NTT

MWS2023プレミーティング

サイバーセキュリティ研究トレンド2023（の調査方法）

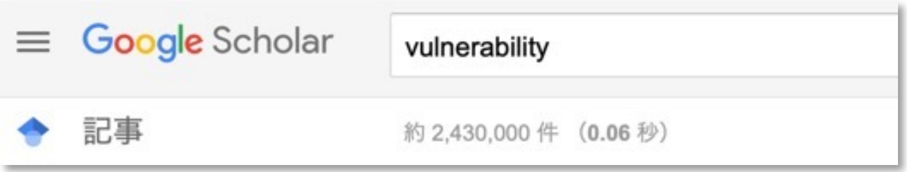
2023年6月29日

NTT 社会情報研究所

秋山満昭

論文が多すぎる

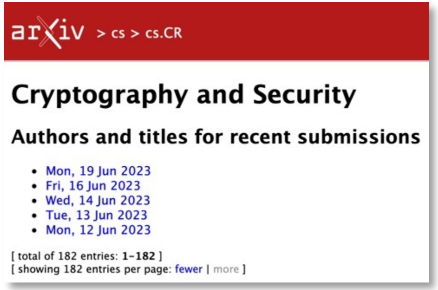
- Google Scholar
  - vulnerability: **約2,430,000**, malware: **約145,000件**,



Google Scholar vulnerability

記事 約 2,430,000 件 （**0.06** 秒）

- arXiv（未査読のプレプリント論文）
  - Cryptography and Securityカテゴリ：**約200件/週**



arXiv > cs > cs.CR

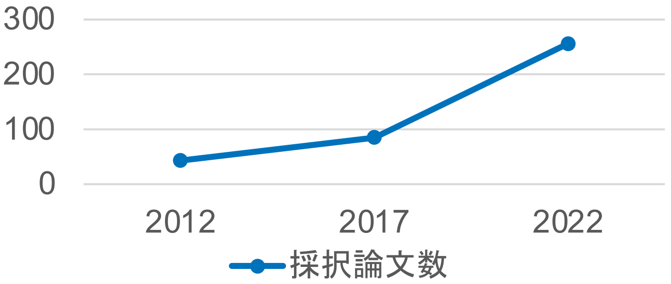
Cryptography and Security

Authors and titles for recent submissions

- Mon, 19 Jun 2023
- Fri, 16 Jun 2023
- Wed, 14 Jun 2023
- Tue, 13 Jun 2023
- Mon, 12 Jun 2023

[total of 182 entries: **1-182**]
[showing 182 entries per page: fewer | more]

- 難関会議採択論文の増加
  - USENIX Security採択論文：2013年～2022年の**10年間で5倍**に増加



査読付き論文 vs. プレプリント

媒体	品質	速報性
査読付き論文	高い （投稿先によって大きく異なるが、査読を経るためある程度の品質は担保されている）	低い （投稿から公開までに数ヶ月～1年以上かかる）
プレプリント	玉石混交 （査読を経ていないので品質は担保されていない）	高い （即座に公開される）

いい研究（論文）を発見するために

- 査読付き論文とプレプリントの特性を理解する
- 品質を重視
  - Top-4（やTier-2）国際会議などの論文を中心に調査する
    - Top-4: IEEE S&P, USENIX Security, ACM CCS, ISOC NDSS
    - 参考: <https://people.engr.tamu.edu/guofei/sec_conf_stat.htm> <http://jianying.space/conference-ranking.html>
  - 引用数の多さ（公開間もない論文は引用がつきにくいので注意）
- 速報性を重視
  - プレプリントを調査する
  - 品質の高い論文であるかどうかをある程度見極める
    - 完結した論文であるか
    - 著者グループがその分野で実績があるか
    - 将来の著名国際会議で採択されているか（著者のウェブサイトで確認できることも）

バランスよく調査する（速報性だけを重視して時間を浪費しないように）

トレンド？

- 研究対象が多様化しているので一言で説明できない
  - Top-4国際会議のセッション割や論文賞を見ればわかるかもしれない

USENIX Security 2022のセッション一覧

NTT

Client-Side Security

Crypto I: Attacking Implementations

Crypto II: Performance Improvements

Crypto III: Private Matching & Lookups

Crypto IV: Databases & Logging

Crypto V: Provers & Shuffling

Crypto VI

Deanonymization

Differential Privacy

Fuzzing I: Networks

Fuzzing II: Low-Level

Fuzzing III

Fuzzing, OS, and Cloud Security

Hardware Security I: Attacks & Defenses

Hardware Security II: Embedded

Hardware Security III

Information Flow

Kernel Security

Measurement I: Network

Measurement II: Auditing & Best Practices

Measurement III

Measurement IV

ML I: Federated Learning

ML II

ML III

ML IV: Attacks

ML V: Principles & Best Practices

ML VI: Inference

Mobile Security

Network Security I: Scanning & Censorship

Network Security II: Infrastructure

Network Security III: DDoS

Network Security IV

OS Security & Formalisms

Passwords

Privacy, User Behaviors, and Attacks

Security Analysis

Security Practitioners & Behaviors

SGX I & Side Channels III

SGX II

Side Channels I: Hardware

Side Channels II

Side Channels IV

Smart Homes I

Smart Homes II

Smart Vehicles

Software Forensics

Software Security

Software Vulnerabilities

User Studies I: At-Risk Users

User Studies II: Sharing

User Studies III: Privacy

User Studies IV: Policies & Best Practices

Web Security I: Vulnerabilities

Web Security II: Fingerprinting

Web Security III: Bots & Authentication

Web Security IV: Defenses

Web Security V: Tracking

Wireless Security

Zero Knowledge

CCS 2022のセッション一覧

Applied Crypto: Advanced Public-Key Encryption Schemes

Applied Crypto: Cryptographic Protocols

Applied Crypto: Digital Currencies & Blockchains

Applied Crypto: Digital Signatures

Applied Crypto: Key-Exchange

Applied Crypto: Secure Multiparty Computation

Applied Crypto: Secure Multiparty Computation & Private- Set Intersection

Applied Crypto: Symmetric-Key Encryption and Attacks

Applied Crypto: Zero-Knowledge 1

Applied Crypto: Zero-Knowledge 2

Blockchain and Distributed Systems

Blockchain and Distributed Systems

Blockchain and distributed systems

Blockchain and distributed systems

FM & PL: Hardware Security

FM & PL: Security Protocols

HW & CPS: Aspects of Masking

HW & CPS: Attacks and Defense

HW & CPS: CPS and IoT

HW & CPS: Side Channels

HW & CPS: Side Channels

HW & CPS: Side Channels: Defences

HW & CPS: Side Channels: Hardware and Microarchitecture

ML: Adversarial Examples in ML

ML: Adversarial Examples in ML

ML: Attacks to ML

ML: Federated Learning Security

ML: Inference Attacks to ML

ML: Inference Attacks to ML

ML: ML for Network Security

ML: Poisoning and Backdooring ML

Network Security: Cloud and IoT Security

Network Security: Cloud and IoT Security

Network Security: Internet Security

Network Security: Network Vulnerabilities

Network Security: Network Vulnerabilities

Priv & Anon: Ads and Location Privacy

Priv & Anon: Ads and Location Privacy

Priv & Anon: Differential Privacy

Priv & Anon: Differential Privacy

Priv & Anon: Federated Analytics and Learning

Priv & Anon: Online, Mobile and Multimedia Privacy

Priv & Anon: Online, Mobile and Multimedia Privacy

Priv & Anon: Privacy Attacks in ML

Priv & Anon: Privacy Attacks in ML

Priv & Anon: Privacy in Graphs

Priv & Anon: Privacy Preserving ML

Priv & Anon: Secure Query Answering

Software Security: Analysis

Software Security: Defenses and Virtualization-Based Security

Software Security: Fuzzing

Software Security: Hardware-Assisted Defense

Software Security: Hardware-Assisted Defense

Software Security: Information Leakage and Access Control

Software Security: Vulnerability Detection

Software Security: Vulnerability Detection

Usability & Measurement: Attacks

Usability & Measurement: Attacks

Usability & Measurement: Finding Violations

Usability & Measurement: Security and Privacy Practices

Web Security: Client Side Security

Web Security: Server-Side Security

Web Security: The C in Web Stands for Crypto

Web Security: The C in Web Stands for Crypto

Web Security: Users Under Attack

S&P 2023のセッション一覧

Applied cryptography

Authentication

Biometric security

Blockchain 1

Blockchain 2

Bug finding

Cryptographic attacks

Cryptographic proof techniques

Cryptographic protocols

Election and device recycling

Fuzzing

Human factors

Human factors 2

Infrastructure security

IoT security

Low-level software security

Machine learning assurance

Machine learning backdoors

Machine learning privacy

Malware and malicious sites

ML attacks

ML Security and Privacy

Model-based software security

Network security

Physical channel attacks

Physical channels 2

Privacy and covert channels

Rowhammer and spectre

Side-channel attacks

SMC

Software isolation

Software security

Software supply chains

Trust and safety

Web security

Web security

NDSS 2023のセッション一覧

- Blockchains I
- Blockchains II
- Cloud and Edge Computing
- Cyber Attacks
- Cyber-Crime and Forensics
- Cyber-Physical Systems Security I
- Cyber-Physical Systems Security II
- Fuzzing
- Keys and Certification
- ML and AI I
- ML and AI II
- ML and AI III
- Mobile Security and Privacy
- Network Protocols
- Privacy and Anonymity I
- Privacy and Anonymity II
- Software Security I
- Software Security II
- Trustworthy Computing
- Usable Security and Privacy
- Web Security I
- Web Security II
- Web Security III

論文賞（distinguished paper awards）

- USENIX Security 2022
  - OpenVPN is Open to VPN Fingerprinting
  - The Antrim County 2020 Election Incident: An Independent Forensic Investigation
  - An Audit of Facebook's Political Ad Policy Enforcement
  - Online Website Fingerprinting: Evaluating Website Fingerprinting Attacks on Tor in the Real World
  - Attacks on Deidentification's Defenses
  - Identity Confusion in WebView-based Mobile App-in-app Ecosystems
  - Provably-Safe Multilingual Software Sandboxing using WebAssembly
  - Faster Yet Safer: Logging System Via Fixed-Key Blockcipher
  - Private Signaling
  - FIXREVERTER: A Realistic Bug Injection Methodology for Benchmarking Fuzz Testing
  - Dos and Don'ts of Machine Learning in Computer Security
  - Augmenting Decompiler Output with Learned Variable Names and Types
- CCS 2023
  - Victory by KO: Attacking OpenPGP Using Key Overwriting
  - Proving UNSAT in Zero Knowledge
  - Automatic Detection of Speculative Execution Combinations
  - Zapper: Smart Contracts with Data and Identity Privacy
  - STAR: Secret Sharing for Private Threshold Aggregation Reporting
- S&P 2023
  - MEGA: Malleable Encryption Goes Awry
  - Practically-exploitable Cryptographic Vulnerabilities in Matrix
  - Weak Fiat-Shamir Attacks on Modern Proof Systems
  - Typing High-Speed Cryptography against Spectre v1
  - Red Team vs. Blue Team: A Real-World Hardware Trojan Detection Case Study Across Four Modern CMOS Technology Generations
  - It's (DOM) Clobbering Time: Attack Techniques, Prevalence, and Defenses
  - The Leaky Web: Automated Discovery of Cross-Site Information Leaks in Browsers and the Web
  - WaVe: a verifiably secure WebAssembly sandboxing runtime
  - Characterizing Everyday Misuse of Smart Home Devices
  - Not Yet Another Digital ID: Privacy-preserving Humanitarian Aid Distribution
  - “In Eighty Percent of the Cases, I Select the Password for Them”: Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya
  - Space Odyssey: An Experimental Software Security Analysis of Satellites
- NDSS 2023
  - Your Router is My Prober: Measuring IPv6 Networks via ICMP Rate Limiting Side Channels

論文賞（distinguished paper awards）

CSS（コンピュータセキュリティシンポジウム）で考えると どのトラックぽい？

暗号ぽい

- Faster Yet Safer: Logging System Via Fixed-Key Blockcipher
- Victory by KO: Attacking OpenPGP Using Key Overwriting
- Proving UNSAT in Zero Knowledge
- MEGA: Malleable Encryption Goes Awry
- Practically-exploitable Cryptographic Vulnerabilities in Matrix
- Weak Fiat-Shamir Attacks on Modern Proof Systems
- Typing High-Speed Cryptography against Spectre v1

PWSぽい

- Attacks on Deidentification's Defenses
- Private Signaling
- STAR: Secret Sharing for Private Threshold Aggregation Reporting
- Not Yet Another Digital ID: Privacy-preserving Humanitarian Aid Distribution

BWSぽい

- Zapper: Smart Contracts with Data and Identity Privacy

UWSぽい

- Characterizing Everyday Misuse of Smart Home Devices
- “In Eighty Percent of the Cases, I Select the Password for Them”: Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya

MWSぽい

- Red Team vs. Blue Team: A Real-World Hardware Trojan Detection Case Study Across Four Modern CMOS Technology Generations
- Augmenting Decompiler Output with Learned Variable Names and Types

システムorMWSぽい

- FIXREVERTER: A Realistic Bug Injection Methodology for Benchmarking Fuzz Testing

システムぽい

- OpenVPN is Open to VPN Fingerprinting
- The Antrim County 2020 Election Incident: An Independent Forensic Investigation
- An Audit of Facebook's Political Ad Policy Enforcement
- Online Website Fingerprinting: Evaluating Website Fingerprinting Attacks on Tor in the Real World
- Identity Confusion in WebView-based Mobile App-in-app Ecosystems
- Provably-Safe Multilingual Software Sandboxing using WebAssembly
- Dos and Don'ts of Machine Learning in Computer Security
- Automatic Detection of Speculative Execution Combinations
- It's (DOM) Clobbering Time: Attack Techniques, Prevalence, and Defenses
- The Leaky Web: Automated Discovery of Cross-Site Information Leaks in Browsers and the Web
- WaVe: a verifiably secure WebAssembly sandboxing runtime
- Your Router is My Prober: Measuring IPv6 Networks via ICMP Rate Limiting Side Channels
- Space Odyssey: An Experimental Software Security Analysis of Satellites

「現場の奥地」からの報告（1）

- The Antrim County 2020 Election Incident: An Independent Forensic Investigation (USENIX Security 2022)
- Investigating State-of-the-Art Practices for Fostering Subjective Trust in Online Voting through Interviews (USENIX Security 2022)
- Helping hands: Measuring the impact of a large threat intelligence sharing community (USENIX Security 2022)
- Why Users (Don't) Use Password Managers at a Large Educational Institution (USENIX Security 2022)
- RE-Mind: a First Look Inside the Mind of a Reverse Engineer (USENIX Security 2022)
- Characterizing the Security of Github CI Workflows (USENIX Security 2022)
- 99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms (USENIX Security 2022)

「現場の奥地」からの報告（2）

- Understanding the How and the Why: Exploring Secure Development Practices through a Course Competition (CCS 2022)
- SoK: Taxonomy of Attacks on Open-Source Software Supply Chains (S&P 2023)
- No One Drinks From the Firehose: How Organizations Filter and Prioritize Vulnerability Information (S&P 2023)
- Vulnerability Discovery for All: Experiences of Marginalization in Vulnerability Discovery (S&P 2023)
- Everybody's Got ML, Tell Me What Else You Have: Practitioners' Perception of ML-Based Security Tools and Explanations (S&P 2023)