All papers can be found by Google Scholar. For those papers accepted by S&P 2019, you can download them from this website: https://www.ieee-security.org/TC/SP2019/program-papers.html

The below papers are published in the top security conferences within 2 years. You should better select your presentation paper from these papers. If you select the paper outsides this list, please make sure this paper has been published by our 1st and 2nd tier conferences within recent years.

Note: When you determinate the paper you will make a presentation in class, please send the paper title to TA one week before your presentation.

1. Mobile Security
2. Electrical Cash and Smart Contracts
3. Machine Learning Security
4. Web Security
5. IoT and Cyber-physical Security
6. Cybercriminal Security
7. Side Channels Attack
8. Authentication and Protocol Security
9. Enterprise Security

1. Mobile Security

- Please Forget Where I Was Last Summer: The Privacy Risks of Public Location (Meta)Data, NDSS 2019
- Time Does Not Heal All Wounds: A Longitudinal Analysis of Security-Mechanism Support in Mobile Browsers, NDSS 2019
- Geo-locating Drivers: A Study of Sensitive Data Leakage in Ride-Hailing Services, NDSS 2019
- ClickShield: Are You Hiding Something? Towards Eradicating Clickjacking on Android, CCS 2018
- Mobile Application Web API Reconnaissance: Web-to-Mobile Inconsistencies & Vulnerabilities, S&P 2018
- Phishing Attacks on Modern Android, CCS 2018
- Precise Android API Protection Mapping Derivation and Reasoning, CCS 2018

- Invetter: Locating Insecure Input Validations in Android Services, CCS 2018
- No Training Hurdles: Fast Training-Agnostic Attacks to Infer Your Typing, CCS 2018
- PatternListener: Cracking Android Pattern Lock Using Acoustic Signals, CCS 2018

2. Electrical Cash and Smart Contracts

- A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence, NDSS 2019
- Perun: Virtual Payment Hubs over Cryptocurrencies, S&P 2019
- Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody, CCS 2018
- MineSweeper: An In-depth Look into Drive-by Cryptocurrency Mining and Its Defense, CCS 2018
- SECURIFY: Practical Security Analysis of Smart Contracts, CCS 2018
- BitML: a calculus for Bitcoin smart contracts, CCS 2018
- teEther: Gnawing at Ethereum to Automatically Exploit Smart Contracts, Usenix 2018
- Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts, Usenix 2018
- Arbitrum: Scalable, private smart contracts, Usenix 2018
- Erays: Reverse Engineering Ethereum's Opaque Smart Contracts, Usenix 2018

3. Machine Learning Security

- TextBugger: Generating Adversarial Text Against Real-world Applications, NDSS 2019
- Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems, NDSS 2019
- Life after Speech Recognition: Fuzzing Semantic Misinterpretation for Voice Assistant Applications, NDSS 2019
- DEEPSEC: A Uniform Platform for Security Analysis of Deep Learning Model, S&P 2019
- Exploiting Unintended Feature Leakage in Collaborative Learning, S&P 2019
- LEMNA: Explaining Deep Learning based Security Applications, CCS 2018
- Effective Program Debloating via Reinforcement Learning, CCS 2018
- Turning Your Weakness Into a Strength: Watermarking Deep Neural Networks by Backdooring, Usenix 2018

4. Web Security

- Measuring and Analyzing Search Engine Poisoning of Linguistic Collisions, S&P 2019
- Master of Web Puppets: Abusing Web Browsers for Persistent and Stealthy Computation, NDSS 2019
- JavaScript Template Attacks: Automatically Inferring Host Information for Targeted Exploits, NDSS 2019
- Latex Gloves: Protecting Browser Extensions from Probing and Revelation Attacks, NDSS 2019
- Fidelius: Protecting User Secrets from Compromised Browsers, S&P 2019
- HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows, S&P 2019
- Deep Fingerprinting: Undermining Website Fingerprinting Defenses with Deep Learning, CCS 2018
- DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning, CCS 2018
- Measuring Information Leakage in Website Fingerprinting Attacks and Defenses, CCS 2018

5. IoT and Cyber-Physical Security

- HoMonit: Monitoring Smart Home Apps from Encrypted Traffic, CCS 2018
- If This Then What? Controlling Flows in IoT Apps, CCS 2018
- IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT, NDSS 2019
- SoK: Security Evaluation of Home-Based IoT Deployments, S&P 2019
- Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems, S&P 2019
- Why Does Your Data Leak? Uncovering the Data Leakage in Cloud from Mobile Apps, S&P 2019
- 6thSense: A Context-aware Sensor-based Attack Detector for Smart Devices, Usenix 2018
- Rethinking Access Control and Authentication for the Home Internet of Things (IoT), Usenix 2018

6. Cybercriminal Security

- Cybercriminal Minds：An investigative study of cryptocurrency abuses in the Dark Web, NDSS 2019
- Characterizing Pixel Tracking through the Lens of Disposable Email Services, S&P 2019
- Resident Evil: Understanding Residential IP Proxy as a Dark Service, S&P 2019
- Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets, Usenix 2018
- Reading Thieves' Cant: Automatically Identifying and Understanding Dark Jargons from Cybercrime Marketplaces, Usenix 2018

7. Side Channels Attack

- Profit: Detecting and Quantifying Side Channels in Networked Applications, NDSS 2019
- Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information, NDSS 2019
- Attack Directories, Not Caches: Side Channel Attacks in a Non-Inclusive World, S&P 2019
- Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers, CCS 2018
- Malicious Management Unit: Why Stopping Cache Attacks in Software is Harder Than You Think, Usenix 2018
- Translation Leak-aside Buffer: Defeating Cache Side-channel Protections with TLB Attacks, Usenix 2018

8. Authentication and Protocol Security

- BadBluetooth: Breaking Android Security Mechanisms via Malicious Bluetooth Peripherals, NDSS 2019
- Understanding Open Ports in Android Applications: Discovery, Diagnosis, and Security Assessment, NDSS 2019
- Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane, S&P 2019
- Robust Performance Metrics for Authentication Systems, NDSS 2019
- How to End Password Reuse on the Web, NDSS 2019
- Blind Certificate Authorities, S&P 2019

- The use of TLS in Censorship Circumvention, NDSS 2019
- PASTA: Password-based Threshold Authentication, CCS 2018

9. Enterprise Security

- Digital Healthcare-Associated Infection: A Case Study on the Security of a Major Multi-Campus Hospital System, NDSS 2019
- Mind Your Own Business: A Longitudinal Study of Threats and Vulnerabilities in Enterprises, NDSS 2019
- NoDoze: Combatting Threat Alert Fatigue with Automated Provenance Triage, NDSS 2019
- The Battle for New York: A Case Study of Applied Digital Threat Modeling at the Enterprise Level, Usenix 2018
- SAQL: A Stream-based Query System for Real-Time Abnormal System Behavior Detection, Usenix 2018