International Journal of Security and Its Applications
Vol.9, No.8 (2015), pp.337-346
http://dx.doi.org/10.14257/ijsia.2015.9.8.30

A Study on a Secure Profile Model for Home Network in Cyber-Physical System

Hoon Ko[1], Libor Mesicek[2]and Kitae Bae[3], Goreti Marreiros[4], Haengkon Kim[5], Hyun Yoe[6] and Carlos Ramos[4]

[1, 2] Department of Informatics, J. E. Purkinje University, Faculty of Science, Ceske mladeze 8, Usti nad Labem, Czech Republic, 400-96
[1]l.mesicek@ujep.cz, [2]hoon.ko@ujep.cz
[3]Department of New Media, Korean German Institute of Technology
661, Deungchon-Dong, Gangseo-Gu, Seoul, 157-033, Republic of Korea
[3]ktbae@kgit.ac.kr
[4]Institute of Engineering Polytechnic of Porto
[4]mgt@isep.ipp.pt , csr@sc.ipp.pt
[5]Department of Computer and Communications, Catholic University of Daegu
[5]hangkon@cu.ac.kr
[6]Department of Information and Communication Engineering, Sunchon National University
[6]yhyun@sunchon.ac.kr

Abstract

Intelligent home network has to notify the context data instantly to the profiler when home device user's main context such as user and access right are changed and renew the profiling with the updated context [1]. To make it sense, we propose the profile based intelligent home network device access control. It includes; (1) Intelligence profiling generation study (2) an intelligent home network configuration and management study, and (3) an intelligent profiling multiple signature study. So, in this study, it suggests a secure profile structure.

***Keywords**: home network, profile, security, smart city, structure*

1. Introduction

Although there is no normal classification of an intelligent home network (including security), they internationally define that an intelligent home network consists of a wire/wired intelligent home network, an intelligent home servers including a gateway [2], an intelligent middleware, an intelligent home network devices, an intelligent home network services and an intelligent home network security. It means that the intelligent home network system absolutely will be the final applications or final services by integrating in all techniques and by extending into them such as remote connection services, remote inspection services, remote medical services and systems, Home healthcare systems, broadcasting systems/game services and so on [3-4].

To know what kinds of intelligent home network services we meet, I define next; Home Entertainments: it is the service that we can watch the high quality media data over the audio / video devices such as movies, MP3 files, HDV and so on which will be transferred from inside as well as from outside, also they can watch the data which area stored in the home server, Home data: it is the service which makes it possible to connect between a computer and a computer, a computer and a printer, and a computer and a scan-

ISSN: 1738-9976 IJSIA

ner, and next try to exchange. And they can use an internet at that same time. And Home automation services: it is the services that they can monitor and control all home devices which are indoor (ex., fixed home devices) or outdoor (ex., mobility home devices) with their smart devices. Although the controller is outside or inside, they can also control and monitor them, at last Home network security services: they have to be processed by differentiated security level that is going to be defined according to a users' life information, a privacy management technique, a connectable security technique between home network and an infrastructure, a convergence security of network middleware, a user profiling.

2. Related Works

CPS (Cyber Physical Systems) is the system to exchange all information in 'Internet of things' by connecting between computing and physical spaces which is controlled automatically and intellectually.

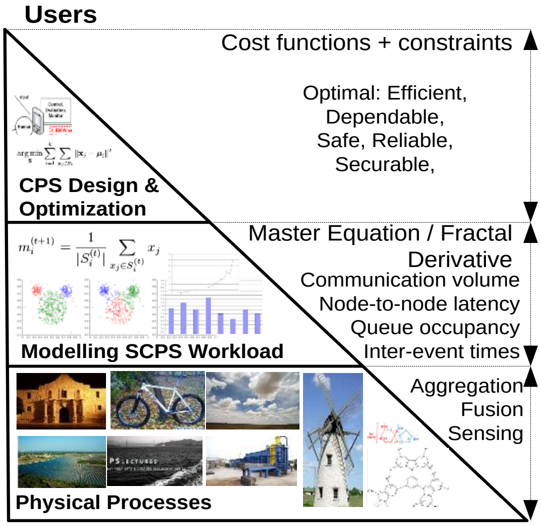

Figure 1. Cyber-Physical System

Recently, it is focused in a computing system because it can be a bridge between two spaces such as a cyber space and a physical space. Also, it keeps an important technical meaning because it is embedded the control function through system relationships of two-spaces in CPS. Also, the CPS usually involves not only the control function which is including operational concepts, but also the extension of technical view to a social view. It means that the CPS with computations and computer processes can manage systems which are able to control the physical processes through feedback loops by network monitors and by computers that are involved in network systems [Figure 1]. However, many experts have been insisting that these days the CPS only defines systems between a cyber-space and a physical-space simply, also, it is just the system that the transmission / exchanging skills are extended and integrated complicatedly in a backbone including RFID / Sensor networks and so on. So, in case there has special troubles, they will be almost impossible to know what happens in future such as where happens and how to solve. In addition, the attackers are able to use all cyber-attack's skills which are using the existing system to attack in CPS [7]; also it has the same damages like the existing systems have. The experts also said continually if it tries to add new techniques into CPS without completed protection against the all cyber-attacks, anther and new security problems will appear [2]. Therefore, new security which has to consider two spaces, cyber-space and physical-space, has to be involved in this study.

3. Existing Problem

Still, many intelligent home network systems don't have own security module and each policy, also they don't have any plan to develop it in future. Now they are just using existing security modules, and following generally policies without their specific policies in their home network systems. In addition, the EU which is the best market in the world more invests the services than security works [7].

Therefore, if we design and implement the security modules for home network in Portugal, it will be a good opportunity to be the first ranked in a home network security area in the world including economic benefits by selling the techniques. Next is the security problem that I analysed [4].

- Each device only accepts the users who have each certification. If the users want to use the devices, they have to process some steps to get the certification and the ownership.
- When they transfer the data to process the certification, the attackers can get the data illegally.
- Because wire/wired usually use together, stronger securities are needed.
- Still weak provisions to vulnerability or privacy trouble in different network co-operations / in convergence environment.
- Possibility increasing from user privacy exposure
- Weak standardization work to interactive between/in various middleware
- Weak integrated authentication service in a context-awareness
- Intelligent services weak for group users/real time application services weak: many services/resource searching protocols have been proposed. However they were only for small network systems such as a home network, also, they considered only for services searching of context awareness. DHT (Distributed Hash Table) also which is to search in a global network is considered a hash function; also it has the limitation that it only provides the keyword matching [5].

Table 1. Related Work and Security Weakness

Title	Contents	Security Weakness
Cloud robotics in google	- It begun to study a rosjava which was the java based ROS (Robot OS) under Android OS. The key point is that they used an android OS because it could connect among cameras, elec.-clocks, bicycles, and all electronics devices in home. - It developed low-cost robots which have a high-quality to work the high level services, also it tried to reduce the robot resources, ex., battery, memory, and sensors by using a cloud.	-To use the robots, they have to be registered. -The attackers can take an authorization and an authentication from the robots to control by attacks.

Android Cellphone NXT Robot	- It downloads the MAP information after it transfers and process in a cloud with a wireless communication from sensors, cameras, and microphone which are installed on smart devices. - It is new tasks from APP to prepare new situations.	- ID/Password using: it has weakness to cyber-attacks ex., spoofing/sniffing.
RoboEarth project (EU)	-This is the projects under a cloud based that the robots do get / exchange / re-use all information through the internet, and they help other robots to do the complicated tasks.	-No crypto algorithms to the transferring data.
Google driverless car	- In google, it develops / developed the driverless car in cloud, the car has a camera and radar sensors to gather all information around the car including the processing to decide routing plan to control the car.	-No crypto algorithms to the transferring data. - In case it uses smart phones to control, the smart phone can be a target to attackers.

Through each project, they studied the robots to the application, and the robots could control the machines following the algorithms. With the result of their study, they can apply in the healthcare systems which are able to care the old and the young such as their health or their security. Also it can expect the roles of the robots in the industry space, in our life, in transportations, in militaries, and in a smart gird and so on. However, they usually operate by connecting among all smart devices ex., smart phones, iPads, Notebooks, but they just do it under the network system. Therefore, it can consider that they have the same security problems like the existing systems have. In addition, the users are supposed to control the robots by their smart devices, but the authentication or authorization to control can be hijacked by attacks. So, we insist that all systems have the potential weakness [Table 1].

3.1 Security Needs

There are three items which is security needs.

(1) The interfaces between cyber-space and physical-space consist of many sensors, computing / network devices and various actuators, they operate in real-time, also at that same time, and many complicated errors will appear in the interfaces including attacks. Therefore, with the attacks, CPS will have security troubles, and then all components of the CPS will be under the troubles.

(2) These days, many researches are proposed new CPS applications which tries to gather and to send the data, and it is integrated the sensors to know their situations. Also, various mechanisms and protocols are suggested that they try to control them in real-time. However, with these functions or by attacks, attackers can take all information.

(3) Finally, to be a secure CPS, a distributed monitor, a data convergence, an intelligent control, a cyber-security / physical security, privacy, system robustness are needed.

3.2 Threats

- DDoS attack: It is to exhaust the CPU, the Memory, Communications bandwidth, and then it make them not use or slow. Finally the purpose is to make impossible to use them. There are three security elements in a DDoS; the names are confidentiality, integrity. The purpose of the DDoS is killing the availability. Availability means that the correct users always can use the system.

- Network Interception (Sniffing, Spoofing): it means that illegally to see the other user's packet in network. That is, it is called the sniffing which is wire-tapping network traffic. Many users can catch other user's ID/Password by using some hacking tools. Therefore, they easily can do the illegal works such as ID/Password intercepting.
- Fraud Serve: Fraud Servers can give the wrong data to all users. The data make them mistake and misunderstand. With this step, they can get user's information. Recently, it knows as Pishing to us. If attackers make the Fake Skeleton and operating, they connect to correct RMI Stub, and the attackers easily get other's information.
- Protocol attack: The protocols could be potential exploited launch cyber-attacks if they are not secured properly. This calls for secure versions of these protocols that not only provide security guarantees, but also the required latency and reliability guarantees needed.
- Routing attacks: This refers to cyber-attacks on the routing infrastructure of the internet. Although this attack is not directly related to the operation, a massive routing attack could have consequences on some of the applications.
- Intrusion: This refers to exploiting vulnerabilities in the software and communication infrastructure which then provides access to critical system elements.
- Malware: It refers to malicious software that exploits vulnerabilities in system software, programmable logic managers, or protocols. It generally scans the network for potential victim machines, users, exploits specific vulnerabilities, replicates the malware payload to the victims, and then self-propagation. These days, the attacks are growing in numbers and sophistication, and it has been a source of major concern for critical infrastructure systems.
- Insider threats: An insider abuses their current system privileges to perform a malicious action. This form of threat is perceived as a source of concern in recent years as identified in many federal documents.
- Hacking websites: Coming back to Willie Sutton, websites are hacked because "That's where the data is." Websites (based on application frameworks, based on web server software, based on operating systems, based on hardware connected to networks) create some of the most complex systems we have. Compounding the problem, web administrators have the mission to provide the content for their websites.

4. Secure Profile Model

Intelligent home network has to notify the context data instantly to the profiler when home device user's main context such as user and access right are changed and renew the profiling with the updated context. To make it sense, we propose the profile based intelligent home network device access control. It includes; (1) Intelligence profiling generation study (2) an intelligent home network configuration and management study, and (3) an intelligent profiling multiple signature study [9-10].

4.1 Basic Concept

Figure 2 and Figure 3 show us its structure and a secure profile structure; they are the member of the family who has each certification to control home devices. In case the son wants to control them, first he needs to request the permission to their server. Surely all member may receive the request, and after their signature, the server makes a temporary certification, finally it sends it to son.

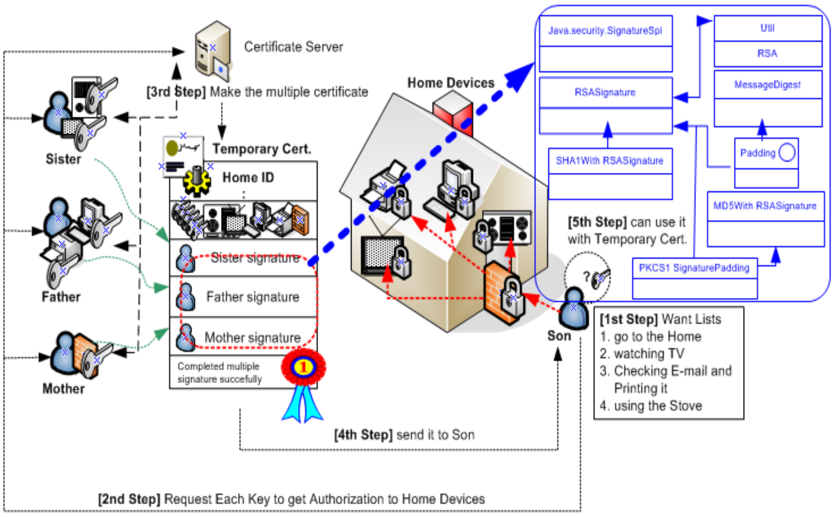

Figure 2. Structure

Through this, I study a profiling making and an operation in an intelligent home network. It has (1) intelligence profiling generation study in a context-awareness, (2) an intelligent home network configuration / management study, and (3) an intelligent profiling multiple signature study. I design including implement the intelligent home network prototype for experiment / simulation based on the output of (1)(2) and (3), and then I try to evaluate them and with the result, I let them to use in many applications in future [6, 8].

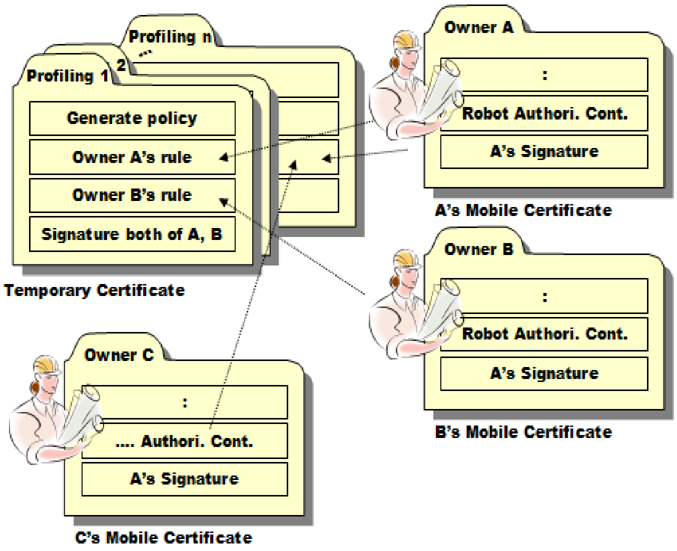

Figure 3. Secure Profile Structure

Each description to lead this study is next;

(1) It is the step to study the element analysis to the location moving and object changing. There are a pub/sub study and element techniques analysis, an authorization delegation study and trend analysis, a data transmission analysis in 5G, and a home network trend analysis.

(2) It is the step to study the continuity of the security process such as a temporary profiling generation requirements analysis, the optimized profiling selection algorithm and transmission requirements analysis, a home device control requirement analysis and a temporary profiling management study.

(3) It is to study the interactive of the dynamic home contexts in evolving intelligent object or in a community. In this step, I study a temporary profiling design, a temporary profiling selection algorithm design, 5G mobility management module design and the requirements analysis of home network multiple profiling application, and a home devices control module study.

(4) It is the step to study the home network framework design which can react against all emergency trouble dynamically. Also it studies the optimized profiling generation/selection algorithm design, 5G intelligent home network design and a multiple signature plan in Smart Cities.

4.2 Differences

The most important key issue to provide intelligence home network services will be an integration of an intelligence home network. The needed information also will be bigger to provide many services, so, it should be safety to process an authentication/an authorization as well as to keep each personal information. Next are new techniques in 5G that I study,

- Privacy and security management in 5G intelligent home network [2-3]
  - User privacy information management skill.
  - Inter-operable technique between 5G home network and infrastructure.
  - Convergence available techniques between networks and middleware elements.
  - Differenced security level in user profiling or configuration.

4.3 Importance

- The community reconstruction to use home devices by users who is not a member of family, that is, if they want to use them, they have to get the authentication / the authorization from the owner. In this case, it takes time to have it, so it can be time wasting. To avoid the wasting, they have to use another community that it will be already set by another owners (by another family member). In this study, I work how to take / to give the authentication / the authorization, and how to transfer.
- The 5G computing is supposed to provide various kinds of services. Therefore, because many users of home devices will share some resources, the access controls to use the shared resources will be needed. Also, the charge according to users consuming may be asked. (In future, according to how many they use the home devices and how much they use the energy; the payment to charge also will be asked.). To do this (Also to save our energy), it has to set the techniques that it confirms to verify and to authorize the reliability of services requesters including different user access control level that the users have each limitation to access following their reliability [1].

5. Derivative Application and Markets

APP1. "Secure Virtual Meeting System", it let her join the meeting by sensors, distributed computing, intelligent concepts and Smart Energy for all devices in Cyber-environment if user is outside.
Expected Markets: We expect system and device market such as private/public devices market, intelligent mobile devices markets, sensors for detecting user information, markets of hologram transfer technique with voices, markets of 3-D algorithm and intelligent distributed computing technique etc.

APP2. "Secure Cyber Medical System", it makes it possible to get users examination remotely by a doctor without the doctor's visiting.

Expected Markets: Bio-information, that is, human computing markets are expected, also some system markets for sensibility awareness technique, sensibility signal evaluate technique, and facial expression recognition technique including voice acceptance technique are expected. In this case, privacy and security issues are very important.

APP3. “Secure Intelligent Cyber Travel System”, this system is that without user visiting some place, they feel that they are there.
Expected Markets: We expect the relevant markets for system/devices. We can consider contexts business from visiting place. With this system, we can also expect GPS markets.

[Expected Impact]
Next is another description to explain expected outcomes and impact.

With Secure Module: Protection and control of utilities (energy, water, oil, gas, etc) production/storage/transmission facilities as well as information/communication networks (fixed-lines, wireless) and transportation systems for people & goods (automotive, rail, avionics, space, naval)
Object: Transportation (automotive, rail) – maximally utilizing the capacity of roads to accommodate increase in traffic demand while improving safety (The EU has a goal that it should be zero traffic fatalities by 2020).
Expected impacts: (1) definition of a new programming model & new types of API to support platform-independent composition; (2) definition of performance & resource management models, metadata and system layers in order to achieve global performance and resource optimization and management.

6. Conclusion

These days, in intelligent home network security, it still would not design and develop them; they only are interested in services. Especially, the EU which is the biggest market also tries to make the many services than securities. So, if we make the high quality security to occupy the intelligent home network area, we can get big benefit through an industry export and technology export. Improvement of Intelligent Home network Life Quality (in Smart Cities): When we serve the services, we need to consider each person or their group meaning what they have in a place of smart cities and group contexts/contents which user belongs to as well as user’s intension and situation at that same time. It is expected to be contributed to improve the quality of our life by suggesting the direction of important origin technique which makes it possible to efficiency urban life with more convenience to have some skills to set ubiquitous environment in space named Urban where is general and where has unique features. We connect with home network system after analysis the visible activity and behaviours features based on persons who has already their unique activity patterns or person’s activity patters in various contexts and scenes in real their daily life, to easily accept and to naturally use these skills in life of real users.

Acknowledgements

This work has been developed under the project EKRUCAmI - Europe-Korea Research on Ubiquitous Computing and Ambient Intelligence, a project receiving funding from the People Programme (Marie Curie Actions) of the European Union's Seventh Framework Programme FP7/2007-2013/, REA grant agreement No 318878 (PIRSES-GA-2012-318878), and also supported by the International Research & Development Program of the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (Grant number: K 2013079410).

References

[1] H. Ko, G. Marreiros, S. H. Kim, C. Ramos, and T. H. Kim, “A study on Security Grade Assignment Model for Mobile users in Urban Computing”, *INFORMATION JOURNAL*, vol. 16, no. 1(B), (**2013**), pp. 581-586.

[2] H. Ko, G. Marreiros, K.-j. An, Z. Vale, T. hoon Kim, and J. Myoung Choi, "A Study on Dynamic State Information (DSI) around Users for Safe Urban Life”, *Computers and Mathematics with Applications*, vol. 63, no. 2, (**2012**), pp. 554-563.

[3] J. S. Oh, H. J. Bang and H. Ko, “An Empirical Study on Smart Safety Management Architecture for Gas Facilities in Korea”, *INFORMATION-AN INTERNATIONAL INTERDISCIPLINARY JOURNAL*, vol. 15, no. 3, (**2012**), pp.1107-1122.

[4] K. An, M. K. Choi and H. Ko, “Utilisation of Photo-Montage Technique for UK Planning Process,” *INFORMATION JOURNAL*, vol. 15, no. 11 (B), (**2012**), pp. 4785-4796.

[5] M. K. Choi, R. J. Robles, G. Marreiros, Z. Vale, C. Ramos and H. Ko, “The Cross Crypto Scheme Cipher Integration for Securing SCADA Component Communication,” *INFORMATION JOURNAL*, vol. 16, no. 3(B), (**2013**), March, pp. 3189-3194.

[6] M. K. Choi, R. J. Robles, Z. Vale, C. Ramos, H. Ko and G. Marreiros, “Utilization of Different Encryption Schemes for Securing SCADA Component Communication”, *INFORMATION JOURNAL*, vol. 16, no. 2(B), (**2013)** pp. 1503-1508.

[7] H. Ko, G. Marreiros, H. Morais, Z. Vale and C. Ramos, “Intelligent Supervisory Control System for Home Devices using a Cyber Physical Approach”, *INTEGRATED COMPUTER-AIDED ENGINEERING*, vol. 19, no. 1, (**2012**), pp. 67-79.

[8] J. Choi, J. Choi, H. Ko, K. Bae, K. J. An, C. S. Kim, and J. Choi, “A Smart Service Robot Middleware on Ubiquitous Network Environments,” *AutoSoft Journal*, vol. 20, no. 1, (**2014)** pp. 1-13.

[9] H. Ko, K. Bae, S. H. Kim and K. J. An, “A Study on the Security Algorithm for Contexts in Smart Cities,” *International Journal of Distributed Sensor Networks*, vol. 2014, (**2014**), pp. 1-8.

[10] H. Ko and K. An, “Analysis on Smart Warning System for Home Network in Smart Grid”, *The Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2013),* pp.714-718, July 3-5, Asia University, Taichung, Taiwan, (**2013**).

Authors

Hoon Ko, He got the B.S. degree in computer science from Howon University, Kunsan-City, S. Korea, in 1998, and M.S. degree in computer science from Soongsil University, Seoul, S. Korea in 2000 and Ph.D. degree in 2004. He had joined in Daejin University as visiting professor from 2002 to 2006. He had worked at Information & Communications University (ICU), Korea Advanced Institute of Science and Technology (KAIST) in 2007. Next, he had worked at GECAD, ISEP, IPP in Porto, Portugal as a Doctor Researcher from 2008 to 2013. Now he is a research professor at the department of informatics, University of J. E. Purkinje since 2013. He is interested to Urban Computing Security, Ubiquitous Computing Security, AmI Security, Context-Aware Security, MSEC (Multicast Security), RFID Security, Home Network Security, etc.

Libor Měsíček, he studied Information systems and technologies at the University of Economics, Prague, Czech Republic and continued as a Ph.D. candidate (finished 2013). Since 2008 he has focused on ICT Project Portfolio Management, Social Networks and IT Project evaluation. Currently, he works as an assistant professor at the Department of Informatics, University of J. E. Purkinje since 2012.

Kitae Bae, He received the M.S. degree in Computer Engineering and the Ph.D. degree in Computer Information Engineering from Chonnam National University, Korea, in 1999 and 2006, respectively. He is an associate professor of the Department of New Media in Korean German Institute of Technology from 2009. His research interest includes Computer Vision, Computer Graphics, HCI, and Image Registration and Media Processing and Affective Computing, Ubiquitous Computing Security.