[일반 과제] 2주차 출석 및 학습 확인

강릉원주대학 / 컴퓨터공학과 / 20171468 / 장성원

1. **정보보호의 3대 목표 설명**

정보보호의 3대 목표에는 기밀성, 무결성, 가용성이 있다. 3대 목표 이외에도 6대 목표로는 책임추적성, 인증, 신뢰성이 있다.

1. 기밀성(confidentiality)

* 기밀성은 정보의 소유자가 원하는 대로 정보의 비밀이 유지되어야 하는 원칙이 있다.
* 정보는 소유자의 인가를 받은 사람만이 접근할 수 있어야 하며, 인가되지 않은 정보의 공개는 반드시 금지된다.
* 기밀성을 보장하기 위하여 접근 통제(물리적 운영체제, 네트워크 등)와 암호화 등을 이용한다.

1. 무결성(Integrity)

* 무결성이란 비인가 된 자에 의한 정보의 변경, 삭제, 생성 등으로부터 보호되어야 한다.

1. 가용성(availability)

* 정보시스템은 적절한 방법으로 작동되어야 하며, 정당한 방법으로 권한이 주어진 사용자에게 정보서비스를 거부하여서는 안 된다는 원칙이 있다.

1. **악성 프로그램의 종류 및 설명**

악성 프로그램은 정당한 사유 없이 정보통신 시스템, 데이터 또는 프로그램 등을 훼손, 파괴, 변경 위조 또는 그 운용을 방해할 수 있는 프로그램이다.

맬웨어(malware, malicious software), 악성코드(malicious code)라고도 하며 컴퓨터에 악영향을 줄 수 있는 모든 소프트웨어의 총칭이다.

1. 웜(Worm)

* 다른 프로그램의 감염 없이 자신 혹은 변형된 자신을 복사하는 명령어들의 조합이다.
* 기억장소에 코드 형태로 존재하거나 혹은 실행파일로 존재하며 실행되면 파일이나 코드 자체를 다른 시스템으로 복사한다.
* 정보시스템을 파괴하거나 작업을 지연·방해하는 악성 프로그램의 일종으로 바이러스와는 달리 감염 대상을 갖고 있지 않으며, 독립적인 프로그램으로 번식력을 가지고 있다.

1. 컴퓨터 바이러스

* 실행 가능한 프로그램 일부분 혹은 데이터에 자기 자신 혹은 변형된 자신을 복사하는 명령어들의 조합이다.
  + 부트 바이러스(Boot Virus)
    - 시스템이 부팅되는 과정을 이용하여 플로피와 하드 디스크의 부트 영역을 감염시키며, 대부분의 초기 바이러스들이 여기에 속한다.
  + 파일 바이러스(File Virus)
    - 파일 자체가 실행되는 과정을 이용하여 COM, EXE, SYS 파일 등에 감염되며, 전체 바이러스의 90% 이상이 파일 바이러스로 구분된다.
  + 부트/파일 바이러스(Boot/File Virus)
    - 부트와 파일을 동시에 감염하는 형태로 바이러스 크기가 매우 커지고 복잡하다.
  + 매크로 바이러스(Macro Virus)
    - 1995년 여름에 처음으로 발견된 매크로 바이러스는 감염 대상이 실행 파일이 아니라 마이크로소프트사의 엑셀과 워드 프로그램에서 사용하는 문서 파일이다.

1. 트로이 목마

* 감춰진 코드를 갖고 있는 프로그램으로 작동이 되면 원하지 않거나 해가 되는 기능을 수행한다.
* 자기 복제 능력이 없다.

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 컴퓨터 바이러스 | 트로이 목마 | 웜 |
| 복사 및 전염 능력 | 있음 | 없음 | 매우 강함 |
| 형태 | 파일이나 부트 섹터 등 감염대상이 필요 | 유틸리티로 위장하거나 유틸리티 안에 코드 형태로 삽입 | 독자적으로 존재 |
| 전파 경로 | 사용자가 감염된 파일을 옮김 | 사용자가 내려 받음 | 네트워크를 통해 스스로 전파 |
| 주요 증상 | 해당 컴퓨터의 시스템 및 파일 손상 | PC 성능 저하, 좀비 PC | 네트워크 성능 저하 |

1. 다양한 악성 프로그램

|  |  |
| --- | --- |
| 종류 | 정의 |
| 루트킷(Rootkit) | 루트 권한을 획득한 공격자가 심어놓은 프로그램을 숨기기 위한 목적으로 사용됨 |
| 백도어(back door) | 원래는 서비스 기술자나 유지보수 프로그래머들의 다른 PC에 대한 액세스 편의를 위해 시스템 설계자가 고의적으로 만들어 놓은 것으로 허가 받지 않은 사용자가 네트워크에 들어갈 수 있을 만큼 허술한 부분을 일컬음 |
| 스파이웨어(spyware) | 사용자의 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성 소프트웨어로, 신용카드와 같은 금융정보 및 주민등록번호와 같은 신상정보, 암호를 비롯한 각종 정보를 수집함 |
| 키로깅(Keylogging) | (키 스트로크 로깅(Keystroke logging)으로도 불린다) 사용자가 키보드로 PC에 입력하는 내용을 몰래 가로채어 기록하는 행위를 말한다 |
| 봇(bot) | 인간이 하는 행동을 흉내 내도록 만들어진 프로그램을 의미 |
| 스턱스넷(Stuxnet) | 산업기반시설의 제어시스템(SCAKA) 가운데 독일 지멘스사의 제품을 공격 목표로 하여 제작된 악성코드(10.6월 발견). 원자력 등 주요 산업기반시설의 제어시스템에 침투해 오작동을 일으키며, USB 및 네트워크 공유폴더 등을 통해 전파된다. |
| 고스트넷(GhostNet) | 특정 컴퓨터를 감염시켜 장악한 뒤 원격 조정할 수 있는 스파이 네트워크로, 해커는 파일을 검색하거나 내려 받을 수 있고 촬영이나 녹음을 지시할 수도 있다. |
| 웹셸(Web Shell) | 해커가 원격으로 웹서버를 조종할 수 있도록 제작한 악성코드로 공격자가 수시로 드나들 수 있다는 일종의 비밀통로 역할을 한다 |

1. **접근 통제 보안 모델 중 벨-라파듈라 모델과 비바 모델의 차이점 기술**

* 접근 통제 보안 모델은 보안이 구현되는 방법으로 정보시스템에 대한 접근 통제 규칙을 기술한 정형화한 것으로 시스템 보안을 위한 규칙과 주체의 객체 접근 허용 범위를 규정하고 있다.

1. 벨-라파듈라 모델(Bell-LaPadula Model)은 허가되지 않은 방식의 접근을 방지하는 모델로 MAC 방식의 접근을 제어하며 시스템 내부에 있는 정보의 기밀성을 보호하지만, 비바 모델(Biba Model)은 데이터 무결성에 초점을 둔 상업용 모델이다. 비인가자들의 데이터 변형 방지만 취급한다.
2. 벨-라파듈라 모델에서의 주체는 보다 높은 보안 수준의 데이터를 읽을 수 없지만(no read up), 비바 모델에서의 주체는 보다 낮은 무결성의 정보를 읽을 수 없다(no read down).
3. 벨-라파듈라 모델에서의 주체는 데이터를 보다 낮은 보안 수준의 객체에 기록할 수 없지만(no write down), 비바 모델에서의 주체는 보다 높은 무결성의 수준의 객체를 수정할 수 없다(no write up).