論文の内容の要旨

Dissertation Title: Trust and Privacy in Ubiquitous Computing:
with activity-based attestation
(ユビキタスコンプーテイングにおける情報の信頼性とプライバシーの保護に関する研究：
アクティビティに基づく認証を中心に )

Name: ヤップ　リーフエン

In the era of ubiquitous computing, information can be generated and distributed easily and almost instantaneously by anyone. Besides this, a lot of information regarding an individual has been generated automatically as a byproduct of many services when the individual interacts with ubiquitous computing environment. These capabilities are results from the proliferation of various enabling technologies for ubiquitous computing such as wireless network technologies, adoption of feature-rich mobile devices and the wide-spread use of web 2.0 applications. Recently, such information has gradually been used for protecting the owner's rights during disputations. It is therefore important to be able to ensure the authenticity of this information. Furthermore, the privacy of information owner needs to be taken care of when such information is captured and/or shared with others.

Information trust is still a complicated problem in ubiquitous computing environment. Location spoofing, virtual presence, illegal modification of information and illegal fabrication of fake documents are some of the known problems that affect information trust. User privacy is another important issue that needs to be addressed because user is generating and sharing more information (knowingly or unknowingly) than before. They could be victims of tracking and profiling attacks when too much personal information is revealed in the public domain. Furthermore, based on traditional social reputation system, it seems that information trust has direct relationship with the identity of the information owner.

Hence, providing both information trust and user's privacy protection for information generated from ubiquitous computing applications is an interesting topic that needs further investigation.

To address the problems, an activity-based attestation service framework has been designed to enable the creation of various attestation services supporting information trust and privacy protection for ubiquitous computing applications. The proposed framework uses the activity-based attestation model for inferring user's action in ubiquitous computing environment. The proposed attestation service framework consists of two software components, namely eTRON software component and redemption software component. The two different software components are used for different usage scenarios i.e., to provide different levels of security protection for different types of applications. Two models namely, Secure User-Centric Attestation Services (SUCAS) and Consumer-Oriented Integrated Services (COIS) have been used to demonstrate different features supported by the two software components. The SUCAS is designed using eTRON software component, which is a tamper-resistant solution with configurable access control. On the other hand, the COIS is a down-graded version of SUCAS, which offers cheaper solution for applications that are less stringent in security and privacy protection. Two prototypes have been built to verify the proposed activity-based attestation service framework.

Applications built using the proposed activity-based attestation service framework can generate and verify information without compromising the user's needs for privacy. Unlike the previous work, the proposed activity-based attestation service framework incorporates user's action information into the spatial-temporal information to produce action-spatial-temporal evidence that can enhance the trust of information. The framework supports user-centric design, which enables user to decide on the generation, reuse, and sharing of the information at anytime without going through any third parties. Secure peer-to-peer sharing of information and protection over illegal redistribution of received information is supported by applications built using the eTRON software component. Finally, the information generated from applications built based on the proposed framework provides different level of information trust and privacy protections, which can be used to protect the owner's rights in various context.

In conclusion, the main contribution of this research is the development of an activity-based attestation service framework that supports the creation of trusted, privacy-sensitive and user-centric attestation services. This framework can be a great reference for application developers, who need to develop ubiquitous computing application with attestation services provisioning. Attestation service has great potential in this information age as it can be used for enhancing the authenticity of information rendered from ubiquitous computing applications and protecting the rights of the information owner in the event of dispute.