ABSTRACT

In the current electronic world, security protocols are widely used to accomplish several tasks via the Internet. The Internet is an insecure medium and messages communicated through it are susceptible to many attacks. In order to withstand such attacks, there is a need to design robust security protocols. Based on the application domain, the designed protocols have to meet certain security requirements. Many formal methods have been established to verify whether the protocols meet the desired security requirements or not.

The primary focus of this research is analysis of some security protocols designed for various applications using popular formal methods, strand space model and BAN logic. Also, after the analysis it focuses on the design of new secure protocols overcoming the flaws identified in the protocol. In the first work, a suitable framework has been presented to formalize and verify the fairness and privacy type properties of electronic voting protocols. A suitable attacker model is established, the fairness and privacy type properties are modelled and verified using the strand space model. FOO protocol is analyzed to illustrate the applicability of the developed framework. The result shows that fairness and vote privacy properties are satisfied and receipt freeness property is not satisfied by FOO protocol. Finally, an improvement of the FOO protocol is proposed so that it achieves receipt freeness property also.

Nowadays payment protocols are facing difficulties in its implementation, as the parties involved in the execution deny their performed actions. In this context, there should be a provision to link the action to the concerned party, which is addressed by the accountability property. In the second work, a new framework in improved strand space model for the analysis of accountability property for the payment protocols using symmetric key cryptosystem is presented that can overcome the drawbacks of the existing models. As a test example, symmetric key based BPAC, a bill payment protocol ensuring accountability property is considered. Fine-grained analysis of accountability property of BPAC protocol is carried out and proved its correctness using the automated support provided by Cryptographic Protocol Shape Analyzer (CPSA) along with the mathematical proof.

In the current scenario, mobile web payment provides a standard platform to the Internet users for online digital goods shopping. Though majority of online transactions use single gateway, there is a need for multi-gateway due to insufficient balance in a customers account in a specific bank. There are a few payment protocols which support a transaction using multiple cards, but they too have some limitations like cards should be of the same bank and the process should be based on independent transactions. Third work presents an efficient payment protocol that is used for making online transactions via two gateways for purchasing digital goods to overcome the above mentioned limitations. The proposed protocol is simulated using the automated tool CPSA and it satisfies accountability, anonymity and atomicity properties. Formal proof of correctness is provided using the strand space model. The protocol is then compared with the state-of-the-art protocols in terms of different security features and computational overhead. Comparison results show that our protocol achieves better performance than other protocols.

In order to avoid using of multiple single servers, the theory of multi-server communication exists and numerous authentication protocols are proposed for providing secure communication. Very recently, Amin & Biswas proposed a bilinear pairing based multi-server authentication scheme by describing some security pitfalls of Hsieh & Leu protocol and claims that it is secured against related security threats. The fourth work in this thesis claims that

Amin & Biswas's protocol is still susceptible to off-line identity and password guessing attack, user untraceability attack, and server masquerading attack. A smartcard based multi-server authentication protocol by utilizing the concept of bilinear pairing operation is presented which satisfies many security properties. The formal method strand space model has been used to prove the correctness of the proposed scheme. Additionally, rigorous security analysis ensures the ability of the protocol to overcome the security threats. The performance and security features of our scheme are also compared with that of the similar existing schemes. The comparison results show that our protocol achieves more security features with less complexity.

The Session Initiation Protocol (SIP) is a communication protocol that controls multimedia communication sessions. As the Internet users widely use SIP services, mutual authentication between the user and SIP server becomes an important issue. Several authentication protocols for SIP have been proposed for enhancing security and improving complexities. Very recently, Lu et al. proposed an authenticated key agreement protocol for SIP and claims that it withstands various attacks and it is efficient. In the last work, It is pointed out that Lu et al.'s protocol does not provide one of the most important security features that is user anonymity. In addition, the same protocol is not able to resist user impersonation attack, server impersonation attack and fails to provide mutual authentication. The last chapter also presents an improved mutual authentication and key establishment protocol that overcomes the security weaknesses in Lu et al.'s protocol. In order to prove mutual authentication and session key agreement, the proposed protocol is analyzed using BAN logic. Informal security analysis is also carried out against several security properties. The performance of the proposed scheme is compared with that of the existing related ECC based schemes for SIP and shown that our scheme outperforms the others.