암호학개론

중간보고서

16. 암호 기술과 현실 세계

2019.04.23

2017204081 최수지

단원 요약

[16장 암호 기술과 현실 세계는 지금까지 배운 암호 기술들을 요약하고(1.1), 암호 기술을 복합적으로 사용할 경우(1.2)와 암호 기술의 기반은 어떤 것인지(1.3~1.4), 암호 기술의 공통점은 어떤 것인지(1.5)를 설명한다. 또한, 암호 기술을 이용한 비트코인의 설명(2.1)과 비트코인의 기반 네트워크(2.2), 거래(2.3), 기반 애플리케이션(2.4)에 대하여 설명한다. 여기에서 블록체인 기술은 어떤 것인지(2.5), 블록체인의 구성은 어떠한지(2.6), 트랜잭션에 대한 설명(2.7), 비트코인의 블록을 추가하는 방법(2.8) 등 비트코인의 전반적인 흐름을 알려준다. 그리고 현재 쓰이는 암호 기술 이외에 미래의 암호 기술인 양자 암호(3.1~3.3)에 대하여, 설령 암호 기술이 완벽하더라도 완전한 보안이 실현되지 않는 이유(4.1~4.4)의 과정을 세세하게 풀어 알려준다.]

(1.1 암호학자의 도구 상자) 먼저, 첫 번째로 지금까지 배운 암호 기술들을 정리해보자. 이들은 일명 '암호학자의 도구 상자(6개)'로 일컬어진다. 이 6가지의 기술은 대칭 암호, 공개키 암호, 일방향 해시 함수, 메시지 인증 코드, 디지털 서명, 의사 난수 생성기이다.
대칭 암호는 암호화&복호화에 같은 키를 사용하고, 공개키 암호는 암호화&복호화에 서로 다른 키를 사용한다. 공개키 암호에 가장 많이 사용되는 알고리즘은 RSA이다. 대칭 암호는 키 배송 문제가 있고, 공개키 암호는 이를 해결할 수 있지만, 중간자 공격을 당할 수 있어 디지털 서명을 이용한 공개키 인증을 함께 써야 한다.
일방향 해시 함수는 긴 메시지를 짧은 해시값으로 변환하며 무결성을 확인할 수 있다.
메시지 인증 코드는 상대에게 온 메시지가 공격자에 의해 수정되지 않았는지를 확인하며 이 또한 무결성을 확인할 수 있다.
디지털 서명은 제 3자가 메시지를 검증하며 상대의 부인 방지를 막을 수 있다.
의사 난수 생성기는 예측 불가능성을 갖는 비트 열을 생성하는 기술이다.

(1.2 암호 기술의 종합 응용) 이러한 기술들을 융합하여 사용된 과정을 설명한다. 단, 이 과정은 제 3의 인증기관을 포함하는 가정이다.
① 메시지 다이제스트 생성→ ② 앨리스의 서명 작성→ ③ 대칭 키를 이용하여 암호화 하기→ ④ 대칭 키의 암호화→ ⑤ 전송→ ⑥ 대칭 키 획득→ ⑦ 암호화된 메시지 복호화→ ⑧ 메시지 다이제스트 획득→ ⑨ 메시지 다이제스트 구하기→ ⑩ 서명에 대한 검증
이를 하이브리드 암호 기술이라 한다.
(1.3 암호와 인증) 강한 암호 기술을 가지는 것도 중요하지만, 이 암호가 공격당하지 않았다는 인증도 중요하다.
(1.4 암호 기술의 프레임워크화) 프레임워크란, 내부에 사용하고 있는 요소 기술을 부품 교환하듯이 결함이 있는 부분만 교체하는 것이다. 프레임워크를 이용하면 시스템 재 이용성이 높고 강력하다.
(1.5 암호 기술은 압축 기술) 암호 기술을 압축 기술로 비유하면, 대칭 암호와 공개 키 암호는 기밀성의 압축 / 일방향 해시 함수는 무결성의 압축 / 메시지 인증 코드와 디지털 서명은 인증의 압축 / 의사난수 생성기는 예측 불가능성의 압축이라 말할 수 있다. 이를 다시 말하면, 기밀성 (키) / 무결성 (해시값) / 인증 (인증자) / 예측 불가능성 (종자) 이렇게 정리할 수 있다.

(2.1 비트코인이란?) 비트코인이란, 인터넷으로 송수신 가능한 가상화폐라고 칭한다. 1비트코인은 1 bitcoin (1 BTC)로 표현한다. 비트코인의 상대적 가치는 변동성이 있으며, 다른 화폐와 달리 이를 관리하는 국가나 은행은 존재하지 않는다. 비트코인 거래에 사용되는 개인 키를 분실하면 재발급이 불가능하므로 유의해야 한다.

(2.2 P2P 네트워크) 일반적으로 가상화폐라 불리긴 하나, 비트코인은 P2P(개개인 간의) 네트워크상에서 동작하는 결제 시스템이라고 생각하는 것이 더 이해하기 편리하다.

(2.3 어드레스) 비트코인 거래는 (비트코인) 어드레스 간에 이루어진다. 어드레스는 공개 키의 해시값으로부터 만든다. 형식은 “1” 또는 “3”으로 시작한다.

(2.4 월렛) 비트코인을 거래할 때 사용하는 애플리케이션을 월렛이라 한다. 이용자는 월렛을 사용하여 공개키 쌍을 생성하고 인터넷으로 거래한다. 여기서 공개키는 비트코인을 주고받기 위해, 개인 키는 비트코인을 송금하기 위해 사용된다. 월렛도 암호와 마찬가지로 개인 키를 보여주면 안 된다.

(2.5 블록체인) 블록체인은 비트코인의 모든 거래가 기록되는 공개 거래기록부이다. 블록은 거래 단위를 의미한다. 공개 거래 장부가 있으면 어느 어드레스가 현재 얼마만큼의 비트코인을 지불 할 수 있는가가 정해진다. 이를 위한 것이 바로 블록체인이다. 블록체인을 구축하고 유지하는 것이 비트코인의 중요한 부분이다.

(2.6 블록 추가) 비트코인의 거래 단위는 트랜잭션이다. P2P 네트워크가 승인되면 트랜잭션 거래가 성립된다. 블록체인에서의 블록은 트랜잭션의 집합과 헤더로 이루어져 있다. 헤더에는 직전 블록 헤더의 해시값과 트랜잭션 집합 전체의 해시값, 그리고 난수가 저장되어 있다. 이로 인해 블록체인을 조금이라도 바꾸었을 경우 블록 헤더 모두를 바꿔야 한다.

(2.7 트랜잭션) 트랜잭션을 좀 더 풀어 설명하면, ‘어느 어드레스에서 어디로 얼마의 비트코인을 보내는가‘라는 거래를 기록한 것이다. 이때 두 이용자는 어드레스만 알면 되기 때문에 본인들이 누구인지 서로 알 필요가 없다.

(2.8 채굴) 이렇게 거래라 어떤 방식으로 이루어지는지는 알았다. 하지만 비트코인이 어떻게 만들어지는 아직 이야기하지 않았다. 비트코인은 블록체인에 블록을 추가하여 지불 가능한 어드레스를 새로 만들 수 있다. 이러한 행위를 채굴이라 하며, 이를 하는 이를 채굴자라 부른다. 블록을 추가한 채굴자에게는 보수와 트랜잭션 수수료를 얻을 수 있다. 채굴자는 비트코인 위조 방지를 위해 채굴 도중에 해시값을 이용하여 자신의 성과를 증명 한다. 비트코인은 블록 추가를 위한 적절한 난이도가 설정되어 있다.

(2.9 승인) 전 세계에는 수많은 채굴자가 존재한다. 만약 한 해시값을 다수의 채굴자들이 채굴하는 경우를 위해 승인이 존재한다. 승인은 P2P 네트워크로 인해 이루어지며, 블록체인에 블록을 추가해도 되는지를 판단하는 것이다.

(2.10 익명성) 비트코인의 거래상, 월렛 어드레스는 본인과 관련이 없으며 거래상에서도 본인의 정보가 알려질 리는 없다. 하지만 특정 어드레스로 행하는 거래는 모두 알려지고, 거래 기록 또한 블록체인에 남겨지게 된다. 게다가 거래 도중 어드레스를 특정인의 것으로 지목해서 알릴 경우나 IP주소 기록이 알려질 경우로 인해 완전한 익명이라 보기는 어렵다.

(2.11 신뢰의 의미) 여기서 신뢰란, 3가지를 생각 할 수 있다. 비트코인을 통해 지불 하는 상대 / 비트코인 거래소 / 비트코인 시스템 이 세 가지를 신뢰하는 것이다. 상대가 거래 도중 도망갈 경우, 비트코인을 맡길 거래소가 도난당하거나 사기를 칠 경우, 특정 비트코인에 사용되는 암호 기술과 월렛 시스템의 안전성, 이 세 가지를 신뢰할 수 있는지를 생각 해봐야 한다.

(3.1 양자 암호) 차세대 암호 기술로 각광 받는 암호 기술인 양자 암호 기술에 대하여 설명하자면 도청 불가능한 통신을 구성하는 것이다. 광자는 도청당할 시 상태가 변화하므로 수신자가 상태를 확인하여 도청 여부를 알 수 있다는 것을 이용하였다. 이 기술을 통해 일회용 암호 패드를 실용화할 수 있다. 1989년 미국부터 2015년 제네바 대학까지 양자 암호 기술 진보를 위해 연구가 꾸준히 진행되고 있다.
(3.2 양자 컴퓨터) 양자 암호는 암호학자의 궁극 도구라면, 양자 컴퓨터는 암호 해독자의 궁극 도구라 볼 수 있다. 지금까지는 전사 공격에는 시간이라는 문제가 걸려 있었으나 양자 컴퓨터를 사용하면 전사 공격을 순식간에 행할 수 있다. 양자 컴퓨터는 양자 암호 기술과 마찬가지로 연구가 계속 진행되고 있다.
(3.3 어느 쪽이 먼저 실용화될까?) 양자 암호 기술과 양자 컴퓨터 중 어떤 것이 먼저 실용화되는지에 따라 다른 결과를 빚을 수 있다. 양자 암호 기술이 먼저 실용화되면 양자 컴퓨터를 사용하더라도 양자 암호는 뚫리지 않는다. 반면 양자 컴퓨터가 먼저 실용화되면 현재 암호 기술로 작성한 암호문은 모두 순식간에 해독된다. 이러한 상황에도 견디는 암호를 위해 포스트-양자 암호 또한 연구가 진행되고 있다.

(4.1 이론은 완전하더라도 현실은 불완전하다) 기술이 이론적으로는 완벽할지라도 현실에 적용하려 하면 무리가 생긴다. 생체 정보를 이용한 인증 기술도 비트열로 전환하는 도중에 도난당할 시 보안이 뚫릴 수 있다.
(4.2 방어는 완전하지 않으면 안 되지만, 공격은 어느 한 곳만 깨면 된다) 게다가 방어는 어떤 상황, 어떤 부분에서라도 공격에 대비해야 하며 이를 24시간 지속해야 한다. 하지만 공격은 한순간 느슨해진 부분을 순간적으로 공략하면 끝이다.
(4.3 공격 예 1: PGP로 암호화된 메일에 대해) 암호 기술은 보안의 한 부분이다. 보안 기술을 정면으로 공격하는 방법보다는 더 쉽게 접근하는 방법이 많으므로 공격자가 어떻게 공격할지는 모르는 것이다. 다운로드 버튼 클릭을 유도하는 메일이나 사용자의 소프트웨어에 악성코드를 심는 방법, 사회공학적 방법 등 다양하다. 이러한 것들을 모두 막아야 하므로 보안은 제품이 아닌 프로세스라고도 불린다.
(4.4 공격 예 2: SSL/TLS 로 암호화된 신용카드 번호에 대해) 보안에 철저한 이용자를 뚫기 위해서 서비스 거부 공격(DOS 공격) 등을 행하여 SSL/TLS로 보호되지 않는 사이트에서 결제를 유도하는 방법도 있다. 암호로 보호되는 사이트를 뚫기 위해서는 아주 힘든 과정이 수반되므로 단순한 도스 공격이 이러한 상황에서는 더 효과적이다.

(5) 이렇게 암호 기술들이 이용된다 해도 사람이라는 요소의 추가로 결코 안전을 과신하지 않고 보안에 신경 써야 한다는 결론이 나온다.