Indian Journal of Science and Technology, Vol 9(24), DOI: 10.17485/ijst/2016/v9i24/96025
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Privacy Issues of Unmanned Autonomous System

Jinkeun Hong*

Division of Information and Communication, Baekseok University, South Korea; jkhong@bu.ac.kr

Abstract

Background/Objectives: This paper reaffirmed the issue of privacy, which is a fundamental right in center of standardization and organization of unmanned autonomous environment. The privacy protection is important both individual and society in respect of value and function. Recently, the research and application of the unmanned autonomous environment with privacy is activated. Also the important of privacy issues in the unmanned auto equipment should be reconsidered. **Findings:** It can find privacy direction and concerns of unmanned aerial through EC and international standard organizations, whose are activated research and application of unmanned autonomous system. Also the main issue of privacy design is whether or not how efficiently is configured objectives, methodology and evaluation system. **Application/Improvements:** On the other hand, we can see that the importance of scalability, flexibility, persistence, opportunity and technology in unmanned autonomous system environment. In additionally, the various countermeasures are required to address the privacy issue in unmanned autonomous environment.

Keywords: Aircraft, Intelligent Traffic, Safety, Security, Standard

1. Introduction

The privacy protection is important both individual and society in respect of value and function. In[1] reviewed the experimental demonstration with integrated health monitoring in UAV task assignment. In[2] reviewed the experimental analysis of cyber security threats against teleoperated surgical robotics. It is considered vulnerability analysis, risk assessment and defense issue, attack identification and characterization and challenges specific to teleoperated procedure. In case of Raven II system, it consisted of joint, roll, tool insertion, grasping, actuator and so on. But there are factors to be considered such as latency, jitter, delay, loss and failure. It is approached to the interested issue about design of optimal controller and Kalman filter in probability of detecting attacks. The accesses of attack vector are endpoint compromise, network and communication based attack. There are 3 types of attacks such as modification, manipulation and hijacking attacks.

Nikolai Vladimirovich Kim review automated decision making in road traffic monitoring of UAV[3]. The UAV, which is included equipment such as automated control system, navigation and vision system, perform autopilot on the roadway. First over all, UAV ensure safety and security about equipment and traffic control management for traffic situation classification.

In[4] reviewed soft computing application issue of robot design. The robots are categorized as wheeled robots, flying robots, hybrid robots, legged robots, and demining robots such as TITAN VII, RIMHO-2, ECERC1, ECERC2, Hyper-Tether robot and field arm robots COMET-I and II. Also it used to fuzzy knowledge based decision system, fuzzy behavior based control, fuzzy inference system, fuzzy classification, fuzzy adaptive control for the control of aerial robot.

In[5] presented UAVs for Humanitarian Mission about autonomy and reliability. In their research, it is approached UAV architecture, which is consisted of avionics sensors, engines control, payload sensors, autonomous emergency control, autonomous flight control, autonomous sensor control, mission planning, telemetry, energy, data storage and processing, internal processing facility, communication, safety and security. Communication channel

*Author for correspondence

are supported command control channel and data sense channel and real time remote video channel. For security and safety in UAV, technology is required to autonomous navigation and identification against attack. The issue of autonomous navigation is sparse and dense 3D reconstruction using camera and autonomous attack detection is identifying individual and groups of attackers.

The consideration of unmanned aircraft system is scalability, persistence, flexibility, opportunity and technology. However, security attacks of unmanned aircraft system are various and countermeasures are various. Countermeasures are needed to various techniques and first over all, must be considered privacy issue.

In this paper, we present standard characteristics of unmanned autonomous system and especially considered privacy characteristics. In Section 2, we illustrate standard characteristics of unmanned autonomous system. In Section 3, we present our concluding remarks.

2. Privacy Standard of Unmanned Autonomous System

2.1 Privacy and Data Protection Characteristics in UAS

Cristina Pauner and Irene Kamara approach challenges and standardization of drones in the field of privacy and data protection[6]. There is not supported data protection of aerial surveillance system and required privacy risks in EU. In consideration of privacy, the regions of category are physical, information, communication and location. As like Cristima et al. there are focused on privacy issues according to lack of vehicle detection and the privacy issues are collection, storage, transmission and processing of related data. Other issues are considered legitimated collection of individual private and public information and captured with discrimination. And then it is not opened the collected private information due to unauthorized and illegal access. Also action and moving pose of vehicle must be profiling officially. In case of EUROCAE, it is researched about certification specification by WG-73 and WG-93.

In ISO, there are established ISO/TC20/SC16 for UAS and developed ISO/IEC 29101:2013 by ISO/IEC JTC1/SC27 for privacy architecture framework, ISO/IEC29100:2011 by ISO/IEC JTC1/SC27 and ISO29100 series for privacy framework. From ISO/IEC 27018 standard, it is built on security technique and control to address risk. From

Table 1. Light RPAS operations of EUROCARE WG93

Group	Items
Safety and security	Command, control and communication
	Airworthiness
	Data collection
	RPA classification
	Generic safety assessment
VLOS operation	VLOS scenarios
	Small RPA visibility characteristics
	VLOS operations – guidance to regulator document
Organizational approval	Design organization, production organization, maintenance organization
Flight crew licensing	Flight crew licensing & training
BVLOS	BVLOS scenarios

CEN M/530, it is guided to privacy and data protection issue. In Organization for the Advancement of Structured Information Standards (OASIS), it is reviewed privacy issues such as OASIS privacy management reference model and considered privacy by design documentation standard[7,8]. The ISO/IEC 29100 for privacy framework was published as international standard to privacy perspective.

The privacy framework of standardization organization is as follows in Table 2.

In ISO 29100, it is focused on privacy principles such as consent and choice, legitimacy and specification, collection limitation, data minimization, use, accuracy and quality, openness, part and access, accountability, security and privacy compliance[9].

In ISO/IEC JTC1/SC27, it is reviewed security techniques[10]. The mission of SC27 includes address of solutions method, technique and guideline about information security management systems, security mechanism and evaluation, testing and specification, controls and services, management and privacy technology. Especially, in security and privacy topic area, there are included requirements and guidance of information security management system, specific security controls, security services and controls, identity management and privacy, accreditation – certification – auditing, evaluation – testing – specification and cryptographic security mechanism.

In ISO/IEC JTC1/SC37, WG2 is biometric technical interface and WG3 is biometric data interchange. WG4 and 5 are biometric functional architecture and testing.

Table 2. Standard organization for privacy

Organization	Standard	Contents
IETF	RFC3552	Guidance for standard process with privacy
	RFC3323	Privacy service for 3rd party
	RFC3325	Privacy service for 3rd party
	RFC3041	Privacy service for IPv6
	RFC4941	Privacy service for IPv6
W3C		Privacy initiatives
ITU-T	SG17	17 recommendation, PII protection
	X.1051	Information security management guideline based on 27002
	X.1054	Governance of Information security based on 27014
	X.1085	Telebiometric Authentication framework using biometric hardware security module based on 17922
	X.cc-control	Code of practice for IS control of cloud computing based on 27002
	X.gpim	Code of practice for PII protection based on WD 29151
ETSI		GSM mobile privacy initiative, Mobile privacy design guidelines
ISO/IEC	JTC1/SC27	Information technology – security techniques
	/SC17	Cards and personal Identification
	/SC37	Biometrics
	/SG38	Distributed application platforms and services
	/SG40	IT service management and IT governance
	/SC31	Automatic ID and data capture
	27001	Information security management systems requirements
	24759	Test requirements for cryptographic modules
	27000	Overview and vocabulary
	27001	ISMS requirement
	27002	Code of practices for information security management
	27003	Information security management system guidance
	27004	ISM monitoring, measurement, analysis and evaluation
	27005	Information security risk management
	27006	International accreditation guidelines for accreditation/ registration of ISMS
	27007	Guideline for ISMS auditing
	27008	Guideline for auditor on ISMS control
	27009	27001 requirement
	27010	ISM for communication
	27011	ISM guideline for telecommunication organization based on 27002
	27013	Guidelines on the integrated implementation of 27001 and 20000-1
	27014	Governance of information security
	27015	ISM guideline for financial service
	27016	ISM guideline for organizational economics
	27017	Guideline on IS control for cloud computing based on 27002
	27019	Code of practices for protection of PII in public clouds, based on 27002
	27021	Competence requirement for ISM professional
	27033	Network security
	27014	Governance of information security
	29192	Lightweight cryptography
	29100	Privacy framework
	29101	Privacy reference architecture
	29190	Privacy capability assessment model
	29115	Entity authentication assurance
	NP11770-6	Key management
	NP TR19249	Catalogue of architecture and design principles for secure
	NP 20009-4	Anonymous entity authentication
	NP 27009	Use and application of 27001

(*Continued*)

	20008	Anonymous digital signature
	20009	Anonymous entity authentication
	NP 27050	Electronic discovery
	NP 29151	Code of practice for protection of PII
	TC68	Financial service (banking, security etc)
	TC215	Health information communication technology
	TC247	Fraud countermeasures
	TC292	Security
	TC223	Societal security
	TC284	System Management for quality of private security

In case of SC17, WG1 is test method for ID cards and WG5 is Registration Management Group (RMG). WG8 is integrated circuit card without contact and WG11 is application of biometrics to cards and personal identification.

For business plan of SC27, there are reviewed security requirement, management of information, cryptographic and other security mechanism, security aspect, conformance assessment, security evaluation and methodology[11].

It is shown organization for privacy reference as follows in Table 3.

Cristina et al. guide standard and challenge in privacy and data protection of drones[13]. In impact of drones, there are not analyzed factors such as fundamental right and element of human dignity, right to privacy interference, potential problems and potential damages. About risk assessment, there are considered lack of transparency, lack of specification and function creep, enhancement of data security and profiling. It is referenced related activities such as EC civil RPAS, EASA, EUROCAE, JARUS, ISO/TC20/SC16 on UAS.

In Privacy Management Reference Model and methodology (PMRM) of OASIS, conceptual model of PMRM is consisted of PMRM services technology, privacy architecture, uses cases, stakeholders, core concerns, policies and principles, laws and regulations, privacy controls and is based on service oriented architecture[14]. Also methodology of PMRM is processed definition stage of scope of use case, detailed stage of use case analysis, stage of operational privacy control requirement, associate stage of PMRM service, stage of map technical and process mechanism, stage of risk/compliance assessment. The analysis of use case is included in actors and systems, domains and owners, roles and responsibilities, data flows, incoming and outgoing. The PMRM service is included in agreement for negotiate permission and rules, usage for control PI use, validation to check PI, certification to check credentials, enforcement for monitor to audit exception conditions, interaction for information presentation and communication and access to view and propose changes.

Table 3. Organization for privacy reference[12]

Country	Items
USA	Privacy Act (1974)
EU	EC 108
OECD	Privacy guideline
UN	Guidelines concerning personal computer file
Hong Kong	Personal privacy ordinance
EU	Data protection directive 95/46
USA	HIPAA privacy (45 CFR part 160 and Subparts A and E of Part 164)
Canada	PIPEDA
ILO	Code of practice on the protection of worker data
USA FTC	Fair information practice principle
USA-EU	Safe harbor privacy principle
USA Ontario	Privacy Diagnostic tool
Australian	Privacy Act
USA California	Senate Bill 1386
AICPA/CICA	Privacy framework
Japan	Personal information protection act
APEC	Privacy framework

Michael presents privacy management reference model[15]. PMRM supports that it understands and analyze privacy policy and requirement. The 18 tasks of PMRM methodology are consisted of use case description and inventory, privacy policy conformance criteria, assessment preparation, identify actors and systems, identify privacy domains and owners, identify roles and responsibilities within a domain, identify touch points and data flows, identify incoming/internally generated/outgoing PI, specify inherited privacy controls and internal privacy controls, specify exported privacy controls, identify services and functions, conduct risk assessment, iterate analysis and refine.

It is considered to evolve OASIS privacy by[16]. The reason of business respect in privacy is loss of reputation and gests, overload of legal action and board dissatisfaction. The major consideration of OASIS privacy for software engineer is TC liaison, technical work, expository work, external resource, mailing list, press and so on. The Privacy by Design (PbD) is related of FIPP, GAPP and NIST 800-53.

The Standard Privacy Assessment (SPA) is guided by WG5[17]. The SPA has 5 steps such as description for detailed understanding of features, data flow which is key to apply SPA, data analysis for understand of scope of personal data, privacy safeguarding requirements to evaluate specification under review, threat analysis to identify inherent vulnerability, threat mitigation to create a robust privacy and deployment considerations to assist enhancement of privacy design.

The privacy of design process is consisted of 4 stages such as definition of principles, legal and policy requirement, definition of detailed privacy requirements, design of architecture for privacy software and building of integrated software implementation. The stage of PMRM includes detailed privacy requirement, multiple point of view, connectivity and contexts, privacy components. It is reviewed multi layers to functional privacy services such as privacy knowledge base management, privacy context and user preference management service, de identification service, redaction services and data classification at layer 1. For service integration of layer 2, there are privacy policy management, data management and analytics, audit, contract and rule management, visualization, compliance management, monitoring, retention management and compliant management. At layer 3 to privacy process, there are user request for access, policy design for implement, monitoring for develop, audit for comply, de identify for partner and assurance and compliant for resolution.

In on-site of sequence diagram, the status diagram is processed from external source, emergency: Communication system, on-site care/incident commander system, contact registry, PID service, service provider and healthcare system, emergency department system, facility HER repository, public health agency system and to PHR.

It is suggested for guideline of ISO standard and requirement of ISO/IEC 29100. The methodology for implementation of privacy framework is approached 4 stages such as plan, do, check and act. The plan stage is initiating of framework, understanding of organization, analyzing of system, project approval, scoping, build up of security policy, risk assessment and control statement. The do stage is structure of organization, document management, design of control, communication, awareness and training, implementation of control, incident management, operation management. The check stage is monitoring and evaluation, inter audit and management review. Also the act stage is treatment and continual improvement. The privacy framework is 4 phases (plan, do, check and act) and consist 18 steps and has 101 activities.

In Europe, the reference to data protection law is as follows: Art.7 DPD, Art. 29 data protection working party, Art.5 GDPR principles, and Art.6 GDPR, Art.16 DPD, ART.17 DP, Art.5 No.1, Art.30 GDPR for information security[18]. In the related of data protection policy of EU, the ePrivacy Directive and Art.14.3 have suggested for privacy by design. The privacy limitation of design is focused on fragility of privacy, metric and limitation, complexity and implementation obstacle and interpretation of privacy. Also 8 strategy of privacy design is guided as data oriented strategy (minimize, hide, separate and aggregate of design patterns), process oriented strategy (inform, control, enforce and demonstrate of design pattern). For right of individual, there are Art.12, Art.14 DPD, Art.5 No. 1, Art.7 GDPR, Art.10a GDPR, Art.13 GDPR, Art.17 GDPR, Art.19 GDPR and Art.12.

3. Conclusions

This paper is focused on privacy trend of standard organization and reference of privacy in unmanned autonomous environment. In ISO standard organization, there are established ISO/TC20/SC16 for UAS and developed ISO/IEC 29101:2013 by ISO/IEC JTC1/SC27 for privacy architecture framework, ISO/IEC29100:2011 by ISO/IEC JTC1/SC27 and ISO29100 series for privacy framework. In the mission of SC27, there include address of solutions method, technique and guideline about information security management systems, security mechanism and evaluation, testing and specification, controls and services, management and privacy technology. In privacy management reference model and methodology of OASIS, conceptual model of PMRM includes PMRM services technology, privacy architecture, uses cases, stakeholders, core concerns, policies and principles, laws and regula-

tions, privacy controls and is based on service oriented architecture.

4. Acknowledgment

This paper is supported from Department of Industry – Academia Corporation of Baekseok University.

5. References

1. Bethke B, Valenti M, How JP. UAV task assignment: Experimental demonstration with integrated health monitoring. IEEE Robotics and Automation Magazine. 2008 Mar; 15(1):39–44.
2. Bonaci T, Herron J, Yusuf T, Yan J, Kohno T, Chizeck HJ. To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robotics. arXiv preprint arXiv. 2015; 1504.04339:1–11.
3. Kim NV. Automated decision making in road traffic monitoring by on board unmanned aerial vehicle system. Indian Journal of Science and Technology. 2015 Dec; 8(S10):2–6.
4. Neshat M, Sepidname G, Mehri E, Zalimoghadam A. The review of soft computing applications in humanitarian demining robots design. Indian Jorunal of Science and Technology. 2016 Jan; 9(4):1–13.
5. Tanzi T, Apvrille L, Dugelay JL, Roudier Y. UAVs for Humanitarian Missions: Autonomy and reliability. Proceedings of IEEE GHTC; USA. 2014. p. 271–8.
6. Pauner C, Kamara I. Drones current challenges and standardisation solutions in the field of privacy and data protection. Proceedings of ITU Kaleidoscope Academic; Spain. 2015. p. 1–7.
7. OASIS. Privacy Management Reference Model and methodology (PMRM) version 1.0. Committee Specification Draft 01; 2012 Mar.
8. OASIS. Privacy by design documentation for software engineers version 1.0. Committee Specification Draft 01; 2014 Jun.
9. Veseli F, Sommer DM, Schallaock J, Krontiris I. Architecture for standardization V2. Attribute based credentials for trust. Public Final Version 2.0; 2014. p. 1–24.
10. ISO/IEC JTC1/SC27 N15410. 2016. Available from: http://www.din.de/blob/90496/1ad9717cec58d162c25e70c2c5cd3197/sc27-corporate-presentation-data.pdf
11. ISO/IEC JTC1/SC27 N15445. 2016. Available from: http://www.din.de/blob/62834/6b2e2d4b07baeb961af431037fb41c1c/sc27-business-plan-data.pdf
12. Jutla DN. Evolving OASIS privacy by design standard. Proceedings of Privacy Engineering Workshop; USA. 2014.
13. Pauner C, Kamara I, Viguri J. Drones current challenges and standardisation solutions in the filed privacy and data protection. Proceedings of ITU Kaleidoscpoe Trust in the Information Society; Spain. 2015. p. 25–37.
14. OASIS Committee. Privacy management reference model and methodology Version 1.0. Committee specification draft 01; 2012 Mar.
15. Willett M. Privacy management reference model. Proceedings of RSA Conference 2013. 2016. Available from: https://www.rsaconference.com/writable/presentations/file_upload/dsp-r35a.pdf
16. ISO/IEC 29101 Committee. Information Technology – Security Techniques – Privacy Archtecture Framework. 2013 p. 1–45. 2016. Available from: https://webstore.iec.ch/preview/info_isoiec29101%7Bed1.0%7Den.pdf
17. ISO/IEC JTC1/SC27/WG5 N514174. Standard Privacy Assessment. WG5 standard document 4; 2014.
18. ENISA. Privacy and data protection by design – From policy to engineering. EU Agency for Network and Information Security Report; 2014.