송유진

Security of ZKP projects : same but different

JP Aumasson

“security audit”

Security audit

설정된 기준 세트를 얼마나 잘 준수하는지 측정하여 security를 체계적으로 평가하는 것

일반적으로 시스템의 물리적 구성과 환경, 정보 처리 프로세스 및 user practice의 security를 평가

Known primitives, known protocol의 사용 및 구현을 확인하여 security 평가

❖ Example

- 보안 제어(security control)
  : 조직이 정보와 시스템을 보호하기 위해 수립한 정책과 절차를 얼마나 잘 구현했는지 평가하는 것이 포함

- 소프트웨어 시스템
  : 소프트웨어 시스템이 제대로 작동하고 정확한 정보를 제공하는지 검사함

❖ Security audit을 수행해야 하는 이유

- Security 문제와 시스템 취약점을 식별
- 내부 조직 보안 정책을 준수
- 외부 규제 요구사항을 준수
- 향후 감사와 비교할 수 있는 보안 기준을 설정

Security audit

설정된 기준 세트를 얼마나 잘 준수하는지 측정하여 security를 체계적으로 평가하는 것

일반적으로 시스템의 물리적 구성과 환경, 정보 처리 프로세스 및 user practice의 security를 평가

Known primitives, known protocol의 사용 및 구현을 확인하여 security 평가

⟶ 다양한 팀에서 방법론, 도구 개발, 새로운 직원 교육

But!!

ZKP를 중심으로 구축된 decentralized project는 아래 이유로 다른 접근 방식을 요구

- Complexity
- 구현된 protocol의 참신함
- 문서화되지 않은 트릭
- 대부분 미개척된 버그 영역
- 제한된 기록 및 버그 문서
- 전문 지식과 경험 부족

This talk

- ~ 10 years doing security audits
- Based on the experience of carrying out the security idea for zk project over the past few years,

  zk project's security audit != crypto audit

제한된 기록과 전문 지식, 도구 및 경험 부족

다음 세대를 위한 더 많은 테스트를 해서 문서화, 버그에 대한 해결, 관심을 가지면 좋겠다.

ZK project에 대한 security audit도 필요하다!

- **Why study zkSNAKRs security?**

  Zk security가 없으면 무의미, 많은 가치가 위험, 많은 돈 & 평판이 걸려있어서 중요함

- **What's zkSNARKs security?**
- **Who can find bugs?**
- **Bug hunting challenges**

  Security auditor로서 가장 큰 어려움은 무엇?

  - 경험 제한
  - 이론과 구현 트릭에 대한 제한된 지식
  - 버그 및 버그 클래스의 제한된 체크리스트
  - 제한된 도구 및 방법론
  - 프로젝트의 제한된 문서

  그럼에도 불구하고 유용한 작업을 만드는 방법은 무엇?

- **New crypto, new approach**
  - 개발자/디자이너와의 협업 강화(공동리뷰 세션, QA 등)
  - Application의 고유한/새로운 위험을 이해하기 위한 더 많은 위협 분석

- **How to break zkSNARKs?**

- **Bug collection**

- **Conclusion**