QoSS의 연구 동향과 적용

함우석*, 김종승*, 이송원*, 박재혁*, 최수길*, 김광조*, 김숙연**, 남택용**

*한국정보통신대학원대학교(ICU), 국제정보보호기술연구소(IRIS),

**한국전자통신연구원(ETRI), 정보보호연구본부

Research Trend of QoSS and Its Application

Wooseok Ham*, Jongseong Kim*, Songwon Lee*, Jaehyrk Park*, Soogil Choi*, Kwangjo Kim*, Sookyeon Kim** and Taekyong Nam**

*International Research center for Information Security(IRIS), ICU

**Information Security Research Division, ETRI

요 약

QoSS(Quality of Security Service)는 보안을 단순한 성능 장애 요소의 관점에서 벗어나 QoS(Quality of Service)의 관점에서 효율적인 네트워크 관리 도구로서 사용하기 위해 등장한 개념이다. QoSS는 보안 서비스들이 적용되는 상황에 따라, 또는 사용자의 요구사항에 따라 다양한 수준으로 제공 가능하다는 가변 보안의 개념에 기초하고 있다. 이를 통해 사용자에게는 제공되는 서비스들에 대한 만족도를 향상시키고, 서비스 제공자 측면에서는 자원의 가용성을 향상시키는 효과를 달성 할 수 있다. 본 논문에서는 이러한 QoSS의 전반적인 구성 요소들을 간략히 소개하고, 차세대 네트워크 보안 서비스의 구축 시 QoSS의 적용 절차와 적용 시 고려해야 할 사항에 대해서 제안한다.

I. 서론

1997년 미국의 DARPA Quorum에서는 전세계적으로 광범위하게 배치되어 있는 육, 해, 공의 다양한 형태의 군사력을 효율적으로 통제하고, 전쟁 발생 시 동적으로 신속하게 대처하기 위한 효율적인 자원관리시스템(RMS, Resource Management System)을 구축하기 위한 다양한 프로젝트들을 진행하였다. QoSS(Quality of Security Service) [1]는 그러한 프로젝트들 중의 하나였던 MSHN(Management System for Heterogeneous Networks) [5]에서 파생되었다. MSHN의 연구를 주도했던 C.Irvine과 T.Levin은 가변 보안(Variant Security)을 이용해 네트워크를 효율적으로 관리할 수 있음을 인식하고, 이를 통해 차등적으로 나타나는 보안서비스의 품질을 QoSS라 명명한 후, 기대 효과 및 구성요소, 사용자 인터페이스, 실제 시스템에서의 프로토타입 구현 등에 대한 연구를 지속적으로 진행해 오고 있다.

보안을 QoS(Quality of Service)의 관점에서 바라보는 시도는 QoSS가 등장하기 이전에도 연구되어져 왔으나, 패킷 인증과 같은 특정 서비스에 한정된 관점으로만 제안되었으며, 전체적인 보안 서비스의 일반적인 관점에서는 제시되지 못하였다.

본 논문은 이러한 QoSS의 정의와 구성요소 들을 간단하게 소개하고, 차세대 네트워크 보안 서비스 [7]와 같은 대규모 시스템에서 QoSS를 보장하기 위한 적용 절차와 적용 시 고려해야 할 사항들을 제안하고 향후 과제를 제시한다.[1)]

1) 본 논문은 ETRI의 '차세대 능동형 네트워크 정보보호 시스템 개발' 사업의 위탁 과제의 결과이다.

II. QoSS (Quality of Security Service)

1. 정의 및 기대효과

QoSS는 제공되는 보안 서비스를 미리 정의된 기준으로 평가하여 나타나는 보안 서비스의 품질을 말한다. 이는 보안이 성능의 저하를 가져온다는 이분법적인 관점에서 벗어나 보안을 QoS(Quality of Service)의 한 구성요소로 고려하는 새로운 개념이다. 이러한 QoSS의 제공을 통해 다음과 같은 기대효과들을 얻을 수 있다.

○ 개별 사용자의 상이한 보안 요구사항에 부합되는 다양한 등급의 보안 서비스 제공 가능

○ 보안을 통해 효율적인 자원의 스케쥴링으로 장비의 효율성 증가

○ 상황에 따른 선택으로 사용자의 서비스 사용 비용 감소

○ 기존 QoS가 제공할 수 있는 가용성, 예측 가능성, 효율성을 더욱 향상시키고, 더불어 보안성을 제공

2. 가변 보안(Variant Security)

가변 보안 [6]의 존재는 QoSS를 적용하기 위한 핵심 개념이다. 각 보안 서비스에 존재하는 가변적인 요소를 분석하여 등급화를 시킨 후 사용자에게 제공함으로써, 사용자는 자신에게 가장 적합한 보안 서비스 사양을 결정하여 사용하게 된다. 실제로 가변 보안은 아래 예제와 같은 다양한 부분에서 존재한다.

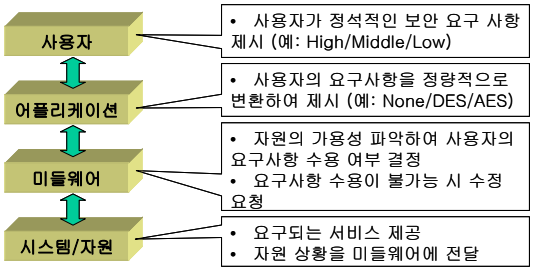
○ 기업 내에서 회사의 출입을 위해서는 IC 카드와 같은 간단한 인증 방법을 사용하면 충분하지만, 중요한 정보를 열람하기 위한 장소로 접근하기 위해서는 생체인식과 같은 별도의 고수준의 인증을 필요로 함

○ 전달되는 문서들의 기밀성 또는 무결성 수준을 통제하기 위해 사용 암호 방법(DES, AES, RSA)이나 키 길이(512, 1024 비트)나 전자 서명과 같은 방법으로 무결성을 검증

○ 네트워크가 폭주하는 시간대에는 성능 유지를 위해 침입 탐지 시스템의 탐지 수준을 완화하고, 상대적으로 여유 시간에 집중 탐지

○ 기업 내부에서의 데이터 전달은 낮은 보안으로도 충분하지만, 외부로의 기밀 데이터 전송 시에는 강력한 보안 기능이 필요로 하는 등 상황에 따라 보안의 강도를 달리 적용

이러한 가변 보안을 바탕으로 하여 사용자의 요구사항은 사용자에서 사용하고자하는 시스템과 자원까지 [그림 1]과 같은 순서를 따라 적용하여 요구사항에 부합되는 서비스를 제공받게 된다.



[그림 1] 가변 보안 모델

3. 보안 벡터(Vector)

사용자의 보안 요구사항들은 QoSS에서 보안 벡터 [3]로 표시한다. 일반적으로 기업이나 조직과 같은 경우에는 보안 요구사항들은 보안 정책으로 표시된다. 즉, 각각의 보안 정책이 개별적인 보안 벡터에 대응된다. 사용자의 등급에 따라 또는 상황에 따라 제공받는 보안 벡터의 내용들은 상이할 수 있다. 보안 벡터의 각각의 요소들은 가용한 한계(limit) 범위를 가지는 보안 메커니즘들에 의해서 구현되며, 사용자는 자신이 가질 수 있는 한계 범위 내에서 제공 받고자 하는 보안 수준을 선택할 수 있다. 이러한 한계 범위는 일반적으로 수치적으로 나타나기도 하지만, 아래 보안 벡터의 예제처럼 선택(S.2)이나 일반 정책(S.3)의 형태로도 나타날 수 있다.

○ S.1: 기밀성을 위한 키 길이, $56 \le k \le 256$, 64 비트씩 증가

○ S.2: 가능한 인증헤더 형태 {HMAC-MD5, HMAC-SHA}

○ S.3: 도메인 A에서 B로의 패킷 이동은 반드시 암호화되어야 함

4. 사용자 요구사항과 메커니즘 할당 [2,4]

위에서 언급된 보안 벡터들의 선택 범위들은 결국 사용자가 요구하는 보안 서비스를 제공하기 위해 사용 가능한 메커니즘에 의존적이다. 이러한 메커니즘들은 실제 구현되어 운영 중에 있고, 성능이 검증된 메커니즘들을 사용할 때 효과적이다.

사용자의 선택적인 보안 요구사항을 실제 메커니즘으로 할당하기 위해서는 각각의 사용자 선택에 따른 메커니즘의 할당표를 작성하여야 한다. 이렇게 작성된 할당 표는 보안정책 서버나 RMS 내부 관리 테이블로 보관되어 사용자가 요청 시 해당 메커니즘을 수행하게 된다. 아래 <표 1>은 보안 서비스와 사용자의 선택 범위에 따른 메커니즘 할당 예제를 보여준다.

<표 1> 사용자 선택과 메커니즘 할당 예 [4]

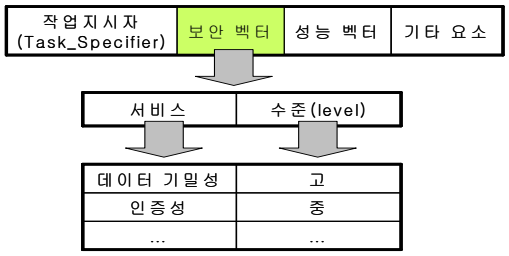
		사용자 보안 선택 범위		
보안 서비스	네트워크모드	Low	Medium	High
데이터 기밀성	Normal	None	OS 접근제어	B3 DAC
	Impacted	None	OS 접근제어	OS 접근제어
	Emergency	OS 접근제어	B3 DAC	B3 DAC
데이터 무결성	Normal	None	DES 56	DES 128
	Impacted	None	None	DES 56
	Emergency	DES 56	DES 56	DES 128
로그인인증기능	Normal	None	B1 I&A	공개키인증서
	Impacted	None	B1 I&A	B1-I&A
	Emergency	OS I&A	B1 I&A	공개키인증서

(I&A : Identification & Authentication B1,B3: TCSEC의 평가 레벨)

위의 표에서처럼 동일한 보안 서비스를 제공하기 위해 다양한 알고리즘 및 메커니즘이 사용될 수 있기 때문에, 보안 서비스 제공자는 자체적인 등급별 분류 방법에 따라 해당 메커니즘들의 수준을 분류하여 제공하여야 한다. 표에서 네트워크 모드란 사용자의 상황 변수로 볼 수 있다. 일반적인 경우(normal), 보안 보다는 시스템의 효율성을 요구하는 경우(impacted), 특수한 메시지 전달이나 특수 상황(emergency)의 경우에 따라 서비스 등급별로 상이한 메커니즘의 적용이 달라질 수 있음을 보여주고 있다.

5. QoSS 요청

사용자의 QoSS의 요청은 QoS의 일반적인 요청문에 보안 벡터를 추가하면서 이루어질 수 있다. [그림 2]는 QoS에 보안 벡터를 추가하고, 보안 벡터의 세부 내용들을 보여주고 있다.

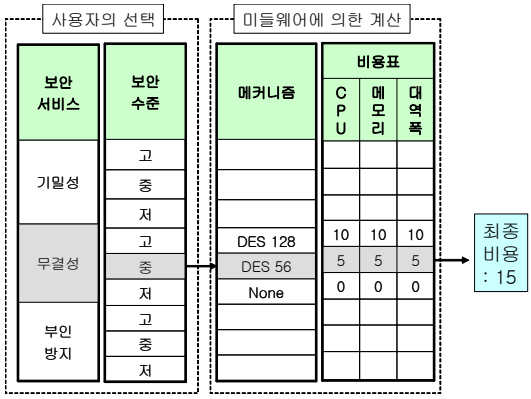


[그림 2] 보안 벡터의 추가

보안 벡터의 내용에는 보안 서비스와 서비스 수준 이외에 다른 요소를 추가하는 것도 가능하다. 이러한 요청이 자원 할당을 담당하는 RMS나 미들웨어 또는 능동형 라우터로 전달되어 서비스의 수용/거부를 결정하게 된다.

6. 비용 [6]

일반적으로 고수준의 보안이 우수하다는 것을 인식하면서도 이를 사용하지 않은 이유는 비용의 차이에서 비롯된다. 보안의 수준이 높아질수록 사용되게 되는 CPU, 메모리, 네트워크 대역폭 등과 같은 자원의 사용량이 증가하기 때문에 사용자가 부담해야 하는 비용도 비례하여 증가하게 된다. QoSS는 사용자 요구사항의 다양성에 부합하도록 시스템이 제공하는 보안 서비스의 다양성을 필요로 하게 되므로, 각각의 상대적인 비용에 따른 정량화가 필요로 한다. 그러나, 자원 비용을 계산하기 효과적인 비용함수에 대한 명확한 모델이 존재하지 않기 때문에 상황에 맞는 비용 함수를 도출하여야 한다. 사용자의 선택과 비용 함수까지의 과정을 도식화해보면 [그림 3]과 같다.



[그림 3] 요구사항에 따른 비용 계산 흐름

IV. QoSS의 적용

최근 연구중인 차세대 네트워크 보안 서비스 [7]는 요구사항 중의 하나로 사용자의 요구 사항에 부합하는 동적인 보안 서비스를 제공하는 것을 목표로 하고 있다. 이는 결국 QoSS를 보장하는 것과 동일하다고 볼 수 있다. 아래에서는 이러한 QoSS를 보장하기 위한 접근법과 고려사항에 대해서 살펴본다.

1. QoSS 보장을 위한 접근법

효과적인 QoSS를 보장하기 위해서는 보안 서비스를 위한 네트워크와 보안 장비를 구축 시 QoSS를 고려하여 설계 및 구축이 이루어질 때 가장 효과적이라 할 수 있다. 일반적으로 보안 서비스의 제공은 보안 서비스 제공자가 다양한 선택사항들을 제시하고, 고객은 자신이 원하는 서비스를 선택하는 형태를 가지고 있다. 이러한 경우에 다음과 같은 순서에 따라 QoSS 적용 구조를 구축하는 것이 권장된다.

가) 제공할 보안 서비스의 정의

나) 보안 서비스 지원을 위한 메커니즘 결정

다) 나)의 메커니즘을 지원할 보안 시스템(H/W, S/W 등) 결정

라) 도입될 보안 시스템의 기능 추가 분석 및 가변 요소 확인

마) 사용자의 서비스 등급(limit) 확정 및 선택 범위(choice) 결정

바) 사용자 인터페이스 개발 및 보안 시스템과 통합

사) 보안 서비스 제공

위와 같은 적용 방법에서의 하나의 문제점은 실제 제공하고자 하는 서비스와 메커니즘을 명확하게 지원하는 검증된 장비나 어플리케이션이 존재하지 않을 수 있다는 것이다. 따라서, 현재 존재하는 보안 장비나 어플리케이션을 바탕으로 보안 서비스를 제공하고자 하는 경우에는 보안 서비스를 정의하고, 정의된 서비스를 지원 가능한 장비 및 어플리케이션을 도입 또는 결정한 후, 이들의 가용한 메커니즘들에 따라서, 서비스 등급을 결정하여야 할 것이다.

2. QoSS 적용 시 고려사항

위에서 제시된 QoSS 제공을 위한 구축 절차 이외에도 효과성을 높이기 위해서는 다음과 같은 사항들을 고려하여야 한다.

○ 고객에게 제공할 보안 서비스 등급의 정도

○ 메커니즘들의 등급별 분류 방안

○ 서비스를 제공받는 고객(기업 또는 개인)의 개별 보안 요구사항

○ 고객 요구사항의 수용/거부 결정 방법

○ 과금을 위한 비용(cost) 함수의 도출 및 비용 계산

○ QoSS의 평가 방법

이 밖에도 효율적인 QoSS를 보장하기 위해서는 제공되는 보안 네트워크가 새로운 기능 추가나 운영 규칙의 신속한 변경 등 다양한 상황 변화에 대처할 수 있는 적응성(adaptability)를 가지고 있어야 한다.

V. 결론

본 논문에서는 QoSS 개념에 대한 소개와 구성 요소들을 간단하게 살펴보았다. QoSS를 보장하는 것은 고객의 보안 요구 사항에 부합하여 서비스에 대한 만족도를 높이고, 서비스 제공자는 자원의 효율성을 높일 수 있다는 장점을 가질 수 있다. 그러나 이러한 QoSS를 효율적으로 제공하기 위해서는 제공하는 메커니즘들의 등급별 분류나 또는 사용자의 선택에 따른 가변의 범위, 과금을 위한 비용 계산 방법 등은 다양한 방법이 존재할 수 있어, 서비스 제공자에 가장 적절한 모델을 만들어 내야 한다. 아울러, 새로운 보안 시스템의 구축에 있어서 QoSS를 제공하기 위한 논리적, 구조적 모델을 적용하여 시스템 설계에 반영하는 것은 향후 과제 중 하나이다.

참고문헌

[1] C.Irvine and T.Levin, *"Quality of Security Service"*, Proc. of the New Security Paradigms Workshop, Cork, Ireland, Sep. 2000.

[2] C.Irvine and T.Levin, *"Toward a Taxonomy and Costing Method for Security Services"*, ACSAC '99, pp.183-188, 1999.

[3] C.Irvien and T.Levin, *"Toward Quality of Security Service in a Resouce Management System Benefit Fucntion"*, HCW '00, pp.133-139, 2000.

[4] C.Irvine, T.Levin, E.Sypropoulou and B.Allen, *"Security as a Dimenstion of Quality of Service in Active Service Environments"*, Proc. of the International Workshop on Active Middleware Services, pp.87-93, 2001.

[5] MSHN, ,Available at http://cisr.nps.navy.mil/mshn.

[6] E.Sypropoulou, T.Levin and C.Irvine, *"Calculating Costs for Quality of Security Service"*, ACSAC '00, pp.334-343, 2000.

[7] S.Kim, J.Jee, T.Nam, S.Sohn and C.Park, *"Framework of Network Security Service for Next Generation"*, WISA '02, pp.123-130, 2002.