早稲田大学審査学位論文
博士（人間科学）
概要書

HUC-HISF: A Hybrid Intelligent Security Framework for Human-centric Ubiquitous Computing

人間中心のユビキタスコンピューティングのためのハイブリッド・インテリジェント・セキュリティ・フレームワーク

２０１２年１月

早稲田大学大学院　人間科学研究科

朴　　鍾　　嫮
Park, Jong Hyuk

New computing paradigms such as H-Ubi Comp are up and coming due to rapid advances in computing power and network development. Such paradigm changes offer convenient and delightful, human-centered services at anytime, anywhere, and in any devices. Recently, H-Ubi Comp has been studied in terms of smart spaces, human-computer interaction, intelligent services, and universal device connectivity. However, H-Ubi Comp is closely related to networks and in this realm there exist essential security issues concerning the vulnerability and exposure of users' privacy. Traditional security mechanisms require manual authentication by users, static access control and static management which significantly restrict adaptability which is absolutely fundamental in H-Ubi Comp environments. In order to provide secure, yet flexible H-Ubi Comp environments, we need intelligent and dynamic security frameworks suitable for H-Ubi Comp environments.

The HUC-HISF, the novel security framework presented in this thesis, provides an advanced key schedule of mCrypton suitable for H-Ubi Comp devices providing better security for mCrypton against related-key rectangle attacks. The framework also provides wireless authentication, key establishment mechanisms, secure authentications and key-exchange protocols suitable for H-Ubi Comp environments. Furthermore, I introduce how the HUC-HISF may be applied to dynamic human-context based access control mechanisms, surveillance service and mobile IPTV service.

We could say that today's computing technology has reached the highest level it can. Personal computers and servers have reached the highest level possible in terms of design and speed and now we are working to reduce the power consumption and heat generated by Central Processing Units (CPU), such as the major chipset, by increase its density. In addition, projects such as multi-core, multi-processor, and grid computing are enhancing computational power through the collaboration of multiple processing devices. In addition, computer network technology is bringing about development in a variety of fields including moving beyond wired communications to wireless communication, mobile communication, and lower energy communications. Recently in the United States, Juniper and Cisco have expanded the bandwidth of wired network communications by developing routers having 10Gb/s interfaces. In the case of wireless communications, 802.11/n has become commercially

available and theoretically promises wireless communication speeds of up to 300Mb/s. The world of mobile communication technologies has witnessed the worldwide popularization of the smart phone and smart pad empowered with 4Generation mobile communication technologies such as Long-Term Evolution (LTE) and Wi-MAX. In addition, thanks to low-power communications technology for wireless sensor networks (WSN), research on applications such as Zigbee and Bluetooth is progressing quite rapidly and many related products are being commercialized and widely used.

Through the advancement of such computer and network technologies, complex functions are increasingly being performed remotely by servers and personal computing devices are becoming increasingly miniaturized. Accordingly we are witnessing the rise of a new services paradigm known as cloud computing. Cloud computing places great importance on inter-operability, a key providing services to devices having respectively different operating systems and hardware specifications. This development came on the back of multiple environment service technologies such as HTML5 and is transferring the life, information exchange, and transactions of offline environments onto online environments. Thanks to these developments in computer and network technology, it has become increasingly convenient for users to produce, share, and use digital information whenever and wherever they like. On the other hand, this growth of proper uses for computers and networks has been paralleled by a rise in opportunities for misuse to malicious ends. We can even see such adverse effects for the portable devises applying the newest computer and network technologies. By cracking the operating system of their portable device, users are able to acquire ultimate administrator access, circumvent the DRM inserted by device and content providers to protect their intellectual property rights, and illegally use for-pay content. Consider the following examples of Sony's PlayStation Portable (PSP) and Apple's iPhone, both sold worldwide. In the case of PSP, hackers developed custom firmware in order to run games illegally. With the iPhone, hackers used jailbreak to acquire maximum administrative authority for the iOS platform, disable Digital Right Management (DRM) for those contents serviced by Apple, and made cracked Apple and contents available fee of charge. Both industries and society responded to these illegal episodes in their own ways and the result for

industries in cases such as the Sony PlayStation Network hacking incident is that they incur enormous damages .

The aforementioned Sony PSN hacking episode is merely one of the many hacking episodes that are currently underway, however the Sony incident has a special meaning. Prior to the PNS hacking incident, attacks had typically included those propagated to acquire information or administrator privileges from a single server, Distributed Denial of Service (DDoS) attacks which were primarily performed with the goal of paralyzing the service of a specific company or organization, or attacks on an individual or specific organization for the purpose of acquiring information possessed by a specific company. However after the PSN incident, America declared war on hackers, hacker groups began to direct ideologically motivated attacks against the government agencies of several countries, and these hacking attacks began to pose a national threat. We use cellular networks in my everyday lives to exchange a variety of information and access apply of services. Were these networks to ever be subject to manipulation or a denial of service attack, it is predicted that the many services using these cellular networks would be paralyzed and that a great calamity would ensue. Also cloud computing and ubiquitous computing will become the base of Internet environments of the future. As user devices become gradually lighter, complicated computing and high volume information will be provided by servers. These systems will take several forms, be applied to a variety of fields, and play an increasing role in the private lives and health of individuals and the information of organizations. As a part of this process, terminal user devices will contain important information for identifying the user's personal information contained in servers. Should this data be leaked, it could result in great harm to individuals and organizations and therefore must be distributed through secure channels. Accordingly, there is a need for research on those methods which enable services to be provided both securely and conveniently. Also, as ubiquitous computing is applied to automobiles and the area of public health, data is exchanged which contains information about individual's health or the control and condition of an automobile. Should this information be altered or made public, it could lead to dangerous situations. Even were the data not altered or leaked, should a DDoS attack or something

like it suspend normal service, the likelihood of unexpected malfunctions and the resultant damage is very high.

This thesis addresses this type of service availability problems for ubiquitous computing environments and defines a security framework maximizing security. This framework proposes a cryptographic algorithm and some protocols which offer both light-weight processes and strong security.

The expected contributions of this thesis are:

- The proposed framework provides a light-weight cryptography algorithm for security in resource-constrained applications, such as low-cost RFID tags and sensors in USN for H-Ubi Comp. It has the structure with some improvements in software and hardware efficiency under resource-restricted environments – such as ubiquitous mobile devices.
- The proposed framework provides improved security protocols for H-Ubi Comp. A session key distribution mechanism for fast secure handover in wireless mobile networks such as H-Ubi Comp: The proposed mechanism is based on the stream control transmission protocol wherein a mobile node actively changes its IP address without a loss of connection.
- A security-enhanced Key Recovery (KR) protocol and a privacy-enhanced KR protocol: The proposed protocol is based on that security-enhanced KR protocol in order to protect users' location privacy. Wireless Authentication and Key Establishment (WAKE) protocols are essential for secure information transmission for in mobile communication environments such as H-Ubi Comp.
- A security simulation model based on Contract Network Protocol (CNP): I design and construct a general simulation environment for a network security model which coordinates by means of a contract net protocol (CNP) for the effective detection of an intrusion.
- The proposed framework provides dynamic human-context role based access control mechanism for H-Ubi Comp. It improves the existing access control mechanism based human-context (temporal and spatial information).

- The proposed framework can be applied to surveillance service and mobile IPTV service for H-Ubi Comp.

The structure of this thesis is as follows.

- **Chapter 1. Introduction**

  In this chapter, this thesis described the overview, scope, aim, method, contribution and outline of this study. I described previous part which described a variety of today's network, it can occur in human-centered computing environment to be considered a sufficient security problems. And the thesis briefly mentioned the problem statements and motivation for a secure and H-Ubi Comp.

- **Chapter 2. Background**

  In this chapter, the thesis discussed the background and related works of secure and H-Ubi Comp. I summarized most important existing human-centered computing environment research especially recent research on human-centered computing. One of them, large-scaled collaboration is critical issues of human-centered computing environment, the actual practices applied by checking the current implemented system. Based on these summarized and analysis and the importance of human-centered computing environment, a report composed which part should be implement of effective and optimized security techniques.

- **Chapter 3. HUC-HISF**

  In this chapter, the HUC-HISF is prposed. To offer security for a human-centered computing environment described above, the development of a wide variety of computing environments and the resulting human-centered computing environment has suggestions for a secure composing.

- **Chapter 4. Advanced mCrypton: Light-weight Crypto Algorithm for HUC-HISF**

  In this chapter, cryptanalytic result on mCrypton is presented. it is worthwhile to apply this attack to other block ciphers and to study simple key scheduling algorithms which may be

resistant to this kind of attack. In addition, for many types of attacks, how to composing the method proposed to prevent and detection as effectively explained.

- **Chapter 5. Security Protocol Issues for HUC-HISF**

  This chapter addresses an effective session key distribution mechanism and a number of WAKE protocols having a key recovery feature.

- **Chapter 6. DH-RBAC: Dynamic Human-context Role Based Access Control**

  In this chapter, dynamic human-context access control mechanism is proposed.

- **Chapter 7. Service and Application using HUC-HISF**

  This chapter presents U-Surveillance service and Mobile IPTV service using HUC-HISF.

- **Chapter 8. Simulation and Analysis of HUC-HISF**

  In this chapter, to show the differentiated properties of HUC-HISF, the proposed schemes were analyzed by the aspects of performance, aspects of security among system requirements for the HUC-HISF.

- **Chapter 9. Conclusion**

  This chapter concludes the thesis with the brief summary of contributions, and presents the expected challenging issues and the future working directions.

HUC-HISF: A Hybrid Intelligent Security Framework for Human-centric Ubiquitous Computing

人間中心のユビキタスコンピューティングのためのハイブリッド・インテリジェント・セキュリティ・フレームワーク

朴 鍾 赫 (Park, Jong Hyuk)　　紹介： 金 群 教授

New computing paradigms such as ubiquitous computing and human-centric computing are up and coming due to rapid advances in computing power and network development. Such paradigm changes offer convenient and delightful, human-centered services. However, the ubiquitous and human-centric computing environments have been integrated; there exists a much greater likelihood of exposure to security threats compared to ordinary computing environments. And there are additional threats not present in traditional computing environments; such threats include tampering, signal interference, and battery consumption attacks. Especially in one of most human closed network environment, the ubiquitous computing environment of the human-centered network is compromised by an attack, which could be network information derived from an individual's privacy can cause problems. Than a typical network environment comprised of a human-centered environments in ubiquitous environment is larger than in recent years expanded by service extension.

In particular environment U-health system for the health of the individual person's, the individual's profile in the center of the system have to configured, also that should be prepare a human-centric services, however in your personally identifiable information, including personal health information, the details of the disclosure, number of frequency health problems, any health insurance available, and any u-health system is used information, are used for any purpose whether can still be pirated and illegal market selling. In addition, sensor network system is one of human centered environment in ubiquitous computing area. Sensor networks is principal of information collecting in the individual's human-centered computing, human-centered information. Because of this, personal information about living in an environment, where temperature, humidity, and any location information, which also collects the most ubiquitous model, is presented in a smart home or ubiquitous environment.

This is also theft to be, the individual pattern of living, any habit that the person have, the current home and whether or not, if the person is home than where stay in the house, and where stay at that time, where all the

information about the acquisition, which the theft occurred, it makes another big problem occurring.

In recent years, human-centered computing environment will develop reaches and clearly. As a representative of the reason, Smart Home and Smart Car system will be mostly important system and role based on Smart Grid as Human-Centric Service or system. In modern society, the electrical energy is the most important energy, energy conservation developed by the ultimate purpose of human-centric networks for large-scale energy that can be. So, we need intelligent and dynamic security frameworks for secure and flexible human-centric ubiquitous computing environments.

In addition, human-centered computing environment to take place in the center of the diversity of individuals, depending on the required profile, and more than profiling to provide services to individuals close to the basic information is available. This human-oriented, close to the human complex network computing technologies in the current configuration, it should be safe, and a variety of attacks that can occur in the future it is clear that the purpose be.

In this thesis, I propose a hybrid intelligent security framework for Human-Centric Ubiquitous Computing: HUC-HISF. The HUC-HISF consists of core technology layer, security layer, application and service layer. The Core technology layer contains wireless sensor network/RFID, context-awareness, mobility and information fusion which are key technologies of H-Ubi Comp, and security layer contains lightweight security algorithms, security protocols, users' privacy and security mechanisms. Finally, in application and service layer, surveillance systems and mobile IPTV for H-Ubi Comp are considered.

In this thesis, I design and simulate light-weight secure advanced cryptography algorithm, effective key distribution for secure fast hand-over, and dynamic context based access control mechanism reflecting human-contexts, and privacy-enhanced key recovery mechanisms. I also propose and analyze surveillance service and mobile IPTV service through applied-service layers.

The HUC-HISF provides an advanced key schedule of mCrypton algorithm suitable for H-Ubi Comp devices to give a better security of mCrypton against related-key rectangle attacks. We also provide wireless authentication, key establishment mechanisms suitable for H-Ubi Comp environments, secure authentications and key-exchange protocols. Furthermore, I propose dynamic human-context role based access control mechanism, and surveillance service and mobile IPTV service which are applied-services of the HUC-HISF.