DIMVA 2022 Call for Papers

Important Dates (AoE)

- Submission: Mar 10, 2022
- Notification: Apr 30, 2022
- Camera-ready deadline: May 10, 2022
- Conference: Jun 29-Jul 1, 2022, Cagliari, Italy

General Information

The annual DIMVA conference serves as a premier forum for advancing the state of the art in the broader areas of intrusion detection, malware analysis, and vulnerability assessment. Each year, DIMVA brings together international experts from academia, industry, and government to present and discuss novel research in these areas. DIMVA is organized by the special interest group Security - Intrusion Detection and Response (SIDAR) of the German Informatics Society (GI). The conference proceedings will appear in Springer Lecture Notes in Computer Science (LNCS) series.

Topics of Interest

DIMVA solicits submissions of high-quality, original scientific papers presenting novel research on malware analysis, intrusion detection, vulnerability assessment, and related systems security topics.

Topics of interest include, but are not limited to:

Intrusions

- Novel approaches and domains
- Insider detection
- Prevention and response
- Data leakage, exfiltration, and poisoning
- Result correlation and cooperation
- Evasion and other attacks
- Potentials and limitation
- Operational experiences
- Privacy, legal, and social aspects
- Targeted attacks

Malware

- Automated analyses
- Behavioral models
- Prevention and containment
- Classification

- Lineage
- Forensics and recovery
- Underground economy
- Vulnerabilities in malware

Vulnerability detection

- Vulnerability prevention
- Vulnerability analysis
- Exploitation and defenses
- Hardware vulnerabilities
- Situational awareness
- Active probing

Papers will be judged on novelty, significance, correctness, and clarity. We expect all papers to provide enough details to enable reproducibility of the experimental results. We encourage papers that bridge research in different communities. We also welcome experience papers that clearly articulate lessons learnt.

Types of Submissions Solicited

We invite submissions of two types:

Full Paper: presenting novel and mature research results. Full papers are limited to 20 pages in Springer LNCS format, including bibliography and appendices.

Short Paper: presenting original, still ongoing work that has not yet reached the maturity required for a full paper. Short papers are limited to 10 pages in Springer LNCS format, including bibliography and appendices. Short papers will be included in the proceedings. The title of short papers must start with the words "Extended Abstract".

Papers that do not follow the above formatting guidelines may be rejected without review.

Submission Guidelines

DIMVA 2022 will adopt a double-blind reviewing process. All submissions should be appropriately anonymized. Author names and affiliations must be excluded from the paper. Furthermore, authors should avoid obvious self-references, and should cite their own previous work in third person, whenever necessary. Papers that are not properly anonymized risk being rejected without review.

Submissions must be original work and may not be under submission to another venue at the time of review. At least one author of each accepted paper is required to physically present the submitted work at the conference, for the paper to be included in the proceedings.

Authors are encouraged to submit code appropriately anonymized, using, e.g., https://anonymous.4open.science/

Papers can be submitted using https://dimva2022.hotcrp.com/

Ethical considerations

Submissions that report experiments with data gathered from human subjects should disclose whether the research received approval from an institutional ethics review boards (IRB), if applicable, and what measures were adopted to minimize risks to privacy.

Submissions that describe experiments related to vulnerabilities in software or systems should discuss the steps taken to avoid negatively affecting any third-parties (e.g., in case of probing of network devices), and how the authors plan to responsibly disclose the vulnerabilities to the appropriate software or system vendors or owners before publication.

If you have any questions, please contact the program chairs at pc-chairs@dimva.org.