A Trust-based Security Architecture for Ubiquitous Computing Systems[1]

Le Xuan Hung, Pho Duc Giang, Yonil Zhung, Tran Van Phuong, Sungyoung Lee and Young-Koo Lee

Department of Computer Engineering, Kyung Hee University, Korea
{lxhung,pdgiang,zhungs,tvphuong,sylee}@oslab.khu.ac.kr,yklee@khu.ac.kr

Ubiquitous Computing (*ubicomp*) is a revolution of computing paradigm that promises to have a profound affect on the way we interact with computers, devices, physical spaces and other people. Traditional authentication and access control which has been applied to stand-alone computers and small networks are not adequate to ubicomp technology. Instead, we need a new security model that is based on notion of trust to support cross-domain interactions and collaborations. This means that ubicomp environments involves the interaction, coordination, and cooperation of numerous, casually accessible, and often invisible computing devices. Authenticating the identity certificate of a previous unknown user does not provide any access control information. Simple authentication and access control are only effective if the system knows in advance which users are going to access the system and what their access rights are. Security information in different domains is subject to inconsistent interpretations in such open, distributed environment. In order to fulfill these security requirements of ubicomp, in this paper we present USEC, A Trust-based Security Infrastructure, for securing ubicomp systems. USEC is being developed for CAMUS[2]. It is composed of seven major components: *hybrid access control*, *entity recognition*, *trust/risk management*, *intrusion detection*, *privacy control*, and *home firewall*. Our objective is to provide a lightweight infrastructure with sufficient security services that tackles most security problems in ubicomp systems.

Entity Recognition is a novel authentication technology for ubicomp paradigm. In USEC architecture, Pluggable Entity Recognition Module (PRM) supports flexibly various devices such as Smart Badges, iButtons, Smart Watchs, PDAs. This component integrates different type of authentications, ranging from conventional authentication approaches (Username/Password, PKI, Kerberos, etc) to emerging identity recognition technology. Trust/Risk Management provides trust value to the Access Control Manager. It supports trust collaborations and interactions among roaming entities. By modeling trust relationships in smart spaces environments, unknown entities from different domains can interact, request services and resources from a given domain in secure and privacy manner. Risk evaluator and Trust calculator cooperate with each other to support making decision. Hybrid Access Control (HAC) is the core part of USEC infrastructure. This is hybrid of Role-based

[1] This work is financially supported by the Ministry of Education and Human Resources Development(MODE), the Ministry of Commerce, Industry and Energy(MOCIE), and the Ministry of Labor(MOLAB) through the fostering project of the Lab of Excellency.
Dr. Sungyoung Lee is the corresponding author.

[2] CAMUS: Context-Awareness Middleware for Ubiquitous Computing Systems

(RBAC), Policy-based (PBAC), Context-based (CBAC) and Trust-based Access Control (TBAC) to solve different shortcomings of those approaches. HAC is critical to preserve confidentiality and integrity. Conventionally, the condition of confidentiality requires that only authorized users can read information, and the condition of integrity requires that only authorized users can alter information and in authorized ways. In USEC, HAC extends scopes of users by using Trust/Risk Management. Privacy Control is integral part in this convenient but obtrusive environment. It provides *location privacy*, *anonymous connections* and *confidentiality* of information to users. In USEC infrastructure, we also integrate Home Firewall to protect smart space against potential outside attackers. Intrusion Detection System is deployed in order to defend against unauthorized access and who has legitimate access to the system but abuse privileges. In ubiquitous environments, this usually occurs due to ubiquity and wireless communication of the systems. In the sensor network layer, USEC provides a lightweight cryptography mechanism in order maintain secure communication among sensors and between sensors and context-aware systems. Trust/Risk Management, Intrusion Detection System, Home Firewall, and Sensor Network Security are together supports Entity Recognition. Fig 1 shows the relationships and interactions among these components.

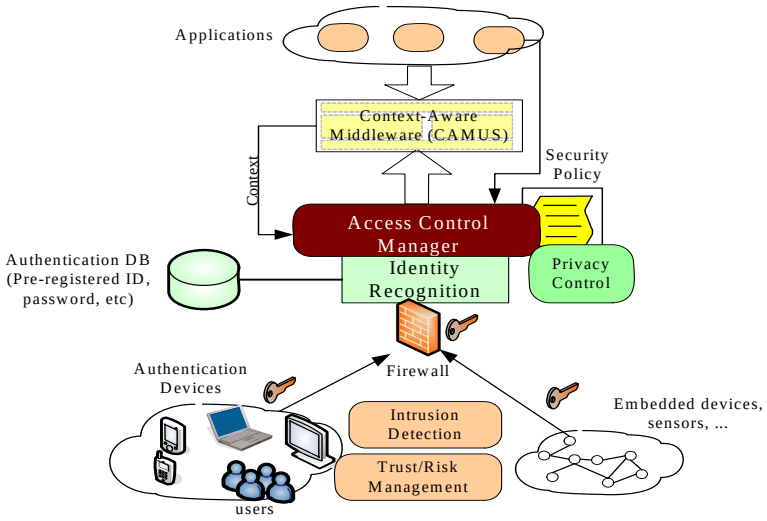

Fig. 1. USEC architecture and its component interactions.

Currently, we have completed deploying a smart environment by CAMUS in our RTMM Lab. This environment facilitates professors, students and staffs of our Lab to work and research as well as to entertain. We also are completing USEC framework to support security for this environment. USEC is component-based architecture and can support various ubicomp systems. After accomplishing in this environment, we will extend to other systems/environments such as parking spaces, airports, and hospitals. We believe that USEC will also fulfill security requirements in such systems/environments.