컴퓨터보안연구실 (Computer and Communication Security Lab)

지도교수
이 희 조
Department of Computer Science and Engineering, Korea University
Office: Room 306, Woojung CIC Building (College of Informatics)
E-mail : heejo@korea.ac.kr
Phone : 02-3290-3208
Homepage : https://ccs.korea.ac.kr

Research Area

Protection of network system

- **IoT fuzzing** : Bluetooth, Wi-Fi, ZigBee, Z-Wave protocol black-box testing
- **PRETT** : Automated protocol reverse engineering and vulnerability analysis (IFIPSec'18)
- **PsyBoG** : Power spectral density analysis for detecting botnet groups by monitoring DNS traffic (ComNet'16)
- **DROP-FAST** : A distributed DDoS defense utilizing multiple replicas of the protected server throughout a cloud infrastructure (SAM'13)
- **UAS** : Universal anti-spoofing mechanism that incorporates existing mechanisms to thwart IP spoofing attacks (LCN'13)
- **MHMP** : Multi-Hoped Multi-Path Routing for high availability

Network Security

Analysis of malicious codes and software

- Obfuscated VBA **Macro Detection** Using Machine Learning (DSN'18)
- **Packer Detection** for Multi-Layer Executables & **Unpacking classification** using entropy analysis (IEEE Malware'13)
- **Mystery Checker :** generating an attestation module and transferring a new attestation module. (IEEE Malware'13)
- **Code Graph** : Defeating self-defense of malware with static analysis and convert the API call sequence of the malware into a graph **(collaboration with MSRA)**
- **Cryptojacking Detection** based on script code

Malware Detection

Software Security

https://iotcube.net

- **IoTcube** : An open platform providing various easy-to-use analysis to discover vulnerabilities of software and hardware systems
- **Pfuzz** : Vulnerable file (PoC) aided binary fuzzing
- **VUDDY**: A scalable approach for vulnerable code clone discovery (S&P'17)
- **CLORIFI**: Software vulnerability discovery using code clone verification
- Automated discovery of software vulnerabilities in source codes using machine learning and security patches (**collaboration with MSRA**)
- **CENTRIS**: Centrifuge to extract modified open-source software components for mitigating risks imposed by code reuse

Discovery of software vulnerabilities

Digital Forensics

- **Integrity verification scheme** of video frames and contents (**Collaboration with NFS-국과수**)
  : Using the artifact of the file system in a storage device, detect the deletion of video frames
  : Detecting the modification of a video file with characteristics of video structure
- Framework of automated **user activity reconstruction**
  : Assisting investigators to reconstruct user activities automatically using signature-based digital forensic approaches (ISPEC'13)

Uncovering evidences in electronic devices