses two secret variables in the login phase, a random number and a timestamp. This condition should be satisfied because there are many variables that need to be sent to the server during the login phase such as the user's identity, the user's password, and the server's secret key. Meanwhile, Wang's scheme uses a secret variable for creating the dynamic variable of user's identity. That dynamic variable is then used for securing the user's password and the server's secret key in the login phase. That dynamic value is also sent to the server as one part of the login message. If the attacker eavesdrops the communication channel and obtains the login message, then the attacker has one advantage in guessing the user's password.

In the proposed scheme, a timestamp value is used for creating the dynamic variable of the user's identity and a random number is used for securing the user's password and the server's secret key. Thus, since the user's password is secured by a secret variable and that secret variable is not sent to the server, the probability of success in password guessing is less than using a dynamic value sent to the server. In other word, the new proposed scheme is more secured or stronger against offline password guessing attack than Wang's scheme.

Taking a timestamp needs less resource than generating a random number. In overall, the login phase in the proposed scheme needs one additional secret variable. This one additional variable makes the computation cost in the login and verification phase higher than Wang's scheme. The computation cost of Wang's scheme is $6T_E + 12T_H$ (six times of exponential operation and twelve of hash function operation).

1.6 Assumption

The smart card used in the proposed scheme is a smart card V3.54 enhanced basic card version with a capacity EEPROM (Electric Erasable PROM) 32 Kbytes and RAM (Random Access Memory) 256 bytes.

1.7 Scope and Delimitation

The scope of this research is to increase the security level of Wang's scheme. This research analyzes the security based on brute force attack and hash collision attack.

1.8 Significance of the Study

This research attempts to improve the security of dynamic identity based remote user authentication scheme using smart card especially the security against offline password guessing attack. To our best knowledge, most of the scheme still have low security level. Therefore, this research takes a part in improving the security level of the scheme. If the security level of authentication using smart card is high, then transaction using smart card for e-banking, e-commerce, e-health will be more secured.