HomeWork #1 연습문제

정보보안 이론과 실제

1장

1. 비밀성, 무결성, 가용성은 정보보안의 근본 주제이다. 비밀성은 필요하지만 무결성은 필요 없는 업무의 예를 제시하라. 그리고 반대로 무결성은 필요하지만 비밀성은 없어도 되는 업무의 예를 제시하라. 마지막으로, 가용성이 절대적으로 필요한 업무의 예를 제시하라.

답변

우선, 비밀성은 필요하지만 무결성은 필요 없는 업무의 예로는 패스워드를 들 수 있다. 패스워드는 바뀌어도 큰 문제는 없지만, 패스워드가 노출된다면 큰일이다.
다음으로, 무결성은 필요하지만 비밀성은 없어도 되는 업무의 예로는 메시지의 목적지 주소이다. 누군가 그 주소를 본다고 메시지가 목적지로 가는데 있어서 큰 문제가 없지만 그 주소를 바꾼다면 메시지는 목적지로 가지 못할 것이다.
마지막으로, 가용성이 절대적으로 필요한 업무의 예로는 웹 서버 관리이다. 예를 들어 이번처럼 큰 지진이 발생했을 때 기상청의 웹 서버가 마비되지 않도록 할 수 있어야 한다.

4. 어떤 저자는 보안을 프라이버시 및 비밀성으로 구분한다. 이러한 용어 사용에 있어서 보안은 이 책에서 사용하는 비밀성과 동일하다. 반면에 프라이버시는 개인적인 데이터나 비밀성에 적용되는 보안으로, 정해진 정보가 누설되지 않도록 해야 하는 의무를 의미한다. 프라이버시가 요구되는 예를 들어 보자. 상기한 의미에서 비밀성의 예를 제시하라.

답변

프라이버시의 예로는 간단하게 인터넷에 연결된 체중계를 생각해보자. 현대 여성에게 있어서 체중은 중요한 개인 데이터이기 때문에 전송 중 누설되어선 안 된다.
이 책에서 사용하는 비밀성의 예로는 흔히 사용하는 패스워드를 들 수 있다. 패스워드는 허가되지 않는 자, 즉 본인이 아닌 다른 사람은 읽을 수 없어야 한다.

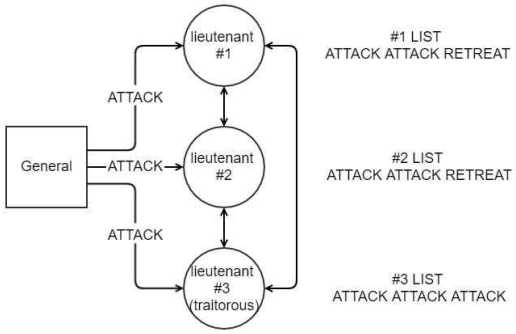
5. 참고문헌 [129]번을 읽어 보자. 여기서 비잔틴의 실패(Byzantine Failures) 문제를 기술하고 만약에 4명의 장군이 있고 그 중 한 명만 배신자라면 문제가 발생하는 이유를 설명하라. 이러한 문제가 정보보안 문제와 관계가 있는지 이유도 설명하라.

답변

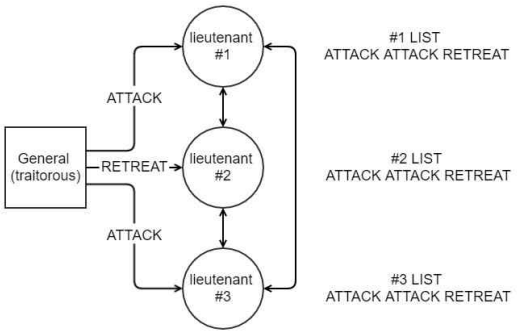
비잔틴의 실패(Byzantine Failures) 문제는 한 도시를 비잔틴의 장군들과 그들의 군대가 포위하고

있는 상황에서 시작된다. 이 문제의 조건을 먼저 살펴보자. 먼저, 장군들은 반드시 어떤 행동에 대한 동의를 해야 한다. 그 행동에는 그 도시를 공격할지 혹은 후퇴할지가 있다. 장군들 중 몇몇은 배신자이고, 그들은 충성스러운 장군들이 만장일치로 합의 보는 것을 막고 싶어 한다. 또는 충성스러운 장군들이 서로 다른 계획에 동의하도록 만들고 싶어 한다. 장군은 다른 어떤 장군이든지 통신병을 통해 직접 메시지를 전달할 수 있다. 그리고 다른 장군들을 통해 구두로 혹은 편지로 메시지를 전달할 수 있다.(단, 구두로 전달된 메시지는 중간에 있는 장군에 의해 변조되어질 수 있다. 그에 반해 편지는 수정될 수 없다.) 통신병은 믿을 수 있다고 가정한다. 여기서 중요한 점은 장군 중 누가 배신자이고 누가 충신인지는 가려내지 않는다.
이때, 문제는 바로 "충성스러운 장군들 사이에 합의가 나는 것이 불가능하기까지 몇 명의 배신자가 있어야 하느냐?"이다. 문제의 답은 메시지를 구두로 전달하느냐, 편지로 전달하느냐에 따라 다르다.

4명의 장군이 있고 그 중 한 명만 배신자인 경우는 결론부터 말하자면 구두로 전달하든, 편지로 전달하든 항상 일치된 의견으로 수렴한다.
먼저, 편지의 경우 최소 3명 이상의 장군이 있다면 편지를 조작할 수 없다는 조건 때문에 누가 배신자인지 알 수 있다. 그래서 항상 일치된 의견을 가질 수 있다.
다음으로, 구두로 전달할 때는 조금 복잡해진다.
우선, 4명의 장군 중에서도 상급자 한명 동급자 3명으로 나누어보자. 상급자는 각 세 명에게 메시지를 전달한다. 첫 번째 경우, 만약 상급자가 배신자라면, 메시지는 공격 1표, 후퇴 2표 혹은 후퇴 2표 공격 1표로 전달할 것이다. 두 번째 경우, 반대로 상급자가 배신자가 아니라면, 메시지는 일관성을 가질 것이다.
그리고 동급자 3명끼리 상급자에게 받은 메시지를 교환한다고 생각해보자. 그렇게 되면 어떤 경우에서도 충실한 자들은 다수의 메시지를 선택하여 일치된 의견을 가질 수 있게 된다. 글로는 설명이 어려우니 간단한 다이어그램을 그려보자.



동급자 중 한 명이 배신자일 경우



상급자가 배신자일 경우

이러한 문제는 정보보안 문제와도 관계가 있다. 비쟌틴의 실패 문제에서 배신자를 트루디, 전달하는 메시지를 네트워크 통신 메시지라고 보면 충분히 그 관계성을 눈치 챌 수 있을 것이다. 메시지를 구두로 전달하는 것과 편지로 전달하는 것은 데이터 무결성을 보장하는가에 대한 것으로, 무결성을 보장하지 않는다면 트루디의 수에 따라 메시지가 일치되는 것이 불가능할지도 모른다. 하지만 무결성이 보장된다면 비쟌틴의 실패는 있을 수 없다. 그만큼 무결성의 중요성을

강조하고 있다. (teamten Lawrence Kesteloot가 대학 졸업 논문으로 작성한 내용을 기반으로 하였으며, 풀이 과정에는 2가지의 가정이 존재한다. 이는 생략하도록 한다.)

2장

7. 암호학 측면에서 혼돈과 확산의 개념을 정의하라. 고전암호에서 혼돈만 적용된 암호와 확산만이 적용된 암호를 구분해 설명하라. 또 이 장에서 다룬 암호 중에서 혼돈과 확산이 모두 적용된 암호는 어떤 것일까?

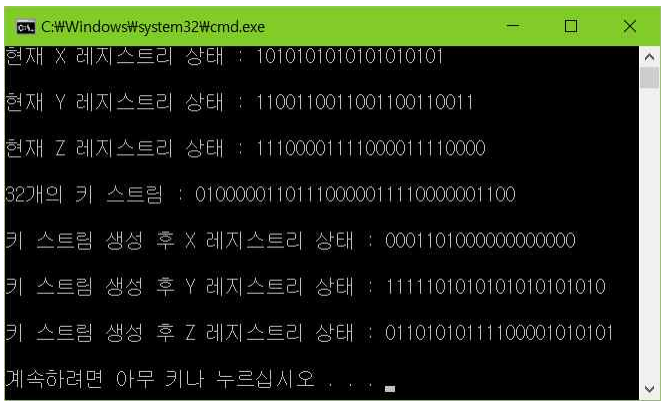
답변

혼돈의 정의는 암호문의 비트 각각이 키의 일부분에 의존해야만 하는 것이다. 쉽게 말해, 평문과 암호문이 쉽게 이해하기 힘든 관계를 가지고 있는 특성이다.
확산의 정의는 예를 들어 평문의 한 비트를 바꾸면 통계적으로 암호문의 절반이 바뀌어야 하고, 반대로 암호문의 한 비트를 바꾸면 거의 평문의 절반이 바뀌어야하는 것을 의미한다. 즉, 평문의 통계적인 성격을 암호문 전반에 확산시킬 수 있다.
2장에서 혼돈과 확산이 모두 적용된 암호는 마지막 잠깐 소개가 되었던 대칭키 암호체계의 '블록 암호'가 있다. 간단한 블록 암호인 DES를 보면 Function 연산을 통해 혼돈을 만족시키고 매 Round마다 비트열의 자리를 바꾸어 확산도 만족시킨다.

3장

8. A5/1 알고리즘을 구현하라. 특정 단계 후에서의 레지스트리들의 값은 다음과 같다고 가정하라.
X = $(x_0, x_1, \ldots, x_{18})$ = (1010101010101010101)
Y = $(y_0, y_1, \ldots, y_{21})$ = (11001100110011001100110011)
Z = $(z_0, z_1, \ldots, z_{22})$ = (11100001111000011110000)
다음 32개 키스트림을 생성해 출력하라. 32개 키스트림이 생성된 다음의 X, Y, Z의 내용을 출력하라.

32개 키스트림 = $(s_0, s_1, \ldots, s_{31})$ = (01000001101110000011110000001100)
X = $(x_0, x_1, \ldots, x_{18})$ = (0001101000000000000)
Y = $(y_0, y_1, \ldots, y_{21})$ = (11111010101010101010)
Z = $(z_0, z_1, \ldots, z_{22})$ = (01101010111100001010101)



C로 구현한 A5/1 알고리즘

9. 페이스텔 암호란 무엇일까? TEA가 페이스텔 암호가 아닌 이유는 무엇일까? TEA가 "거의" 페이스텔 암호라고 할 수 있는 이유는 무엇일까?

페이스텔 암호란 많은 현대 블록 암호의 기반이 되는 암호의 설계원리를 의미한다.
TEA가 페이스텔 암호가 아닌 이유는 페이스텔 암호는 회전함수에 무관하게 암호화의 역순으로 복호화 할 수 있지만, TEA는 암호화와 복호화의 처리 순서를 구분해야하기 때문이다.
하지만 또, TEA가 "거의" 페이스텔 암호라고 할 수 있는 이유는 연산의 종류가 다른 것을 제외하면 두 알고리즘 사이에 큰 차이점이 없기 때문이다.

10. 아래의 규칙에 따라 암호화하는 블록암호를 사용한다고 가정하자.
$C_0 = IV \oplus E(P_0, K),\ C_1 = C_0 \oplus E(P_1, K),\ C_2 = C_1 \oplus E(P_2, K),\ \ldots$
이에 대응하는 복호화 규칙은 무엇일까? CBC 모드와 비교해 이 모드가 가지는 두 가지 보안상의 단점을 간단히 기술하라.

답변

이 규칙에 따르면 복호화는 암호문의 뒤에서부터 앞으로 이루어진다. 이 암호화 규칙 또한 CBC모드와 같이 통신 중에 생기는 노이즈나, 비트 에러가 생기면 그 이후 몇 블록은 복호화가 이루어지지 않는다는 단점이 있다. 또 하나의 단점은 Cut and Paste 공격 방법이 조금 더 복잡해지긴 했지만 가능은 하다는 점이다.

17. 암호문 $C_0, C_1, C_2, ..., C_9$ 블록이 CBC 모드로 암호화되었다고 가정하자. 이 경우, 복사-붙여넣기 공격이 가능함을 보여라. 즉, 어떤 블록은 순서는 틀리지만 바르게 복호화 되도록 블록을 재정리할 수 있음을 보여라.

답변

전체 암호문은 $IV, C_0, C_1, C_2, ..., C_9$가 되고, 여기서 좌우 끝 부분은 잘라내어도 복호화 하는 데는 전혀 문제가 없다. 그리고 가운데 부분을 잘라낸다고 하여도 하나의 잘못된 평문 블록이 생길 뿐이다. 그리고 같은 키를 사용한 다른 암호문의 순차적인 블록들을 복호화 할 때 paste 하면 평문의 내용을 알 수 있다.

23. 4개의 회전과 $P = (L_0, R_0)$인 페이스텔 암호를 고려하자. 만약 회전함수가 다음과 같으면 암호문 C는 무엇일까?

a. $F(R_{i-1}, K_i) = 0$

$$round_1 = (R_0, L_0)$$
$$round_2 = (L_0, R_0)$$
$$round_3 = (R_0, L_0)$$
$$round_4 = (L_0, R_0)$$

b. $F(R_{i-1}, K_i) = R_{i-1}$

$$round_1 = (R_0, L_0 \oplus R_0)$$
$$round_2 = (L_0 \oplus R_0, L_0)$$
$$round_3 = (L_0 \oplus R_0)$$
$$round_4 = (R_0, L_0 \oplus R_0)$$

c. $F(R_{i-1}, K_i) = K_i$

$$round_1 = (R_0, L_0 \oplus K_1)$$
$$round_2 = (L_0 \oplus K_1, R_0 \oplus K_2)$$
$$round_3 = (R_0 \oplus K_2, L_0 \oplus K_1 \oplus K_3)$$
$$round_4 = (L_0 \oplus K_1 \oplus K_3, R_0 \oplus K_2 \oplus K_4)$$

d. $F(R_{i-1,}K_i) = R_{i-1} \oplus K_i$

$round_1 = (R_{0,}L_0 \oplus R_0 \oplus K_1)$

$round_2 = (L_0 \oplus R_0 \oplus K_{1,}L_0 \oplus K_1 \oplus K_2)$

$round_3 = (L_0 \oplus K_1 \oplus K_{2,}R_0 \oplus K_2 \oplus K_3)$

$round_4 = (R_0 \oplus K_2 \oplus K_{3,}L_0 \oplus R_0 \oplus K_1 \oplus K_3 \oplus K_4)$

27. 앨리스와 밥은 항상 같은 초기화 벡터를 선택한다고 가정하자.
a. CBC 모드를 사용하였을 때 발생하는 보안성 문제 한 가지를 들어라.
b. CRC 모드를 사용하였을 때 발생하는 보안성 문제 한 가지를 들어라.
c. 항상 같은 초기화 벡터가 사용되었을 때 CBC와 CTR 모드 중 어느 것이 더 안전할까?

답변

a. 만약 초기화 벡터 IV를 재사용 한다면, 같은 평문에 대해서 같은 암호문이 나오게 된다. 따라서 초기화 벡터는 반드시 임의로 선택되어야 한다.

b. CBC 모드와 같이 초기화 벡터 IV를 재사용해서는 안 된다. CTR 모드는 키스트림을 생성하는 데 사용하므로, 이는 같은 키 스트림을 사용하는 one-time pad와 같은 결과를 초래한다.

c. CBC 모드의 경우에는 같은 평문을 사용했을 경우 같은 암호문이 나오기 때문에 암호문을 보고도 어느 정도 평문을 예측할 수 있게 된다. 그에 반해 CTR 모드의 경우에는 모든 암호문을 그대로 복호화 할 수 있으므로 CBC 모드의 경우가 더 안전하다고 생각된다.

32. 앨리스는 4개의 블록 $P_{0,}P_{1,}P_{2,}P_3$으로 구성된 평문을 CBC 모드를 이용해 암호화한다. 앨리스는 암호문 블록 $C_{0,}C_{1,}C_{2,}C_3$과 초기화 벡터를 밥에게 전송한다. 밥이 그것들을 수신하기 이전에 트루디가 암호문의 어떤 블록이라도 변경할 수 있다고 가정하자. 만약 트루디가 P_1을 알고 있다면 P_1을 X로 바꿀 수 있음을 보여라. 즉, 밥이 C_1을 복호화하면 P_1 대신 X를 얻게 될 것이다.

답변

트루디가 P_1을 알고 있기 때문에 C_0 대신에 $C_0 \oplus P_1 \oplus X$로 바꿔치기 할 수 있다. 그렇게 되면 C_1은 $E(C_0 \oplus X_{,}K)$가 되고, 절차에 따라 복호화를 하면 P_1대신 X가 나오게 된다.