On the Mismatch of Disclosure Practices in Security and Privacy Research

Simon Koch, Jannik Hartung, Rainer Böhme, David Klein

Max Planck Institute for Security and Privacy

david.klein@mpi-sp.org

MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

universität
innsbruck

Technische
Universität
Braunschweig

Security Research for Vulnerability Detection

> *. . . we fuzz over 1,000 API endpoints of the 115 most popular WordPress plugins, resulting in over 20 security issues and 2 new CVE-IDs.*
>
> *—Abstract of "What All the PHUZZ Is About: A Coverage-guided Fuzzer for Finding Vulnerabilities in PHP Web Applications"*

Security Research for Vulnerability Detection

Usually done in the following steps:

- Identification of a vulnerability

Security Research for Vulnerability Detection

Usually done in the following steps:

- Identification of a vulnerability
- Reproduction

Security Research for Vulnerability Detection

Usually done in the following steps:

- Identification of a vulnerability
- Reproduction
- Identify responsible Party

Security Research for Vulnerability Detection

Usually done in the following steps:

- Identification of a vulnerability
- Reproduction
- Identify responsible Party
- Disclose Vulnerability to responsible party

Security Research for Vulnerability Detection

Usually done in the following steps:

- Identification of a vulnerability
- Reproduction
- Identify responsible Party
- Disclose Vulnerability to responsible party

The community has widely adopted responsible disclosure for vulnerability disclosure

Security Research for Vulnerability Detection

Usually done in the following steps:

- Identification of a vulnerability
- Reproduction
- Identify responsible Party
- Disclose Vulnerability to responsible party

The community has widely adopted responsible disclosure for vulnerability disclosure . . . and actually enforces disclosure takes place!

Security Research for Vulnerability Detection

Usually done in the following steps:

- Identification of a vulnerability
- Reproduction
- Identify responsible Party
- Disclose Vulnerability to responsible party

The community has widely adopted responsible disclosure for vulnerability disclosure . . . and actually enforces disclosure takes place!

> **Reasons to Reject the Paper:**
> *Notification: I didn't see any discussion of plans to notify vulnerable sites*
>
> — *Reviewer #2*

Duality with Privacy Research?

Since GDPR and similar legislature, we have seen a variety of compliance research

Duality with Privacy Research?

Since GDPR and similar legislature, we have seen a variety of compliance research

> *. . . out of* 13 082 *apps implemented consent notices, we identify* 2688 *(*20.54*%) apps violate at least one of the GDPR consent requirements, . . .*
>
> —*Abstract of "Freely Given Consent?: Studying Consent Notice of Third-Party Tracking and Its Violations of GDPR in Android Apps"*

Duality with Privacy Research?

Since GDPR and similar legislature, we have seen a variety of compliance research

> *. . . out of* 13 082 *apps implemented consent notices, we identify* 2688 *(*20.54*%) apps violate at least one of the GDPR consent requirements, . . .*
>
> —*Abstract of "Freely Given Consent?: Studying Consent Notice of Third-Party Tracking and Its Violations of GDPR in Android Apps"*

Does the privacy community follow similar procedures?

Conference Point of View

Requirements By Conferences

Do the call for papers require disclosure?

Requirements By Conferences

Do the call for papers require disclosure?

We looked at Security and Privacy venues ranked A or A* between 2018 and 2026

Requirements By Conferences

Venue	Disclosure Requirements as Specified by CfP								
	'18	'19	'20	'21	'22	'23	'24	'25	'26
IEEE S&P	●	●	●	◐	◐	◐	◐	◐	◐
ACM CCS	○	○	○	○	○	○	○	○	⊗
USENIX Security	●	●	●	●	●	◐	◐	⊗	⊗
NDSS	**N/A**	◐	◐	◐	◐	◐	◐	◐	◐
PETS	○	○	○	○	○	○	○	○	○
ACSAC	○	○	○	○	○	◐	◐	◐	**N/A**
IEEE Euro S&P	○	○	○	○	⊗	⊗	⊗	⊗	○
ACM Asia CCS	○	○	○	○	○	**N/A**	○	○	○
RAID	○	⊗	⊗	⊗	⊗	⊗	⊗	⊗	**N/A**
ESORICS	**N/A**	○	○	○	○	○	○	○	○

Table: Venue requires disclosure for Security vulnerabilities (◐), both (●), mention disclosure but do not specify whether for security or privacy (⊗), or do not mention disclosure at all (○).

Requirements By Conferences: Summary

Notable Findings:

- CfPs are often kept rather vague regarding disclosure and change over time
- Usenix and S&P used to require privacy disclosure but switched to either security only or ambiguous wording
- PETS does not require any disclosure according to the CfP

Author Point of View

Dataset

- We built a dataset of potentially interesting papers by scanning the abstracts of papers published at these venues since 2018

Dataset

- We built a dataset of potentially interesting papers by scanning the abstracts of papers published at these venues since 2018
- Search terms:
  - Privacy: “GDPR” or “CCPA” and any form of “violation”
  - Security: “vulnerability” and any form of “detection”

Dataset

- We built a dataset of potentially interesting papers by scanning the abstracts of papers published at these venues since 2018
- Search terms:
  - Privacy: “GDPR” or “CCPA” and any form of “violation”
  - Security: “vulnerability” and any form of “detection”
- This left us with 35 matches for privacy and 421 for security
  - Due to imbalance in the numbers we sampled a subset of security papers
    - Distributed across years and disclosure requirements from the CfPs
  - Based on abstracts we filtered for in scope papers

Dataset

- We built a dataset of potentially interesting papers by scanning the abstracts of papers published at these venues since 2018
- Search terms:
  - Privacy: “GDPR” or “CCPA” and any form of “violation”
  - Security: “vulnerability” and any form of “detection”
- This left us with 35 matches for privacy and 421 for security
  - Due to imbalance in the numbers we sampled a subset of security papers
    - Distributed across years and disclosure requirements from the CfPs
  - Based on abstracts we filtered for in scope papers
- Ultimately: 19 privacy and 23 Security papers

Methodology

We then analyzed every paper about mentions of disclosure and grouped into:

- **disclosure**: Issues were disclosed to all affected parties
- **partial disclosure**: Issues were disclosed to some affected parties
- **no disclosure**: No mention of disclosure

Methodology

We then analyzed every paper about mentions of disclosure and grouped into:

- **disclosure**: Issues were disclosed to all affected parties
- **partial disclosure**: Issues were disclosed to some affected parties
- **no disclosure**: No mention of disclosure
- Done by two researchers independently and resolved conflicts
- No disclosure statement does not imply no disclosure!

Disclosure Practices for Security Research

Security (23 papers):

- **disclosure**: 16
- **partial disclosure**: 1
- **no disclosure**: 6, with two papers discussing disclosure

Disclosure Practices for Security Research

Security (23 papers):

- **disclosure**: 16
- **partial disclosure**: 1
- **no disclosure**: 6, with two papers discussing disclosure

- Not always completely clear whether disclosure is required
- Two papers without disclosure did not disclose due to:
  - Upstream independently fixed everything
  - Concerning smart contracts without clear responsible party

Disclosure Practices for Privacy Research

Privacy (19 papers):

Disclosure Practices for Privacy Research

Privacy (19 papers):

- **disclosure**: 4
- **partial disclosure**: 3
- **no disclosure**: 12, with one paper discussing disclosure
- One paper without disclosure did not disclose due to:
  - False Positives from their Pipeline, so not every finding is a true violation

Differences: Summary

Stark difference between privacy and security research wrt disclosure

- Security: 69% did disclose all findings
- Privacy: 21% did disclose all findings

Differences: Summary

Stark difference between privacy and security research wrt disclosure

- Security: 69% did disclose all findings
- Privacy: 21% did disclose all findings

Security has well established practices and a community consensus...

Differences: Summary

Stark difference between privacy and security research wrt disclosure

- Security: 69% did disclose all findings
- Privacy: 21% did disclose all findings

Security has well established practices and a community consensus... ... that privacy research lacks

Can we Transfer Security Disclosure Practices to Privacy?

- **Identification**:
  - Requires understanding of local legal particularities
  - Harm/impact of privacy violations is not always fully clear
- **Reproduction**:
  - More difficult to create/communicate
  - Often requires interaction with third parties: ethical challenges
- **Responsible Party**:
  - Developer? Authorities? Wildly different implications
  - Is the violated regulation actually enforceable
- **Disclosure**:
  - More difficult to communicate
  - Authors have different feeling how to approach disclosure
  - Risk of repeating the CVE situation

Can we Transfer Security Disclosure Practices to Privacy?

- **Identification**:
  - Requires understanding of local legal particularities
  - Harm/impact of privacy violations is not always fully clear
- **Reproduction**:
  - More difficult to create/communicate
  - Often requires interaction with third parties: ethical challenges
- **Responsible Party**:
  - Developer? Authorities? Wildly different implications
  - Is the violated regulation actually enforceable
- **Disclosure**:
  - More difficult to communicate
  - Authors have different feeling how to approach disclosure
  - Risk of repeating the CVE situation

Challenging, does not directly translate

Closing Words

Should the community adopt a disclosure model for privacy?

How could a model for privacy disclosure look like?

Are we happy with the current security disclosure practices?

Contact

david.klein@mpi-sp.org
leinea
twitter.com/ncd_leen