**<블록체인 공격과 보안 방법 >**

1. 공격의 종류에는 eclipse Attack, BGP Hijacking, 화폐 환율조작, 내부 참여자의 담합, 사용자 프라이버시 침해, 블록체인 권한 오남용 등이 있다.
2. 공격사례 1
   1. BXH : 코인데스크에 “1억 3900만 달러의 자금이 유출된 사건”
      1. 사이트 : https://finance.yahoo.com/news/139m-bxh-exchange-hack-result-112810649.html
      2. 내부자에 의한 해킹이 의심된다. 해커가 관리자의 개인 키를 얻은 후 거래소의 스마트 체인 주소에 침입할 수 있었고, 그것으로 코인이 유출되었다. 해커가 관리자가 클릭한 사이트에 바이러스를 설치하여 소유자 컴퓨터의 키에 액세스 할 수 있도록 했을 가능성을 조사중임.
3. 공격사레 2
   1. 화폐 환율 조작
      1. 암호화폐인 비트코인과 이더리움은 코인 거래소를 이용하여 가상 화폐를 실제 화폐로 환전이 가능하다.가상 화폐도 제 화폐와 마찬가지로 수요자에 따라 화폐의 환율이 변동된다.
      2. 최근 2017년 5월 12일에워너크라이 랜섬웨어가 규모 감염되는 사건이 발생하였다. 워너크라이에 감염된 희생자는 공격자로부터 300$ 상당의 금액에 상응되는 비트코인을 요구 받게 된다. 감염된 희생자들은 자신의 컴퓨터를 복구하기위해 실제 화폐를 가상 화폐로 환전하여 공격자에게 전송하게 된다. 2017년 5월 1일에는 1 비트 코인의 가격이 1,635,000원 이였다. 워너크라이가 발생하기 전날인 5월 11일에는 1 비트 코인의 가격이2,352,000 원까지 오르게 된다. 워너크라이가 대규모로 감염된 후 5월 25일에는 1비트코인에4,681,000 원까지 상승하게 되었다
4. 블록체인 공격과 방어방법
   1. **Eclipse Attack:** 
      1. 정의
         1. 한 개의 노드를 대상으로 하는 네트워크 공격으로, 특정 노드가 정직한 노드로부터 정보를 수신 받는 것을 막기 위해 다수의 노드가 악의적으로 네트워크를 독점하는 것이다. 다수의 노드는 허위 전송 내역이 담긴 블록을 타겟 노드에 전파하여 블록체인에 대한 노드의 보기를 모호하게 함으로써 이중지불 공격을 가능하게 한다.
      2. 방어 방법
         1. 이 공격을 방어하기 위해 비정상적인 Packet을 탐지하는 Anomaly Detection을 하거나, 희생자 노드의 Table에 저장된 노드만 선택하여 연결하는 것이 아닌 Table에 저장된 노드의 정보이외에도 랜덤하게 선택하여 연결되도록 해야 한다.
   2. **BGP Hijacking**
      1. 정의 :
         1. BGP(Border Gateway Protocol) 을 사용하여 유지 관리 되는 인터넷 라우팅 테이블을 손상시켜 IP 주소 그룹을 불법적으로 탈취하는 것이다. 블록체인의 노드들은 인터넷 서비스 공급자(ISP)에 의해서 연결된다. 악의적인 IPS는 블록체인에서 발생하는 트래픽을 공격할 수 있다. 악의적인 ISP가 주변 라우터에게 잘못된 라우팅 정보를 광고하여 비정상 처리되도록 하는 공격 방법이다.
      2. BGP Hijacking을 통해Partitioning Attack과 Delay Attack이 가능하다.
         1. Partitioning Attack
            1. 네트워크를 두 개로 분할하는 공격으로, Attacker는ISP1에 연결 되어있는 노드(192.168.0.1)가 자신에게 연결 되어있는 것처럼 Fake IP주소(192.168.0.1)를 생성하고 라우팅 테이블을 업데이트하여 인접한 ISP로 전송한다. 인접한 ISP는Attacker가 보낸 라우팅 정보로 업데이트하고192.168.0.1로 전송되는 패킷을 Attacker에게 전송하게 된다. Attacker는 수신한 패킷들을 중간에서 가로채 전달해주지 않음으로써 네트워크를 분할시킬 수 있다.
            2. 방어 방법

Partitioning Attack을 방어하기 위해서는Monitor Round-Trip time 방법이 있다. 이 방법은 RTT를 모니터링 하여서 패킷이 잘 전달되는지 확인하고, 잘 전달되지 않는다면 다른 ISP로의 연결을 통해 패킷을 송수신한다

* + - 1. Delay Attack
         1. 네트워크에서 발생하는 트래픽(거래, 블록) 전달을 지연시키는 공격이다.
         2. 방어 방법

Delay Attack을 방어하기 위해서는 EncryptBitcoin Communication and/or adoptMAC(Message Authentication Code) 방법이 있다. 이 방법은 메시지를 암호화하여 어떤 메시지인지 공격자가 확인할 수 없도록 , 메시지 인증 코드를 사용하여 메시지의 내용이 변경되지 않았음을 확인할 수 있도록 하는 방법이다.

* 1. **내부 참여자의 담합 공격**
     1. 프라이빗 블록체인의 경우 공격자가 내부 참여자에 침투해 장악할 위험성을 가지고 있다.
     2. 방어 방법
        1. 블록체인 내부 참여자의 담합을 방지하고 대외투명성을 확보하기 위해 앵커링에 기반한 검증방식을 사용한다. 앵커링은 프라이빗 블록체인과 퍼블릭 블록체인을 연계하는 기술이다. 이를 기반으로보안 대상인 프라이빗 블록체인의 대표 해쉬값을주기적으로 비트코인등의 퍼블릭 블록체인에 기록하고, 내부 담합이 의심되면 이 기록과 프라이빗 블록체인 정보를 비교해서 검증을 수행한다. 제안 방식을 통해 내부 담합으로 프라이빗 블록체인 내용을 변경하려는 시도를 방지할 수 있다.
  2. **사용자 프라이버시 침해 공격**
     1. 퍼블릭 블록체인은 공격자가 모든 거래내역과 정보를 쉽게 볼 수 있기 때문에 참여자의 프라이버시를 침해할 가능성이 높다. 또한 스마트 계약 코드가실행중에 사용자 개인정보에 접근해서 개인정보 침해가 발생할 가능성도 있다.
     2. 방어 방법
        1. 완전동형암호(FullyHomomorphic Encryption)을 적용한다. 완전동형암호는 암호화된 정보의 복호화 없이 정보의 처리 및 연산이 가능해진다. 블록체인 내의 사용자 정보와 거래 내역에 대해 이를 적용해서 개인정보의 유출을 방지하고 거래내역을 숨겨 익명성을 강화할 수 있다.
  3. **권한 오남용 공격**
     1. 탈중앙화 된 블록체인 시스템에서는 참여자들에 대한 접근제어와 권한 통제에 어려움이 있다. 특히 프라이빗 블록체인에서는 특정 참여 노드나 내부직원의 권한 오남용으로 정보의 조작과 보안 사고가 발생할 가능성이 높다. 참여자들의 권한을 제어하고 오남용을 방지하기위해서는 블록체인 내에서의 접근제어가 필요하다
     2. 방어 방법.
        1. 스마트계약 기반의 접근제어를 사용한다. 참여자 권한에 대해 설정된 정책 자체가 스마트 계약의 형태로 배포되며, 요청에 대한 접근제어도 스마트 계약 시행을 기반으로 동작한다. 이 방식은 분산 환경에서 누구나 정책을 검증할 수 있고,자동화되고 안전한 방식으로 접근 제어를 수행할 수 있다.

1. 블록체인의 취약점인 프라이버시 강화
   1. 프라이버시 취약점들이 나오게 되면서 비트코인의 기본적인 설계원리를 깨지 않고 프라이버시를 강화하고 익명성을 향상시키는 기법들이 제안되었다[2]. 현재 프라이버시를 강화하는 제안기법들을 분류하면 세 가지 유형으로 분류할 수 있다.
      1. P2P 믹싱(mixing) 프로토콜
      2. 분산(Distributed) 믹싱 네트워크
      3. 비트코인 확장 또는 Altcoin
   2. **P2P 믹싱(mixing) 프로토콜**
      1. 믹싱 시스템은 익명성 서비스 제공자로서 트랜잭션의 추적을 어렵게 하는 믹싱 프로토콜을 사용한다. 믹싱 과정에서 클라이언트 자금은 작은 부분으로 램덤으로 나누어지며 다른 클라이언트 자금의 작은 부분과 램덤으로 섞이며 결과적으로 새로운 코인을 생성하게 된다. 이것은 사용자와 코인과의 연결을 깨뜨림으로써 익명성과 비연결성을 강화한다.
   3. **분산(Distributed) 믹싱 네트워크**
      1. 분산 믹싱 네트워크는 익명 지불이 가능한 제 3자 믹싱 프로토콜을 사용한다. 대표적으로 MixCoin기법은평판(reputation) 기반 암호화 회계 책임(accountability)기법으로 다른 사용자가 절도나 프로토콜을 혼란시키는 것을 방지한다. MixCoin은 표준 크기의 트랜잭션을 이용하여 제 3자 믹싱 시스템을 통해 자금을 송수신한다.
   4. **비트코인 확장 또는 Altcoin**
      1. 비트코인은 사실상의 표준이지만 비트코인으로 파생되어 생성된 다른 코인도 있으며 알트코인(altcoin)이라고 한다. 대표적인 것은 ZeroCoin 기법이다[19]. 완전히 암호화된 트랜잭션을 수행하는 영지식(zero-knowledge)기법을 이용하여 익명성을 제공하는 비트코인의 확장형이다. 사용자는 코인에 대한 추적 문제를 완전히 해결할 수 있다. 왜냐하면 전송되는 화폐의 양과 수혜자 주소 등의 트랜잭션의 추가적인 정보가 숨겨 지기 때문이다