



Yepeng Pan

CISPA, Germany
Google Scholar
Homepage

Tel. +49 15235809914
Eml. panyepeng@gmail.com
Wechat. pyp1739

Research Interests

- Network Security
- Protocol & Application Security
- Network Measurement
- Denial-of-Service Attacks

Education

- PhD | CISPA Helmholtz Center for Information Security2023-04 to 2026-09
 - Supervisor: Prof. Christian Rossow
 - Expected to finish the PhD defense in September 2026.
- MSc | University College London2021-09 to 2022-09
 - Information Security
 - Distinction Degree (First Class Degree)
- BEng | Hunan University2016-09 to 2020-06
 - GPA: 3.89 / 4.5
 - 2019 First Class Scholarship

Publications

- TCP Spoofing: Reliable Payload Transmission Past the Spoofed TCP HandshakeCCF-A | IEEE S&P 2024
 - Yepeng Pan, Christian Rossow
 - Demonstrated methods to assist blind off-path TCP spoofing through weaknesses in TCP specification, TCP stack implementations, and TCP-based applications.
 - Led to Linux and FreeBSD kernel patches; findings contributed to an IETF Internet-draft.
- Loopy Hell(ow): Infinite Traffic Loops at the Application LayerCCF-A | USENIX Security 2024
 - Yepeng Pan, Anna Ascheman, Christian Rossow
 - Uncovered application-layer traffic loops across UDP-based services (DNS, NTP, TFTP, QUIC) and measured their prevalence through an Internet-wide study.
 - Identified hundreds of thousands of vulnerable devices; coordinated disclosure with CERT/CC to 20 vendors, with impact confirmed by major service providers including Google.
- GET /large.file HTTP/1.1: Connection-Based TCP Amplification AttacksCCF-B | ACSAC 2025
 - Yepeng Pan, Lars Richter, Christian Rossow
 - Revealed connection-based TCP amplification attacks enabled by predictable TCP initial sequence numbers in real-world HTTP deployments.
 - Identified six predictable ISN patterns and over 50K vulnerable devices through Internet-wide measurement, enabling amplification factors of up to 16.77×. Coordinated disclosure led to vendor investigations and patches.
- FRAGJAM: DoS Attacks Using IP Reassembly CongestionCCF-A | USENIX Security 2026
 - Yepeng Pan, Christian Rossow
 - Proposed a buffer-congestion-based denial-of-service attack that exploits the IP fragment reassembly implementation of Linux-based NAT gateways and UDP services that rely on fragmentation.
 - Demonstrated practical attacks against widely deployed services, including RADIUS, Video conferencing, VPN, as well as deployments by major providers such as Zoom, and confirmed their real-world prevalence through empirical measurement.

Teaching Experience

- Network Security (Master)
- CTF Challenges for the Network Security Course
- CTF Challenges for the Network Security Course
- Instructor | 2026-10 to 2027-02
- Teaching Assistant | 2024
- Teaching Assistant | 2023

Student Supervision

• Research on state of IP Spoofing in Cloud Providers	Bachelor's Thesis 2026
• CGNAT Laser DoS Attack	Master's Thesis 2026
• State Learning for TCP Stack Fingerprinting	Master's Thesis 2025
• CGNAT Congestion-based DoS Attack	Bachelor's Thesis 2025
• Measurement of Information Disclosure by MQTT Servers	Bachelor's Thesis 2025
• Fuzzing-based Application Layer Traffic Loop Identification	Bachelor's Thesis 2024

Professional Service

• Program Committee Member	ACM CCS 2026
• Program Committee Member	USENIX Security 2027