정보시스템보안 연구실 (Information System Security Lab)

지도교수

Prof. Junbeom Hur (허 준 범)

Department of Computer Science & Engineering, Korea University

Office: Room 609B, Science Library Building

E-mail: jbhur@korea.ac.kr

Phone: 02-3290-4603

Homepage: http://isslab.korea.ac.kr

Research Area

Network system attack & defense

- **Web Security**
  > HTTPS cookie hijacking attack and defense
  > Certificate transparency
- **SSL/TLS Security**
  > Vulnerabilities detection in TLS protocol (Theory, protocol, and implementation)
  > Downgrade attack and defense of TLS 1.3
- **Anonymous network security**
  > Deep web security (Tor, I2P)
  > Dark web analysis and profiling

NETWORK SECURITY

Secure cloud storage & data management

- **Cloud data encryption and access control**
  > Forward secure searchable encryption, functional encryption
- **Security-as-a-service architecture in cloud computing**
- **Secure proof-of-storage and verifiable computation**
- **Secure data deduplication**
  > Message-locked encryption with dynamic ownership management

CLOUD COMPUTING SECURITY

MICROARCHITECTURE SECURITY

Microarchitectural attack & defense

- **Microarchitectural attack on modern processors**
  > Cache side-channel attacks on core/uncore of CPU
- **Microarchitecture vulnerability and attack detection**
  > PMU based detection and validation
  > AI-based CPU attack detection
- **Trusted execution environment (TEE) security**
  > Intel SGX, AMD SME, ARM TrustZone

BLOCKCHAIN & AI SECURITY

AI-based blockchain analysis & attack defense

- **Blockchain transaction trace and analysis**
  > Machine learning-based blockchain data clustering
- **Cryptocurrency deanonymization**
  > De-mixing of Bitcoin mixing services
- **Adversarial machine learning**
- **Machine learning-based attack detection**
  > Microarchitectural attack detection
  > Content pollution attack detection in future Internet architecture (e.g., NDN, SDN)