

Adaptive Security Support in Future Internet through Class of Security Level

Jong-Ho Park, Moon-Young Jung, Seung-Woo Seo
Seoul National University
{[jhpark](mailto:jhpark@cnslab.snu.ac.kr), [moon](mailto:moon@cnslab.snu.ac.kr)}@cnslab.snu.ac.kr, sseo@snu.ac.kr

1. Introduction

Future internet is one of the hottest topic in the field of network and communication. Since the current internet has been developed and used several decades, it has been improved continually accommodating various requirements of newly developed services. In spite of the improvements of the current internet, there are still many problems in the current internet, e.g. the difficulty of supporting global mobility, user-centric service and extensibility. To provide much functionality beyond current internet's limitations, new kinds of network architecture and protocols are needed. Such a network should accommodate the personal networks as well as global communication networks such as cellular networks.

For the sake of secure future internet, various security features should be considered. Security requirements like confidentiality, integrity, availability and authenticity will be needed differently according to various networks and users in order. For these requirements to be a real part of internet functionalities, users need to decide security level or quality, and networks need to provide their security capability. This raises the need to quantify the security features. The quantification of security features gives most significant contribution to secure future internet.

This paper provides 1) the concept of Class of Security Level, 2) how to quantify the security features, and 3) how to select the routing paths satisfying the security level. The remainder of this document is structured as follows: Section 2 provides the related work; Section 3 describes an overview of Class of Security Level; Section 4 provides how to quantify the security features and how to setup the routing paths; Section 5 is a conclusion.

2. Related work

Quality of Security Service(QoS) is proposed in [1], which is a similar concept to Class of Security Level. The QoS divides user's security choice into three level. When a user selects a security level, security costs are calculated according the security level, application serviced, and network modes. According to the calculated values, the user can make a connection to the application

in a peer node. In other word, the QoS is an application centric method.

3. An Overview of Class of Security Level

Class of Security Level(CSL) is to provide security services in the network layer. Class of Security Level(CSL) works as follows.

A user has CSL and it is composed of quantified security features. He can get a security service from network under his CSL. A user who wants to receive security guarantee service from network sets several security features such as confidentiality, integrity, availability, authenticity and privacy guarantee. For example, users will select AES as a confidentiality algorithm, 128bits as a confidentiality key length, SHA-1 as an integrity algorithm, 128bits as an integrity key length, no packet authentication and no privacy guarantee. These features are selected as components by user, and the selected features will be converted to quantitative level. The sum of converted levels should be smaller than the user's CSL. If the sum is larger than the user's CSL, the user has to delete selections or reduce each selection's degree.

After the user's selection is submitted to the network, network decides two things. One is whether the network itself can support user's selection, and the other is whether the user's selection can be supported through the routing paths. If the network can provide the security level above the user's selection by itself, the network judges the possible paths to the destination of the user. If such a path exists, the network accepts the user's request. If such a path does not exist, the network will notify the user nonexistence of such a path, and suggest the other possible candidate paths with less security level. In this step, the possibility of existence of candidate paths is decided by not only the user's selection and routers' functionality, but also the intermediate routers' availability such as CPU, memory and bandwidth usages.

The network can suggest the several possible paths which have different characteristics. For example, one path experiences low delay but low bandwidth. The other path may experience opposite characteristics keeping the same security level. Among the candidate paths, the user

can choose the best path for him according user policy. Or the user's application can choose the best to the destination.

4. Details of Class of Security Level

4.1 Quantification of security features

To realize the functionalities mentioned above, we will quantify the security features. The quantification contains several steps as follows.

The first step is to measure the degree of safety for embodiment of security features, i.e., security algorithms. For example, confidentiality is guaranteed by encryption and decryption. The degree of safety of confidentiality is determined by the key length, assuming the same algorithms used. One of the metrics to measure the degree of safety is the time spent to break the encrypted message without any key information. Therefore, we can say that the degree of confidentiality is determined by the key length. However, this argument is true considering the same algorithm because the degree of safety of encryption algorithm will be different according to the encryption method. We have to make criteria to evaluate the degree of safety of different algorithms and have to measure the degree of safety of algorithms following the criteria.

The second step is to measure the resources needed to implement the security algorithms. Algorithms which have the almost same degree of safety have different resource requirements. Some algorithms need more computation power, and some algorithms need more memory spaces. These resource requirements should be considered and quantified in the network supporting the security features. For example, because routers and switches forming the network handle high speed traffic, they do not have extra resources to support extra security functions. Thus, extra burden of security functions for the security feature support to the high-speed routers and switches should be considered and calculated to guarantee the operation of them. Therefore, it is required to select the specific security algorithms according to the routers and switches' current resource status. This is why we have to measure and quantify the amount of resources needed for the security algorithms.

The third step is to consider link's bandwidth. The bandwidth is not a big deal in the wired networks. However, future internet will integrate various networks such as small sensor network, Wireless LAN, WiBro, and the global cellular networks. Future internet will have many wireless links which have different bandwidths. Thus, the links' bandwidth used by security features should be regarded.

As a final step, the calculation of relative importance of security features is needed. The degree of safety of a security feature calculated in the first step is a criterion applicable only to the security feature. For example, the

criteria to evaluate the degree of safety of confidentiality cannot be applicable to that of integrity. However, the degrees of security features have to be summed up according to one criterion. Thus, the relative importance of security features has to be calculated.

4.2 Routing path setup

The network should provide not only the selected security service but also the best performing routing paths. It means that if a user selects his preferred security services within the boundary of security level, the network suggests the best routing path to the destination guaranteeing the required security services.

To perform these operations, the network needs to complete the following operations.

As the first step, the network should determine whether the network can satisfy the user's security requirements or not. For this determination, the network considers supportable security algorithms, key length and the extra resources to implement and execute the algorithms. Also, the network has to determine the delay experienced by the user when the user's traffic is inserted to the network. This step requires the network to monitor and manage the network's resources such as routers, switches and other network devices.

As the second step, the network should be able to transfer the network's status to the other networks. The network status contains the availability of security algorithms and the resources like computation power and memory in the routers and switches. This means that each network has to be able to grasp the status of other networks.

5. Conclusion

This paper provides and explains the concept of Class of Security Level, the sketch of quantification, and routing path setup requirements.

As a next step, more data and measurements for the quantification of security features should be performed. Also, routing path setup and routing protocol supporting Class of Security Level should be studied.

Reference

- [1] C. E. Irvine and T. Levin, "Quality of Security Service", in *Proc. of New Security Paradigms Workshop 2000*, Cork, Ireland, September 2000.
- [2] C. E. Irvine and T. Levin, "Toward a taxonomy and costing method for security services", in *Proc. of 15th Annual Computer Security Applications Conference*, December 2000, pp 183-188.
- [3] D. L. Brinkley and R. R. Schell, *Concept and Terminology for Computer Security*, in *Information Security : An Integrated Collection of Essays*, Abrams, Jajodia and Podell, IEEE Computer Society Press, Los Alamitos, CA, 1995.