ABSTRACT

With recent trend in Information Technology (IT) systems and rapid development of the Internet, researchers indicated the need for different thinking when it came to designing security systems for future applications. Client/server systems were traditional and widely deployed, but they were known to have some shortcomings. Client/server transaction architectures have now become multi-party transaction architectures. In a multiparty transaction architecture more than two parties are simultaneously involved in a single transaction.

The main objectives of this thesis “A Model Of Architecture For Security With Particular Reference To Multi-Party Transactions” was developed together with all supporting security protocols and this model is regarded as Multi-Party Security System (Multi-PaSS). Multi-PaSS provides authenticity, integrity, confidentiality, and non-repudiation security services to users and applications. It supports Multi-Application ATM (Automatic Teller Machine) Card and on Multiple Interrelated Public Key Infrastructure (PKI) domains, Single Sign-On authentication protocol with multiple verifiers, for secure multi-party transactions which is our security infrastructure.

The topology of a Multi-PaSS comprises the following components and provides the following security services:

- Security infrastructure, supporting secure transactions between several parties in an open global environment with registration, certification, distributed remote authentication, and trusted security administration;
- Secure multi-party protocols for protection of transactions in transfer, storage, authenticity delegation, authorization forwarding, etc.; and
- Security extensions of various network applications suitable for multi-party transactions providing user authentication, cryptography, certification function, message protection, etc.

The structure of the Multi-PaSS may be in the form of three layers. The bottom layer, called security platform, contains cryptographic modules and security tokens, such as ATM cards. The middle layer comprises a collection of security proxies (Multi-PaSS proxies), which can securely
communicate with each other performing security operations in a multi-party environment. The
top layer, *security infrastructure*, comprises multiple cross-certified Public Key Infrastructure
(Multi-PKI domains) and other supporting servers. All participants of a transaction must
communicate through *Multi-PaSS proxy* servers and they handle authentication and all
transactions between them. This authentication is performed using *sequential* and *parallel*
concept. Since MPT protocol messages contain corresponding timestamps, verifiers can verify
creation time and verification time. Multiple signatures together with timestamps provide
authenticity, integrity and non-repudiation security services for multi-party transactions.

The bottom layer of our model which is Multi-Applications ATM cards for Multi-Party
Transaction System. It first explains existing multi-application approaches. Then it discusses
problems with existing approaches and it describes solutions obtained in this study. It also
deals about the top layer of our model, i.e. Multiple Interrelated PKI (Public Key Infrastructure)
domains. It provides a reliable and scalable certification infrastructure. This Multi-PKI
infrastructure must support creation, distribution, verification and revocation of certificates
between one or more PKI domains, which may have different certification policies. Cross-
certificate concept and other supporting concepts and protocols represent flexible and scalable
certification infrastructure for secure multi-party transactions. Cross-certification through a
Bridge Certificate Authority enables flexible trust model between different certification
hierarchies.

The middle layer of our model, which are Multi-Party Authentication Protocol And Web
services. It discusses the Security Requirements, Characteristics of Web Service model, Web
Service Standards and Protocols, Web Service security, Network Access Layer Security Protocol,
Digital certificates and public key cryptography, a new model of a scalable(Static/Dynamic)
multi-party authentication protocol to support strong authentication between an initiator(Client)
and multiple verifiers(Servers) and Single Sign-On procedure for secure multi-party
transaction. we regard this model as Multi-Party Security System (Multi-PaSS). It also attempts to
develop standard and secure communication between service instances in Web Services. This
objective was achieved by designing an online book ordering system.
The middle layer of our model, which is a model of a secure Multi-Party Transaction (MPT) Protocol. The MPT protocol to support for secure creation, distribution, verification and different legal assurance levels of signatures of multi-party (sequential and parallel) processing of transactions between multiple signers and verifiers. Therefore, it may be used for protection of various electronic transactions or documents exchanged between multiple participants.

The overall model of a security architecture for secure multi-party transactions, all participants of a transaction must communicate through Multi-PaSS proxy servers and they handle authentication and all transactions between them. This authentication is performed using sequential and parallel concept. Since MPT protocol messages contain corresponding timestamps, verifiers can verify creation time and verification time. Multiple signatures together with timestamps provide authenticity, integrity and non-repudiation security services for multi-party transactions.

The major results and contributions of this research are:

- A set of new theoretical concepts which have been developed to handle multi–party security protocols, transactions, and applications supporting operations suitable for various environments different from the current, classical, client–server security models;

- Topology and architecture of a security model supporting simultaneous transactions between multiple participants, including components of the security model (security proxies, Multi-application ATM cards), their interactions (security protocols), various recursively structured security tokens for multi–party transactions, and functional interfaces to all security services (security APIs(Application Program Interfaces) and security methods);

- Several security protocols such as multi–party authentication protocol, and secure multi–party transaction protocol.

The results of this research represent the first model of a security architecture that supports secure multi–party transactions, which are important and necessary for many types of real–life applications in global networks.