네트워크 정보 시스템의 취약성 분석과 Survivability

남영우*, 이장세*, 지승도*, 박종서*, 구경옥**

*한국항공대학교, 컴퓨터공학과, 강릉영동대학 컴퓨터정보계열 인터넷사무정보전공**

Network Information System Vulnerability Analysis and Survivability

Young-Woo Nam*, Jang-Se Lee*, Sung-Do Chi*, Jong-Sou Park*, Kyung-Ok Koo**

*Department of Computer Engineering, Hankuk Aviation Univ,
**Division of Computer Information Internet Office Information Course, Gangneung Yeongdong College

요 약

기존의 개별적 보안 사항에 맞추어 서비스를 제공하는 여러 보안 솔루션들이 급변하는 네트워크 환경에 적절한 대응을 못하고 있는 실정이다. 단순한 보안 문제에 대한 특화된 솔루션에 의존을 해왔기 때문에 해당 네트워크와 시스템 환경에 맞는 적절한 대응책을 마련하지 못하고 있으며, 그 이전에 취약성 분석조차도 미비하기 때문이다. 그러므로 적절한 취약성 분석에 대한 방법론 제시가 필수적이다. 사이버 공격과 방어 메커니즘 분석을 통해 얻어지는 시스템의 각 요소들을 Modeling하고, 시뮬레이션 기법을 이용하여 취약성을 평가하고 다시 재구성하여 적용해보는 취약성 분석 방법을 기술하고자 한다. 다양한 공격들로부터 전체 시스템을 보호하고, Survivability를 증가시키기 위해서는 취약성 분석이 기반이 되어야 하며, 그 시스템은 취약성에 의한 결함이나, 공격에 의한 장애에도 불구하고, 고유의 기능을 완전하게 제공하기 위해서 지속적으로 수행되는 속성을 유지해야 할 것이다.

I. 서론

현대는 인터넷이라는 필수 불가결한 매체를 통해 거대한 네트워크 환경으로 확장해 나가는 시기임을 누구도 부인하지 못한다. 단순히 네트워크로 연결된 시스템에서 data를 처리하는 예전과는 달리, 네트워크를 통해 전달되는 중요한 정보(Information)가 있고, 그 정보를 필요한 목적에 따라 보호(Security)해야 하고, 그 정보를 주고받는 당사자들간에 신뢰구축 과정 중에, 그러한 신뢰성을 악용하는 자들로부터 자신의 시스템을 보호해야 하는, 복잡하고도 아주 상식적인 시대로 도래한 것이다. 그러나 기존의 정보 시스템들이 갖추고 있는 보안에 관한 분석력과 그 활용도는, 인터넷의 확대라는 환경의 변화와 함께 그 요구사항과 중요도가 증가함에도 불구하고, 보조를 맞추고 있지 못하는 실정이다.

다양하고 지능적으로 급변하는 불법적 공격 기법에 효과적인 대응을 하기 위해 여러 가지 보안 솔루션들이 서비스를 하고 있지만, 개별적이고, 기능 중심적인 한계를 극복하지 못하고 있다. 그 이유는 지금까지의 네트워크 정보 시스템은 단순한 보안 문제에 대한 특화된 솔루션에 과한 의존을 해왔기 때문에 새로운 패러다임의 도입이 필요한 시점에 놓였다. 예를 들어, 네트워크 시스템을 보호하기 위한 인증과 암호는 그 뜻과 취지와는 달리 더 많은 취약성을 추가하고 있을 뿐이다[1]. 그 외에 방화벽, IDS, 디지털 서명, 라우팅 프로토콜 등, 기술적 측면에서 점차 나아지고 있는 것은 분명하지만 네트워크 취약성에 노출되고 있는 것은 부인할 수 없는 사실이다.

이렇듯 수많은 보안 솔루션과 방법론들이 있음에도 불구하고 시스템 및 기타 네트워크 환경에 취약성이 계속해서 존재하고 있다. 해킹의 기법과 공격 유형이 복잡해지는 추세에서, 단순 패치나 업그레이드, 그리고 개별 공격에만 적용되는 보안시스템은 만족스런 신뢰성을 제공하지 못하고 있으며, 기존 보안 시스템의 기능 중심적인 보안 솔루션은 확장되는 요구사항에 대한 적절한 기능을 제공하지 못하고 있다. 단편적인 공격에 대한 단기적인 대응전략으로 보안 시스템을 구축하던 보안 솔루션은 점차적으로, 장기적인 대응전략 수립에 중점을 두는 추세로 변하고 있다. 최근의 보안 시스템은 이러한 요소를 두루 갖춘, 지능적이고, 정책 지향적이며, 장기적인 대응전략을 갖춘 통합적 시스템을 필요로 한다.

취약성 분석/복구에 대한 노력으로 최근 System survivability paradigm 이란 이름의 개별적 컴포넌트들의 보안 솔루션을 넘어선 목적으로서 Network Information Survivability가 제안되었다. Survivability 연구의 주된 목적은 시스템

의 주위에서 생성되는 취약성을 최대한 감소 시키고, 취약성에 따른 복구 능력을 증가시키고자 하는 것이다[1].

Survivability는 사용자의 요구 변화를 네트워크 상에서 원활히 수용할 수 있도록 하기 위한 방안이다. 특정한 기능을 갖추거나 서비스를 제공하는 네트워크 시스템은 그 본연의 목적에 충실하기 위해 시스템을 유지시키고, 서비스의 연속적 실행을 보장해야 한다.

본 논문은 여기서 네트워크로 연결된 정보 시스템의 Survivability를 논의하고자 한다. 시스템의 Survivability를 증가시키고, 전체 네트워크 시스템에 존재하는 취약성을 줄여 보안 시스템이 원활히 제 기능을 다할 수 있도록 하는 것이 목적이다.

2장에서는 취약성이 무엇이며, 취약성 분석 방법과 Survivability와의 연계성에 대해서 논의하고, 3장에서 Survivability의 활용방안에 대해 서술했다. 마지막 4장에서 결론과 함께 향후 연구 계획에 대해 요약하겠다.

II. 네트워크 시스템 취약성 분석

1. 취약성 평가

인터넷 보급의 확대로 인한 여러 취약요소들이 증가하고 있다. 이는 곧 해킹, 불법 접근 등 외부적 위협 요소의 증가를 의미함과 동시에 네트워크를 이룬 시스템 자체의 Bug를 비롯해서 Program error, 운영체제 결함 등의 내부적인 결함이 끊임없이 생겨나고 있고, 또한 다양해지는 라우팅 경로 여러 우회 경로를 제공하기 때문에 해킹 방지에 난해함만 더해가고 있다[2].

네트워크 정보 시스템의 Survivability 값을 측정하기 위한 방편으로 취약성 평가가 선행되어야 하는 이유는 위의 내용에서 알 수 있듯이 네트워크 시스템을 공격 대상으로 정하여 이루어지는 각종 불법적인 접근들이 그 시스템을 이루는 여러 요소들의 상태와 밀접한 관계가 있기 때문이다. 일반적인 공격의 패턴이 공격 대상의 정보를 수집하고, 대상의 취약한 곳으로 접근하여 권한을 획득한 후, 소기의 목적을 달성한다고 볼 때, 공격자는 관리가 허술한 네트워크를 통해 접근을 하여 해당 시스템의 결함이 있는 Bug를 이용하여 관리자 권한을 획득하게 되고, 네트워크 시스템에 치명적이 될지 모르는 불법행위를 하게 되는 것이다.

네트워크 단위로 연결된 각각의 그룹이 가지고 있는 취약성 요소를 Network Vulnerability라 하고, 네트워크상의 각 호스트들의 주요 component들이 갖는 취약성을 Node Vulnerability라 한다. 그렇게 해서 네트워크에 연결된 호스트들에 가해지는 공격의 빈도 수와 성공여부 등을 시뮬레이션을 통한 분석으로 네트워크간 Link Vulnerability를 측정할 수 있다[2].

하지만 위의 세 가지 요소만으로 네트워크 정보 시스템의 취약성을 평가하기에는 어려움이 많다. 점점 방대해지는 인터넷 환경으로 인해 그 만큼 보안 시스템이 확보해야하는 영역은 넓어지게 된다. 또한 영역의 확대뿐만 아니라 하위 레벨의 취약성까지도 상세한 분석이 가능해야 할 것이다. 그리고 취약성 평가를 통한 Survivability 측정을 위해 실망에서 테스트 및 분석을 하기에는 그 비용과 연구 기간은 증가할 것이고, 그렇게 해서 나온 결과를 적용하는 측면에서도 속도와 적응 유연성은 줄어들 것이다.

2. 취약성 평가 방법 연구

여러 가지 제약 조건을 극복하면서 가장 효과적인 결과를 산출하여 적용하는 방법으로, 각 취약성 요소들과 네트워크 컴포넌트들의 Modeling을 통한 시뮬레이션이 적합하다 하겠다[3].

가상 공격 시뮬레이션 모델 생성을 위해, 공격자의 일반적인 공격패턴을 조직하고 명세화하여 Attack tree 구조를 생성한다[4]. 여러 가지 Attack tree를 생성하여 시뮬레이션 함으로써 공격의 패턴을 분석할 수 있고, Attack tree의 구조를 상세화하여, 취약성 분석에 활용할 수 있는 것이다.

또한 취약성 분석 결과를 다시 공격 시나리오로 재구성하여 시뮬레이션을 수행함으로써 취약성의 변화로 인한 Survivability의 증가 효과를 볼 수 있다. 같은 의미로, 반복적으로 시도되는 같은 유형의 공격들은 보안 정책 설정 후 재구성되어 차단되기 때문에 재발 방지의 효과를 높일 수 있다.

그림 1과 같이 테스트 베드를 구성하여 취약성 평가를 수행하였다. Target1의 구성 설정 오류를 이용하여 접속하고 다시 Target2를 공격대상으로 하여 국방 망에 침입하는 시나리오를 만들어 테스트해 보았다. 공격에 의해 취약해진 네트워크의 상태를 관리 시스템이 자체 시뮬레이션을 통해 취약성 분석하고 그 결과를 다시 재구성하여, 그림 2와 같이 노드의 설정을 변경하고 라우터에 명령을 내림으로써 공격을 차단할 수 있음을 보여주고 있다.

취약성 분석을 통한 재구성으로 해당 네트워크 시스템은 계속적인 서비스 수행을 유지할 수 있으며, 일시적인 결함이나 공격에 의한 성능저하에도 신속하고 빠르게 대응방안을 수립, 적용할 수 있다. 시뮬레이션 기법을 이용하면 많은 비용과 시간을 절약할 수 있으며, Survivability를 증가시킬 수 있는 하나의 해결책이 되는 것이다. 부가적으로, 시뮬레이션을 지원할 수 있는 공격/방어의 시나리오 생성을 위한 방대한 자료가 준비되어야 한다.

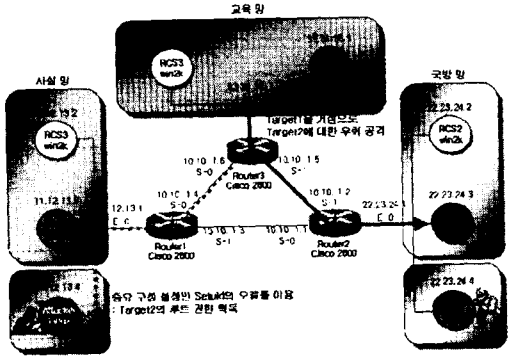

그림 1 우회 경로를 이용한 다중 공격

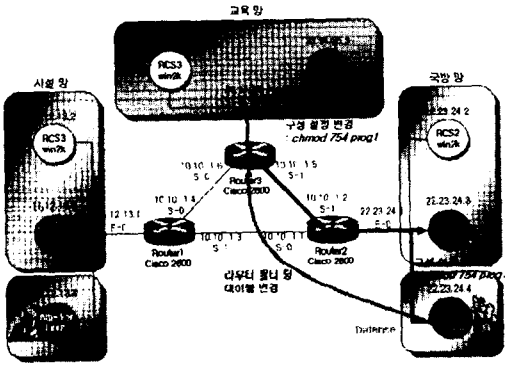

그림 2 우회 경로를 이용한 다중 공격 관리

III. Survivability 활용

Survivability System은 컴포넌트들이 사용 불가능하게 되는 상황에서 주어진 시간 안에 요구되는 기능들을 수행(the continuance of mission)하는 능력을 가진 시스템이다. Survivability 개념이 추가된 네트워크 정보 시스템은 위와 같이 재 정의되고 있다. 그리고 Survivability-Over-Security(SOS)라는 이름의 연구를 통해 네트워크 시스템 Survivability를 증가시키는 연구를 하고 있다[1]. 또한, 보안 관리자들은 공격에 대비한 방어 정책을 강화하고 있다. 그럼에도 불구하고 불법적인 공격이 성공하는 이유는 그들이 생각지도 못한 여러 곳에 취약성이 도사리고 있고, 공격자는 그것을 악용한다는 사실이다. 위 테스트에서 보듯, Survivability가 있는 네트워크 정보 시스템을 분석하는 연구를 통해 일반적인 모든 시스템 컴포넌트들 즉, 외부로 연결되는 링크들과 노드들의 가상적인 추상화는 많은 영역에 응용 가능하고, 더욱 더 견고한 네트워크 시스템을 구축하는 밑거름이 된다.

기존의 보안 관리 방법 중 하나인 Redundancy(동일한 정보 또는 동일한 장치를 두 개 이상 사용하는 방법)는 결함 허용 시스템에서 장치의 고장을 대비하거나 데이터 관리 시스템에서 불의의 데이터 파괴에 대비하기 위하여 여분의 시스템을 마련해두는 방법을 사용했다[5]. 이는 서비스를 제공하는 비즈니스에서 결함 복구에 많은 비용을 요구한다는 것을 의미하고, 긴급한 서비스를 제공해야하는 데 위협적인 요소이며, 국방과 경제분야의 보안에 극단적인 위험을 초래할 수 있다. 그러나 예산 제약에 따른 소프트웨어 공학적인 측면에서 볼 때, 위 방법은 좋은 방향이 아님을 알 수 있듯이 주어진 조건에서 최대한의 효과를 얻기 위한 Survivability를 제공하는 것이 해결책이라 할 수 있겠다.

Survivability의 연구를 통한 보안 솔루션 개발은 인터넷처럼 한정되지 않은 무한한 네트워크 공간에서, 불완전하고 불명확한 정보들로 널리 분산된 시스템들의 모든 문제를 해결할 수는 없다. 하지만 네트워크 시스템에 Survivability를 적용하기 위해 놓쳐서는 안 되는 가장 중요한 개념은 네트워크 상에서 서로 의존하는 모든 컴포넌트들을 결합하는 효율적인 방법에 중점을 둬야 한다는 것이다. 위의 시뮬레이션 기법을 통한 테스트 방법도 취약점들의 합을 계속해서 감소시키고, 복구 능력을 증가시키는 알고리즘을 사용하고 있으며 시뮬레이션 기법을 사용하여, 네트워크 정보 시스템의 survivability를 증가시키고자 하고 있다.

결론적으로 볼 때, 정보 시스템의 survivability를 증가시키고자 하는 연구의 목적을 크게 두 가지로 나누어 볼 수 있다. 첫째, 시스템에 일어나는 여러 가지 취약성들의 합(Sum of System Vulnerability)을 감소시키는데 초점을 두어 시스템 결함을 견뎌내는 데 목적을 두고 있다. 둘째로, 시스템 결함을 견뎌내는 동시에 시스템 복구 능력의 합을 증가시키는 것을 목표로 하고 있다.

네트워크 정보 시스템에 Survivability를 제공하기 위해, Survivable 한 메커니즘을 종료 또는 활성화시키면서, 이러한 동작을 제어하는 또 다른 상위 메커니즘은 일종의 Strategy 혹은 Policy로 정의가 되어 있어야 하며[6], 메커니즘 수행을 위한 규칙의 집합들은 단계적인 확대 전략을 가지고 생성되고 참조되어야 한다. 이러한 연구는 기존의 연구방식이나 보안 솔루션들과는 대조적인 차이를 보일 수 있다. 왜냐 하면 형식적이고, 단순 통계적이거나 경험치를 바탕으로 한 실험들은 점점 더 광범위하고 복잡해지는 네트워크 시스템들간의 보안 유지에 있어서의 중요한 요점들을 간과할 수 있기 때문이다.

연구 자문 기관인 Gartner Group은 2003년까지 자체 네트워크 보안을 관리하고 인터넷을 사용하는 기업들 중 50%가 인터넷 침해를 경험하게 될 것으로 예측했다. 더구나 60% 이상은 침입당한 사실조차도 알지 못할 것이라고 경고했다. 또한, Gartner Group은 계획되지 않은 시스템 다운의 40%가 소프트웨어 응용상의 결함으로 인해

발생한다고 평가했다[7]. 결함이 발생하거나 시스템의 일부가 사용 불가능하게 되었을 때, 서비스를 제공하는 응용 소프트웨어를 재구성하는 능력을 Survivability라 할 때, 이는 시스템 운용 소프트웨어가 보안측면에서 매우 유연해야 하며 서비스 수행 지원을 위한 포괄적인 연구가 필요함을 나타낸다.

IV. 결론 및 향후 연구 방향

시스템은 구성 이전의 알려지지 않고 예상되지 않은 공격들에 대해 여전히 노출되어 있다. 그러므로 각 시스템은 그런 위험성을 여과 없이 인식하기 위해 유연해져야 할 필요가 있다. 앞에서 살펴보았듯이, 지능적이고, 악의적인 공격들로부터 전체 시스템을 보호하기 위해, Survivability는 효율적이고 효과적으로 네트워크 정보 시스템에 제공될 수 있다. 그리고 Survivability는 시스템 취약성에 의한 결함이나, 공격에 의한 장애에도 불구하고, 고유의 기능을 완전하게 제공하기 위해서 지속적으로 수행되는 통합 시스템의 속성을 유지하고 있다.

취약성에 대한 가장 근접한 분석 데이터는 시스템 보안에 있어서의 가장 기초적인 요소가 되어야 하며, 그 네트워크 정보 시스템은 복구 능력을 갖춘 보안 시스템으로 재구성됨으로써 미래의 지능적이고 예상하지 못한 치명적인 공격에 대응할 수 있는 기반이 될 것이다.

이 연구를 기초로 하여 향후에는 Survivability 뿐만이 아니라 Security와 S/W 공학적인 접근을 통한 S/W Rejuvenation의 개념을 활용한 Fault Tolerant System에 대해서 연구할 것이다.

Acknowledgements

본 논문은 과학기술부. 한국과학재단 지정 경기도 지역협력연구센터(RRC)인 한국항공대학교 인터넷정보검색연구센터의 지원에 의한 것임.

본 논문은 지능형 네트워크 보안 관리 시스템 개발의 부분으로 산업자원부의 산업기술 개발사업(Spin-off)의 지원에 의한 것임.

참고문헌

[1] Yurcik, W. and Doss, D "A Survivability - Over - Security(SOS) Approach to Holistic Cyber-Ecosystem Assurance", Proceedings of the 2002 IEEE, Workshop on Info. Assurance, United States Military Academy, West Point, NY June 2002.

[2] J.S. Lee et al, "Simulation-based Vulnerability Analysis", IEICE Transactions on Information and Systems(Submitted)

[3] S.D. Chi et al, "Network Security Modeling and Cyber-attack Simulation Methodology", Lecture Notes on Computer Science series, 6th Australian Conf. on Information Security and Privacy, Sydney, July, 2001.

[4] Andrew P. Moore, Robert J. Ellison and Richard C. Linger "Attack Modeling for Information Security and Survivability", Technical Note, CMU/SEI-2001-TN-001, March 2001.

[5] Yurcik, W. and Tipper, D. "Survivable ATM Group Communications: Issues and Techniques." 8th Intl. Conf. on Telecom. Systems, pp. 518-537, 2000

[6] Patton, S., Yurcik, W., and Doss, D. "An Achilles'Heel in Signature-Based IDS: Squealing False Positives in SNORT," 4th Intl. Symp. on Recent Advances in Intrusion Detection (RAID), University of California - Davis, 2001.

[7] Grzywa, M., Yurcik, W., and Brumbaugh, L. "Application-Level Survivability: Resumable FTP," IEEE Military Communications Conference (MILCOM), 2001