論文の内容の要旨

Hybrid and Context-Aware Access Control Measures for Ubiquitous Computing Services
（ユビキタスコンピューティングサービスのためのハイブリッドと
コンテクストアウェアなアクセス制御方式）

カン　エム　ファヒム　フェルドウス

The fact that ubiquitous computing represents the latest paradigm shift in computing necessitates a paradigm shift in how security is addressed in conventional computing. This paradigm shift in computing security – as believed by many researchers – can effectively be achieved by making security context - aware. Context-awareness is the essence of ubiquitous computing, so much so that it is often dubbed as context-aware computing. Moreover, the relation between security and context is rather intuitive: what is secure in one context may not be secure in other contexts.

This research explores the relationship between security and context-awareness in ubiquitous services, taking healthcare system – which poses an array of context-dependent security requirements – as an example. Ubiquitous healthcare systems collect, store and manage sensitive information about patients and, hence, it is imperative for such systems to maintain data confidentiality and integrity, and provide strong authentication features with a view to thwarting potential security and privacy threats. Traditional security wisdom often does not quite carry over to address the context - sensitive issues of ubiquitous computing. Let us consider access control for example: in traditional models, access control depends on specific attributes of the users and the objects. In ubiquitous computing applications, however, attributes of the users and objects are important, but so are other environmental contexts, such as location and time. These contexts will determine where and when certain access is allowed. For instance, a doctor or nurse or any other relevant medical practitioner should be able to access a patient's health record while in appropriate location (hospital or patient ward), and during the time frame that best suits the case in hand (during or beyond office

hours, etc.) In addition to the environmental contexts of location and time, there are application - dependent contexts which may have to be taken into account for granting or denying access. For example, in an emergency situation, a patient ' s health record may be shared with out - of - network physicians, but this type of access is prohibited when the patient is in normal condition. Moreover, the context of delegation is also important in healthcare, where a patient, due to age or mental illness, should have the provision to delegate her health record's access control rights to someone she trusts.

Security in ubiquitous healthcare can be addressed at different levels, like securing data collection by medical sensors, controlling access to health information, designing legislative frameworks for regulating secure usage of health information, and so on. However, in this research we mainly focus on the access control issues in ubiquitous healthcare, with the goals of designing and developing access control mechanisms contingent upon various environmental and application - dependent contexts with secure provision for delegation of access control rights. In particular, we propose a hybrid approach amalgamating features of discretionary access control (DAC), role - based Access Control (RBAC) and context-aware access control. The access control process is essentially composed of four steps: (a) Identification, (b) Authentication, (c) Authorization, and (d) Access decision. The eTRON (Entity and Economy TRON) architecture – which advocates use of tamper - resistant chips equipped with functions for mutual authentication and encrypted communication – is used for authentication and implementing the DAC - based delegation of access control rights. For implementing steps (c) and (d), we used the RBAC model and implemented contextual-attribute verification on top of it. In this dissertation, we also present an evaluation of the proposed hybrid approach in terms of various security and performance issues. We also explain the rationale behind the combined design, and argue that our approach is applicable to other application domains on a fairly general basis as the notion of spatio-temporal context, emergency- and delegation-related context are congruent to many other ubiquitous services.