Label-based Security Management Mechanism for Universal Identifier Network

Jianfeng Guan[*], Jinsuo Jia, and Mengxin Liu
Beijing University of Posts and Telecommunications, Beijing, 100876, China
{jfguan, jjs, mxliu}@bupt.edu.cn

Abstract

The current Internet is an open global interconnected system and lacks of the systematic security design. Most security issues of current Internet are due to the drawbacks of the original design of traditional Internet. Besides, some optional security mechanisms are independent without enough cooperative mechanism. Therefore, it facilitates the network attacks and brings various security threats to network services. In this paper we design a security management mechanism and several relevant evaluation methods under Universal Identifier Network (UIN) architecture, aiming to provide a finer granularity, adaptive network security management system, which consists of the following features: (1) supporting multi-dimensional properties description by introducing the detailed user and service classification; (2) supporting the label-based policy-driven management mechanism in perspective of user and service to provide the fine granularity access control; (3) providing the multi-dimensional evaluation metrics. The proposed label-based security management and evaluation methods will provide great benefits for the future network security.

Keywords: Universal Identifier Network, classification, label, security management

1 Introduction

Various networks eavesdropping and leaking bring a serious impacts on the network services, which show that the Internet is still lack of effective security management mechanisms. Reviewing the Internet development, the root cause of Internet security threats is mostly due to the open design principle of Internet architecture, in which anyone with the legitimate IP address can connect to others, and at the same time network users are difficult to perceive the malicious attack behaviours even with the help of security tools. To prevent these threats, many security mechanisms are proposed, however, most of them are optional while not the inherent part of the network architecture, which cannot be mandatory implemented to resist the threats such as virus, Trojan horse, network deception, phishing, and application software security holes. Most recently, with the economic incentives, some network attackers are booming with the objective to steal the confidential information of banks, financial and securities institutions, which have resulted in serious privacy leakages and financial loss problems. Even worse, some illegal organizations adopt the network as a platform to declare their heresies and spread rumours, and mislead the netizens. All of these make the Internet services face more challenges, and the need of effective security management is urgent.

To provide the better security guarantee, the policy-based or policy-driven management method is superior to traditional management to provide dynamic, autonomous and trustworthy security management, which can be applied in many domains including IoT [13, 20], network slicing management [4] and OpenFlow networks [19]. The policy-based management architecture [9, 17] are general consists

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 4, Article No. 6 (August 15, 2018)

[*]Corresponding author: Room 432, The National University Science Park of BUPT, Beijing, 100876, China, Tel: +86-186-1121-1658

of the four parts including the Policy Repository (PR), Policy Decision Point (PDP), Policy Enforcement Point (PEP) and Policy Authorization Point (PAP). In this architecture, the policy maps the system security requirements to specific and implementable operations in term of domain or device independent intermediate format. Therefore, the policy definition and selection is the key point of the security management although it still faces with the policy conflict detection of intra-policy and inter-policy, and resolution problems [12].

In spite of there are lots of researches focusing on the security issue, the challenges are still diverse and complicated [7]. First, it is difficult to provide the effective security management for various participants such as network users, service providers. Second, it is not practical to specify the security policies relating to individual entities for the large-scale security. Third, the policies are time-variant, so the existing management policy specifications such as Lucent's policy definition language [15] are difficult to capture the dynamic requirements. For example, when the emergence happens it is difficult to update the administration policies timely. To support the effective security management, it's difficult to solve these problems in one solution under the current Internet architecture. Some recent appeared new network architectures aim to enhance the security at the beginning of design to avoid these security threats. In this paper we investigate these existing new network architecture projects and focus on analysing their security mechanisms, and then we propose a new security management scheme based on the Universal Identifier Network (UIN) [8, 22], which can provide the following functions. (1) Support the user and service classification to provide the label-based fine granularity security management; (2) Support the dynamic policy update by capturing the dynamic characters of the users and services; (3) Provide the detailed network defence according to the dynamic network management requirements. The organization of this paper is shown as follows. Section 2 gives the overview of related work. Section 3 describes the architecture of our security management system. Section 4 presents the implementation of our solution in detail. Section 5 introduces the related evaluation metrics. Finally, section 6 concludes this paper.

2 Related work

The current network security technologies such as Firewalls, IDS, VPN, Access control, anti-virus, and data encryption, which can easily prevent the known attacks or malicious behaviours. However, they cannot solve the problems from the root, especially when the attacks become more distributed and more sophisticated with high evolvement ability [5]. Besides, the current security management is mostly coarse-grained which cannot provide the delicacy management.

To realize the fine-grained security management, the policy-based management maybe a better choice [11] which can protect the sensitive information especially in the emerging satiation. The policy-based management is original designed to simplify the management of the large scale system [21], but now it can be used for the multiple domains [13, 20, 4, 19]. The current Internet has involved many different organizations including the network providers, service providers, and various social departments which make the network too complicated to realize the effective security management for all participants. Meanwhile, considering the dynamic feature of the network users and services, the security management policies will change with time, which requires the security management should be operated in a timely manner and provide the fine-grained operations to prevent the impacts on other users and services. However, under the current network architecture, it is hard to satisfy these requirements. Luckily, the security issue has been attracted the attention from the future network architecture designs, and even some projects are launched with objective to solve these problems. For example, NSF has launched the Future Internet Architecture (FIA) program [18], which has supported five projects including the NDN, MobilityFirst, NEBULA, XIA and ChoiceNet.

Among these projects, eXpressive Internet Architecture (XIA) project focuses on security to support the trustworthy, long-term evolution of usage models, long term technology evolution, and allows all participants to operate effectively. XIA is designed to provide the intrinsic security by introducing the self-certifying identifiers for all principals, without depending on external configurations, actions, or databases to support current host-to-host communication, content retrieval and accessing services security, therefore the malicious actions can be easily identified. To do so, XIA depends on the underlying architecture with the well-foundedness (Identifiers, associations match user's intent), fault isolation (reduce the dependencies), fine-grain control (allow users to specify their intent) and explicit chain of trust (allow users to understand the basis for trust) design principles, and adopts three security-relevant mechanisms: (1) multiple principal types including Hosts XIDs support host-based communication like IP, and service XIDs (identify what the service does and who provides it) route to services and content XIDs (identify what the content is) specify specific chunks of content. (2) Intrinsically secure identifiers without dependence on the external configuration, to insure the security properties once you know the ID. (3) Flexible trust management, name resolution from name to secure XID to support source of trust such as CAs, DNSSSEC-like mechanisms, PGP model, physical interaction. More specifically, it adopts the Accountable Internet Protocol (AIP) [3], in which all hosts are named by their public key, and therefore the cryptographic security are easy to deploy once they know other hosts names. The core is to support the communication between various types of principals which are content, host and service.

Similar to the XIA, the main idea of NDN security is to secure the content by built-in security mechanism, but the difference is that NDN does not provide the security channel such as SSL or VPN. In NDN, it requires the authentication on all contents, and it provides a basic security building block by signing all named data. Therefore, it can provides the data integrity and origin authentication and further to support trust. However, to realize this objective, it has to support the cost-effective fine-grained signature operations, and functional and usable trust management infrastructure. Besides, NDN only provides to validate content and its provenance, which cannot prevent the malicious or unwanted content such as spam from a legitimate signature [23]. More recently, there are some researches focusing on the Interest Flooding Attacks [2] and Content pollution attacks [10]. However, it still lacks of an effective security management to distinguish the different users.

Although MobilityFirst [16] is a mobility-centric network architecture based on the global name resolution and store forwarding, it still emphasizes on the strong security and privacy services such as authentication, confidentiality, non-repudiation built into the architecture to resist to common IP network attacks. In practice, it considers the public keys to ensuring accountability, access control, provide the secure routing and prevent the address hijacking. Currently, it proposed to secure the name resolution service [14] to provide the powerful authentication and security.

NEBULA focuses on the highly-available and extensible core network interconnecting data centers, and pays more attentions on the privacy-enhanced communication by keeping secret content, and it tries to develop new techniques that can apply accountability to primitives provided directly by the network, and also combine the accountability with confidentiality.

Form the above analysis, the security in new network architectures is trying to provide the security path and ensure the security of the content from the architecture design. However, to support the fine-grained security management, it still lacks effective systematic security management solution. While in this paper, we combining the policy-based management and the core idea of new network security design, and propose a label-based security management under the new network architecture to provide the fine-grained dynamic adaptability security management.

3 Security management architecture of Universal Identifier Network

Based on the above analysis, we propose a label-based security management under the universal network architecture, in which both users and services are marked with the labels that are the combination of the multi-dimensional properties. These labels consist of the static information and dynamic information which can be updated according to the behaviours. The security policies are based on the labels to map the different security management requirements. To support the fine-grained management, our design depends on the new network architecture, users and services classification, and the effective policy implementation.

3.1 New network architecture

UIN is a novel network architecture, which integrates the traditional network architecture model into two lays that are network layer and service layer. The network layer completes the underlying data transmission, which is responsible for the network accessing and interconnection. The service layer implements the applications of service and business.

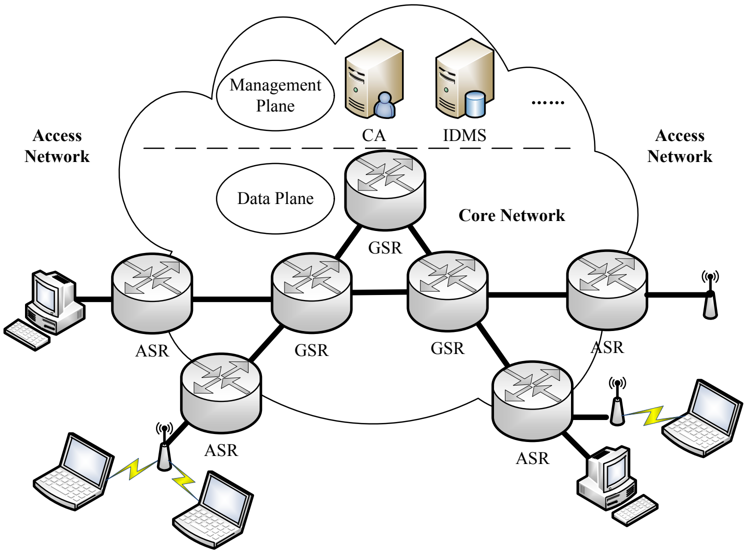


Figure 1: The basic components of universal identifier network

The network layer is divides into access network and backbone network as shown in Figure 1. The access network includes different devices and Access Switching Routers (ASRs). When a user accesses to the network, the ASR is responsible for maintaining the user's access and assigning a globally unique Access Identifier (AID) to the user. In the access network, both of the source and destination for the data packet are using AID, while the Routing Identifier (RID) is used in the backbone network. The mapping of AID and RID is based on the theory of the separation and aggregation of AID and RID. The backbone network solves the location management and routing technology, which consists of the General Switch Router (GSR) and various functional servers, such as user authentication center (Responsible for the system user access authentication and management), service authentication center (Responsible for the registration management of network service), Identifiers Mapper Server (IDMS) (Responsible for maintaining and managing the mapping rules) and so on. When the RID arrives at the correspondent node, it will be replaced to the original AID. And then the whole communication process is completed. From the above process, it can be observed that in the universal identifier network, the user's identity information is denoted by AID and the address information is denoted by RID. The separation of the two kinds of information can avoid the problem that IP represents both identity and address information in traditional network. When a user accesses and executes the authentication, it needs to provide the valid identity and fill in the necessary network information. The user can access the network only after the successful certification through the authentication center. The AID based authentication mechanism provides the guarantees for the integrity and reliability. The transform scheme of AID and RID separates the user terminal from the backbone network. Even if the information is intercepted or monitored during the transmission, the information cannot be traced back to its source and destination, which further safeguards the user's privacy and the security of the network.

3.2 Security management model analysis

Based on the above universal network architecture, any host attached to the network will generate information including the users' basic information, service information and their behaviors information, as shown in Figure 2.

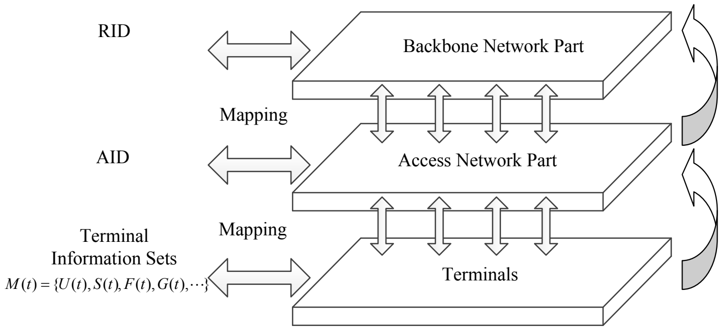


Figure 2: The basic information model in our design

All these information can be expressed as

$$M(t) = \{U(t), S(t), F(t), G(t), ...\} \tag{1}$$

Where $M(t)$ is the set of all information, and $U(t)$, $S(t)$, $F(t)$, $G(t)$ represent the sets of users, services, user properties and service properties, respectively. Here, we introduce the t to describe their dynamic characters.

At the given time t, the user and service can be express as the set of the various users and huge services as follows.

$$U(t) = \{u_1, u_2, u_3, ..., u_i, ..., u_{N_U}\}, \quad (i \leq N_U) \tag{2}$$

$$S(t) = \{s_1, s_2, s_3, ..., s_i, ..., s_{N_S}\}, \quad (i \leq N_S) \tag{3}$$

Where u_i and s_i represent the different users and services in the network, N_U and N_S are the number of users and services, respectively.

As for each user or service, they have separated properties. For a given user u_j , these various properties can be expressed as

$$F^{u_j}(t) = \{f_1^{u_j}, f_2^{u_j}, ..., f_p^{u_j}\} \tag{4}$$

Similar, for a given service s_k, its properties can also be expressed as

$$G^{s_k}(t) = \{g_1^{s_k}, g_2^{s_k}, ..., g_q^{s_k}\} \tag{5}$$

Based on these properties, we can uses the functions $\alpha_{u_j}(\bullet)$ and $\beta_{s_k}(\bullet)$ to generate their labels L_{U_j} and L_{s_k} can be expressed as

$$L_{U_j} = \alpha_{u_j}(F^{u_j}(t)) \tag{6}$$

$$L_{S_k} = \beta_{s_k}(G^{S_k}(t)) \tag{7}$$

These labels are dynamic and multi-dimensional which can be easily classified into different groups for the security management.

Assuming that $P = \{p_1, p_2, ..., p_i\}$ is the set of policies, which each policy is expressed as following.

$$p_i = \{L_{U_i}, L_{S_i}, A_i, W_i\} \tag{8}$$

Where L_{U_i} and L_{S_i} denote the label of the given user i and the given service i. A_i represents the related operations which can be discard, redirection and so on. And the W_i represents the priority of this policy p_i.

Based on the universal network, the policy implementation is based on the identification/location separation mechanism, by controlling the mapping between AID and RID to perform the security management.

Under the universal network architecture, once the user acquires its user label $\alpha_{u_j}(F^{u_j}(t))$ and service label $\beta_{s_k}(G^{S_k}(t))$, we can perform the policy management in IDMS to control the mapping between AID and RID.

$$R_{AC} = (\alpha_{u_j}(F^{u_j}(t)), \beta_{s_k}(G^{S_k}(t))) \oplus P \tag{9}$$

Where R_{AC} is the security management result, and the $\oplus$ presents the policy match operation. After acquiring the matching results, we can use it to control the mapping between user's AID and RID to support the security management.

3.3 Label generation design

To realize the policy-based security management, the label generation is the foundation. To improve its effectiveness, we should specify the security policies relating to the groups. Therefore, the user and service should be classified at first in spite of the fine-grained user classification and service classification is still lack. Besides, abstracting the policies from the various conditions and then take them into the policies implementable under the given security management should consider the dynamic of users and service, therefore the label should also update to capture these dynamics behaviors of users and services.

3.3.1 User label generation

The Internet users have experienced an explosive growth during the past decade, as an important role of network, its classification and behaviors analysis become an active research hot spot recently due to its important impact in terms of network management, recommendation service, target AD. User classification is a kind of user model to define the users group with similar properties and behaviors, which may involve the man-machine interaction, machine learning, and data mining.

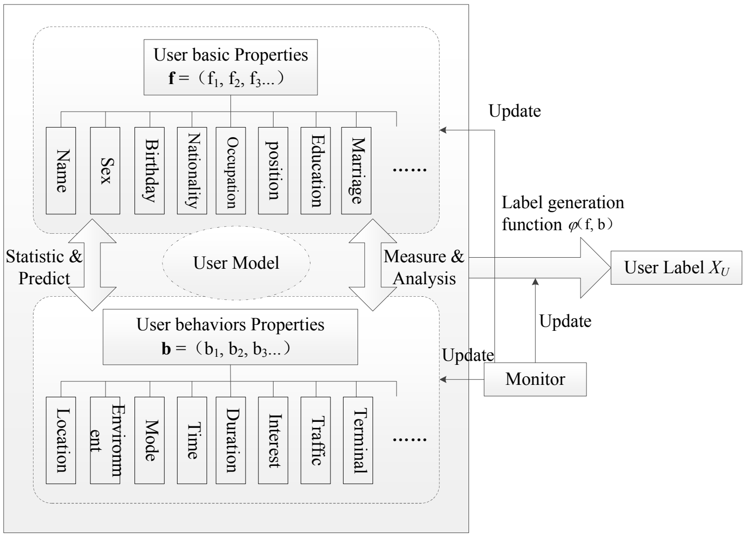


Figure 3: User label generation and update procedure

User label is based on the user's properties, and Figure 3 shows the user label generation process. In our design, we model the user from both user basic properties and user behaviours properties to comprehensively describe user's properties. The basic properties are general the relatively static information and invariant with time once user accessed to network, which is similar to the population register consisting of the name, gender, profession, birthplace, education, etc. These information are required when user firstly apply the network accessing service. After the authentication of the network ISP, the information will be stored as the basic properties. In the universal network, all users wanted to acquire the network services have to register their static information in the CA server. Beside the static information, the dynamic information is abstracted from the user behaviours which are multidimensional, dynamic and more complicated than basic information and also hard to capture. In our design, we combine the ASR and CA to capture the network access time, access model, traffic, interests and so on, and then perform the user behaviours analysis to generate the users' dynamic information such as the kinds of network services, the Internet period and so on. By extracting the information from the user basic and behaviour properties, we generate the user label to represent the user's classification. Considering that the user properties may change with the time, we design a feedback mechanism by capturing the changes to update the user label.

3.3.2 Service label generation

To generate the service label and provide the group-based policy, we have to classify the services at first. Due to the rapidly booming of various Internet services, the service classification becomes more diversity and more difficult, and it still lacks of a general accepted classification method. While the current network management adopt the coarse-grained classification such as SLA or service port to distinguish the network service which cannot support the fine-grained management especially for some emergence situations. Current the service classification is mainly focusing on the Web services with the objective to enable the automatic service organization and service discovery [6]. The existed automatic classification of web service can be divided into heuristic and no-heuristic methods. While in terms of service discovery and selection, service composition and service replacement, the service descriptions such as WSDL, WADL, WSMO play a crucial role, but these service descriptions from the service providers are poor. As a result, some human-generated automatically-extracted annotations are proposed which can be group into four categories , namely the semantic approaches, information retrieval approaches, data mining approaches and linking approaches. However, the methods cannot present the dynamic character of the services. Therefore, the dynamic tag generator are proposed [1] to annotate the invoked web services. Even so, all of these solutions mainly focus on the web services. In fact, the Internet consists of many other services such as Email, FTP, P2P, Instant message and so on. So, there still lack of the effective service classification for all of them. In our paper, we propose to set up service registration mechanism to describe these services and enrich the descriptions via the service behaviours analysis.

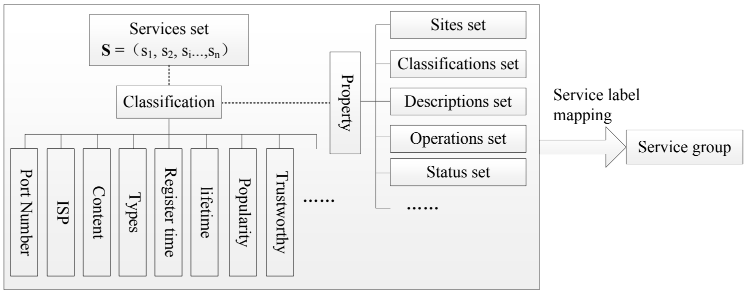


Figure 4: Service label generation and update procedure

The service label generation procedure is shown in Figure 4. In our design, we extend the service classification from traditional single-dimension to multiple dimensions by describing the service from the port, service contents, service kinds, service location and so on. Based on these descriptions, we extract the orthogonal properties to generate the service label. Similar to the user classification, we also introduce the feedback mechanism to update the service label. Based on the unified filter criteria, naming mechanism and service description, we classify the services into different groups with the purpose to support the fine-grained service management.

4 Assessment considerations

To evaluate its effectiveness, we also discuss the assessment method in this section. Perfect evaluation system is an important basis to determine the quality of a system. As shown in Table 1, the establishment of an evaluation system is based on the following principles: scientificity, comprehensiveness, operability, independence, orientation, and continuity.

Table 1: Principles of assessment

Principle	Description
Scientificity	Based on the internal elements and essential contact, complying with UIN security feature
Comprehensiveness	Consider more factors from different perspectives and levels
Operability	Less theoretical, more practically. Clear the metrics for quantitative analysis
Independence	Orthogonality
Orientation	Better service for network management
Continuity	Consider the future development

Internet is a complex giant system which contains many protocols, various services and users. It is difficult to evaluate the proposed security management system in the test-bed. Therefore, we propose an evaluation procedure as shown in Figure 5.

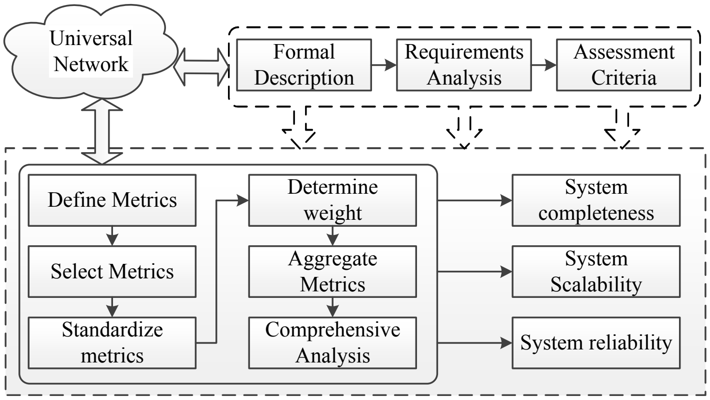


Figure 5: The evaluation procedure

Firstly, analysis the usage of the current network, and give a detailed description based on UIN. These descriptions are based on the mathematics method to insure the accuracy. And then, specific the objects for evaluation, and assign the weight factor for the comprehensive analysis, and consider the system requirements.

5 Conclusion

In this paper, we proposed a label-based security management model and evaluation methods for the future network architecture, to ensure the reliability, security to manage the various users and services. The proposed solution depends on the rich user and service description of the static information and dynamic information to group them in detail for the fine-grained security management. The further work is to implement our design in the test-bed and evaluate its performance in the real network environments.

6 Acknowledgments

This work was partially supported by the National High-Tech Research and Development Program of China (863 Program) under Grant No. 2011AA010701, in part by the National Basic Research Program of China (973 Program) under Grant No. 2013CB329102, in part by the National Natural Science Foundation of China (NSFC) under Grant No. 61232017.

References

[1] M. AbuJarour and F. Naumann. Dynamic tags for dynamic data web services. In *Proc. of the 5th International Workshop on Enhanced Web Service Technologies (WEWST'10), Ayia Napa, Cyprus*, pages 3–9. ACM, December 2010.

[2] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang. Interest flooding attack and countermeasures in named data networking. In *Proc. of the 2013 IFIP Networking Conference (IFIPNC'13), Brooklyn, New York, USA*, pages 1–9. IEEE, May 2013.

[3] D. G. Andersen, H. Balakrishnan, N. Feamster, T. Koponen, D. Moon, and S. Shenker. Accountable internet protocol (aip). In *Proc. of the 2008 ACM Special Interest Group on Data Communication (SIGCOMM'08), Seattle, Washington, USA*, pages 339–350. ACM, August 2008.

[4] A. H. Celdrán, M. G. Pérez, F. J. G. Clemente, F. Ippoliti, and G. M. Pérez. Policy-based network slicing management for future mobile communications. In *Proc. of the 2018 5th International Conference on Software Defined Systems (SDS'18), Barcelona, Spain*, pages 153–159. IEEE, April 2018.

[5] Z. Chen, F. Han, J. Cao, X. Jiang, and S. Chen. Cloud computing-based forensic analysis for collaborative network security management system. *Tsinghua Science and Technology*, 18(1):40–50, February 2013.

[6] M. Á. Corella and P. Castells. Semi-automatic semantic-based web service classification. In *Proc. of the 2006 International Conference on Business Process Management (BPM'06), Vienna, Austria*, volume 4103 of *Lecture Notes in Computer Science*, pages 459–470. Springer-Verlag, September 2006.

[7] W. Ding, Z. Yan, and R. H. Deng. A survey on future internet security architectures. *IEEE Access*, 4:4374–4393, July 2016.

[8] P. Dong, Y.-j. Qin, and H.-k. Zhang. Research on universal network supporting pervasive services. *Acta Electronica Sinica*, 35(4):599–606, April 2007.

[9] E. Ellesson, B. Moore, J. Strassner, and A. Westerinen. Policy core information model – version 1 specification. `https://tools.ietf.org/html/rfc3060`, [Online; accessed on August 19, 2018], February 2001.

[10] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang. Dos and ddos in named data networking. In *Proc. of the 22nd International Conference on Computer Communication and Networks (ICCCN'13), Nassau, Bahamas*, pages 1–7. IEEE, August 2013.

[11] W. Han, Z. Fang, L. T. Yang, G. Pan, and Z. Wu. Collaborative policy administration. *IEEE Transactions on Parallel and Distributed Systems*, 25(2):498–507, May 2013.

[12] W. Han and C. Lei. A survey on policy languages in network and security management. *Computer Networks*, 56(1):477–489, January 2012.

[13] W. Li, H. Song, and F. Zeng. Policy-based secure and trustworthy sensing for internet of things in smart cities. *IEEE Internet of Things Journal*, 5(2):716–723, June 2017.

[14] X. Liu, W. Trappe, and Y. Zhang. Secure name resolution for identifier-to-locator mappings in the global internet. In *Proc. of the 22nd International Conference on Computer Communication and Networks (ICCCN'13), Nassau, Bahamas*, pages 1–7. IEEE, July 2013.

[15] J. Lobo, R. Bhatia, and S. Naqvi. A policy description language. In *Proc. of the 1999 Artificial intelligence and the eleventh Innovative applications of artificial intelligence conference innovative applications of artificial intelligence (AAAI'99), Orlando, Florida, USA*, pages 291–298. AAAI, July 1999.

[16] MobilityFirst. Mobilityfirst future internet architecture project overview. `http://mobilityfirst.winlab.rutgers.edu/`, [Online; accessed on August 19, 2018], 2011-2017.

[17] B. Moore. Policy Core Information Model (PCIM) extensions. `https://tools.ietf.org/html/rfc3460`, [Online; accessed on August 19, 2018], January 2003.

[18] NSF. NSF future internet architecture project. `http://www.nets-fia.net/`, [Online; accessed on August 19, 2018], 2011-2015.

[19] D. Rosendo, P. T. Endo, D. Sadok, and J. Kelner. An autonomic and policy-based authorization framework for openflow networks. In *Proc. of the 13th International Conference on Network and Service Management (CNSM'17), Tokyo, Japan*, pages 1–5. IEEE, November 2017.

[20] M. Uriarte, J. Astorga, E. Jacob, M. Huarte, and M. Carnerero. Expressive policy-based access control for

resource-constrained devices. *IEEE Access*, 6:15–46, July 2017.

[21] D. C. Verma. Simplifying network administration using policy-based management. *IEEE Network*, 16(2):20–26, August 2002.

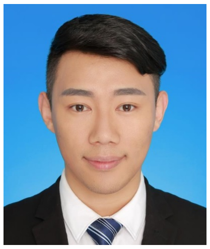
[22] H. Zhang, W. Quan, H.-C. Chao, and C. Qiao. Smart identifier network: A collaborative architecture for the future internet. *IEEE network*, 30(3):46–51, May 2016.

[23] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornton, and D. K. Smetters. Named data networking (NDN) project. http://named-data.net/publications/techreports/tr001ndn-proj/, [Online; accessed on August 19, 2018], October 2010.

Author Biography

Jianfeng Guan received his B.S. degree from Northeastern University of China in July 2004, and received the Ph.D. degree in communications and information system from the Beijing Jiaotong University in Jan. 2010. He is an associate professor in the Institute of Network Technology at Beijing University of Posts and Telecommunications (BUPT). His main research interests focus around Mobile Internet, network security and future network.

Jinsuo Jia received the Bachelor of engineering degree in network engineering in North China University of science and technology in 2017. He is currently studying for master's degree in the Institute of network technology, Beijing University of Posts and Telecommunications.His research interests include access control technology under the civil and military Internet, machine learning technology, Internet of Things security related technologies.



Mengxin Liu received a bachelor's degree in computer science and technology from Jmu University in 2016. She is currently studying for a master's degree at the Network Technology Research Institute of Beijing University of Posts and Telecommunications (BUPT). Her research interests focus on machine learning and cybersecurity related fields.