information technology

– Call for Papers –

Special Issue on

Information Security Methodology and Replication Studies

Guest Editors:

Steffen Wendzel
Worms University of Applied Sciences, Germany / FernUniversität in Hagen, Germany
wendzel@hs-worms.de

Luca Caviglione
Inst. Appl. Math. & Inf. Techn., National Research Council (CNR), Italy
luca.caviglione@ge.imati.cnr.it

Aleksandra Mileva
University Goce Delcev, Macedonia
aleksandra.mileva@ugd.edu.mk

Jean-Francois Lalande
CentraleSupélec / Inria, France
jean-francois.lalande@irisa.fr

Wojciech Mazurczyk
Warsaw University of Technology, Poland
w.mazurczyk@tele.pw.edu.pl

Background & Call for Manuscripts

It is a trend of recent years that the scientific community started to foster the discussion on fundamentals of information security. These fundamentals include several important aspects such as the unified description of attacks and countermeasures, the reproducibility of experiments and means to achieve reproducibility, the sharing of research data and code, the discussion of quality criteria for experiments and the design and implementation of testbeds.

The related academic publications contributed to the advancement of information security research, e.g., by making research contributions easier to compare. Moreover, work on terminology and taxonomy addressed redundancies and unified the understanding between different sub-domains of information security.

This special issue desires to foster the progress in research on the scientific methodology of information security, to improve the links between sub-domains of information security research and to advance the discussion on the scientific methodology in information security. Moreover, this special issue welcomes submissions that address aspects of higher education in information security and works that evaluate existing research results by reproducing experiments.

Topics of interest include, but are not limited to:

- Data collection and measurement in information security research.
- Work that reproduces existing experiments, i.e., that confirms/disproves experimental results or that shows how replication platforms can be realized in information security.
- Work that discusses the underlying criteria for the design and evaluation for cyber security research testbeds.
- Provision of novel testbeds that advance the understanding of information security sub-fields, e.g., by using visual analytics or by automating steps previously conducted manually.
- Evaluation of the novelty of research contributions and handling of scientific re-inventions.
- Methodology in network security, cryptography, information hiding, IoT security, system security, digital forensics, and other sub-disciplines of information security.
- Methodology for privacy, information sharing and collaborative work in the context of information security.
- Advanced methods and evaluations of approaches in teaching information security in higher education.
- Submissions that present shared information security research infrastructure, e.g., multi-national/multi-institutional testbeds or frameworks.
- Scientometric/bibliometric analyses, e.g., citation behavior, in information security.

Tentative Schedule

Submission Due: 15th November 2021
First Review Notification: 20th December 2021
Revision Due: 20th January 2021
Second Review Notification: 8th March 2022