IoT보안 강의개요

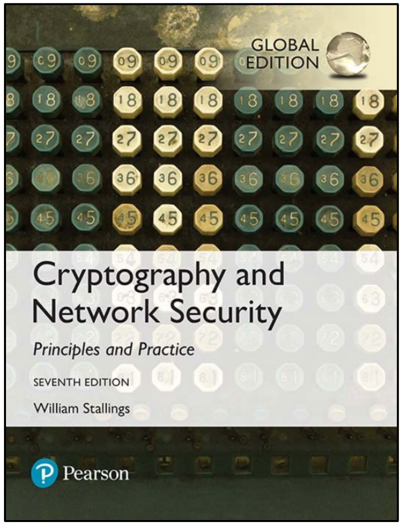
정보보안

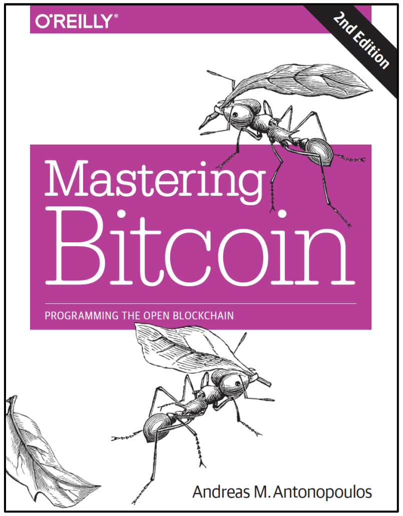
교과 기본 사항

- 담당교수
  - 염대현 (daehyun.yum@gmail.com)
  - Y5614
- 시험 및 출석
  - 성적 = 시험 90% + 출석 10%
  - 기말시험: 12월 7일 (수) 18:00
  - 전체 수업일수 5분의 4이상 출석해야 함. (지각 3회 = 결석 1회)
  - 유고결석 (학칙 제 71조)
    - … 사유발생 전이나 발생 즉시 또는 부득이한 경우에는 발생일로부터 5일 이내에 학생이 유고결석신청서와 증빙서류를 갖춰 소속 학부 과 전공 주임교수의 확인을 받은 후 수업담당 교 강사에게 제출하여야 한다 …
- 주의사항
  - 수강생 암호화폐 투자 절대 금지!

강의교재

- 정보보안
  - 저자: William Stallings
  - 서명: Cryptography and Network Security
  - 출판사: Prentice Hall (Pearson)
- 번역본
  - 저자: 최용락 외 11인 옮김
  - 서명: 컴퓨터 보안과 암호
  - 출판사: 도서출판 그린
- 블록체인
  - Mastering Bitcoin





Cryptography

- From Wikipedia
  - Cryptography (or cryptology; from Greek κρυπτός, "hidden, secret"; and γράφειν, graphein, "writing", or -λογία, -logia, "study", respectively) is the practice and study of techniques for secure communication in the presence of third parties (called adversaries).
  - More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation.
  - Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Crypto Pitfalls?

1. Bad cryptography, bad implementations, bad design
2. Even good cryptography can be ‘circumvented’ by adversaries operating ‘outside the model’
   - Systems are complex, and your model may not exactly match reality
   - Side channel attacks 다른 비정상적인 방법으로 뚫음.

     전력을 이용하여 0,1 등 전기량 측정하여 뚫음
3. Even the best cryptography only shifts the weakest point of failure elsewhere.
   - Reduced entropy of PINs 0000 ~ 9999 지만 본인과 관련된 숫자로 설정..
   - Poor key management 사용하는 비번 기억 못함. or 비번파일을 만듦.

     이것을 해싱하려해함
   - Insider attacks

     내부의 경우.

     ex) 회사에 있다가 짤림. 등. 해킹보다 돈을 주거나 고문? 등.

     스턱스넷 Stuxnet 특정타겟을 찾을때까지 감염.

Enigma Machine