[10-56]

역추적장치기능을 응용한 종합침해사고 대응시스템연구

* 신승중 * 최운호 * 황경준 ** 진승할
* 한세대학교 * 한세대학교 * 한세대학교 ** 군포창업보육센터
* expersin@hansei.ac.kr, bzs320@hansei.ac.kr, harri@hanmir.com

A Study of Function to Automated Traceback when Computer Virus/Worm Attack on Integrated Computer Emergency Response System

* Seung-Jung Shin * woon-ho Choi * kyeong-joon Hwang ** sheong-hal Jin
* hansei university * hansei university * hansei university **kbi

요약

본 논문에서는 인터넷환경에서 증가하는 컴퓨터 바이러스/웜의 공격에 의한 침해사고 발생 시 정의되어야할 정보와 이를 활용한 대량 트래픽을 발생시키는 탐지하는 방안을 제안하였다. 이에 따라 종합 침해사고 대응시스템에서의 자동화된 역추적 방안에 대한 설계와 기능에 대한 개념을 제시한다.

Ⅰ. 서론

인터넷의 발달로 악의를 가지고 침입하여 개인정보와 신용카드, 인터넷뱅킹에 사용되는 공인인증체계의 정보 등 금융신용정보가 유통되는 시스템의 정보를 획득한 후 불법적인 일에 사용하는 경우가 자주 발생하고 있으며 컴퓨터 바이러스나 웜 등을 확산시켜 정보를 파괴하거나, 중요서비스를 마비시켜 정보통신기반보호법에 규정된 중요시설 에 대한 사이버 테러나 해킹 등 사이버 범죄를 일으키고 있다.

종래에 이러한 해킹 등의 침해 사고를 처리하기 위해서는 피해자가 일일이 해당 시스템에 대한 피해 정도나 관리자, 블랙리스트(IP 주소와 같은), 사고 발생 시점까지의 해당 시스템에 대한 로그/패치 정보, 이력 관리 그리고 백업 등에 관한 정보 등을 침해사고대응팀 (CERT : Computer Emergency Response Team; 이하 "CERT"라 한다)) 등의 정보보호 전문 기관에 전화나 이메일로 상담하며, 해당 전문 기관에서는 각각의 상담 내용을 자신의 시스템으로 수동 입력하고 이를 근거로 침해 사고 내용을 분석하여 판단하고 있다.

또한, 각 조직의 정보보호 담당자가 자신이 보유한 시스템의 취약성 및 이력을 상세히 파악하여, 새로 나오는 취약점을 매일 패치하고, 이를 연계하여 침입탐지시스템에서 알려주는 공격 정보에 효과적으로 대응하기는 더더욱 어려우며, 수시로 발생하는 악성 바이러스 및 웜에 실시간 대응도 못하는게 현실적인 문제점이다. 이렇듯, 회사의 중요 정보 시스템 및 전산센터/전산시스템 그리고 금융, 통신 등 정보통신기반보호법(법률 6383 호) 상에 정의된 주요 정보통신 기반시설 (CIP : Critical Infrastructure Protection)과 같은 여러 중요한 시스템을 해킹이나 사이버테러로부터 보호해야할 필요가 대두되고 있음에도 그에 대한 효율적이고 일괄적인 방법이 제시되지 못하고 있는 실정이다.

본 논문에서는 정보보호관련 정보의 안전한 공유시스템 및 네트웍 제공, 각 침해사고에 대한 공격평가와 조기 경보가 가능하며, 새로운 침해사고에 대한 테스트(시뮬레이션)를 수행하고, 조기경보시스템 (EWIS(EarlyWarning Information System)) 설계와 기능에 대한 개념을 논의한다.