HomeWork #3 중간시험 풀이

1. 다음을 간략히 설명하라

a) Feistel 암호

암호학에서 Feistel 암호는 block 암호의 구조에서 사용되는 대칭적 구조이다. IBM의 독일 암호학자 Horst Feistel의 이름을 땄다. 그 자체가 암호학은 아니지만 DES 암호화를 포함한 많은 block 암호들이 Feistel 구조를 사용한다.

b) 3중DES

암호학에서 3중DES은 각 데이터 block에 DES 암호 알고리즘을 세 번 적용한 대칭키 블록 암호화이다. 기존 DES 알고리즘은 키의 길이가 56비트인데 컴퓨터 계산 기술의 발달로 인해 전수검사로 Breaking이 가능해졌다. 3중DES는 전혀 새로은 block 암호 알고리즘을 디자인 할 필요 없이, DES 알고리즘의 키 길이를 확장시키는 효과를 낸다.

c) Hash(보안에서의)

Hash는 어떤 입력 데이터에 매핑되는 Hash 값은 쉽게 구할 수 있지만 만약 입력 데이터를 모른 채, Hash 값으로 입력 데이터를 구하는 것은 극도로 어렵다. 이러한 Hash 함수의 단방향 성질은 보안에서 전달되는 데이터의 무결성을 보장하고, 더 나아가 송신자의 인증까지 가능한 HMAC을 만드는 데 사용할 수 있다.

d) HMAC(Hashed MAC)

HMAC은 특별한 타입의 MAC인데, HMAC은 메시지와 대칭키를 적절히 잘 섞어서 Hash한 인증코드이다. 이 인증코드에는 대칭키도 잘 섞여 들어가 있으므로 메시지의 무결성뿐만 아니라 송신자의 인증까지 보장된다.

e) 기만율(Fraud Rate), 모욕률(Insult Rate)

기만율과 모욕률은 각각 False Acceptance Rate, False Rejection Rate라고도 한다. 직역해 보면 잘못된 승인 비율, 잘못된 거부 비율이다. 즉, 저장된 생체 데이터와 다른 데이터를 가진 사람을 승인하는 비율과, 저장된 생체 데이터와 같은 데이터임에도 불구하고 거부하는 비율을 말한다. 서로 반비례하는 관계를 가지기 때문에 기만율과 모욕률이 같은 비율이 인증 기술의 질을 판단하는 데 사용된다.

2. CBC(Cipher Block Chainning) 모드와 CTR(CounTeR)모드의 특징과 용도를 비교 설명하라.

CBC 모드는 이전 block에서 생성된 암호문을 사용해 다음 암호문은 만들기 때문에 암호화는 병행적으로 수행이 불가능하다. 하지만 복호화는 인접한 암호문만 있으면 병행적으로 가능하다.

ECB 모드의 약점을 보완하는데 주로 사용된다.

CTR모드는 암호화와 복호화가 완전히 같은 구조이고, 프로그램으로 구현하는 것이 아주 간단하다. 또한 암호화, 복호화 모두 병렬적으로 수행 가능하다. 병렬적으로 암호화, 복호화가 가능하기 때문에 멀티프로세서 시스템에서 효력을 발휘한다.

3. 대칭키 암호와 공개키 암호의 특징을 비교 설명하라.

대칭키 암호는 하나의 키를 사용하여 암호화 복호화를 수행하는 암호 알고리즘이다. 대칭키 암호 알고리즘은 하나의 비밀 키를 공유하고 있어야 한다. 반면에 공개키 암호는 공개키와 개인키를 사용한다. 암호화는 공개키로 하고 복호화는 개인키로 한다. 따라서 대칭키와는 다르게 키 공유 문제가 자동으로 해결된다. 그리고 공개키 암호 알고리즘은 암호화뿐만 아니라 전자 서명 및 부인 방지 기능도 가지고 있다.

4. RSA를 사용하여 비밀성과 부인봉쇄를 하는 방법으로 선 서명, 후 암호화 방식이 있다. 이를 설명하고 문제점과 보안대책을 설명하라.

선 서명, 후 암호화 방식은 전달받은 메시지를 복호화할 수 있는 키를 가진 사람이 메시지를 해독하면 송신자의 서명이 된 메시지를 가지게 된다. 이 서명된 메시지를 다시 다른 사람의 공개키로 암호화함으로써 송신자를 난감한 상황에 빠뜨릴 수 있다. 이 문제에 대한 대책으로는 선 암호화, 후 서명 방식이 있다.

선 암호화, 후 서명 방식은 앞서 소개한 문제는 방지할 수 있지만 중간에서 전송 내용을 가로채어 송신자의 공개키로 서명을 풀고 자신이 서명을 해서 다시 보내는 방식으로 변조를 한다면 송신자 대신 자신이 어떤 이익을 챙길 수 있다.

5. 온라인 뱅킹시스템에서 컴퓨터 보안의 핵심인 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)이 어떻게 요구되는지 예를 보이고 대비방안을 설명하라.

현재 진행 중인 온라인 뱅킹시스템은 사용자를 인증하는 방식으로 패스워드를 사용한다. 시스템이 네트워크를 통해 통신을 하므로 제 3자가 중간에서 훔쳐보기 및 변조가 가능하다. 따라서 통신되는 메시지의 기밀성을 보장해줄 필요가 있다. 대표적으로 통신 전후로 메시지를 암호화시키는 방법이 있다. 하지만 기밀성을 보장한다고 해서 안전한 것은 아니다. 왜냐하면 굳이 암호의 내용은 알 필요 없이 암호문 그대로를 그대로 사용하는 Cut and Paste 공격이 가능하기 때문이다. 이는 전송되는 데이터가 중간에 변조되지 못하도록 무결성을 보장해주어야 한다. 무결성을 보장하는 방법으로는 인증 프로토콜을 잘 설계하는 방법인데, 그 중에서 NONCE와 해시를 잘 사용하는 방법이 있다. MAC도 무결성을 보장하는 데 사용된다. 하지만 기밀성과 무결성이 잘 보장된다고 하더라도 공격자가 시스템이 사용 불가능한 상태로 만들 수 있다. 이는 시스템의 가용성을 떨어뜨리는 공격인데, 그 중에는 DoS 공격이 대표적이다. 대비방안으로는 방화벽 및 IDS, IPS를 잘 구축하여 외부에서 오는 이상적인 행위들을 파악하여 처리하는 방법이 있다.