시뮬레이션 기반의 필수 서비스 연속성 평가 방법론

이익섭* · 김형종*

A Methodology of Simulation-based Essential Services Continuity Test

Ik-Seob Lee* · Hyung-Jong Kim*

Abstract

최근의 일상 생활들은 정보통신 네트워크를 기반으로 제공되는 서비스와 밀접하게 연관되어 있다. 지난 1.25 인터넷 대란을 통해서 볼 수 있듯이, 네트워크 침해사고로 인해 네트워크 필수 서비스가 중단되었을 때 사용자를 위해 네트워크 기반으로 제공되는 주요한 서비스에 막대한 피해가 발생한다는 것을 직접 확인하였다. 컴퓨터 네트워크에서 필수 서비스의 가장 중요한 특성 중 하나는 서비스의 연속성이다. 필수 서비스의 연속성이 보장되지 못하게 되면 네트웍의 정상적인 동작에 큰 문제를 야기한다. 따라서 대상이 되는 네트워크가 필수 서비스를 보장하는 능력을 평가하여 안전하고 신뢰성 있는 네트워크 서비스를 제공하기 위한 연구가 필요하다.

본 논문에서는 시뮬레이션 기반 필수서비스의 연속성 평가 방법론을 제안한다. 이를 위해 평가 모델의 구성, 실행, 분석 등의 단계를 가지는 평가 절차를 제시한다. 또한 평가 프레임을 제시하고 프레임의 구조 및 동적 특성을 살펴본다. 마지막으로 서비스 연속성의 정도를 평가하기 위한 평가 지표를 가용성, 권한보호성, 정보비밀성, 복구가능성 등 4가지로 분류하고 각각에 대해 살펴본다.

Ⅰ. 서론

최근 몇 년 동안 컴퓨터 기술은 비약적으로 발전하였다. 그리고 컴퓨터 기술의 발달은 인터넷이라는 거대한 사이버 우주 공간을 만들어 내었다. 그러나 이러한 사이버 공간에도 현실세계의 9.11 테러와 같은 일이 일어날 수도 있다. 현재 사이버 테러의 경우는 국가 기간 시설(은행 및 금융 시스템, 전기 및 전력 산업, 정보통신기반시설, 물류 및 운송 시스템, 국가 방위 체계)들을 위협하기에 충분한 요소들을 내포하고 있는 실정이다. 우리나라에서는 사이버 테러 등과 같은 악의적인 정보통신 침해 행위를 방지하기 위하여 제도적으로 정보통신기반보호법을 제정하기도 하였다. 그러나 제도적인 방지에 맞물러 기술적인 사이버테러의 방어 및 정보보호 기술의 뒷받침이 필요하다.

국외에서는 이러한 사이버 테러 등과 같은 정보통신 위협에 대비하여 1990년대 중반부터 컴퓨터 침해에 대응 기술들을 활발하게 연구하고 있다. 초기 해킹 방지 기술은 단일 컴퓨터 상에서 연구되었지만, 네트워크의 발달로 인하여 점차 네트워크 차원에서의 방지 및 대응 기술을 개발하게 되었다.

최근 몇 년간 연구에 대하여 가장 활발하게 진행하고 있는 곳이 CMU(Carnegie Mellon University)의 CERT이다. CMU에서는 CERT를 운영하면서 축적된 기술 및 정보를 바탕으로

* 한국정보보호진흥원 시스템기술팀

1997년부터 본격적으로 생존성(Survivability)라는 이름으로 관련 연구를 진행하고 있다[1,2]. 연구의 내용은 보안 취약성의 틈, 즉 악의적인 공격이나 재난에 대하여 시스템을 견고하게 하고, 공격에 대하여 제한된 피해만을 보장하기 위하여 이를 인식하고 방지하여 좀더 개선된 보안 기술을 찾아내는 것이다. 미국 아리조나 주립대학의 ITL Lab에서는 DARPA에서 진행하고 있는 FTN 과제의 일부를 수행하고 있다[3]. 이 연구에서는 공격 및 결함시 중요 정보통신 기반 네트워크의 공격점 또는 취약점을 실시간으로 발견하고 행위의 특징을 나타내는데 사용될 수 있는 온라인 네트워크 취약점 분석을 위한 프레임워크를 제안하였다. 이와는 별도로 다른 여러 연구기관에서 네트워크 필수서비스의 연속성에 대한 연구가 활발하게 진행되고 있다[4,5].

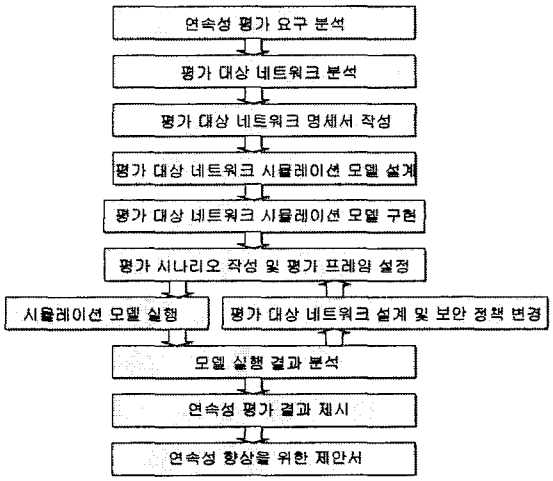
외부의 공격이 있을 때 적용된 방어 메커니즘이 정보통신기반시설의 필수 서비스에 대해 일정 수준의 기능 및 성능을 유지시키는가를 평가하는 평가 도구의 개발이 필요하다. 실제 운용시스템의 공격을 통한 평가는 평가 대상 시스템에 대한 피해를 가져오기 때문에 시뮬레이션 기반의 평가가 수행되어야 한다.

본 논문에서는 시뮬레이션 기반 필수서비스의 연속성 평가 방법론을 제안한다. 이를 위해 2장에서 평가 모델의 구성, 실행, 분석 등의 단계를 가지는 평가 절차를 제시하고, 평가 프레임의 구조 및 동적 특성을 살펴본다. 3장에서는 서비스 연속성의 정도를 평가하기 위한 평가 지표를 가용성, 권한보호성, 정보비밀성, 복구가능성 등 4가지로 분류하고 각각의 세부 평가 방법을 정의한다. 마지막으로 4장에서 본 논문의 결론을 기술한다.

2. 평가 절차 및 프레임

2.1 평가 절차

〈그림 1〉의 순서도는 필수서비스 연속성에 대한 평가 절차를 나타낸다.



〈그림 1〉 생존성 평가 절차

연속성 평가 요구 분석에서는 네트워크 관리자나 보안 담당자로부터 해당 네트워크의 주요 평가 대상 시스템 및 서비스에 대한 정보를 수집하고, 해당 시스템들에 대해서 이슈가 되는 평가 요소를 얻어내는 일을 수행한다. 이러한 요구 분석을 통해서 정보통신기반의 모든 구성요소에 대한 생존성 평가를 수행하는 것을 피하고, 요구사항에 근거하여 특정 중요 요소의 평가에 자원을 집중시킬 수 있게된다.

평가대상 네트워크 분석에서는 생존성 평가 대상이 되는 네트워크의 토폴로지, 네트워크 대역폭, 주요 제공 서비스, 구성 호스트 정보 등을 수집하여 이를 문서화한다. 이러한 수집과 분석의 결과는 평가대상 네트워크의 명세서 형태로 도출되며, 이렇게 만들어진 명세서는 네트워크 시뮬레이션 모델 설계의 근거 자료가 된다. 네트워크의 명세라고 함은 네트워크가 갖는 특성 정보들을 특정 표현 레벨에 맞게 표현한 기술(Description)로서, 여기에서 네트워크는 연결 시스템(Coupled System) 레벨에서 호스트, 네트워크 장비와 물리적 연결관계를 표현한 형태로 나타난다. 또한, 각 호스트 및 네트워크 장비 모델들은 각 모델이 가지고 있는 동적 특성이 나타나

도록 상태와 상태전이 정보가 정의되어 있다. 이러한 모델 설계 결과물은 바로 생존성 평가를 위한 모델의 구현에 활용되고, 구현된 모델은 연속성 평가 요구분석에 근거한 연속성 평가 대상 네트워크 모델 구현물을 얻게된다.

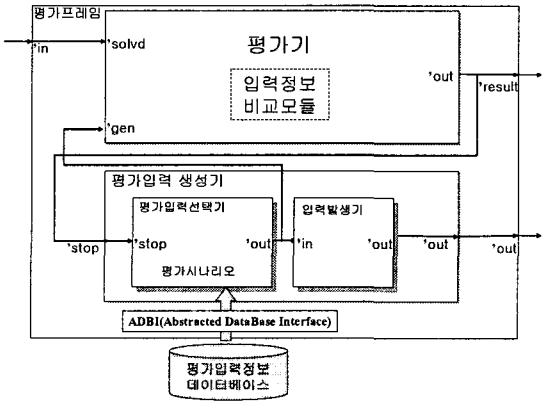
얻어진 연속성 평가 대상 모델은 평가프레임과 연결되어 다양한 시험의 대상이 되어 진다. 특히, 이러한 시험을 수행하기 위해서는 적절한 평가 시나리오가 있어야 한다. 평가 시나리오는 평가 요구분석에 근거한 것으로 요구사항에서 추출하기를 원하는 평가 지표를 찾아내기 위한 시나리오를 작성하도록 한다. 이렇게 작성된 시나리오는 이를 실행하기 위한 구체적인 설정 값으로 변환되어야 하고 이는 평가 프레임의 입력정보로 활용되어 평가대상 네트워크 모델에 입력을 제공하고 그 반응을 살피도록 한다. 이러한 평가 프레임과 대상 네트워크사이의 연동은 시뮬레이션 모델이 실행된 후 시뮬레이션 관측 시간동안 지속적으로 이루어지고 이 결과는 평가 프레임 내부의 분석모델에 의해서 분석되고 그 결과가 다양한 방법으로 제시될 수 있다. 이렇게 제시된 결과는 바로 평가대상 네트워크 모델의 디자인 변경 및 새로운 보안 정책의 적용에 활용될 수 있으며, 이에 근거해서 다시 평가 시나리오 및 평가프레임 재 설정이 이루어진다. 이후에 평가를 어느 정도 반복할지는 평가 요구분석에 근거해서 원하는 수준의 보안 요구사항에 이를 때까지 수행할 수 있다. 이러한 작업이 완료되면, 시뮬레이션 결과는 실 시스템의 설계 변화나 보안 설정 변경에 활용되어지도록 연속성 향상 제안서(Suggestion for Enhancing Continuity)를 제시하도록 한다.

〈그림 1〉의 단계 중 평가 시나리오 작성 및 평가 프레임 설정에서는 다음 장에서 소개할 각 평가 지표별로 시나리오가 존재하며 이를 위한 평가 프레임의 설정도 다르게 나타난다. 특히, 각각의 경우의 공통점은 모두 공격 입력과 이에 대한 반응을 조사한다.

2.2 평가 프레임

본 논문에서 평가 프레임의 설계에 대해서 기술하고 특히, 평가 프레임의 구조와 동적인 특성을 살펴 보기 위해 Zeigler의 [6]에서 제안한 DEVS(Discrete Event System Specification) 시뮬레이션 모델의 평가 환경을 도입하였다.

평가 프레임의 구조는 〈그림 2〉와 같다.



〈그림 2〉 평가 프레임 구조

평가 입력 생성기에서는 평가를 위한 입력을 특정 시간에 발생시키는 일을 하게된다. 이러한 일을 수행하기 위해서 필요한 두 가지 요소는 평가를 위한 시나리오와 평가 입력 정보이다. 일단 적당한 시나리오가 선택되면 이 시나리오에 부합되는 '평가 입력 정보'가 선택되고 이 정보에 근거해서 입력 발생기는 평가 입력을 생성한다. 여기서 평가 시나리오는 각 평가 지표 추출 시나리오에 근거해서 작성되고, 이는 평가 수행자가 평가 요구분석서에 근거해서 적절한 평가를 수행하게 한다. 평가 시나리오는 평가를 위해서 필요한 절차들을 모두 기술한 것으로서 평가자는 요구분석서에 맞는 시나리오를 선택하면 되도록 한다. 그리고, 시나리오에 근거한 평가 입력 정보는 평가 입력정보 DB에서 추출해 오도록 한다.

즉, 시나리오는 평가 입력정보의 선택을 위한 지식으로 활용되는 것이다. 평가 입력 정보는 입력 발생기에게 어떤 입력들을 평가 대상에게 전달해 줄지를 결정하는 데에 사용되는 정보이다.

3. 평가지표

본 장에서는 필수서비스 연속성 평가를 위해 필요한 필수적인 평가 지표에 대한 관련 연구 동향을 살펴보고, 본 연구에서 제시되는 평가 지표의 항목에 대해 각각의 요소들의 의미와 평가 내용에 대해 살펴본다.

〈표 1〉 생존성 평가 요소 및 점검 항목

요소	점검 항목	테스트 방법
가용성	자원 상황	자원의 고갈을 일으키는 상태의 점검
권한 보호성	취약성	권한 획득이 가능한 상황들에 대한 탐지 및 가능성 점검
정보 비밀성	취약성	정보 수집 가능성 여부에 대한 점검
복구 가능성	방어 메커니즘	적용된 방어 메커니즘이 복구에 대해서 어느 정도 기능을 갖고 있는지에 대한 테스트
필수 서비스 연속성	가용성, 권한보호성, 정보비밀성, 복구가능성	4가지 테스트 항목을 조합한 결과를 통해 네트워크의 연속성을 지수화 하도록 함.

앞서 제시한 평가 절차 개발에 있어서 주요 평가 요소를 다음 〈표 1〉과 같이 평가 대상의 연속성에 영향을 주는 4가지 요소, 즉 가용성, 권한보호성, 정보비밀성, 복구 가능성으로 선정, 분류하였다.

3.1 가용성(Availability)

가용성은 공격에 대한 자원의 고갈을 일으키는 상태를 점검하는 요소이다. 요청된 서비스를 수행하기 위해서 할당되는 자원의 양의 적정성, 효과적인 자원 관리 메커니즘의 사용 등 내부적인 문제를 다루는 부분과, 공격에 대응하는 관점에서 적용되는 방어메커니즘 평가에 의해 수치적으로 표현된다.

예를 들어, 서비스 거부 공격시 한정되어 있는 시스템 메모리의 양과 서브 네트웍의 할당 대역폭 등을 이용하여 반복적인 Sync 신호를 통한 메모리 고갈 현상과 의미 없는 방대한 트래픽을 발생시켜 네트웍의 대역폭을 고갈 시키는 방법으로 서비스, 시스템 및 네트웍의 생존성을 저해하는 공격을 가하게 된다. 이때 시스템 할당 메모리와 네트웍의 할당 대역폭은 각 평가 대상의 필수서비스 연속성에 큰 영향을 미치게 된다. 또한 자원을 얼마나 효율적으로 관리하는 메커니즘을 가지는 가에 따라 한정된 자원을 가지고 연속성을 높일 수 있게 된다. 이와는 달리 공격자에 의한 DoS 공격을 원천적으로 막을 수 있는 대응 기법으로 시스템 상에 방어 메커니즘을 가지는 방법이 있다.

3.2 권한보호성(Privilege Protection)

권한 보호성은 시스템 및 소프트웨어의 권한 획득이 가능한 상황들에 대한 탐지 가능성 및 사용자 권한의 관리적 영역을 점검하는 요소이다.

권한 보호성의 세부적인 평가 요소를 살펴 보면, 우선 시스템이 가지고 있는 취약점을 이용하여 비인가자에 대해 권한을 부여 하거나, 관리자 자체적인 요인에 의한 패스워드 유출 하는 경우를 예로 들 수 있다. 이때 악의적인 공격자가 권한을 가졌을 시에 생존성의 상당한 감소 요인으로 작용한다. 또한 루트 또는 사용자 권한 등 부여된 권한의 레벨에 따른 차이도 생존성 지수에 영향을 미치게 된다.

시스템 관리 측면에서 패스워드의 주기적인 교체, 패치의 수행, 소프트웨어 업그레이드, configuration 체크 등의 부당한 권한 부여에 대한 취약점을 없애기 위한 노력의 정도 역시 생존

성에 영향을 미치는 세부적인 요소이다. 이런 과정은 노력의 과정에 대한 평가로써 평가 지수를 높일수 있을 뿐만 아니라, 발견된 취약점을 없애므로써 이후의 평가시 더 높은 평가를 얻을 수 있게 된다.

3.3 정보비밀성(Information Confidentiality)

정보 비밀성은 권한 보호성 요소와 마찬가지로 시스템의 취약점을 이용한 상황이라는 점에서 비슷하며, 정보의 수집 가능성 여부에 대한 점검을 수행하는 요소이다.

정보 비밀성의 세부 평가 요소는 여러 가지가 있다. 우선 현재 평가 대상이 가지고 있는 정보 유출에 대한 취약점의 개수에 의한 평가가 가능하다. 공격자는 이런 취약점을 이용하여 정보획득을 시도하므로 취약점의 개수가 많을수록 연속성 평가지수는 감소하게 된다. 네트워크에 사용되는 프로토콜의 자체적인 설계 결함을 이용하여 정보 비밀성에 영향을 줄 수 있다. 또한, 네트워크의 접근 제어의 정책이나 수준, 위의 권한 보호의 예와 마찬가지로 시스템 관리 측면의 패스워드의 주기적인 교체, 패치의 수행, 소프트웨어 업그레이드, configuration 체크 등의 부당한 권한 부여에 대한 취약점을 없애기 위한 노력의 정도 역시 정보 비밀성에 영향을 미치는 세부요소이다.

3.4 복구가능성(Restorability)

복구 가능성은 공격 발생 후 나타난 공격 흔적에 대응하기 위해 적용된 방어 메커니즘이 복구에 대해서 어느 정도 기능을 갖고 있는가에 대한 평가 점검 요소이다. 공격 이후에 발생하는 복구의 관점은 두 가지로 나누어 생각 할 수 있다. 공격이 성공 될 수 있었던 원인과, 결과에 대한 문제이다. 원인 측면에서 살펴보면 공격이 성공하게 된 원인, 즉 상태를 평가 대상이 가지고 있는 방어 메커니즘을 통해 막을 수 있는가에 대한 문제가 중요시 된다. 또한 공격의 결과로 발생하는 평가 대상의 문제에 대한 해결책을 가지고 있는가에 대한 문제도 중요한 평가 요소가 될 것 이다. 마지막으로 공격 발생 후 복구에 걸리는 시간도 중요한 요소가 된다. 만약 공격에 의해 제공되는 서비스가 중단되었을 때 서비스 중단 시간은 서비스 공급자, 사용자 측면 모두 상당히 부정적인 영향을 가지게 된다.

4. 결론

본 논문에서는 필수서비스 연속성 평가를 위한 방법론을 제시하였다. 이를 위해 평가를 위한 실험 프레임(Experimental Frame)의 구조를 제시하고, 이러한 구조를 기반으로 테스트 대상 정보통신기반을 분석하는 절차를 제시하였다. 또한 평가를 위한 평가 지표에 대한 내용을 다루었다. 세부 평가 지표를 가용성, 권한보호성, 정보비밀성, 복구 가능성 등 4가지로 분류하였다. 본 문에서 제시된 평가 방법론은 차후 필수서비스 연속성 평가 소프트웨어 개발에 활용 될 것이다.

참고문헌

[1] N. R. Mead, R. J. Ellison, R. C. Linger, T. Longstaff, and J. Mchugh, "Survivable Network Analysis Method," Technical Report No. CMU/SEI-2000-TR-013, Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, March, 2000.

[2] Richard C.Linger, Andrew P.Moore, "Foundations for Survivable System Development: Service Traces, Intrusion Traces, and Evaluation Models" oct. 2001

[3] Guangzhi Qu et. al., "Vulnerability Analysis for Network Faults and Attacks", submitted to DISCEX 3.

[4] S. Jha et. al., "Survivability Analysis of Network Specification", DSN 2000

[5] HyungJong Kim, KyoungHee Ko, DongHoon Shin and HongGeun Kim, "Vulnerability Assessment Simulation for Information Infrastructure Protection", Proceedings of the Infrastructure Security Conference 2002, LNCS Vol. 2437, pp. 145-161, October. 1-3, 2002.

[6] B. P. Zeigler, H. Praehofer and T. Kim, Theory of Modeling and Simulation, Second Edition, Academic Press, 2000.