An ISO/IEC15408-Based Security Design for Active Networks

4G－4

Chih-Chang Hsu, Terumasa Aoki, Hiroshi Yasuda
Research Center for Advanced Science and Technology
The University of Tokyo

1. Introduction

Although almost all of the researchers in Active Networks field recognize that the security concern is one of the most significant issues in the designing of AN, there is little research related to the security concern. Most of the current Active Networks researches focus on the issues concerning the support of flexible, dynamically changing, various applications and fine-granted quality of service.

Security is indispensable to the success of Active Networks. The paper discusses the design concepts of the components of a secure AN node by using ISO/IEC15408 (Common Criteria), which is useful as a guide for the development of products and systems with IT security functions.

2. Background

2.1 Active Networks (AN)

Active Networks is a new generation network architecture, which intends to solve those problems existed in the current passive network, such as (1) Difficulty in integrating new technologies and accommodating new services, (2) Poor performance due to redundant operations at several protocol layers, (3) Difficulty in supporting new applications which sometimes need to perform computation [1]. The expected goals of AN include: (1) Quantifiable improvement in network services. (2) Audio/video synchronization and full rate video over multicast. (3) Fewer retransmitted packets. (4) Fault tolerance mechanisms. (5) Multi-tiered mobile security [2].

2.2 ISO/IEC15408 (Common Criteria)

The purpose of the ISO/IEC15408 evaluation was to provide assurance for the effectiveness of the Target of Evaluation (TOE), which is presented here as a node of AN system, in meeting their Security Targets (ST) by following the design guideline of ISO/IEC15408 [4]. *(Figure 1.)*

By clearly defining the possible threats, security policies and assumption before we implement a new framework, we know how we can set the objectives for the security functions of a framework detailedly.

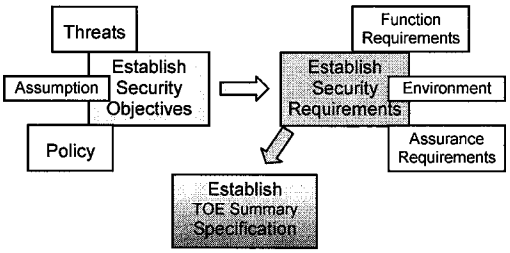

Figure 1. *The design guideline of ISO/IEC15408*

And then, we can implement the necessary security requirements according to those security objectives, which we have established, by considering its function requirements, assurance requirements, and the environment factors. At the final, we can complete a TOE summary specification, which would be included in ST, that provides a high-level definition of the security functions claimed to meet both the requirements in functions and assurances.

3. Active Networks Security Design

3.1 Threads Model

In our approach, first, we started in identifying what kinds of threats and where types of attacks are possible incorporated in AN. According to the latest architecture released by AN Security WG, specific

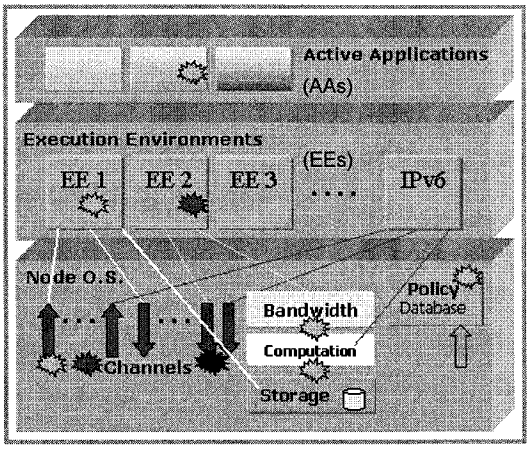

Figure 2. *Possible threats of Active Networks*

security components of AN are needed in order to counter the attacks that are possible incorporated in AN, such as unauthorized disclosure, deception, disruption, and usurpation (i.e. misuse by tampering, theft of services) [3]. *(Figure 2.)*

3.2 Security Objectives and Requirements

Second, we stated the security objectives that counter the identified threads and address the identified security policies (*Table 1&2*).

Threat	Objective
T.Denial of Service	O.Resource_Isolation
T.Masquerade	O.Encrypted_Channel
	⋮
	O.Trusted_Path
	O.User_Authentication
T.Replay	O.Access_Control
	⋮
	O.Encrypted_Services
	O.Encrypted_Channel
T. UnAuthorizied_Access	A.Physical (*Assumption)
	O.Access_Control
	O.Discretionary_Access
	⋮
	O.Self_Protection
⋮	

Table 1. *Objectives derived from threads*

Policy	Objective
P.Resource_Lebels	O.Marking
	⋮
P.Authorizied_Users	O.User_Authentication
	O.User_Identification
P.Authorization	O.Access_Control
	⋮
	O.User_Identification
⋮	

Table 2. *Objectives derived from policies.*

Third, we defined the security requirements for TOE (i.e., AN), which will ensure that the TOE will meet its security objectives. We think that the following specific security features required for AN should be included: identification & authentication, integrity assurance discretionary access control, cryptographic services, and auditing system (*Table 3*).

Fourth, we discussed about the rational between the security objectives and the function & assurance requirements. The rational presents the evidence that a conformant AN would provide an effective set of its security countermeasures within the security environment (*Table 4*).

Function / Assurance Requirement	Acronym
Function of Identification and Authentication	FIA
Function of Cryptographic Support	FCS
⋮	⋮
Assurance of Develpoment_Documents	ADV
Assurance of Vulnerability Assessment	AVA

Table 3. *Definitions of Function & Assurance Requirements.*

Objectives from Threats/Policies	Requirements Meeting Objectives
O.Encrypted_Channel	FCS_COP.1, FPT_ITT.1
	⋮
O.User_Authentication	FIA_SOS.1, FIA_UAU.1
	FMT_MOF.1, FMT_MSA.2
	⋮
	ADV_FSP.2, ADV_HLD.2
	ADV_LLD.1, ADV_SPM.1

Table 4. *Rational between Objectives and Requirements.*

4. Conclusions

We have presented here our approach that tries to combine the well-known IT security standard and AN. One of our future works is to implement a set of reference Protection Profiles (PPs) for the related components of AN. The PPs mentioned above can then be applied to the frameworks of other AN researchers, who may be encouraged to establish the related STs for their specific frameworks and have those frameworks evaluated under ISO/IEC15408.

We believe that unless suitable requirements are established at the beginning of the development process, the resulting product, however it is well designed, may not meet the objectives of its anticipated customers.

The approach we proposed here, a security design concept for AN, based on ISO/IEC15408, can provide a fundamental base in the direction of designing a flexible and comprehensive AN, which integrates various security mechanisms and services.

References

[1] Kounstantinos Psounis, Active Networks: Applications, Security, Safety, and Architecture. IEEE Communications Surveys. 1st Q 1999

[2] http://www.arpa.mil/ito/research/anets Darpa ITO Active Networks.

[3] AN Security WG, Security Architecture for Active Nets. May 2001.

[4] International Standard ISO/IEC15408 Part1~Part3 Dec.1999