중간고사 정리

보안의 3대 목표

- 기밀성

정보 보안에서 가장 널리 알려진 분야로, 조직은 정보의 기밀성을 위협하는 악의적인 행동들에 대응해야 하고 군대에서는 민감한 정보가 노출되는 것을 방지해야 한다. 그리고 산업체에서는 조직의 운영을 위하여 필수적으로 경쟁자에게 정보를 숨겨야 하고, 은행 업무를 볼 때, 고객의 계좌 정보는 보호되어야 한다.

- 무결성

변경이 인가된 자에 의해서 인가된 매커니즘을 통해서만 이뤄져야 한다는 것으로, 은행에서 고객이 돈을 입금하거나 출금할 때, 그 계좌의 금액을 변경되어야 한다. 그러나 무결성 왜곡이 항상 악의적인 행동의 결과로 나타나는 것이 아니다.

- 가용성

인가된 자가 접근할 수 있어야 한다는 것으로, 조직이 생산하고 저장하는 정보는 인가된 자가 사용할 수 있어야 하며, 정보가 유용하지 않으면 쓸모가 없다.

5개의 보안 서비스

(1) 데이터 기밀성

데이터 기밀성은 노출 공격으로부터 데이터를 보호하기 위하여 고안되었다. 매우 광범위하고, 메시지의 일부분이나 전체에 대한 기밀성을 포함하며 트래픽 분석에 대응한다. 데이터 기밀성은 스누핑과 트래픽 분석 공격을 막기 위하여 고안되었다.

(2) 데이터 무결성

공격자가 데이터의 변경, 삽입, 삭제, 재전송 등으로부터 데이터를 보호하는 것이며 메시지의 일부나 전부를 보호한다.

(3) 인증

이 서비스는 통신의 상대편에 대한 인증을 제공한다. 연결형 통신에서는 연결 설정 시 송신자 또는 수신자에 대한 인증을 제공하고, 비연결형 통신에서는 데이터의 출처를 인증한다.

(4) 부인봉쇄

데이터의 송신자나 수신자가 부인하기 못하도록 한다. 출처 증명을 제공하는 부인봉쇄에서 데이터의 수신자는 그 메시지가 부인될 경우 송신자의 신원을 증명할 수 있다. 배송 증명을

제공하는 부인봉쇄에서는 데이터의 송신자가 이후에 의도된 수신자에게 데이터가 전달되었음을 입증할 수 있다.

(5) 접근 제어

비인가된 접근으로부터 데이터를 보호한다. 접근이라는 용어는 매우 광범위하고, 읽기, 쓰기, 변경, 프로그램 실행 등을 포함한다.

8개의 보안 메커니즘

(1) 암호화

데이터를 숨기거나 보호하는 것은 기밀성을 제공할 수 있으며 다른 서비스를 제공하기 위한 다른 메커니즘을 보완하는데 이용될 수도 있다. 오늘날 암호와 스테가노그래피 등의 두 기술은 암호화에 이용된다.

(2) 데이터 무결성

데이터 자체를 이용하여 특정 프로세스에 의해 생성된 짧은 검사값을 데이터에 추가한다. 수신자는 데이터와 검사값을 받는다. 수신자는 수신한 데이터에서 새로운 검사값을 생성하여 수신된 검사값과 비교한다. 두 개의 검사값이 같은 경우에 있어서 데이터의 무결성은 보장된다.

(3) 디지털 서명

송신자가 전자적으로 데이터에 서명을 하고 수신자가 전자적으로 그 서명을 검증할 수 있는 방법이다. 송신자는 공개적으로 알려진 자신의 공개 키와 개인 키를 갖고 있음을 입증하는 절차를 진행한다. 수신자는 메시지가 메시지를 보냈다고 주장하는 송신자에 의해 서명된 것임을 증명하기 위해 송신자의 공개 키를 사용한다.

(4) 인증 교환

두 사람은 자신의 신원을 알고 있는 다른 사람에게 증명하기 위하여 어떤 메시지를 교환한다. 예를 들어, 사용자는 자신만이 알고 있는 비밀을 자신이 알고 있다고 증명할 수 있다.

(5) 트래핑 패딩

공격자가 트래픽 분석을 하지 못하도록 방해하기 위하여 데이터 트래픽에 가짜 데이터를 삽입하는 것을 의미한다.

(6) 라우팅 제어

공격자가 특정 경로에서 도청하지 못하도록 송신자와 수신자 사이에 다른 가용 경로를 선택하고 지속적으로 변화시키는 것을 의미한다.

(7) 공증

두 사람 사이의 통신을 제어하기 위하여 신뢰할 수 있는 제 3자를 선택하는 것을 말한다. 예를 들어, 이 방법은 부인봉쇄에 이용될 수 있다. 수신자는 송신자가 추후에 자신이 그러한 요청을 했다는 것을 부인하지 못하도록 믿을 만한 제 3자에게 송신자의 요청을 저장하도록 할 수 있다.

(8) 접근 제어

사용자가 시스템의 데이터나 데이터 출처에 대한 접근권을 가지는 지 여부를 입증하기 위한 방법을 사용한다. 입증의 예로 패스워드나 PIN 등이 있다.

보안 목표를 위협하는 공격 유형

기밀성

(1) 스누핑

데이터에 대한 비인가 접근 또는 탈취를 의미한다. 예를 들어, 인터넷으로 전송되는 파일은 기밀 정보를 담고 있을 수 있다. 비인가자가 전송되는 메시지를 가로채고 자신의 이익을 위하여 그 내용을 사용할 수 있다.

(2) 트래픽 분석

비록 데이터를 암호화하여 도청자가 그 데이터를 이해할 수 없다고 할지라도, 도청자는 온라인 트래픽을 분석함으로써 다른 형태의 정보를 얻을 수 있다. 예를 들어, 도청자는 수신자 또는 송신자의 전자 주소를 알아낼 수 있으며 전송의 성향을 추측하는데 도움이 되는 질의와 응답의 쌍들을 수집할 수 있다.

무결성

(1) 변경

공격자는 정보를 가로채거나 획득한 후 자신에게 유리하도록 정보를 조작한다. 때로 공격자가 시스템에 해를 입히거나 이익을 얻기 위하여 메시지를 지우거나 전송을 지연시킬 수 있다.

(2) 가장

다른 사람으로 위장할 때 가장 또는 스푸핑 공격이 행해진다. 예를 들어, 공격자는 은행 고객의 현금 카드나 PIN을 훔쳐서 그 고객으로 위장할 수 있다. 때로는 공격자가 수신자로 가장하기도 한다.

(3) 재전송

공격자는 사용자가 보낸 메세지 사본을 획득하고 나중에 그 메시지를 다시 사용한다.

(4) 부인

송신자에 의한 부인의 예로서, 은행 고객은 자신의 은행이 제 3자에게 돈을 송금하도록 요청하고 나중에 그러한 요청 사실을 부인하는 경우가 있다. 수신자에 의한 부인은 어떤 사람이 상점에서 물건을 사서 전자 지불을 했지만 상점에서 나중에 지불한 사살을 부인하고 지불 요청을 하는 경우를 볼 수 있다.

가용성

(1) 서비스 거부

DoS는 시스템의 서비스를 느리게 하거나 완전히 차단할 수 있다. 공격자는 서버의 과부하로 서버가 다운될 정도로 많은 거짓 요청을 보낼 수 있고, 고객이 서버가 대답하지 않는다고 믿게 하면서, 서버가 고객에게 대답하는 것을 가로채거나 지울 수 있다. 또한 고객의 요청을 가로채어 고객이 시스템에 많은 요청을 보내도록 함으로써 시스템에 과부하가 걸리도록 한다.