NATIONAL UNIVERSITY OF PUBLIC SERVICE
DOCTORAL SCHOOL OF MILITARY ENGINEERING

Author's summary

Dávid Ferenc Vránics

Security questions of cloud-controlled unmanned aircraft systems

Consultant: Dr. Mátyás Palik PhD

BUDAPEST, 2022

Relevance and actuality of the topic

Nowadays cloud based services are in focus to serve the ever-growing performance demands of telecommunication services. We store personal messages, data, files in cloud storage, we use cloud-based services for searching or shopping on the internet, and we keep in touch with our friends over such services. Today some companies carry their whole business in cloud, thus the security of such services shall be considered top priority.

With the advancements of technology and the decrease of physical size and manufacturing cost, remote-controlled and later fully autonomous unmanned aircraft systems (UAS) became available to everyone, and are widely used for photo and video recording, package delivery, not mentioning military and law enforcement applications.

The sudden spread of drone usage made the need for regulations obvious. For this, especially in case of more complex and dangerous operations – apart from legal regulations – a technical solution could be to provide their control and monitoring as a centralized service, ensuring their supervision and avoidance of aerial traffic incidents.

Since the 1990s, usage of both cloud systems and unmanned aircraft systems have spread in an ever-increasing pace.

By the 2010s, as an effect of popular media the two separate concepts spread in everyday life, and nowadays there are examples

even of their joint application – as cloud controlled unmanned aircraft systems.

These systems first surfaced in the fields of agriculture and geoinformatics. After the success of these applications, more research, development, and innovation projects were initiated.

Identification of the scientific problem

Performance and testability of these systems is unclear still, and which widely used protocols could provide reliable remote control and tracking in case of unmanned aircrafts over internet protocol (IP) is still an open question.

It is also worth investigating the application of these services from financial point of view. From which point is it worth renting cloud solutions instead of maintaining physical servers – or the other way around? Flexible resource management capabilities of the cloud provide previously unseen economic possibilities to maintenance and end users, which carry significant financial and reliability advantages: automatic scaling and self-healing of resources could be exceptionally useful properties in case of unmanned aircraft systems.

Abilities of cloud computing and bandwidth of fourth (fifth in several locations) generation telecommunications networks enable server-side, real-time video feed analysis and immediate correction of flight path, to avoid collision or other risk factors, processing immediate, dynamic sources of danger on operations.

Take as example avoidance of dangerous meteorological phenomena or occasional search and rescue flights. Apart from danger avoidance, the situational analysis of aircraft in need can highlight the physical limits of such systems.

It is also a question if data (e.g., position data) collected during the operation of such systems can be interesting for other aerial or ground-based traffic control systems, so it is worth researching which interfaces could provide secure interconnection. The communication channel and the communicating parties shall ensure the integrity, and availability, sometimes even the confidentiality of data, while taking into consideration the regulations regarding the chosen radio frequency spectrum bandwidth, and saturation.

We must differentiate in terms of usage defense, commercial, and hobby purpose unmanned aircraft systems based on abilities and required security levels, and place specific requirements on the cloud system infrastructure accordingly. For this, different military, governmental, and civilian recommendations are available as guidance, which define the boundary conditions in both legal and technological sense.

Iterating the types of data handled on the system, we can deduct that some types of data are more crucial or critical, as they are responsible for the control of the aircraft or correspond to personal data identified by European legal guidance. Other data however are of public interest, such as the position and identifier of the aircraft, or other properties that can be publicly broadcasted on an open

channel to implement traffic collision avoidance. This brings the need for evaluating and classifying data and subsystems based on data handling and access point of view. Thus, as part of the ground subsystem, the remote pilot's identification shall be ensured, as they have access to a critical point of the system remotely, over the internet: control. This not only important from accountability point of view, but also to prevent hijacking attacks.

Happenings of the recent years spread light on the previously underestimated area of supply chain security in case of information technology systems – both hardware and software vendors can sabotage the system by placing backdoors in their products, not mentioning the countless surveillance scandals that surfaced recently. This could be partially helped by utilizing open-source software and hardware, so I strive for applying such technologies during my research – through this on itself does not solve the problem, as in some cases such systems build not only on software and hardware, but also on reliability of external data sources.

Apart from results derived from in-flight testing (e.g., actual flying drone) there is a need for evaluation of testcases that are not safe or feasible executing in-situ (e.g., performance test with multiple hundreds of drones, or testing faulty behavior). To execute these, a simulated software environment is needed, where we can analyze these extreme cases safely and ethically, which would be possibly outlawed by regulations in real life scenarios.

Research objectives

My aim is to

- **Discover** and **present** the current possibilities of unmanned aerial vehicles (UAV) and cloud computing systems;
- **Analyze** available standards, recommendations, and legal regulations;
- **Investigate** widely used unmanned aerial vehicle control protocols from security point of view;
- **Explore** the prossibilites of a joint application of the two areas;
- **Conduct case studies** and integrate a cloud based UAS system;
- **Conduct** in-flight and simulation **tests**;
- **Place recommendations** on testing and designing cloud based UAS.

Research hypotheses

- Testing of cloud controlled unmanned aircraft systems can be successfully conducted in a two-way approach: replacing ground control and the aircraft themselves with simulated counterparts
- Cloud based service aids adequate remote-control and monitoring from a physical security point of view.

- Cloud based service aids adequate operation and process coordination from an administrative security point of view.
- Cloud based remote-control and monitoring aids adequate operation and reliable identification of parties involved in the UAS from a personnel security point of view.
- Cloud based remote-control aids the adequate operation of unmanned aircraft systems from an electronical security point of view.

Research methods

The applied research methods and methodological approach of the analysis are the following:

- Foundation of theoretical knowledgebase by processing relevant scientific learning material and literature.
- Practical research and development while creating an experimental system and test environment.
- Conducting computer aided lab experiments and simulations on the integrated system.
- Analysis and evaluation of self-produced results and measurements.
- Collaboration with experts, scholars, specialists in Hungary and abroad.
- Participate in a scientific university project.

- Conduct case studies on selected open systems to evaluate their security defects.
- Discover and analyze parallels among relevant technologies, conduct comparative critical analysis, deduct implications regarding the problem under examination.

Brief chapter-by-chapter description of the conducted analysis

In **chapter 1.** of the dissertation I present different aspects, history, abilities, and application of unmanned aircraft systems. From a similar point of view, I present the security and privacy concerns of cloud computing. Finally, I present basics of public key infrastructure (PKI), on which later chapters are built.

In **chapter 2.** I give an in-depth technical description of requirements regarding cloud based UAS, widely used control protocols, then I discover similarities with internet of things (IoT) systems.

In **chapter 3.** I present the created test environment: the aircraft used for in-flight testing, the airspace, the (then current) legal background, the architecture of the developed simulator software, and the background of the testcase selection. During the design phase, I strived for using open-source software, the successful implementation has shown that the limits of testing such systems are mostly of legal and technical kind – the needed infrastructure can be implemented in an economic way, using mostly free software.

In **chapter 4.** I present the executed in-flight testcases, which have highlighted limitations (e.g., the not supported automatic takeoff and land commands in case of the outdated flight controller, coordinate system incompatibility) and possibilities (e.g., the surprisingly fast response time over 4G data connection) of the system. Based on the learnings collected, I give recommendations on the details of designing such systems in the later chapters.

During the lab testcases I simulate 100 drones using the proprietary software, while I demonstrate the scaling capabilities and survivability of the system during network overload and catastrophe, which has shown that cloud based UAS provide high level of reliability and cost-effective resource management possibly even in case of defense or governmental application.

I present a comparison between cloud based and physical servers' performance and cost in case of weather model execution. Based on the comparison, it can be deducted in case of smaller, less-parallel meteorological calculations it is worth renting cloud services, and in case of more parallel and longer-term projects it is financially better maintaining dedicated physical server(s).

However, based on the measurement results it can also be deducted that in sense of computation performance cloud-based services can compete with their similarly set up physical counterparts, sometimes also outperforming them, even during more complex, parallel computation tasks.

I compare different ways of wind measurement in case of UAVs, and I present a technical solution for avoiding dangerous weather phenomena in an autonomous way.

In **chapter 5.** I introduce the possibilities of UAS-specific public key infrastructure, picturing a possible European-level process and organizational setup. Secure internal communication of cloud systems is usually also based on an open or closed PKI, using certificates, thus the described approach can also be used on the cloud infrastructure level, moreover identification of connecting UAVs as clients can also be integrated into the solution.

I summarize the dimensions of UAS-specific data handled in the cloud. Special care is needed in case of the listed flight-related data types stored in the cloud, of which the access and risk levels need to be carefully defined in such a flight safety critical system. In case of international systems, the placement of this data can even be question of national security.

In **chapter 6.** I present technical solutions around the topic of personnel security for ad-hoc association between remote pilots and drones, remote authorization of takeoffs, and possibilities of law enforcement intervention.

I present the content of OpenDroneID messages used for remote identification of remote pilots and operations, which satisfy European Union regulatory requirements for electronic identification. Analyzing the possibilities of UAS-specific public key infrastructure I concluded that a Europe-level process can provide the means

of ad-hoc association between remote pilots and drones, remote authorization of takeoffs, and law enforcement intervention. For this, a targeted solution can be the OpenDroneID system extended with a PKI-based trust chain, which is currently not covered in the specification. The concept can be generalized by utilizing an external, centrally verified, and certified on-board device for commercial drones.

In **chapter 7.** I examine the Open Glider Network regarding the question of electronic security, and I demonstrate through a case study the importance of ensuring information security in case of open systems.

I present the architecture and operation of the OpenDroneID system, together with its limitations and possibilities. Currently, as details are still partly under specification, it does not provide a ready solution for package authentication, but most of the open questions can be answered by integration with the PKI concept (authentication key distribution, revocation, configuration, etc.).

Via mathematical calculations I present a possible probability-based attack against the signature field of MAVLink 2.0. After examination of the signature field, it can be said that it does not make the protocol completely hijack-proof, but in case of low bandwidth radio channels it enhances the integrity protection of the packages.

Finally, I present lab testcases simulating the ground control station towards the flight controller. Based on the results of these testcases, I concluded that the chosen flight controller's robustness level is

truly adequate from an electronic security point of view to conduct the in-flight testcases.

Scientific novelties

1. **I defined** the term *Mission as a Service*, which covers unmanned missions planned and executed (over land or water, under water, aerial or spatial) with cloud support. Based on my definition, **I concluded** that none of the existing cloud service types cover the defined task.
2. I developed a proprietary cloud-based unmanned aircraft system, on which I executed various, but targeted testcases, and by validating their results **I proved**, that the integration of the ground subsystem into cloud infrastructure can aid implementation of physical and electronical security in case of UAS. Comparing it with the case of a traditional physical server, it would have caused significant disturbance in the continuity of the service, while the survivability of the cloud service was demonstrated by the passing of the executed testcases.
3. **I created an extensive model** of PKI and OpenDroneID-based identification and registration of unmanned aerial vehicles conforming to European Union regulations, through the process examples of which **I deducted** that the application of the model would aid the implementation of person-

nel and administrative security regarding unmanned aircraft systems.

4. **I concluded** that in case of an unmanned traffic management (UTM) flight meteorology support system, even though cloud computing can be financially less feasible than maintaining dedicated physical servers in case of highly parallelized computation tasks, cloud computing can achieve the performance level of, or even outperform dedicated physical hosts, even in case of highly parallelized tasks.

Recommendations

In my view, the results of the research can be applied not only in theoretical and practical education and training, but also during defense, law enforcement, and civilian practical implementation of such systems:

- The dissertation can be relevant during lectures of our university, especially during BSc and MSc classes of Department of Aerospace Controller and Pilot Training, Department of Aircraft Onboard Systems, Department of Information Technology, Signal Department, and Department of Electronic Warfare.
- The described system can be generalized also for implementation of software container-based systems, the research of which can be an interesting thesis subject.

- The case study presented over the OGN system can be a (negative) example in my opinion regarding the design of critical systems. I suggest keeping in mind the results of the examination, and the identified vulnerabilities not only on technical, but management level too.
- The demonstrated properties, abilities of the system can give guidance for designing other various governmental cloud-based systems.
- The possibilities of the recommended PKI and OpenDroneID model can give ideas to colleagues of the National Transport Authority – Civil aviation Authority and Lawmakers to implement a mostly electronic administration process regarding drones, while satisfying requirements of the European Union.
- Generalization of the WRF-specific performance cost measurement can be interesting to my fellow researchers for planning private and university research projects' hardware acquisitions.

List of publications on the topic of the thesis

Peer reviewed publications in Hungarian

S1 Vránics Dávid, Üveges András: Pilóta nélküli légi járművek fejlődése, Felderítő Szemle XIV: (2) pp. 124-140.

S2 Vránics Dávid Ferenc: Felhő alapú rendszerekkel irányított pilóta nélküli légijármű rendszerek szakirodalmának kutatása, Hadmérnök XII.: (1. különszám) pp. 217-233.

S3 Vránics Dávid Ferenc: Egy felhőalapú, pilóta nélküli légijármű-tesztrendszer bemutatása, Bolyai Szemle XXVI.: (2) pp. 37-44.

S4 Vránics Dávid Ferenc, Palik Mátyás, Bottyán Zsolt: Esettanulmány egy nyílt repüléstámogató rendszer biztonságáról, Repüléstudományi Közlemények (1997-től) 30: (1) pp. 185-194.

S5 Vránics Dávid Ferenc, Palik Mátyás: Mission as a Service: Egy felhőalapú UAS megvalósítása, Repüléstudományi Közlemények (1997-től) 31: (3) pp. 153–167.

Peer reviewed publications in English

S6 Vránics Dávid Ferenc, Palik Mátyás, Bottyán Zsolt: Electronic administration of unmanned aviation with public key infrastructure (PKI), International Scientific Journal Security & Future III: (4) pp. 152-155.

S7 Vránics Dávid Ferenc, Lovas Róbert, Kardos Péter, Bottyán Zsolt, Palik Mátyás: WRF Benchmark Measurements and

Cost Comparison. Virtualized Environment Versus Physical Hardware, REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK (1997-TŐL) 29: (2) pp. 257-272.

S8 Vránics Dávid Ferenc: Testing of a cloud-based unmanned aircraft system, REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK (1997-TŐL) 32: (1) pp. 175–190.

Conference presentations not published in peer reviewed proceedings

S9 VRÁNICS Dávid Ferenc, BALOGH Miklós, GYÖNGYÖSI András Zénó, ISTENES Zoltán, WEIDINGER Tamás, MAKKAY Imre, BOTTYÁN Zsolt, PALIK Mátyás: Meteorological sensor placement considerations for a fixed-wing Unmanned Aircraft System, In: ISARRA Conference 2019, Lugo (Spanyolország), 2019.07.16., prezentáció online elérhető: http://www.isarra.org/wp-content/uploads/2019/08/ISARRA_2019_Tue_Vranics.pdf

Professional and scientific curriculum vitae

Personal details:

Name: Dávid Ferenc Vránics
Date of birth: 11. July 1990.
E-mail address: vranicsd@gmail.com

Job/assignments:

2020-	**Researcher-developer – Mould Tech Systems Ltd,** MyDroneMet
2011-	**Software developer – Ericsson Hungary Ltd,** TitanSim, Cloud Execution Environment
2016-2021	**IT expert – National University of Public Service,** GINOP 2.3.2-15-2016-00007 “Increasing and integrating the interdisciplinary scientific potential relating to aviation safety into the international research network at the National University of Public Service - VOLARE”.

Education:

2016-2018	**National University of Public Service, Faculty of Military Sciences and Officer Training,** Doctoral School of Military Engineering
2013-2015	**National University of Public Service, Faculty of Military Sciences and Officer Training,** Defence C3 Systems Management MSc
2008-2012	**Eötvös Loránd University, Faculty of Informatics,** Computer Scientist BSc

Membership:

2019-	Drónpilóták Országos Egyesülete
2019-	International Society for Atmospheric Research using Remotely piloted Aircraft

Professional courses:

ISTQB:
Advanced Level Test Analyst
Advanced Level Specialist - Security Tester
EC-Council:
Certified Ethical Hacker v10

Language skills:

English C1, Italian B1

Others:

Category B driver's license
A1/A3 Open category drone remote pilot certification