Security and Privacy Protection of Smart Home Based on IPv6

Zhenyu Liu
State Key Laboratory of Digital Household Appliances
Qingdao, China

Yang Pan
State Key Laboratory of Digital Household Appliances
Qingdao, China

Qinglei Cao
College of Information Science and Engineering
Ocean University of China
Qingdao, China
cql.levi@gmail.com

Gui Chen
State Key Laboratory of Digital Household Appliances
Qingdao, China

Abstract—At home and abroad, smart home, after more than ten years development is getting more and more widely welcomed. Smart home technology is developing rapidly, and with the emergence of IPv6, smart home based on IPv6 is becoming a trend. Meanwhile, security and privacy protection of smart home is receiving more attention. Although IPv6 is more secure than IPV4, there are still issues of privacy loss. In this paper, we focus on the security and privacy protection of smart home based on IPv6 and propose two different solutions respectively, that is, security and privacy protection based on trust as well as that based on strategy. These two solutions achieve security and privacy protection via model about trust and strategy mechanism respectively. On the basis of these two solutions, a framework of security and privacy protection system of smart home is designed. Through the system we designed, the security and privacy protection of smart home based on IPv6 is achieved.

Keywords- Smart Home; IPv6; Security and Privacy Protection; Trust; Strategy;

I. INTRODUCTION

Internet of Things (IOT) is a huge network, which gathers the existing technologies of EPC technology, RFID technology, WSN technology, GPS, video recognition, infrared, laser, scanning, and other technologies together [1, 2]. With the developing of IOT, as well as the high-speed growth of computer control technology and communication technology, more and more applications have appeared, and the smart home is one of the most important.

Nowadays, smart home technology is developing rapidly [3, 4, 5], and more and more families are urgent to access outside information sources at home, or control the family home appliances outside, and achieve intelligence. Fig .1 shows the framework of smart home. The emergence of IPv6 [6, 7, 8] makes this ideal realize more quickly. Plenty of IPv6 address space for each appliance can be assigned a global IPv6 address on the planet to connect devices to the Internet, which solves the shortage bottlenecks, due to Ipv4 address, to build intelligent home network system. Now, some researchers have built smart home system based on IPv6 [9, 10, 11]. Although IPv6 is more secure than IPV4, there are still issues of privacy loss. With respect to the security and privacy protection of smart home without IPv6, a lot of researches have been done [12, 13 14, 15], but little is about that of IPv6.

In this paper, focusing on needs to security and privacy protection of smart home interaction, we aim at different types of application environments to carry out security and privacy protection technology research from different angles. As shown in Fig .2, when user's private information is collected by system or other's requests, information control method based on trust is adopted, which computes the credibility by trust evaluation mechanism and makes decisions according to the prior trust control table of user's, for interactive entities unknown and application environments that cannot be described structurally. While for interactive entities known and application environments that can be described structurally, we use reasoning decision-making methods based on strategy to achieve reasoning and decision-making by the system itself, according to the prior strategies established by the users.

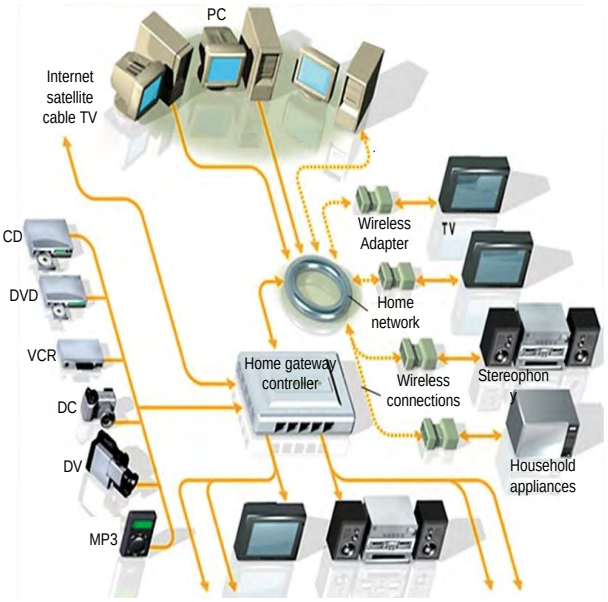

Figure 1. Framework of smart home

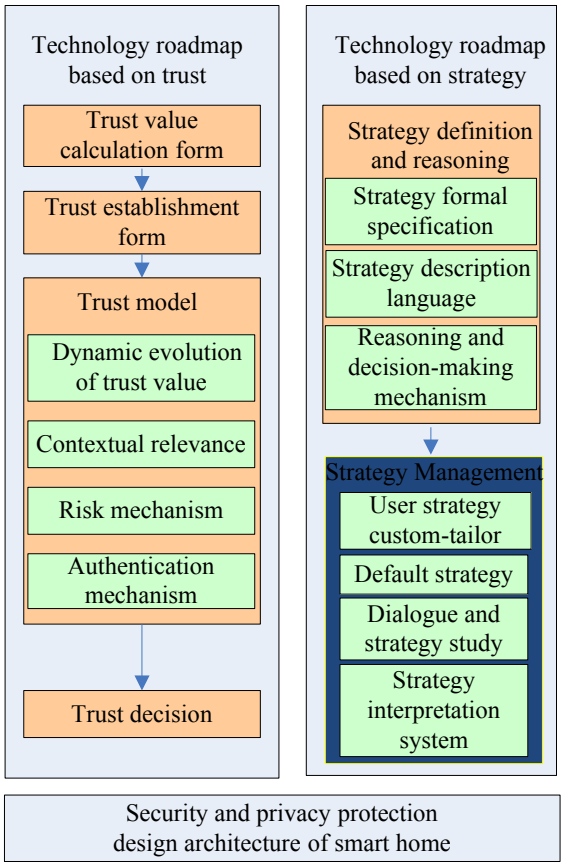

Figure 2. Research process of security and privacy protection

The remainder of the paper is organized as follows. In Section 2 and Section 3, we propose two different solutions of security and privacy protection of smart home based on IPv6 respectively, that is, security and privacy protection based on trust in Section 2 as well as security and privacy protection based on strategy in Section 3. Section 4 describes a framework of security and privacy protection system of smart home. Finally, we conclude the paper in Section 5.

II. SECURITY AND PRIVACY PROTECTION BASED ON TRUST

Aiming at security and privacy protection based on trust, we focus on the trust value calculation forms for privacy, trust models about establishing way of trust and environment traits fitting smart home.

A. *Trust value calculation form*

We research trust value calculation form for privacy on the basis of clear trust value representation. Because through trusted way it determines the exposure and its degree of security and privacy information, so the calculated trust value here represents the trust degree, which is about peer entity able to guarantee not to violate user's privacy. Content should be calculated for privacy, mainly including assessments of peer entities in the past, such as privacy-related behavior and investigation commitment to the privacy protection of peer entities. The former learns whether peer entities have taken over privacy violations according to the interaction history records or information about other people's recommendations, where there are problems about how to define acts of violating privacy.

We investigate the peer entity's commitment to privacy protection through the understanding for commitment to privacy of information collection, use, sharing, and propagation process, and then will compare it with privacy protection requirements defined by users to calculate matching similarity. If the match is high, then both protect privacy issues with higher consistency. Here there are problems of how to define undertaking clauses in the way of collection, use, sharing and propagation of the relevant privacy information. Through these two methods, the trust, which is about security and privacy protection issues between both, can be obtained more comprehensively and accurately.

B. *Trust establishment form*

The main way to establish trust refers to which means will be taken to obtain the final overall trust value. The main researches focus on integration issues on direct and indirect trust value (recommended trust value) and what kind of factors calculated as weighted factors.

C. *Trust model*

According to the former two forms, we further research the trust model, which fits for smart home environment. It includes selecting the appropriate dynamic evolution model, considering the model authentication mechanisms and risk mechanisms, as well as issues of contextual relevance.

1) *Trust dynamic evolution model*

Through the investigation and analysis, mathematical model is researched to suit with the dynamic evolution of trust value in smart home. Because of the breadth of trust applications, currently, there are many mathematical models to describe definitions, evaluation and evolution of trust. By comparison analysis on a variety of mathematical models, we clear advantages and disadvantages of the various models and propose a more suitable dynamic mathematical model for smart home environment.

2) *Authentication mechanism*

Trust relationship is built on a clear specific object, which relates to certification issue. However, a clear identity often result in violation of user's privacy. However, how to build trust is also an important research field, while protecting user's identity. The principal research is about how to use a pseudonym or blind signature way to solve the issues.

3) *Risk mechanism*

Risk mechanism adapted to trust model of smart home is researched. It mainly includes three aspects. First, how to effective and clearly identify the potential risks. Second, assessment methods of the risk possibility. Third, how to integrate risk mechanism with trust model to guide behavioral decision-making.

4) Contextual relevance

Contextual features are researched in trust model. There are significant relevance between trust and context, and changes of contextual relationships tend to affect changes of trust values. For example, the same service requestors request for service to the the same service provider. Due to the different security level or privacy level required by each service, the trust level needed for successful implementation of the request must not be the same. So we research how to properly express context information and how to be integrated into the trust model as a factor.

III. SECURITY AND PRIVACY PROTECTION BASED ON STRATEGY

Drawing lessons from relevant theories and methods of computer security management and security strategy, we study smart home security and privacy protection solutions based on strategy. First, security and privacy strategy itself are researched, and then we study the security and privacy strategy management platform, finally implementation mechanism of security and privacy strategy is studied. Strategy, strategy management platform and strategy implementation mechanism constitute the architecture of smart home security and privacy protection system.

A. Security and privacy strategy

We ultilize rule-based strategies to achieve security and privacy protection of smart home, which could separate guidance rules from functions of the system operation. For the new privacy threats, it could increase the appropriate strategies and implementation mechanisms without modifying the core system and improve dynamic adaptability to privacy protection needs and environmental changes, as well as system flexibility and scalability. There are three parts，strategy model selection, strategy framework design and strategy language.

(1) chosing discretionary access control strategy model as a blueprint, we study security and privacy strategies of smart home, as well as their implementation mechanisms and applications.

(2) strategy framework is divided into three layers, abstraction layer strategy , describing layer strategy and strategy implementation layer, each of which expresses different levels of strategy.

(3) according to the formal strategy language and constitution, we establishe privacy strategy ontology descriptions of component elements and design templates of security and privacy strategy according to XML-based ontology and DF Resource Description Framework, so as to form coupling mechanism of strategy management platform.

B. Implementation mechanism

Strategy implementation mechanism should be able to provide the appropriate decision and execution mechanisms for different types of strategy rules. So we mainly research on mechanisms of security and privacy strategy from strategy decision and implementation.

Prior to the strategy implementation, strategy decision is the use of strategies, which includes three steps: selecting strategies from the strategy storage collection, interpretation and conversion strategies, as well as importing strategies into strategy implementation layer. The core of strategy implementation layer is rule-based reasoning system and we adopt the forward inference engine CLISP as inference engine of strategy rules.

IV. FRAMEWORK OF SECURITY AND PRIVACY PROTECTION SYSTEM

In smart home, users formulate, understand and adjust the relevant security, privacy and notification strategies by interaction with devices. There are two challenges to formulate and manage security and privacy strategies for users: (1) how to generate user strategies under the premise of not increasing the user's burden; (2) how to pass the information contained in strategies to users, so that users could understand the system, know which strategy is valid at a given time, as well as the effect of the revised strategy, which will be particularly difficult to small screens of mobile devices.

To solve these issues, we combine Agent technology, semantic Web services technology, ontology methods and some latest research results of rule reasoning machine and propose logical architecture of security and privacy protection system, following the idea of computer network OSI layered model, shown in Fig .3. From the bottom to the top, there are transport layer, environment layer, strategy language layer, strategy management layer, strategy decision-making layer and strategy execution layer.

A. Strategy language layer

Strategy language layer is mainly to design languages to describe security and privacy strategies. In addition to include a complete grammatical structure, It should support semantics, so as to apply strategies in the rule-based reasoning system.

B. Strategy management layer

Strategy management layer could support users to design easy-to-use strategy management platform. Because there is asymmetric information between users and the system in smart home system, the strategy management platform designed by these technologies, which include techniques not only for access control strategies but also for helping users formulate trust-based strategies achieving exposure, could effectively reduce user’s burden.

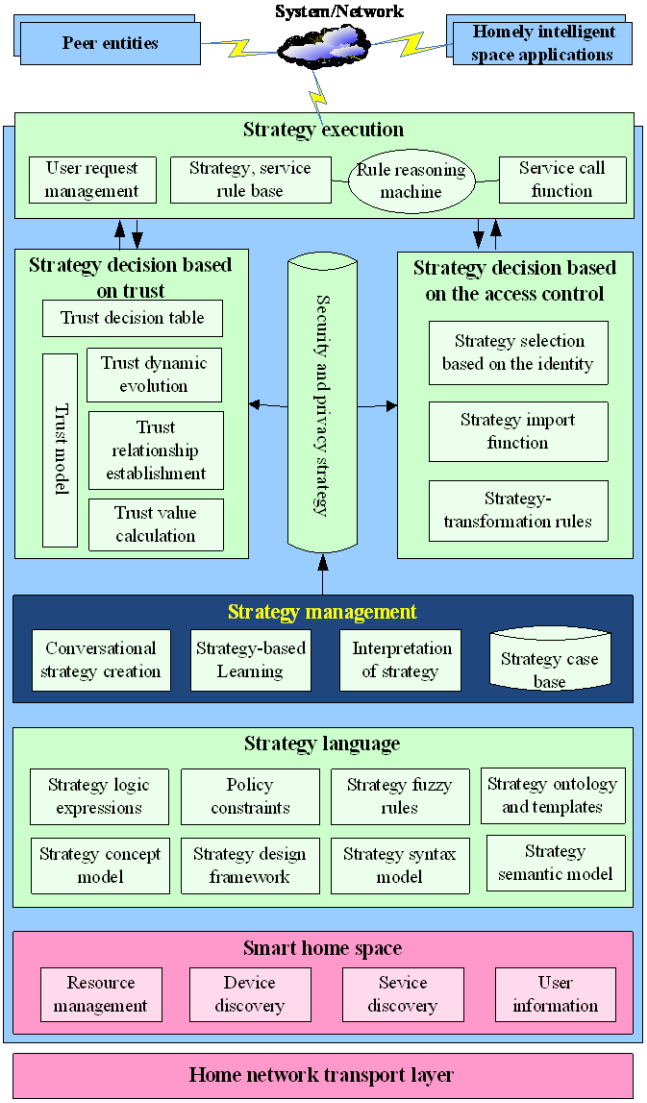

Figure 3. Framework of security and privacy protection system

C. *Strategy decision-making layer*

Strategy decision-making layer is mainly designed to achieve automated decision of security and privacy system. For unknown interaction entities, we adopt decision-making moduls to achieve credibility computing and updating, as well as matching and decision-making of user's trust decision tables. While for known interaction entities, access control decision modules are used to achieve rule-based reasoning and decision-making function of user's security and privacy strategies through appropriate user's authentication mechanisms.

D. *Strategy execution layer*

Strategy exccution layer is mainly to realize strategy rules, as well as service invocation rules of reasoning and execution environment. It receives requests of access subjects and send the relevant information to strategy decision-making layer. After receiving results from strategy decision-making layer, strategy execution layer puts the results, which finally are inferred and executed by the inference engine, into the rule base. If the relevant Web services are required, the function will be invoked by inference engine.

V. CONCLUSIONS

This paper focuses on security and privacy protection of smart home based on IPv6 for different types of application environments from different angles. Through previous researches on the common smart home framework, IPv6 and network security mechanism, two different solutions are proposed respectively: security and privacy protection based on trust as well as security and privacy protection based on strategy. On the basis of these two solutions, a framework of security and privacy protection system of smart home is designed.

REFERENCES

[1] Gustavo G R, Organero M M, Kloos C D. Early infrastructure of an Internet of things in spaces for learning. Proc. 8th IEEE International conference on advanced learning technologies, 2008: 381~383

[2] Sarma A C, Girao J. Identities in the future Internet of things. Wireless personal communications: An International Jouranl, 2009, 49(3): 353~363

[3] Cook D J, Youngblood M, Heierman III E O, et al. MavHome: An agent-based smart home[C]//2013 IEEE International Conference on Pervasive Computing and Communications (PerCom). IEEE Computer Society, 2013: 521-521.

[4] Portet F, Vacher M, Golanski C, et al. Design and evaluation of a smart home voice interface for the elderly: acceptability and objection aspects[J]. Personal and Ubiquitous Computing, 2013, 17(1): 127-144.

[5] Feng X Y, Huang X Q. The Research of Smart Home Robots Based on 3G Mobile Network[C]. Applied Mechanics and Materials. 2014, 631: 184-187.

[6] Deering S E. Internet protocol, version 6 (IPv6) specification[J]. 1998.

[7] Thomson S. IPv6 stateless address autoconfiguration[J]. 1998.

[8] Johnson D, Perkins C, Arkko J. Mobility support in IPv6[J]. 2004.

[9] Zou Z, Li K J, Li R, et al. Smart home system based on ipv6 and zigbee technology[J]. Procedia Engineering, 2011, 15: 1529-1533.

[10] Liu X, Deng Y, Study and design of smart home network based on IPv6 [J]. China science and technology information, 2011 (17): 88-88. In Chinese

[11] Wang Y, Jiang L, The research and thinking of smart home system based on IPv6 [J]. Computer Knowledge And Technology: academic communication, 2008, 3(11): 942-943. In Chinese

[12] Theoharidou M, Tsalis N, Gritzalis D. Smart Home Solutions: Privacy Issues[J]. 2014.

[13] Medaglia C M, Serbanati A. An overview of privacy and security issues in the Internet of things. Proc. The Internet of things: The 20th Tyrrhenian workshop on digital communications, Sardinia, Italy, 2010: 389~395

[14] Kun Wang, Jianming Bao, Meng Wu,Weifeng Lu. Research on Security Management for Internet of Things [A], 2010 International Conference on Computer Application and System Modeling (ICCASM) [C]. Oct. 22-24, 2010:133-137

[15] Vladimir Oleshchuk. Internet of things and privacy preserving technologies [A], Wireless VITAE 2009 [C], Aalborg, Denmark, May 2009: 336-340