Network Security: Recommended Papers

Prerequisite

- How to Read a Paper (ACM SIGCOMM CCR'07)

App and service security

- Learning from Limited Heterogeneous Training Data: Meta-Learning for Unsupervised Zero-Day Web Attack Detection across Web Domains (ACM CCS'23)
- Silence is not Golden: Disrupting the Load Balancing of Authoritative DNS Servers (ACM CCS'23)
- Realistic Website Fingerprinting By Augmenting Network Traces (ACM CCS'23)
- TsuKing: Coordinating DNS Resolvers and Queries into Potent DoS Amplifiers (ACM CCS'23)
- DNSBomb: A New Practical-and-Powerful Pulsing DoS Attack Exploiting DNS Queries-and-Responses (IEEE S&P'24)
- Pudding: Private User Discovery in Anonymity Networks (IEEE S&P'24)
- Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3 (NDSS'23)

Transport-level security

- Stealth Key Exchange and Confined Access to the Record Protocol Data in TLS 1.3 (ACM CCS'23)
- TCP Spoofing: Reliable Payload Transmission Past the Spoofed TCP Handshake (IEEE S&P'24)
- Exploiting Sequence Number Leakage: TCP Hijacking in NAT-Enabled Wi-Fi Networks (NDSS'24)

IP security

- BGP-iSec: Improved Security of Internet Routing Against Post-ROV Attacks (NDSS'24)
- MirageFlow: A New Bandwidth Inflation Attack on Tor (NDSS'24)

Network access control security

- P4Control: Line-Rate Cross-Host Attack Prevention via In-Network Information Flow Control Enabled by Programmable Switches and eBPF (IEEE S&P'24)
- Formal Analysis of Access Control Mechanism of 5G Core Network (ACM CCS'23)

Cloud security

- Lost along the Way: Understanding and Mitigating Path-Misresolution Threats to Container Isolation (ACM CCS'23)
- Take over the Whole Cluster: Attacking Kubernetes via Excessive Permissions of Third-party Applications (ACM CCS'23)
- REPLICAWATCHER: Training-less Anomaly Detection in Containerized Microservices (NDSS'24)

Intruders and firewalls

- Pryde: A Modular Generalizable Workflow for Uncovering Evasion Attacks Against Stateful Firewall Deployments (IEEE S&P'24)
- Break the Wall from bottom: Automated Discovery of Protocol-Level Evasion Vulnerabilities in Web Application Firewalls (IEEE S&P'24)

Wireless networks

- Watch This Space: Securing Satellite Communication through Resilient Transmitter Fingerprinting (ACM CCS'23)
- Privacy Leakage via Speech-induced Vibrations on Room Objects through Remote Sensing based on Phased-MIMO (ACM CCS'23)
- Bluetooth Forward and Future Secrecy Attacks and Defenses (ACM CCS'23)
- Password-Stealing without Hacking: Wi-Fi Enabled Practical Keystroke Eavesdropping (ACM CCS'23)
- The Dark Side of Scale: Insecurity of Direct-to-Cell Satellite Mega-Constellations (IEEE S&P'24)
- On SMS Phishing Tactics and Infrastructure (IEEE S&P'24)
- 5G-Spector: An O-RAN Compliant Layer-3 Cellular Attack Detection Service (NDSS'24)
- CP-IoT: A Cross-Platform Monitoring System for Smart Home (NDSS'24)

Network protocol security

- Lifting Network Protocol Implementation to Precise Format Specification with Security Apps (ACM CCS'23)

- AAKA: An Anti-Tracking Cellular Authentication Scheme Leveraging Anonymous Credentials (NDSS'24)
- PriSrv: Privacy-Enhanced and Highly Usable Service Discovery in Wireless Communications (NDSS'24)