Security and Safety for Intelligent Unmanned Autonomous Systems (SecIUAS)

ABSTRACT

Recent advances in artificial intelligence, sensing, communication, computation and storage techniques have improved the way Unmanned Autonomous Systems (UAS) interact, exchange and process information. In recent years, Intelligent Unmanned Autonomous Systems (IUAS), such as unmanned vehicles, unmanned aerial vehicles (UAV) and robots, have emerged for various applications without surveillance by humans. Yet, the success, prosperity and advancement of these intelligent systems strongly depend on the security and safety of the cyber-physical devices, system software, and application software. These systems are prone to suffering from various security and safety issues, such as hardware defects, system and application vulnerabilities, network eavesdropping, side-channel attacks and so on. These successful attacks targeted the IUAS do not only affect the security of information but also the safety of the system, which may lead to the malfunction of systems with severe financial, environmental and health losses. The goal of the 2023 SecIUAS workshop is to bring together internationally leading academic and industrial researchers in an effort to identify and discuss the major technical challenges and recent results to meet the security and safety requirements of future IUAS applications in various fields.

CCS CONCEPTS

• **Security and privacy** → **Operating systems security**; *Database and storage security*; *Formal security models*; *Embedded systems security*; • **Networks** → **Security protocols**.

KEYWORDS

Unmanned autonomous systems, operating systems security, security protocols, data security

TOPICS OF INTEREST

We solicit high-quality position papers and research papers that address opportunities and challenges in the areas of hardware security, intelligent system security, application security and network security. We welcome contributions to all relevant research on attacks on IUAS, hardware protections, secure software modelling and verification, security and safety analysis, network security and so on.

The topics of interest include, but are by no means limited to:

(1) Attacks on IUAS including spoofing, eavesdropping, side-channel attack and so on
(2) Adversarial machine learning on IUAS
(3) Hardware's vulnerabilities detection for IUAS
(4) Security protection for IUAS based on TPM (Trust Platform Model)
(5) Modelling, simulation and tools for secure and safe design of IUAS
(6) Software's vulnerabilities detection for IUAS
(7) Automatic security and safety verification for IUAS software
(8) Efficient authentication and key management between IUASs
(9) End-to-End secure communication between IUASs

MOTIVATIONS

Unmanned autonomous systems (UAS) have been widely used in the Internet of Things (IoT) to provide communication relay, data collection and other services for IoT devices. However, as a typical Cyber-Physical Systems (CPS), UASs will also have an impact on the physical world while providing digital services. For example, autonomously flying umnammed aerial vehicles (UAV) can receive control commands from the digital space and then monitor specific areas over physical space. In this process, the three levels of UAV platform, network and control may be subject to security attacks, resulting in the destruction of data integrity, confidentiality and availability, which in turn affects the flight safety of UAV. The above problems have aroused widespread concern in the security community [1–4]. However, due to the complex scenes and the progress of attack methods, the existing security protection has been unable to cope with the endless security threats. Therefore, this workshop intends to collect research on the security of UAVs to promote the development of this field. In the early stage, we have held a workshop in 2020, namely *SecICPS 2020, https://secicps.github.io/cfp.html*, and invited excellent researchers from China and the United States to communicate. Now, in order to provide a communication platform for researchers in the global UAS security community and discuss the latest research results in the past three years, we are preparing to hold a new workshop to focus on the security of UASs.

IMPORTANT DATES

(1) Paper Registration and Abstract: August 17, 2023 (AoE)
(2) Paper Submission: August 24, 2023 (AoE)
(3) Notification of Acceptance: September 24, 2023 (AoE)
(4) Camera-Ready: October 8, 2023 (AoE)

CHAIRS

Jianfeng Ma (Professor, Xidian University, China)

(1) **Email address**: jfma@mail.xidian.edu.cn
(2) **Homepage**: https://faculty.xidian.edu.cn/MJF2/zh_CN/index.htm
(3) **Biography**: Prof. Ma's research interests include the wireless network security protocols, data security and the security design of mobile intelligent systems. He has published more than 200 papers, like IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Computers, IEEE INFOCOM. He has been continuously selected as a highly cited scholar in 2019 and 2020. He has been funded by the National Natural Science Foundation of China, National Key R&D Program of China in wireless network security, unmanned system security and other aspects. Prof. Ma has been Authorized 78 technical invention patents, formulated 3 ITU safety standards, 1 national standard. He is a Member of IEEE.

Xiaohong Jiang (Professor, Future University Hakodate, Japan)

(1) **Email address**: jiang@fun.ac.jp
(2) **Homepage**: https://www.fun.ac.jp/en/faculty/jiang-xiaohong
(3) **Biography**: Dr. Jiang's research interests include computer communications networks, mainly wireless networks and optical networks, interconnection networks for massive parallel computing systems, routers/switches design for high performance networks, network coding for wireless networks, VoIP over wireless networks, network security, VLSI/WSI systems, etc. He has established the long last cooperation with top researchers in USA, Italy, Canada and China. He has supervised 5 post doctoral fellows and 25 PhD students from Japan, China, Egypt, Vietnam, Iran, etc. He has over 11 grants including Japan/USA NSF grant, Japan NSF grant and Japan JST grant, and has published over 250 technical papers at premium international journals and conferences, which include over 40 papers published in top IEEE journals and top IEEE conferences, like IEEE/ACM Transactions on Networking, IEEE Journal of Selected Areas on Communications, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Communications, IEEE INFOCOM. Dr. Jiang was the winner of the Best Paper Award and

Outstanding Paper Award of IEEE HPCC 2014, IEEE WCNC 2012, IEEE WCNC 2008, IEEE ICC 2005-Optical Networking Symposium, and IEEE/IEICE HPSR 2002. He is a Senior Member of IEEE, a Member of ACM and IEICE.

PROGRAM COMMITTEE

(1) Ning Xi (Xidian University, China)
(2) Zhiwei Zhang (Xidian University, China)
(3) Yin Chen (Keio University, Japan)
(4) Jinxiao Zhu (Toyo University, Japan)
(5) Zhenqiang Wu (Shaanxi Normal University, China)
(6) Weidong Yang (Hangzhou Institude of Technology, Xidian University, China)
(7) Zhibin Zheng (Pengcheng Laboratory)
(8) Dawei Wei (Xidian University, China)
(9) Huihui Wu (Tsinghua University)

AFTER THE CONFERENCE

Papers for accepted workshops will be published in conference companion proceedings.

REFERENCES

[1] Muhammad Adil, Mian Ahmad Jan, Yongxin Liu, Hussein Abulkasim, Ahmed Farouk, and Houbing Song. 2022. A Systematic Survey: Security Threats to UAV-Aided IoT Applications, Taxonomy, Current Challenges and Requirements With Future Research Directions. *IEEE Transactions on Intelligent Transportation Systems* 24, 2 (2022), 1437–1455.

[2] Hassan Jalil Hadi, Yue Cao, Khaleeq Un Nisa, Abdul Majid Jamil, and Qiang Ni. 2023. A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs. *Journal of Network and Computer Applications* 213 (2023), 103607.

[3] Yassine Mekdad, Ahmet Aris, Leonardo Babun, Abdeslam El Fergougui, Mauro Conti, Riccardo Lazzeretti, and A Selcuk Uluagac. 2023. A survey on security and privacy issues of UAVs. *Computer Networks* 224 (2023), 109626.

[4] Alessio Rugo, Claudio A Ardagna, and Nabil El Ioini. 2022. A security review in the UAVNet era: threats, countermeasures, and gap analysis. *ACM Computing Surveys (CSUR)* 55, 1 (2022), 1–35.