ABSTRACT

This thesis is a study of password based authentication and key agreement protocols. Due to simplicity and convenience, password is the most commonly used authentication technique to authenticate users on the web. The main advantage of passwords is that users can memorize them easily without needing any hardware to store them. Efficient password authentication schemes are required to authenticate the legitimacy of remote users over an insecure communication channel. In this thesis, we propose some password based authentication protocols for different types of environments as well as an anti-phishing protocol. Improvements to several static and dynamic identity based authentication protocols have also been suggested.

Password based authentication is used in online web applications and is highly susceptible to phishing attacks. The average user can not distinguish a well designed phishing website from the legitimate site because the phishing site is designed in a manner that imitates visual characteristics of the target organization's website by using similar colors, icons, logos and textual descriptions. Phishing is doing direct damage to the financial industry and is also affecting the expansion of e-commerce. One of the reasons for success of phishing attacks is high rate of password reuse because users tend to use the same password with more and more accounts. Users find it difficult to remember several complex passwords and hence it is difficult to prevent phishing and dictionary attacks. In 2007, Gouda et al. proposed a single password based anti-phishing protocol for Hyper Text Transfer Protocol authentication that allows a user to choose a single password of his choice for multiple online accounts on different web servers. In this thesis, we show that Gouda et al.'s protocol is insecure against offline dictionary attack, denial of service attack and man-in-the-middle attack in presence of an active attacker. Also an improvement to Gouda et al.'s protocol is proposed that can resist offline dictionary attack and denial of service attack. It is however found that Gouda et al.'s protocol is not repairable for man-in-the-middle attack. We propose a new single password based anti-phishing protocol that resolves aforementioned problems and is secure against different types of attacks. In this protocol, the client machine's browser generates a dynamic identity and a dynamic password for each new login request to the server. The dynamic identity and dynamic

password generated for a client are different in different sessions of the Secure Socket Layer (SSL) protocol.

Password based authentication protocols are susceptible to dictionary attacks by means of automated programs because most of the user chosen passwords are limited to the user's personal domain. We propose a cookie based and an inverse cookie based virtual password authentication protocols. In cookie based virtual password authentication protocol, the web server stores a cookie on the user's computer if the user has successfully authenticated himself to the web server from that computer. On the other hand, in an inverse cookie based virtual password authentication protocol, the web server stores cookie on the user's computer when he has not submitted correct identity and password for his authentication to the web server. In both these protocols, the computational effort required from the attacker during login on to the web server increases exponentially with each login failure. The concept of trust has been used so that the legitimate client can easily authenticate himself to the web server from any computer irrespective of whether that computer contains cookie or not. The client generated virtual password for a user is different in each new session of SSL protocol. These concepts combine traditional password authentication with a challenge that is easy to answer by a legitimate client but the computation cost of authentication for an attacker increases with each login failure. Therefore, even automated programs can not launch online dictionary attacks on these proposed protocols. These protocols removes some of the deficiencies of previously suggested password based authentication protocols and are shown to be secure against different types of attacks that can be launched by the attacker.

Most of the password based authentication protocols rely on a single authentication server for user's authentication. The user's password verification information stored on the single server is a main point of susceptibility and remains an attractive target for the attacker. We present Single Sign-On (SSO) password based two-server authentication protocol that issues a ticket to the user for a specific time period. The user can use this ticket to generate dynamic ticket information to login on to the authentication server. Ticket issued for one authentication server can be used for user authentication on another authentication server that is under the control of the same control server. Our protocol uses two-server paradigm by imposing different levels of trust upon the two servers so that password verification information is distributed between two servers (an authentication

server and a control server). Therefore, the proposed protocol is more resistant to dictionary attacks as compared to other existing single-server password based authentication protocols. The proposed protocol is efficient and practical for its implementation because it does not use public key that causes computation and communication burden in a resource constrained environment.

Next, a brief review of some static identity based smart card authentication protocols is presented. Cryptanalysis of these protocols is carried out for different types of attacks and improved protocols are proposed. The comparison of the cost and functionality of the proposed protocols with the other related protocols is also done. Yoon et al. (2005) proposed a remote user authentication scheme which is an improvement on Hwang et al.'s scheme. However, we found that Yoon et al.'s scheme can easily reveal a user's password and is susceptible to impersonation attack using stolen smart card. This scheme is also found to be susceptible to parallel session attack and man-in-the-middle attack. We propose a remote user authentication scheme that resolves the aforementioned problems, while keeping the merits of Yoon et al.'s scheme. We also analyze the smart card based authentication protocols of Kim and Chung (2009), Xu et al. (2009) and Liu et al. (2008) and show that they are susceptible to different types of attacks. We propose improvements of these protocols to overcome their weaknesses.

Next, this thesis investigates some smart card authentication protocols for different attack scenarios and improved dynamic identity based smart card authentication protocols are proposed. In 2004, Das et al. proposed a dynamic identity based remote user authentication protocol. Many researchers demonstrated that Das et al.'s protocol is susceptible to several types of attacks. In 2005, Liao et al. published an improved protocol and claimed that this improved scheme withstands password guessing attack and insider attack. However, we found that Liao et al.'s protocol is also susceptible to malicious user attack, impersonation attack, stolen smart card attack and offline password guessing attack. Moreover, Liao et al.'s protocol does not maintain the user's anonymity and its password change phase is insecure. We present a secure dynamic identity based authentication protocol using smart cards to resolve the aforementioned problems, while keeping the merits of different dynamic identity based authentication protocols. We also analyze the smart card based authentication protocols of Liou et al. (2006), Wang et al.

(2009), Lee et al. (2005) and Hsiang and Shih (2009) and show that they are susceptible to different types of attacks. We propose improvements of these protocols to overcome their weaknesses. The security analysis of the proposed improved protocols is presented. The comparison of the cost and functionality of the proposed protocols with the other related protocols is also done.

In e-commerce, the number of servers providing the services to the user is usually more than one and hence secure authentication protocols for multi-server environment are required. Moreover, the multi-server architecture based authentication protocols make it difficult for the attacker to find out any significant authentication information related to the legitimate users. In 2009, Liao and Wang proposed a dynamic identity based remote user authentication protocol for multi-server environment. But we found that Liao and Wang's protocol is susceptible to malicious server attack and malicious user attack. We propose a dynamic identity based authentication protocol for multi-server architecture using smart card that resolves the aforementioned security flaws, while keeping the merits of Liao and Wang's protocol. In 2009, Hsiang and Shih improved Liao and Wang's dynamic identity based remote user authentication protocol for multi-server environment. However, we show that Hsiang and Shih's protocol is susceptible to replay attack, impersonation attack and stolen smart card attack. Moreover, the password change phase of Hsiang and Shih's protocol is incorrect. We present a dynamic identity based authentication protocol for multi-server architecture using smart card that resolves the aforementioned flaws, while keeping the merits of Hsiang and Shih's protocol. The proposed protocols use two-server paradigm by imposing different levels of trust upon the two servers and the user's authentication functionality is distributed between these two servers known as the service provider server and the control server.

In our proposed single password based anti-phishing protocol, client can use a single password for different online accounts and that password can not be detected by any of the malicious server or the attacker. This protocol is equally secure for security ignorant users, who are not very conversant with the browser's security indicators. The protocol does not allow the server to know the client's password at any time. This protocol can be easily integrated into different types of services such as banking and enterprise applications. The proposed cookies based and inverse cookie based virtual password authentication protocols are very effective to thwart online dictionary attacks because the

computation cost of login on to the web server increases exponentially with each login failure for an attacker. The legitimate client can easily authenticate himself to the web server from any computer irrespective of whether that computer contains cookie or not. SSO authentication is time efficient because it allows the user to enter his identity and password once within a specific time period to login on to multiple hosts and applications within an organization. Most of the existing SSO password based authentication protocols are designed for single-server environment. We proposed an efficient SSO password based two-server architecture in which the user has to login once to get a valid ticket. Smart card based password authentication is one of the most convenient ways to provide multi-factor authentication by acquiring the smart card and knowing the correct identity and correct password for the communication between a client and a server. Improvements to several static and dynamic identity based authentication protocols have also been suggested. User's privacy is an important issue in e-commerce applications. The proposed dynamic identity based authentication protocols aim to provide the privacy to the user's identity so that users are anonymous in communication channel. Also the concept of two-tier authentication for the client makes it difficult for an attacker to guess out the information pertaining to password and ticket. Confidence of clients in e-commerce and other online transactions can be enhanced by negating phishing, dictionary and other possible attacks. The work presented in this thesis is a step toward making e-commerce transactions more reliable and secure.