論文内容の要旨

論文題目　Authentication Protocols and Secure Service Discovery in Ubiquitous Computing Environment

(ユビキタスコンピューティング環境における認証プロトコルと安全なサービス発見に関する研究)

氏名　　林　素娟

The advanced technologies of heterogeneous computing device, service contents, and networking create ubiquitous computing environment. It realizes for users to easily access to the Internet from anywhere at any time. Service mobility and service discovery are notable schemes to extend the scope of ubiquitous computing. Service mobility achieves the connection to service contents regardless of the kind of the devices and the networks. Service discovery protocol allows detection and selection of devices and services that users can use. However, ubiquitous computing environment includes various devices and services that are possessed by malicious one. Each entity, which may be a user, service content, or server, should be correctly authenticated its identity. We describe authentication protocols for service mobility support and service discovery.

Service mobility provides seamless service migration of heterogeneous devices even across network boundaries. Users can switch from one resource to another preserved resource for communication without disrupting their current service. This attribute of service mobility occur different security issues from two traditional mobility, personal mobility and terminal mobility. Terminal mobility refers to the ability of a terminal to remain connection to the network while roaming from one location to anther while personal mobility refers to the ability of the user to access their service independent of their location or terminal. Terminal mobility and personal mobility have invariable parameters like individual owned terminal and

Universal personal Telecommunications number respectively. Service mobility has non-fixed parameter even though involved terminal may be foreign or public one. This attribute makes difficult to authenticate each end entity.

We focus on forward secrecy as the most devastating threat against service mobility. Forward secrecy refers to the notation that acquisition of a single keying material does not permit access to the secrecy keying materials of any other period. This means that even though an attacker can obtain a secret key at a certain period, he can not read or write any data after the permitted time period. To resolve this threat we first present previous research on authentication protocols using one-time password and generic public key scheme. We realize using one time password authentication protocol achieves end-to-end authentication but need the password state synchronizing. Using generic public key cryptosystem, X.509 certificate scheme, also realizes end-to-end authentication. However, this scheme it takes heavy overload on certificate verification to obtain a certificate chain and unwrapping a certificate path in sequence to recover a trusted certificate public key. It is necessary to generate a new key pair and revoke it in order to achieve forward secrecy since it is left on malicious device even after usage. We introduce key-insulated public key cryptosystem and ID-based public key cryptosystem to achieve forward secrecy as well as reduction of overload on certificate verification and new key regeneration.

We have realized authentication protocol using key-insulated public key cryptosystem and ID-based public key cryptosystem be able to offer same security level with that of using generic public key cryptosystem : data integrity, data confidentiality and evading replay attack. Using key-insulated public key, principals can update the private key without changing public key. This feature conducts the forward secrecy and reduces the computational complexity for verifying public key certificate at service handover. The callee authenticates the caller with a public key obtained before even though the caller uses updated secret key which is pair of public key obtained by callee. However, key-insulated public cryptosystem needs large storage to store public key parameters that include random elements to be used by private key updating. Large storage problem can be reduced by setup public key parameters with respect to the expecting frequency of the handoff. Using ID-based public key cryptosystem, principals need not verify identity of public key like certificate because the public key information itself is identification information. It shows attractive merit of using ID-based public key to reduce the overload caused by obtaining public key and verifying it. However, it is necessary to assume that private key generator conducts careful checking of identity information of a principle and correct key distributing when a user registers at the setup.

We have compared the proposed authentication protocols which are using one-time password, generic public key, key-insulated public key, and ID-based public key. The comparison has showed that authentication protocols that using key-insulated public key and ID-based public key are suitable to satisfy the forward secrecy requirement for service mobility. From this consideration, we have evaluated the overhead time and storage resource of them in order to select proper cryptosystem according to the system condition and requirements.

On the other hand, the careful security issues for service discovery protocol have been studied. Service discovery protocol enables devices and services to properly discover and communicate with each other. It is an important skill to discover ambient services available in network without any centralized administrator and server since devices and services in ubiquitous computing environment are not always online even though they are still offering their services. For instance, printer, large screen, or copy machine can offer their service while they are not connected with Internet. Moreover, users will often refrain from making use of these services due to anxiety regarding their security and due to insufficient knowledge of service location (despite the existence of discovery tools such as Windows printer sharing service). We have considered the protocol using devices equipped with short range wireless modules. This protocol offers mutual authentication with end-to-end encryption without requiring online state.

We have introduced hierarchical ID-based public key cryptosystem that consists of private key and arbitrary-string public key. Principals can encrypt the service information or its private preference with their identities which are known by everyone during the service discovery process and authenticate each other. ID-based public key does not require the acquisition of certificate and its chain. This attribute make principals discover proper service and authenticate each other even offline state. It is very efficient since acquisition of shared secret information beforehand is not feasible to principals in ubiquitous computing.

We have presented two service discovery protocols that are user-requesting discovery and service-broadcasting discovery protocols. These protocols are assumed that there is a reliable key generation server which plays a role to manage the key generation with checking of the identity information of principal at user registration. User-requesting discovery protocol is triggered by sending request message of user while service-broadcasting discovery protocol is broadcasting its service information.

We have evaluated these protocols according to their service area scale. When service provider has one key generation server the latency caused by secure service discovery protocol depends on cipher process of authentication message and service matchmaking process. When service provider has hierarchical key generation servers the cipher process time is proportional to the hierarchical depth. Which one is suitable for that environment is decided by specification of discovery equipments, radio reachable range or computational ability, and the hierarchical depth of the key generation server.