A Secure and Flexible e-Health Access Control System with Provisions for Emergency Access Overrides and Delegation of Access Privileges

M. Fahim Ferdous Khan [a], Ken Sakamura [ab]

[a] *Interfaculty Initiative in Information Studies, The University of Tokyo, Tokyo, Japan*

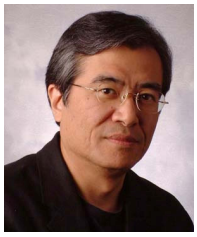
[b] *YRP Ubiquitous Networking Laboratory, Tokyo, Japan*

khan@sakamura-lab.org, ken@sakamura-lab.org

***Abstract*—Protecting electronic health records (EHR) from unauthorized access and data breaches has been a great challenge for healthcare organizations in recent times. Controlling access to EHR demands a delicate balance between security and flexibility: There are emergency cases where the default access control policy must be circumvented in order to save patients' life – and cases where management of access control rights needs to be delegated to some trusted parties. Therefore, e-Health access control systems must be robust and flexible at the same time. Conventional general-purpose access control schemes like role-based access control (RBAC) and its derivatives emphasize mainly on the robustness of the access control mechanism, and treat flexibility issues like emergency access overrides and delegation management as addenda. However, in order to comply with the care first principle of the healthcare domain, an ideal e-Health access control system should consider such flexibility issues from the ground up. Recognizing these special requirements mandated by the very nature of the healthcare profession, in this paper, we propose a secure and flexible access control system for e-Health. The user-role and object-operation mappings in our proposed system lend themselves to the RBAC model, and we implemented context verification atop this layer in order for the system to make access decision responsive to emergency incidents. For managing delegation of access control rights, we developed a secure mechanism for creation, transfer and verification of a delegation token, presentation of which to the access control system enables a delegatee to access a delegator's EHR. Every access request in our system is preceded by mandatory user authentication which we implemented using eTRON tamper-resistant cards. Security and performance analysis of the proposed system showed promising results for achieving the desired level of balance between security and flexibility required for an e-Health access control system.**

***Keyword*—Access control, authentication, cryptography, eTRON, e-Health**

M. Fahim Ferdous Khan, PhD is an assistant professor at the Graduate School of Interdisciplinary Information Studies in the University of Tokyo. He obtained his Master's and Doctoral degrees from the same university in 2009 and 2012 respectively. Prior to joining the University of Tokyo, he had been serving as a lecturer at the Department of Computer Science and Engineering in Islamic University of Technology, Bangladesh. His current research focus includes developing resource-aware security mechanisms for the Internet of Things and cyber-physical systems, and exploring the intersection of context-awareness and security in ubiquitous computing. He is also investigating various security, privacy and trust issues related to e-commerce, smartcard, RFID and other emerging distributed applications. He is a member of the IEEE, IEEE Computer Society, IEEE Communications Society, and the ACM.



Ken Sakamura, PhD is a professor at the Graduate School of Interdisciplinary Information Studies in the University of Tokyo, and the director of Institute of Infrastructure Application of Ubiquitous Computing there. As the founding leader of the TRON project initiated in 1984, he has designed the TRON open computer system architecture, which has been widely used in many consumer electronics appliances including mobile phones, digital cameras, FAX machines, engine control of automobiles, etc. Currently, as the chairman of the TRON Forum (www.tron.org) and the Ubiquitous ID Center (www.uidcenter.org), he has been leading cutting-edge IoT and ubicomp research. He has held the position of the director of YRP Ubiquitous Networking Laboratory since January 2002. He has been elected as fellow and golden core member of the IEEE Computer Society. He has won numerous awards, most notably, the Takeda Award in 2001, the Medal with Purple Ribbon from Japanese government in 2003, Okawa Prize in 2004, Prime Minister Award in 2005, Japan Academy Prize in 2006 and ITU150 Award in 2015.