4th International Workshop on Software Security: Challenges, Opportunities, and Lessons Learned

Workshop Organisers

Dr. Sajjad Mahmood
Associate Professor
Information and Computer Science Department,
Interdisciplinary Research Center for Intelligent Secure Systems,
King Fahd University of Petroleum and Minerals, Saudi Arabia
Email: smahmood@kfupm.edu.sa

Dr. Mohammad Alshayeb
Professor of Software Engineering
Information and Computer Science Department,
Interdisciplinary Research Center for Intelligent Secure Systems,
King Fahd University of Petroleum and Minerals, Saudi Arabia
Email: alshayeb@kfupm.edu.sa

Dr. Mahmood Niazi
Professor of Software Engineering
Information and Computer Science Department,
Interdisciplinary Research Center for Intelligent Secure Systems,
King Fahd University of Petroleum and Minerals, Saudi Arabia
Email: mkniazi@kfupm.edu.sa

Abstract

Over the last decade, many organizations have focused on software security because modern applications typically operate in a hostile network-based environment. Traditionally, organizations have tried to address security concerns by finding and fixing security vulnerabilities once the software development cycle is completed. Software needs to be secured against any unauthorized users, and this can be achieved by incorporating security mechanisms into different phases of the software development lifecycle. However, incorporating security practices and processes into different software development life cycle phases remains a challenge. Software security is evolving due to increasing failure rates of software projects, economic downturn, software development without security in mind, globalization, and outsourcing. The empirical software engineering researchers need new approaches, models, and tools for addressing various emerging software security challenges in this modern age. There is a need for empirical evidence to support different new approaches in software security research and practice. This will provide researchers with innovative knowledge on developing different software security processes and practices. This will also help improve existing software security approaches and processes to build secure software effectively. This workshop will bring together and advance the work undertaken on software security. The outcome of this workshop will provide researchers and practitioners with a firm basis on which to develop different practices/ tools/ techniques based on an understanding of how and where they fit into secure software development and research. New practices/ tools/ techniques could then be developed targeting the secure software engineering community.

Workshop Motivation

In recent years, numerous organizations have placed considerable emphasis on software security. Software security is often delegated to organizations' network infrastructure, firewalls, and intrusion detection systems [1]. For this purpose, organizations spend much money purchasing good firewalls and antivirus programs, thinking that these applications will be enough to make software secure. However, this approach is still not working perfectly, and organizations remain prone to security risks and cyber-attacks, taking advantage of security flaws [2].

Software security is defined in various ways. ISO 25010 defines security as "the degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization" [3]. There are other definitions that exist in the literature, McGraw defined it as "software security is the ability of software to resist, tolerate, and recover from events that intentionally threaten its dependability" [4]. Verdon and McGraw defined it as "Software security is about building secure software: designing software to be secure, making sure that software is secure, and educating software developers, architects, and users about how to build secure things" [1].

Several factors introduce new problems to secure software, such as the lack of software development methodologies [5], the exponential increase in Internet-enabled applications [6], the threat from hackers and the susceptibility of inexperienced Internet users [7], and the lack of empirical studies on software security. One of the most crucial points relating to these problems is the vulnerability and weak spots of software that hackers can target. Software vulnerability is "a weakness in the security system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm" [6].

With the evolving vulnerable nature of software, it is crucial to conduct empirical studies on software security to collect evidence, which can be used to evaluate and improve different tools, techniques, methods, and models used in secure software development.

Software needs to be secured against unauthorized users, which can be achieved by incorporating security mechanisms into different phases of the software development lifecycle [4]. This will guarantee that security is not an afterthought issue, i.e., only considered in the end. Previously, some work has been conducted on information security maturity, the capability of digital forensics organizations, and IT security maturity, in which the focus is on the ability of organizations to fulfill their security objectives. However, incorporating security practices and processes into different software development life cycle phases remains challenging.

Software security is evolving due to increasing failure rates of software projects, economic downturn, software development without security in mind, globalization, and outsourcing. Empirical software engineering researchers need new approaches, models, and tools to address various emerging software security challenges in this modern age. There is a need to use empirical evidence to support different new approaches in software security research and practice. This will provide researchers with innovative knowledge on developing different software security processes and practices. This will also help improve existing software security approaches and processes to develop secure software effectively. This workshop will bring together and advance the work undertaken on software security. The outcome of this workshop will provide researchers and practitioners with a firm basis for developing different practices/ tools/ techniques based on an understanding of how and where they fit into secure software development and research. New practices/ tools/ techniques could then be developed targeting the secure software engineering community.

Topics of Interest

This workshop aspires to provide international researchers and practitioners an opportunity to present the state-of-the-art, the state of the practice, and the future directions on the following topics of software security.

- Systematic literature reviews and mapping studies on software security
- Tertiary studies on software security
- Empirically based decision making
- Controlled experiments and quasi-experiments on software security
- Case studies, surveys, observational studies, Delphi studies, and field studies on software security
- Empirical studies on software security using qualitative, quantitative, and mixed methods
- Evaluation of software security techniques, tools, and models
- Secure software requirements
- Secure software design
- Secure software coding
- Secure software testing
- Secure software acceptance
- Secure software deployment, operations, and maintenance
- Secure software acquisition
- Project management for secure software development
- Software security in global projects
- Best practices and lessons learned in secure software development projects
- Secure software metrics
- Insider threats

Workshop Aim and Format

This workshop aims to provide a venue to discuss software security challenges, opportunities, and lessons learned under the umbrella of empirical software engineering and software evaluation. This workshop will bring together researchers and practitioners from academia, industry, and governments to report empirical studies and discuss the issues relating to Software Security.

This workshop will seek submissions reporting original, unpublished research on software security covering any aspect of Experimental, Empirical, and Evidence-Based Software Engineering, for example, quantitative and qualitative methods for empirical evaluation of software security techniques, processes, methods, tools, and best practices. This will be a one-day paper-based presentation workshop, accepting research and software industry papers on software security.

Paper Submission and Reviewing process

The workshop will accept submitted for both short and full papers. The maximum page length for the short paper is five. The maximum page length for the full paper will be ten pages. Submitted papers must be written in English, contain original unpublished work, and conform to the ACM proceedings format. The reviewers (minimum two reviewers per paper) for this workshop will include well-known researchers and practitioners in software security.

Previous experience of the organizers

The proposed team has significant experience in organizing such academic events.

The team successfully organized the three workshops, "International Workshop on Secure Software: Challenges, Opportunities, and Lessons Learned," with EASE 2020, EASE 2022 and EASE 2023.

Moreover, Dr. Niazi organized the EASE 2009 and EASE 2010 conferences and worked as a co-chair for these international conferences. He also worked as a poster chair for EASE 2019. In addition, he chaired IEEE INMIC 2012 and PROFES 2010 doctoral symposium. Moreover, Dr. Niazi has worked as an editor for three issues of the IET Software journal and one issue of the Information and Software Technology Journal.

Dr. Alshayeb was a technical committee member for SANER 2019, LASD'19, ICSED 2018, ICSED 2017, ICSEA 2017, FIT 2016, ICSEA 2016, ICCET 2014, ICCET 2013, IEEE INMIC 2012 and IACeT'2012 and a member in the international Program Committee for SERP'09, SERP'10. He also was a member of the organizing committee of ICICS 2004. Dr. Alshayeb is a member of the editorial board of the Software Engineering Journal, Journal of Software, Journal of Information Technology & Software Engineering, and Arabian Journal of Science and Engineering.

Dr. Sajjad has worked as an editor for one special issue at Information and Software Technolgoy Journal. Moreover, he was a technical committee member for iiSC2011, INMIC 2012, CISIS 2013, ICSEA 2013, ICCCT 2014, ICET 2014, AHFE 2014, ICSEA 2014, ICCCS-2015, ICSEA 2015, INCoS 2015, ICSEA 2016 and IoT4TD 2017. Furthermore, Dr. Sajjad has reviewed papers for Information and Software Technology, Software-Practice and Experience, Journal of Software: Evolution and Process, IET Software, and Computer Standards & Interfaces.

Organization Details

Dr. Sajjad Mahmood is an Associate Professor of software engineering at the Information and Computer Science Department, King Fahd University of Petroleum and Minerals, Saudi Arabia. He received his Ph.D. from La Trobe University, Melbourne, Australia, in May 2008. Before pursuing his Ph.D., he also worked as a software engineer in the United States and Australia. He taught and designed several courses related to software engineering at KFUPM. He is an active researcher in software engineering and has published over 85 articles in peer-reviewed journals and international conferences. He has worked as principal and co-investigator in several research projects investigating issues related to global and secure software development. He has reviewed articles for international journals and has been a program committee member for international conferences. His research interests include empirical software engineering, evidence-based software engineering, global software development, secure software development, and software process improvement in general.

Dr. Mohammad Alshayeb is a Professor at the Information and Computer Science Department, King Fahd University of Petroleum and Minerals, Saudi Arabia. He received his MS and Ph.D. in Computer Science and certificate of Software Engineering from the University of Alabama in Huntsville in 2000, 2002, and 1999 respectively. Dr. Alshayeb worked as a senior researcher and Software Engineer and managed software projects in the United States and the Middle East. Dr. Alshayeb taught and coordinated industrial training courses. He provided consulting services to major industrial and educational institutes. Dr. Alshayeb is a member of the editorial board of the Software Engineering Journal, Journal of Software, Journal of Information Technology & Software Engineering, and the Arabian Journal of Science and Engineering. Dr. Alshayeb received several certificates of excellence and appreciation from many companies. Dr. Alshayeb received the Khalifa award for education as "the distinguished University Professor in the Field of Teaching within the Arab World" in 2016. He also received the "Excellence in Teaching," the "Excellence

in Advising" award, and the "Instructional Technology" awards from KFUPM. Dr. Alshayeb is a member of several professional associations. He is a certified project manager (PMP). Dr. Alshayeb's research interests include empirical studies in Software Engineering, software refactoring, software quality, software measurement, and metrics and object-oriented design.

Dr. Mahmood Niazi is a Professor of Software Engineering at the Information and Computer Science Department, King Fahd University of Petroleum and Minerals Saudi Arabia. He has received an MPhil degree from the University of Manchester, U.K., and a Ph.D. degree from the University of Technology Sydney, Australia. He has spent more than a decade with leading technology firms and universities as a Process Analyst, a Senior Systems Analyst, a Project Manager, and a Professor. He has participated in and managed several software development projects.

Dr. Niazi is an active researcher in the field of empirical software engineering. Dr. Niazi has published over 100 articles. He is interested in developing sustainable processes to develop systems, which are reliable, secure, and fulfill customer needs. His research interests include evidence-based software engineering, requirements engineering, sustainable, reliable, and secure software engineering processes, global and distributed software engineering, software process improvement, and project management.

Previously Dr. Niazi worked for Keele University UK, National ICT Australia, University of Technology Sydney Australia, the University of Sydney Australia, and the University of Manchester UK.

A provisional list of the reviewers

- Asif Gill, University of Technology Sydney, Australia
- Azeem Akbar, Lappeeranta-Lahti University of Technology, Finland
- Siffat Ullah Khan, Malakand University, Pakistan
- Saqib Ali, Sultan Qaboos University, Oman
- Samuel Ajila, Carleton University, Ottawa, Canada
- Sajid Anwer, Griffith University, Australia
- Richard Lai, La Trobe University, Melbourne, Australia
- More reviewers to be added.

References

[1] McGraw, G., Software Security. IEEE Security and Privacy, 2004. **2**(2): p. 80-83.

[2] Ahmed, S., Secure software development - Identification of security activities and their integration in software development lifecycle. 2007(March): p. 40-40.

[3] ISO, ISO/IEC 25010:2011: Systems and software engineering - Systems and software Quality Requirements and Evaluation 2011.

[4] McGraw, G., Software Security: Building Security. 2006: Addison Wesley.

[5] Mohaddes, H. and I. Tabatabaei, Effects of Software Security on Software Development Life Cycle and Related Security Issues. 2015. **6**(8): p. 4-12.

[6] McGraw, G., Managing software security risks. Computer, 2002. **35**(4): p. 99-101.

[7] Nash, E., Hackers bigger threat than rogue staff. 2003, VNU Publications, May.