컴퓨터 네트워크의 보안 품질

신장균, 박병호[0], 유진철
육군사관학교 전산학과

The Security Quality of Computer Network

Jang-Kyun Shin, Byung-Ho Park, Jin-Cheol Yoo
Department of Computer Science, Korea Military Academy

ABSTRACT

This research suggests a criterion, security quality, which is a unifying principle in computer network security that has the lack of a unifying principle. The security quality includes secrecy, integrity, recording, and availability among the factors that represent the security evaluation of the computer system. So, we defined the security quality, which is a basis for determining the security level, as the grand total of evaluation about each factor.

제 1 장 서 론

최근 컴퓨터 통신의 급속한 발전과 함께 컴퓨터 네트워크를 통한 분산되어진 개소간의 다양한 데이터베이스의 공유와 정보 자료 처리가 급속히 발전되고 그 이용이 날로 증가되고 있다. 그러나 국가기관 등의 컴퓨터 망에 적의 스파이나 허가되지 않은 자의 불법 침입으로 외교 단절, 전쟁유발 등의 국가 존망과 직결되는 아주 중요한 데이터의 불법 유출, 복제, 복사, 변경, 파괴, 도난 및 개인 정보 유출 등의 그 피해의 심각성은 실로 대단하게 되고 현재에도 다양한 범죄가 기승을 부리고 있어 사전에 차단, 보호에 대한 대책이 절실한 실정이다.

컴퓨터 네트워크 보안 문제는 정보를 어떻게 통제하여 보호할 것인가 하는 보호 메커니즘의 설계와 구현, 그리고 보호 메커니즘을 어느 정도 신뢰할 수 있는가 하는 보안에 대한 평가와 검증으로 분류할 수 있다. 국내에서도 행정 전산망을 비롯한 국가 기간 전산망 구축을 국가적인 과제로 추진하고 있는 현 시점에서 중요한 정보를 취급하는 컴퓨터 네트워크를 개발하고자 하는 업체에게 보안 기능과 승인 등급에 대한 표준을 제공하고 컴퓨터 네트워크 보안의 신뢰 수준을 평가하기 위한 척도를 제공하기 위해 컴퓨터 네트워크 보안 평가 기준의 제정은 매우 시급한 수준이다. 그러나 네트워크 보안에서의 또 하나의 문제는 단일의 원칙이 결여되어 있다는 것이다. 물리적 보안, 논리적 보안, 프라이버시, 기밀성, 위험성들을 다룰 때마다 다른 시각에서 각 자의 주관으로 보기 때문에 이런 문제들을 통합할 수 있는 단일의 원칙을 필요로 하고 있다. 따라서 본 논문에서는 이 문제들을 통합할 수 있는 방법론으로써 보안 품질(Security Quality)이라는 단일의 기준을 새로이 제시하여 보안을 나타낼 수 있도록 하였다. 이 보안 품질은 소프트웨어 품질 요소 중 비밀성, 무결성, 가용성, 기록성을 포함하고 있으며, 각 요소에 대한 시스템의 보안 정도를 평가하여 이들의 합으로 보안 수준을 결정할 수 있다.

본 논문의 구성은 다음과 같다. 제2장에서 보안 품질의 정의와 요소에 대한 내용을 살펴보고, 제3장에서는 보안 품질에 대한 평가로써 보증 수준에 의한 평가 방법과 품질 요소에 의한 평가 방법을 연구하고 이를 토대로 종합적인 보안 품질 평가 방법을 제시하였고, 제4장에서는 결론 및 앞으로의 연구 방향을 논의한다.

제 2 장 보안 품질 이론

1. 보안 품질 정의

보안이란 보호해야 할 대상을 각종 위해 행위로부터 보호, 차단, 격리하여 안전을 보장하는 것으로서 보안의 품질은 각 대상 기관마다 다소 상이할 수 있으나 보호 수단으로서의 안전 보장의 정도라고 할 수 있겠다. 즉, 비인가자나 불순 침입자에 대하여 비밀의 누설, 도난, 분실 및 기타 파괴 등의 위해 요소로부터 적극적 소극적 방지 행동의 질이라 하겠다. 현재 네트워크 보안에서 겪는 일반적인 문제 중의 하나는 단일의 원칙이 결여되어 있다는 사실이다. 물리적 보안, 논리적 보안, 프라이버시, 기밀성, 위험들을 다룰 때마다 이들 개념들을 각기 다른 시각에서 개별적으로 본다는 점이다. 따라서 이런 문제들을 통합할 수 있는 방법론이 필요한데 소프트웨어공학의 소프트웨어 품질 이론을 보안 문제에 적용하여 보안 품질(security quality)이라는 단일의 기준으로 보안을 나타낼 수 있다. 여기서 보안 품질은 "한 컴퓨터 시스템의 보안이 요구 사항을 얼마나 잘 혹은 잘못 작동하는가"를 나타내는데 이를 단일 측정 도구로 정량적으로 평가하는 것이다.

2. 보안 품질 요소

컴퓨터 네트워크가 제공해야 할 보안 품질의 요소는 크게 비밀성(secrecy), 무결성(integrity), 기록성(recording), 가용성(availability)으로 구분할 수 있다.

가. 비밀성

정보가 외부로 노출되는 것을 방지하는 것을 의미하며, 비밀의 누설 확률은 무단 침입자의 비밀의 인지도와 같다.

$$SP(\text{비밀 보호 확률}) = 1 - SN(\text{비밀의 인지도})$$

또한, 인지 자가 다수인 경우 비밀을 동시에 보호할 수 있는 확률은 각 개인의 보호 확률의 곱들로 표시되는데 인지 자가 다수가 될수록 비밀의 보호 확률은 감소되어진다.

$$P(\text{동시에 보호할 수 있는 확률}) = \prod_{i=1}^{n} P_i(\text{각 개인의 보호 확률})$$

예를 들면, 3인이 비밀 보호 확률을 0.7, 0.3, 0인 경우 동시에 보호할 수 있는 확률은 $0.7 \times 0.3 \times 0 = 0$ 이 된다. 그러므로 두 사람이 적극적으로 보호하려고 하여도 한 사람이 보호할 의지가 없다면 비밀은 누설되어 진다.

나. 무결성

허가되지 않은 자에 의한 정보의 무단 변조를 막는 것과 허가된 자에 의한 오조작에 의한 변조와 고의에 의한 변조로부터 정보를 보호하는 것이다.

다. 기록성

보안 관련 모든 사건을 기록하여 보안위규 사항을 추적하고 분쟁을 해결하는 것으로써 컴퓨터 사용자를 추적할 수 있도록 컴퓨터의 모든 활동을 시간별로 기록해 놓고 안전을 고려하여 이 기록은 운영 체계가 관리하도록 하는 것이 바람직하다.

라. 가용성

정보가 분실되지 않고 항상 존재하며 획득 가능한 상태를 의미한다.

보안 품질 요소는 사용 부서와 용도에 따라 상이할 수 있다. 예로서, 국가의 안위를 책임지는 국방부나 정보 관련 기관에서는 보안 품질의 최우선 순위를 비밀성에 둘 것이며 최하위에 가용성을 둘 것이다. 그러나 은행 등의 금융기관에서는 우선 순위를 가용성에 다음으로 무결성, 최하위에 비밀성을 둘 것이다.

제 3 장 보안 품질 평가

1. 보증 수준에 의한 평가

네트워크의 4단계 보안 등급은 각 등급별로 서로 다른 수준의 보안 요구 사항을 포함하고 있다. 이러한 보안 등급으로 평가되기 위해서는 각 등급의 보안 요구 사항을 일정한 수준으로 만족시켜야 한다. 보안 요구 사항의 만족은 보증(assurance)의 개념으로 볼 수 있는데 만족시키는 수준에 따라 다양한 보증 수준이 존재할 수 있다. 효용성 있는 보증 수준으로는 보안 평가 방법론의 침투 검사, 비공식 검증, 공식 증명을 고려할 때 다음 표와 같이 4단계로 구분할 수 있다.

보증 수준	보 증 내 용
1 등 급	공식 방법으로 증명
2 등 급	비공식 검증(화이트박스 침투검사)
3 등 급	침투 검사(블랙박스 침투검사)
4 등 급	시험 운영

< 보 증 수 준 >

4등급인 시험 운영은 보호 시스템이 안전하다는 것을 시험적으로 운영하여 보이는 수준이고, 3등급 침투 검사는 보호 시스템을 블랙박스로 간주하고 다양한 입력 자료에 대한 출력 결과를 생성하여 분석함으로써 보호 시스템의 허점이 없다는 것을 보이는 수준이며, 2등급 비공식 검증은 보호 시스템의 내부 구성까지 고려한 화이트박스 침투 검사에 의해 보호 시스템의 허점이 없다는 것을 보이는 수준이다. 끝으로 1등급 공식 방법으로 증명하는 것은 보호 시스템이 안전하다는 정리를 수학적으로 증명하는 수준인데 이 방법은 시간(time)과 복잡성(complexity)의 문제가 있다. 공식 증명 방법은 각 단계에서 주장을 정리하고 그 주장의 논리적 흐름을 증명하는데 이들은 매우 느린 과정이므로 전체적으로 많은 시간을 필요로 하는 작업이다. 또한 공식 증명의 주장 설정과 증명은 매우 복잡한 과정이다. 따라서 실제적으로 유용한 보증 수준은 2등급 비공식 검증까지이며, 네트워크의 보안 등급으로 평가되기 위해서는 4등급 시험 운영, 3등급 침투 검사, 그리고 2등급 비공식 검증을 통과하여야 한다.

2. 품질 요소에 의한 평가

네트워크 시스템의 보안 정도를 측정하기 위해서는 이들 속성에 대한 시스템의 정도를 평가하여 이들의 합으로 보안 수준을 결정할 수 있다. 그러므로 다음과 같은 공식으로 네트워크 보안 품질을 정의한다.

$$SQ = K1*CQ + K2*IQ + K3*AQ + K4*RQ$$

여기서, SQ : 네트워크 보안 품질
CQ : 비밀성 품질
IQ : 무결성 품질
AQ : 가용성 품질
RQ : 기록성 품질
평가 요소별 가중치(i=1,2,3,4), (K1+K2+K3+K4=1)

네트워크의 보안 품질은 평가 요소별로 가중치를 곱하여 합함으로써 결정되는데 네트워크의 운영 환경에 따라 가중치를 설정하여 운영할 수 있다. 예를 들어 국방 분야의 네트워크는 정보의 노출에 대한 보호가 가장 중요시되며 다음으로 무결성 그리고 끝으로 기록성이 유지되어야 한다. 이때 가중치 적용은 비밀성>무결성>기록성으로 설정할 수 있다.

가. 비밀성 품질의 측정

네트워크 환경에서 보안의 비밀성 속성을 유지하기 위해서는 원거리에 있는 사용자를 확인하고, 그 사용자의 엑세스 권한을 조회하며, 정보 전송시 암호 기법을 적용하기 때문에 비밀성 보안 품질은 원거리 인증, 엑세스 제어, 그리고 암호 알고리즘으로부터 추론될 수 있다. 따라서 비밀성 품질은 다음 식과 같이 각 보호 기법의 균등한 합으로 정의한다.

$$CQ = (RA + AC + EQ) / 3$$

여기서, CQ : 비밀성 품질
RA : 원거리 인증 등급
AC : 엑세스 제어 등급
EQ : 암호 알고리즘 등급

원거리 인증은 일방향 인증 또는 양방향 인증 그리고 영지식 증명 적용에 따라 분류될 수 있으며 엑세스 제어도 역시 임의적 엑세스 제어와 강제적 엑세스 제어에 따라 분류될 수 있다. 원거리 인증과 엑세스 제어를 4단계의 평가 등급으로 분류하면 다음 표와 같다.

평 가 등 급	원 거 리 인 증	엑 세 스 제 어
0	없 음	없 음
1	일방향 신원 인증	그룹식별자에 의한 DAC
2	양방향 신원 인증	개인식별자에 의한 DAC
3	영지식 상호증명 방식	MAC

< 원거리 인증과 엑세스 제어 등급 >

한편 보호 시스템에는 다양한 암호 알고리즘이 존재하며 이는 각각 일정한 중요성을 갖고 있으므로 균등한 가중치를 적용하여 평가한다. 특정한 암호 알고리즘은 알고리즘에 대한 공격 복잡도를 공격하는 알고리즘이 수행될 때 실행되는 기본 연산의 수에 따라 0-3등급으로 분석하고 암호 알고리즘에서 입력에 대한 출력 결과의 임의성(randomness)을 빈도 검사(frequency test),

시리얼 검사(serial test), 런 검사(runs test)등의 기법(2)을 수행하여 0-1등급으로 분석한다.

$$EQ = 1/N \ (C1 + C2 + ... + Cn)$$

여기서, EQ : 암호 알고리즘 등급
N : 암호 알고리즘 개수
Ci : (i=1..n):암호 알고리즘i의 평가 등급

한편,

$$Ci = Ri * Bi, \quad i=1..n$$

여기서, Ri : 암호 알고리즘i의 임의성 정도(0-1)
Bi : 암호 알고리즘i에 대한 공격 복잡도 등급(0-3)

나. 무결성 품질의 측정

네트워크 환경에서 보안의 무결성 속성은 전문가 시스템을 이용하여 시스템 내부의 불법적인 흐름을 통제하는 방법과 침입 탐지 모델에 의해서 외부 침입을 탐지해 내는 방법 등에 의해서 유지된다. 침입 탐지의 방법은 그 품질을 측정하기 어려운 보호 기법이므로 여기서는 무결성 품질을 측정하기 위하여 감사 추적 자료를 기록 유지하고, 시스템의 처리 절차를 규정하는 정보 흐름의 모든 경우를 분석하며 불법적인 흐름을 통제할 수 있는 보안 전문가 시스템의 추론 규칙을 사용한다. 전문가 시스템의 모든 추론 규칙을 정의하는 것은 어렵지만 많이 존재할수록 무결성 품질의 향상을 기할 수 있기 때문에 무결성 품질은 다음 식으로 표현할 수 있다.

$$IQ = \text{보안 규칙의 수} \ / \ \text{정보의 흐름의 경우 수}$$

여기서, IQ : 무결성 품질

다. 가용성 품질의 측정

가용성 품질은 하드웨어가 파괴되는 경우에 어떤 서비스도 제공할 수 없으므로 하드웨어를 보호하는 메커니즘이 많으면 많을 수록, 정확히 수행되면 수행될 수록 가용성의 품질은 향상된다. 네트워크 환경에서 보안의 가용성 속성은 주로 통신 선로와 호스트 컴퓨터의 평균적인 가용 비율에 근거하기 때문에 다음 식과 같이 가용성 품질을 정의한다.

$$AQ = (\text{통신 선로의 안정성} + \text{호스트 컴퓨터의 신뢰성}) \ / \ 2$$

여기서, AQ : 가용성 품질

이 때 통신 선로의 안정성과 호스트 컴퓨터의 신뢰성은 고장 빈도에 따라 없음(0), 보통(1), 높음(2), 매우 높음(3)으로 등급을 설정할 수 있다.

라. 기록성 품질의 측정

네트워크 환경에서 보안의 기록성은 송·수신자가 자신만의 이익을 위하여 받은 메시지도 안 받았다고 주장하거나 그러한 메시지는 보낸 일이 없다고 하는 경우와 자신에게 이롭게 내용을 변조하여 추후 이를 본래의 메시지였다고 주장하는 경우 등의 많은 논쟁으로부터 보호하는 것이다. 이러한 점에서 신뢰할 수 있는 전산망을 운영하기 위해서는 송·수신자의 신뢰성을 유지하

고자 하는 포괄적인 개념으로서 부인 봉쇄(Non-repudiation)를 요구하고 있다. 부인 봉쇄는 데이터의 송신자가 거짓으로 송신 사실을 부인하는 것으로부터 수신자를 보호하는 발신 증거를 제공하거나, 수신자가 거짓으로 수신 사실을 부인하는 것으로부터 송신자를 보호하는 배달 증거를 제공하는 보안 서비스로서 발신자 부인 봉쇄와 수신자 부인 봉쇄로 구분할 수 있다. 한편 기록성 품질에 영향을 주는 다른 보안 기능으로서는 중요한 객체의 접근 상황을 기록하여 불법적인 접근을 추적할 수 있게 해주는 감사 증적 메커니즘이 있다. 감사 기록에는 불법적인 로그인 시도, 사용자의 시스템 사용/종료시간, 객체의 사용 식별자와 사용시간 등의 보안 관련 사항이 포함되어야 한다. 이와 같이 부인 봉쇄와 감사 증적으로 나타나는 보안의 기록성 품질은 다음 표와 같이 단계별 평가 등급으로 분류할 수 있다.

평가등급	보 안 기 능
0	없음
1	감사 증적 메커니즘
2	감사 증적 메커니즘 수신자 부인 봉쇄
3	감사 증적 메커니즘 수신자 부인 봉쇄와 발신자 부인 봉쇄

< 기록성 품질 등급 >

마. 네트워크 보안의 종합평가

제시된 네트워크 보안의 품질 평가는 보안 요소인 비밀성, 무결성, 가용성, 기록성별로 중요한 보안 기능을 도출하고 이를 정량화 함으로써 수행되는데 이를 종합하면 다음 표와 같다.

평 가 요 소		개별등급	평균등급	종합등급
비밀성(CQ)	인증	0 - 3	0 - 3	0 - 3
	엑세스 제어	0 - 3		
	암호 알고리즘	0 - 3		
무결성(IQ)	감사 추적 능력	0 - 3	0 - 3	
가용성(AQ)	통신 선로의 안전성	0 - 3	0 - 3	
	호스트 컴퓨터의 신뢰성	0 - 3		
기록성(RQ)	감사증적/부인 봉쇄	0 - 3	0 - 3	

< 네트워크 보안의 종합평가 >

네트워크 보안의 종합 등급은 비밀성(CQ), 무결성(IQ), 가용성(AQ), 기록성(RQ)의 등급에 각각 가중치를 곱하여 합함으로써 얻어진다.

제 4 장 결 론

본 연구는 네트워크 보안에서 겪는 일반적인 문제 중의 하나인 단일의 원칙의 결여를 통합할 수 있는 방법론으로서 보안 품질 (security quality)이라는 단일의 기준을 제시하였다. 행정전산망 등 국가 기간 전산망의 표준 운영체제로 되어 있는 컴퓨터 네트워크에 적용할 수 있는 보안 품질의 각 요소의 정의와 보안 평가 기준을 제시하고, 이를 검증할 수 있는 네트워크 보안의 평가 방법을 개발하였다.

한편 컴퓨터 네트워크에 적용될 수 있는 보안 검증 방법은 보증 수준에 의한 평가와 품질 요소에 의한 정량적 평가로 구분하여 제시하였다. 보증 수준에 의한 보안 평가는 시험 운영/침투 검사/비공식 검증/공식 증명의 평가 등급으로 분류하였으며 품질 요소에 의한 정량적 평가는 다음 식으로 정의하였다.

$$SQ = k_1 * CQ + k_2 * IQ + k_3 * AQ + k_4 * RQ$$

여기서, SQ : 네트워크 보안 품질
CQ : 비밀성 품질, IQ : 무결성 품질
AQ : 가용성 품질, RQ : 기록성 품질
$k_i(i=1..4)$: $(k_1+k_2+k_3+k_4=1)$

이와 같이 개발된 컴퓨터 네트워크 보안 평가를 위한 보안 품질 방법론은 국내에서 최초로 연구된 결과이나 보안 검증 방법론의 세분화 등에 관한 사항이 추가로 연구되어 컴퓨터 네트워크 보안에 관한 국가 표준으로 제정되어야 할 것이다.

<참고문헌>

(1) Chow, T.S., Software Quality Assurance : A Practical Approach, IEEE Press, 1985.

(2) Gustafson H., E. Dawson, and B. Caelli, "Computer of Block Ciphers."

(3) ISO, Security Frameworks, Part1-Part7, CD 10181, 1993.

(4) Orlandi E., " Computer Security: A Consequence of Information Technology Quality", IEEE Symposium on Security and Privacy, pp. 109-112, 1990.

(5) William Stallings, "Network and Internetwork Security", Prentice Hall International, 1995.

(6) 신장균, " 컴퓨터 네트워크의 보안 평가 기준 및 검증 방법 연구", 陸士論文集 第46輯, pp 281-305, 1994.