정보통신망 제 14 강

네트워크 보안(I)

컴퓨터과학과
손진곤 교수

학습 목차

제 14 강 네트워크 보안 (I)

학습 내용

- 네트워크 보안 개요
  - 필요성
  - 보안의 종류
  - 네트워크 보안의 요구 사항
- 네트워크 보안 위협 유형
  - 사람(제3자, 통신 당사자)
  - 악성 프로그램
  - 기타 위협 요소

학습 목표

- 보안의 목표 3가지를 설명할 수 있다.
- 네트워크 보안의 요구사항에 관하여 설명할 수 있다.
- 네트워크 보안을 침해하는 위협 요소들을 유형별로 구분할 수 있다.
  (제3자, 통신 당사자, 악성 프로그램, 기타)

1. 개요

(1) 보안의 필요성

(2) 보안의 종류

(3) 네트워크 보안의 요구 사항

1 보안의 필요성

보안의 필요성

- 종이 문서와 전자 문서의 차이
- 정보통신망을 통한 문서의 공개

1 보안의 필요성

보안의 3가지 목표 : 보안 원칙

- 기밀성 (confidentiality)
  - 허가되지 않은 사람에게 정보가 노출되지 않는 것을 보장
- 무결성 (integrity)
  - 허가되지 않은 사람에 의해 정보가 변경되지 않는 것을 보장
- 가용성 (availability)
  - 허가된 사람에게 부당한 지체 없이 정보가 접근되고 사용할 수 있도록 하는 것을 보장

2 보안의 종류

보안의 종류

- 시스템 보안
- 네트워크 보안

2 보안의 종류

시스템 보안

- 권한이 없는 사람에 의한 파일 및 장치 등의 사용을 제한함으로써 시스템을 보호하는 방법

- 시스템 보안 방법
  - 접근통제 : 권한이 있는 사용자들에게 접근을 제한
  - 감시통제 : 시스템에서의 활동을 감시

2 보안의 종류

네트워크 보안

- 내부 네트워크가 인터넷과 같은 외부의 네트워크와 연결되면서 내부 조직의 네트워크 보안이 점점 중요해지고 있음
  - 예 : 인터넷 뱅킹, 전자상거래, 각종 증명서 발급 (공인인증서 이용)
- 권한이 없는 사람의 접근이나 우연 또는 의도적인 방해나 파괴로부터 네트워크를 보호하기 위한 방법
- 하드웨어나 소프트웨어, 인위적인 보안 조치를 총칭

3 네트워크 보안의 요구 사항

네트워크 보안의 요구 사항

① 실체 인증
- 통신에 참여한 실체에 대한 진위 검증

② 데이터 무결성
- 데이터가 파괴되거나 변경되지 않도록 보호

③ 데이터 보안성
- 정보의 비밀 보장, 합법적 사용자의 접근 보호

④ 데이터 인증
- 데이터가 신뢰할 수 있는 발신처에서 전송된 것인지 확인

⑤ 부인 방지
- 데이터의 수신이나 전송 사실에 대한 확인

2. 네트워크 보안 위협 유형

(1) 제3자에 의한 불법적인 공격 유형
(2) 통신 당사자 간의 부정 유형
(3) 악성 프로그램의 감염 유형
(4) 기타 유형

보안 위협 유형

유형 분류

- 사람
  - 제3자, 통신 당사자 (송신자, 수신자)

- 악성 프로그램
  - 바이러스, 웜, 트로이 목마

- 기타
  - phishing, pharming

1 제3자에 의한 불법적인 공격 유형

제3자에 의한 불법적인 공격 유형

1) 가로채기 (interception) – 기밀성 위협
2) 변조 (modification) – 무결성 위협
3) 위조 (fabrication) – 무결성 위협
4) 방해 (interruption) – 가용성 위협
5) 서비스 거부 (Denial of Service) – 가용성 위협

1 제3자에 의한 불법적인 공격 유형

(1) 가로채기 (interception)

- 공격자가 전송되고 있는 정보를 몰래 열람, 또는 도청하는 행위
- 예 : 네트워크 상에서 개인 정보 데이터를 부정한 방법으로
  복사하거나 도청하는 행위 등

- 정보의 기밀성 (confidentiality) 보장을 위협

1 제3자에 의한 불법적인 공격 유형

(2) 변조 (modification)

- 공격자가 시스템에 접근하여 데이터를 조작하여
  원래의 데이터를 다른 내용으로 바꾸는 행위
- 예 : 송수신자가 알아채지 못하도록 전송 중인 메일 내용을
  변경하거나 데이터 파일 내의 값들을 변경하는 것

- 정보의 무결성 (integrity) 보장을 위협

1 제3자에 의한 불법적인 공격 유형

(3) 위조 (fabrication)

- 공격자가 거짓 정보나 잘못된 정보를 삽입하여 수신자에게 전송하고 수신자가 정당한 송신자로부터 정보를 수신한 것처럼 착각하도록 만들어 이를 통해 이득을 보려는 행위
- 예 : 위조된 메시지를 수신자에게 전송하는 행위 등

- 정보의 무결성 (integrity) 보장을 위협

1 제3자에 의한 불법적인 공격 유형

(4) 방해 (interruption)

- 송신자와 수신자 간의 정보 송수신이 원활하게 이루어지지 못하도록 시스템의 일부를 파괴하거나 사용할 수 없게 하는 행위
- 예 : 통신회선의 절단이나 파일 관리 시스템의 파손 등

- 정보의 가용성 (availability) 보장을 위협

1 제3자에 의한 불법적인 공격 유형

(5) 서비스 거부 (Denial of Service ; DoS)

- 공격자가 처리 용량을 넘는 데이터를 전송하여 과도한 부하를 일으켜 시스템을 마비시킴으로써 정당한 이용자가 시스템을 사용하지 못하게 만드는 행위
- 예 : 메일 서버 시스템에 엄청난 양의 스팸 메일을 보내
  시스템의 원활한 서비스를 방해하는 행위 등

- 분산 서비스 거부 (Distributed DoS)

- 정보의 가용성 (availability) 보장을 위협

2 통신 당사자 간의 부정 유형

통신 당사자 간의 보안 위협

- 부정 (사기; fraud)
- 송신자
  - 송신 자체를 부인
- 수신자
  - 수신 자체를 부인
- 부인 봉쇄 방법의 필요

3 악성 프로그램의 감염 유형

(1) 컴퓨터 바이러스(computer virus)

- 컴퓨터에서 실행되는 일종의 명령어들의 집합으로서
  컴퓨터 프로그램이나 데이터 파일을 감염시킴
- 감염은 정상 파일에 바이러스 코드를 붙이거나
  본래 목적 이외의 작업을 처리하며 동시에 자신을 복제시킴
- 증상
  - 컴퓨터 부팅 시간이 오래 걸리거나 부팅이 안 되는 증상
  - 프로그램이 오동작하거나 동작되지 않는 증상
  - 저장된 데이터가 변조되거나 삭제되는 증상 등
- 최신 바이러스 백신 사용

3 악성 프로그램의 감염 유형

(2) 웜 (worm)

- 네트워크를 통해서 자신을 복제, 전파할 수 있는 프로그램
- 감염시키지 않고도 복제할 수 있음
- 감염 경로 : email, P2P, 메신저 등
- 주요 피해 유형
  - DDoS
  - 침입자가 시스템에 쉽게 접근할 수 있는 통로 제공

3 악성 프로그램의 감염 유형

(3) 트로이 목마 (Trojan horse)

- 컴퓨터 사용자의 정보를 빼내가기 위한 목적으로 제작된 악성 프로그램
- 악성 코드를 유틸리티 프로그램에 내장하여 배포하거나
  그 자체를 유틸리티 프로그램으로 위장하여 배포함
- 자기 복제능력 없음

4 기타 유형

(1) 피싱 (Phishing)

- Private information + Fishing
- 인터넷에서 송신자를 알리지 않는 스팸 메일을 이용하여
  수신자의 개인 정보를 빼낸 뒤 이를 불법적으로 이용하는 범죄
- 예
  - 거짓 이메일을 통해, 가짜 웹 사이트로 유인하여
    신상 정보를 요구
  - 이벤트, 설문조사 등
  - 전화를 이용한 피싱도 있음 (voice phising)

4 기타 유형

(2) 파밍 (Pharming)

- Phishing + Farming
- 정당한 웹 사이트의 도메인을 탈취하거나 DNS 이름을 속여 미리 정해 놓은 웹 사이트로 data traffic을 유인한 뒤, 개인 정보를 빼낸 뒤 이를 불법적으로 이용하는 범죄
- 피싱의 한 유형이지만 더 위협적임

학습 내용 정리

제 14 강 네트워크 보안(I)

(1)보안

- 필요성
- 보안의 3가지 목표 : 기밀성, 무결성, 가용성
- 보안의 종류 : 시스템 보안, 네트워크 보안
- 네트워크 보안의 요구 사항
  - ➢ 실체 인증, 데이터의 무결성,
    보안성, 인증, 부인 방지

학습 내용 정리

제 14 강 네트워크 보안(I)

(2)보안 위협 요소

- 제3자에 의한 위협
  - 변조, 위조, 가로채기, 방해, 서비스 거부
- 송수신자에 의한 부정
- 악성 프로그램
  - 컴퓨터 바이러스, 웜, 트로이 목마
- 기타 위협 요소 : 피싱, 파밍

다음 차시 강의

제 15 강 네트워크 보안(II)

(1) 네트워크 보안 강화 방법

- 암호 기법
- 디지털 서명
- 웹 보안 프로토콜
- 방화벽
- 프락시 서버

좋은 글, 좋은 생각

白頭山石磨刀盡 백두산의 돌들을 칼 가는데 다 쓰고

豆滿江水飮馬無 두만강의 물을 말 먹이는데 다 쓰며

男兒二十未平國 남자가 20살에 나라를 지키지 못한다면

後世誰稱大丈夫 훗날 누가 대장부라고 부르겠는가

- 남이(南怡) 장군 (세조시대 병조판서)

-이 시에서 '未平國'을 '未得國'으로 고쳐 모반을 꾀한다고 모함을 받아 죽음