NEXT
GENERATION
INTERNET

Open Call 5

SecureUAV: Energy-efficient malware detection in Unmanned Aerial Vehicles via advanced AI models

Deliverable 3: Experiment Results and Final Report

Authors	Andrii Shalaginov (andrii.shalaginov@kristiania.no, Kristiania University College, Norway), Houbing Song (songh4@erau.edu, Embry-Riddle Aeronautical University, USA)
Due Date	07.12.2022
Submission Date	07.12.2022
Keywords	Cybersecurity, artificial intelligence, drones, UAV, computer viruses

Deliverable 3: Part I

Analysis, results, and wider impact

1 Abstract

The goal of SecureUAV project is to develop a platform and framework for increased cybersecurity protection and end-user awareness of cyberthreats in unmanned aerial vehicles (UAV). Through AI and human-understandable decision support models, we will build and evaluate a resilient mechanism to detect malicious activities and cyber-physical threats as well as to ensure a timely incident response by the drone operator. In particular, the cyber-security awareness telemetry will be transmitted from the UAV to the operator in an energy-efficient way. The research includes cooperation between Songlab at Embry-Riddle Aeronautical University, US focusing on the architecture of UAVs as we as SmartSecLab at Kristiania University College, Norway bringing intelligent cybersecurity mechanisms. Cross-domain cooperation and expertise make it feasible to test and validate proposed solutions in consumer drones using real-world attack scenarios.

2 Project Vision

Malicious software and cyberattacks have been affecting cyber-physical infrastructure over decades, mainly targeting large organisations' computers and server infrastructure. The advancement of technologies and ubiquitous distribution of embedded devices such as smartphones and Internet of Things (IoT) components is leading to new trends in malware development, and how viruses can spread is constantly growing. The infection of IoT devices has been considered unlikely until 2017 when Mirai botnet showed unexpectedly that such tremendous attacks are entirely possible. Currently, IoT devices' vulnerabilities and cyber threats landscape are even more complex than traditional computer systems are exposed to.

Consumer and prosumer UAVs have been actively used in recreational and critical infrastructure missions for already a decade, resembling the IoT backbone due to the usage of resource-constrained platforms and components with an interruptible power supply such as batteries or solar power. The first significant incident in the UAV industry came to light as early as 2019 when the Keylogger virus disrupted computers at Creech US air force base in Nevada, demonstrating the danger of such incidents. Further, in 2015 Maldrone backdoor was successfully used to maintain persistence across UAV even after a system reset. Moreover, in several attacks on supply chains, traces of malicious software or similar hardware components have been detected being injected into the electronics. There is a substantial risk that such attacks can affect drone motherboards worldwide.

SecureUAV project's vision is to enhance the overall operational UAVs security as well as Linux-based and similar mainboards that run mission-critical functionality, process video streams and maintain communication with drone operators through sophisticated remote controllers. Such communication is usually maintained with the help of AES-256 or similar standards while transmitting altitude, distance, GPS location, velocities, battery level and temperature. However, there is no low-threshold information about the drone system's cybersecurity status or if any virus infection or attack is happening. Such information and data pieces include memory-based system artefacts as well as irregularities in resource utilization. So, modern UAV system needs a toolkit to provide insight into cyber-physical cybersecurity awareness and telemetry. Even though there are available commercial cybersecurity solutions to guard Linux, such as anti-virus (AV) or intrusion detection systems (IDS), energy consumption aspects make them nearly inapplicable.

UAV design's primary consideration is real-time performance and mission-critical functionality, which cyber-physical security awareness has not been priorities enough. The disadvantage of conventional tools such that AV signature-based solutions lie in the inability to detect malware variants when using cryptographic hash sums. In addition, outdated firmware, standard passwords, and poor security practices make UAVs a good target for adversarial attacks. This project is backed by years of the EU-US team cross-domain experience. EU team has been working on the AI-based cybersecurity middleware under the

Co-funded by the Horizon 2020
Framework Programme of the European Union

NGI Pointer-funded project *"ENViSEC: Artificial Intelligence-enabled Cybersecurity for Future Smart Environments"* which resulted in a software solution used on the level of IoT nodes and IoT gateways to monitor and detect any attacks by using data-driven methods. The solution includes integration as an Operating System-based daemon (NVIDIA Jetson and similar devices) as well as low-level code snipes in hardware firmware (ESP32, Arduino and other devices). Furthermore, SmartSecLab contributes with its funding to support SecureUAV project's hardware capabilities, such as drones and radio frequency communication measurement devices. The US team has been already working on building a UAV cybersecurity laboratory for evaluation of the drones' cybersecurity through NSF-funded projects: *"SaTC: EDU: Collaborative: Bolstering UAV Cybersecurity Education through Curriculum Development with Hands-on Laboratory Framework"* (https://www.nsf.gov/awardsearch/showAward?AWD_ID=1956193) that is matched funding to SecureUAV project from US side; research results from the relevant project *"REU Site: Swarms of Unmanned Aircraft Systems in the Age of AI/Machine Learning"*.

During the experiments, we will develop a telemetry protocol and corresponding novel AI models to be used in the drone on the lower system level, as indicated in the EU team's work. The overarching goal would be to push for changes towards more privacy-by-design and security-by-design frameworks in UAVs that are based on open-source components and software.

3 Details on participants (both EU and US)

EU: Kristiania University College

Andrii Shalaginov (PhD) is an associate professor and a head of SmartSecLab, whose work is widely related to the application of AI for cybersecurity, the detection of computer viruses and the protection of IoT devices. Before he has more than a decade of industry and academic experience with cybersecurity, including work as a cybersecurity researcher in the EUIPO/UNICRI framework related to malware analysis on copyright-infringing websites and is a management committee member from Norway to COST Action CA17124 DigForAsp. Moreover, Shalaginov is a project leader for NGI Pointer-funded project ENViSEC, aimed at developing a middleware architecture to be used in intelligent cybersecurity enhancement for Smart Environments. The project team includes Tor-Morten Grønli (Professor), Andreas Lyth (hardware engineer) and Guru Prasad Bhandari (software engineer). The project outcomes resulted in several publications, international workshops and developed AI-based middle tested on several designed IoT-enabled use cases using the most up-to-date hardware components. Expertise and insights into low-level IoT cyber security are being used to support activities of SecureUAV project implementation. This is particularly relevant when applying security principles toward Operating System-based devices as well as firmware-based microcontrollers, considering the generic architecture components of UAVs.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Previous relevant funding from EU partner side:

- Title: ENViSEC: Artificial Intelligence-enabled Cybersecurity for Future Smart Environments
- Sponsor: NGI Pointer (Grant No: 871528)
- Amount: EUR 200,000
- Period: October 2021 – October 2022.
- URL: https://smartseclab.com/envisec/

US: Embry-Riddle Aeronautical University

Houbing Song (PhD) is a professor and a head of Songlab, served as a subject matter expert on AI and counter-cyber for autonomous unmanned collective control for the US Special Operations Command (USSOCOM), in 2019, and a visiting faculty research fellow with the US Air Force Research Laboratory, in 2018 and 2021. With NSF's support, SONG Lab has developed a UAV cybersecurity experimental platform for research and education of UAV cybersecurity by leveraging Embry-Riddle's unsurpassed research capability in the field of aerospace. SONG Lab's research in the field of UAV cybersecurity has resulted in 2 patents and 20+ papers, including 9 which received Best Paper Awards. SONG Lab's research on UAV cybersecurity has been featured by popular news media outlets, including IEEE GlobalSpec's Engineering360. SONG Lab’s 3 Ph.D. students have been hired as tenure-track assistant professors at US universities. Several labs and centres at ERAU, including the Security andOptimization forNetworkedGlobe Laboratory, the Cybersecurity Engineering Laboratory (CybEL), and Cybersecurity and Assured Systems Engineering (CyBASE) Center, participate in the relevant activities and projects with SONG Lab, also including following faculty members: Prof. Yongxin Liu, Mr. Justus Renkhoff (PhD Student), and Mr. Waleed Raza (PhD Student).

The exact NSF grant details matching SecureUAV from US partner side is:

- Title: SaTC: EDU: Collaborative: Bolstering UAV Cybersecurity Education through Curriculum Development with Hands-on Laboratory Framework
- Sponsor: National Science Foundation (Grant No: 1956193)
- Amount: $472,060
- Period: May 1, 2020-April 30, 2023
- URL: https://www.nsf.gov/awardsearch/showAward?AWD_ID=1956193

Other relevant NSF grants that US partner got funding for:

- Title: REU Site: Swarms of Unmanned Aircraft Systems in the Age of AI/Machine Learning
- Sponsor: National Science Foundation (Grant No: 2150213)
- Amount: $322,866
- Period: May 1, 2022-April 30, 2025

Experimentation timeline and load

Co-funded by the Horizon 2020
Framework Programme of the European Union

- **M1** - July, 2022: Preparation and requirements specification of the AI-based agents deployable both on the UAV main board as well as on the remote control, corresponding communication and status delivery protocol. (EU – 0.5PM, US – 0.2PM)
- **M2** - August, 2022: 10 days research stay with US project team aimed installation and preparation of an experimental platform and integration with the existing lab activities. (EU – 0.5PM, US – 0.2PM)
- **M3** - September, 2022: The scenarios preparation, realistic malware infection data collection with AI models performance testing using TensorFlow Lite, specifically designed for IoT devices and applications. (EU – 0.5PM, US – 0.2PM)
- **M4** - October, 2022: Development of a lightweight agent system that can indicate possible malicious activities and share cybersecurity awareness information in addition to data telemetry on UAV. This will include CoAP- and MQTT-based secure communication protocol for AI models delivery and telemetry exchange. (EU – 0.5PM, US – 0.2PM)
- **M5** - November, 2022: Dissemination and communication activities, possible consultation with industrial partners. Also, the project team conducted the final extended 10-days visit for the final demonstrator preparation and corresponding workshop presentation that will conclude the project. Delivery of the final technical report generated real-world data and experimental setup specifications for reproducible research. (EU – 0.5PM, US – 0.2PM)

4 Results

In this section, we reflect on the project KPIs and corresponding implications, both practically and theoretically.

Summary of the achieved results and overarching applicability in a real-world scenario. During requirement specification and analysis of the technical documentation of drone platforms, we have identified the two most general types of drones based on their capabilities and used components. Based on such categorization we can define the applicability of the SecureUAV results towards cyber security awareness and viruses detection:

- **Basic drones with firmware** (non-OS) have limited capabilities and usually are controlled by a microcontroller-based flight controller that has several I/O ports with capabilities of two-way communication with the operator. Telemetry includes battery, speed, temperature and acceleration information. There is a very limited possibility to add own software snippets, therefore, SecureUAV project results can be used on the drone operator side to observe and make an assumption about cyber attacks. However, no OS artefacts can be used due to the resource-constrained environment. Moreover, there is a considerably smaller risk of getting a virus infection on such platforms.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- **Advanced drone platforms with OS** drones that use Linux-like systems and resemble rather IoT gateways capabilities. Such devices have room to integrate custom configuration, develop software and deploy it in the communication routines. The system telemetry includes system load, CPU load, RAM and I/O loads, which are the main indicators of malicious behaviour in the system and cyber attacks. SecureUAV project results are fully applicable to such drones as well as drone fleets used in automated mission controls.

To reflect achieved results of the SecureUAV project, the following table summarizes KPIs, corresponding measurement and achieved target.

KPI	Measure	Achieved Target
KPI1: Requirements specification	Number of applicable requirements for ARM-based devices. We must develop a set of functional and non-functional requirements for the selected hardware and software components, defining a protocol for data sharing and a AI model format.	It was developed a set of functional and non-functional requirements for the selected hardware and software components defining a telemetry protocol for data sharing and an AI model format. The requirements are applicable apply to at least 1 UAV platform and 1 general-purpose microcomputer for simulation purposes. Moreover, a specification of universal testbed design can be applied to a wider range of relevant platforms.
KPI2: Low threshold cybersecurity awareness alerting and AI-based detection system	Cybersecurity awareness and AI-based malicious software detection-related information that can be transmitted to the controller that allows over-the-air data sharing and operator decision support	Defined cybersecurity awareness and AI-based malicious software detection-related information that can be transmitted to the controller that allows over-the-air data sharing and operator decision support.

Co-funded by the Horizon 2020 Framework Programme of the European Union

		This resulted in 5 cybersecurity-related indicators of compromise-related information generated and transmitted: a list of suspected malicious files, system load (DoS indicator), memory consumption, irregularities in the CPU load and suspicious filesystem indicators. MQTT-alike mechanism was utilised for cybersecurity telemetry exchange and AI model delivery.
KPI3: Realistic energy consumption and computing overhead analysis	It will be evaluated: (i) energy consumption of ARM-based drone components under malware infection and cyber-attacks on UAVs and simulation on general-purpose microcomputers, (ii) energy consumption of deployed AI model and cybersecurity awareness agent. Both need to have a clear baseline of attack indicators.	The utilization of SecureUAV protection mechanism did not create a significant delay in drone/main board operation (up to 2% on average idle load of the AI model) and did not result in a higher drain of the battery (up to 10% more current in some operations when the model was actively used).

4.1 Discussion and Analysis of Results

KPI 1: AI and data processing modules requirements specification. To be able to use the experimental setup in various environments and stimulate reproducibility of the research results, there was done work on developing a set of functional and non-functional requirements for the selected hardware and software components defining a telemetry protocol for data sharing and an AI model format. The requirements apply to at least 1 community-used UAV platform and 1 general-purpose microcomputer for simulation purposes. Moreover, a specification of universal testbed design can be applied to a wider range of relevant UAV platforms with similar characteristics and operational needs. To

Co-funded by the Horizon 2020
Framework Programme of the European Union

reflect different requirements, it was used [Fx] – for general functional requirement, [Ax] – for specific functional requirements of the proposed solution and [NFx] – for general non-functional requirements.

1. Functional Requirements

[**F1**] The next modules of the novel cyber protection in drones must be implemented:

- AI module
- Cybersecurity monitoring protocol
- Communication protocol
- Cloud and threats intelligence capabilities

[**F2**] Each module needs to include the following

- Basic overview and description

- Resource consumption estimation (RAM, flash/disk and execution time)
- Involved software dependencies (libraries, environment path, other software)
- Required hardware on each level (ports, minimal CPU, RAM, disk required to deploy)
- Network deployment specification (IP address of the agents, RF communication protocols)

1.1. **AI module**

[A1] AI model deployment and operation

- AI model to be trained and implemented using an applicable programming language
- AI model to be stored on microSD
- Extensive logging
- Training AI models for malware detection using data from Cloud
- Deploying AI models for malware detection received from Cloud
- Ability to forcibly update and propagate AI model on the drone initiated by the operator

[A2] Utilization of trained model

- Active analysis of Indicators of Compromise
- Proactive response to cyber-attacks
- Communication and energy consumption patterns are to be included if applicable

1.2. **Cybersecurity monitoring protocol**

[A3] Underlying infrastructure

Co-funded by the Horizon 2020
Framework Programme of the European Union

- WiFi, Bluetooth, RF communication, 4/5G, Ethernet
- Data encryption to avoid man-in-the-middle attacks and replay attacks

[A4] Drone telemetry measurements

- At least battery, time, altitude, temp, barometer, gyroscope, GPS
- Ability to propagate measures from human experts

[A5] Mainboard OS telemetry

- CPU, RAM, I/O stat, filesystem, average system load 1,5,10 min (Linux)

- Possible ability to measure Radio Frequency Communication parameters

1.3. **Communication protocol (MQTT and further CoAP)**

[A6] Underlying Infrastructure

- Work over standard Wide Area Network Communication
- Clear addressing, data flow and TCP/IP-compatibility
- Possibility to handle irregularities in RF communication
- Provide platform- and device-independent communications

[A7] Application Level

- Allow minimal source code footprint without major software

dependencies.

- Asynchronous communication for resource-constrained environments.
- Straightforward delivery of a variable number of parameters.
- Minimal bandwidth and processing overhead and used energy

1.4. **Cloud and threats intelligence capabilities**

[A8] Cloud connectivity

- Large-scale collection and processing of previous historical data

- AI models for both (i) different types of viruses, platforms and generalization

[A9] Cyber Threats Intelligence

Co-funded by the Horizon 2020
Framework Programme of the European Union

- Distributed collection of relevant viruses, attacks and indicators of compromise data
- Real-time updates and OSINT

[A10] Information Security Data Enrichment API

- Aggregation of applicable telemetry in compressed format for later processing
- Ability to detect ongoing attacks based on advanced behavioural AI models and characteristics
- Connection to the community-accepted platforms such that VirusTotal and MISP

2. **Non-functional requirements**

[**NF1**] Designed software components should be deployable on at least OS-based UAV platforms

[**NF2**] Software dependencies and libraries should be open-source to avoid license issues

[**NF3**] Implemented source code must follow commonly accepted coding conventions

[**NF4**] The middleware should maintain a modular system and be easily adaptable to changeable drone mainboards architecture and used components

KPI 2: Low threshold cybersecurity awareness alerting and viruses detection system. To be able to recognize irregularities in the system performance connected to cybersecurity awareness, the operator needs to receive a low threshold cybersecurity awareness (with a known baseline) and AI-based malicious software detection-related information that can be transmitted to the controller that allows over-the-air data sharing and operator decision support. To support the baseline detection using possible indicators of compromise-related information and proactive monitoring, there is a needs to fetch and transmit the following information, but not limited to:

- a list of suspected malicious files (“rkhunter”)
- system load - DoS indicator (“htop” / “top”)
- memory consumption (“htop” / “top”)
- irregularities in the CPU load (“htop” / “top” / “ps”)
- suspicious filesystem indicators (“chrootkit”)

Considering that the goal is to focus on the Linux OS-based drone platforms, most of the required indicators can be retrieved using standard Debian tools as well as in-system software capabilities. *Chkrootkit* and *Rootkit Hunter* both are host-based, passive, post-incident auditing tools meant to check for signs of malicious activity. Chkrootkit (check

Co-funded by the Horizon 2020
Framework Programme of the European Union

rootkit) is a UNIX-based rootkit detection program which provides users to check their system for rootkits. A *rootkit* is malicious software that allows an unauthorized user to get access to a system and to its restricted software. These rootkits may contain keyloggers, credential stealers etc. *Rkhunter* (Rootkit Hunter) is a Linux/Unix-based tool to scan possible rootkits, backdoors and local exploits. It does this by comparing SHA-1 hashes of important files with known good ones in online databases, searching for default directories (of rootkits), wrong permissions, hidden files, suspicious strings in kernel modules, and special tests for Linux [5].

Further, we need to encounter **an appropriate communication protocol** that is needed to be deployed for the solution developed in SecureUAV project. As we can see, drone mainboards and IoT platforms have a wide range of similarities – in used software and hardware components. Before, CoAP- / MQTT-alike mechanisms were utilised for cybersecurity telemetry exchange and AI model delivery in IoT platforms. MQTT is a standard messaging protocol for the IoT. It is designed as an extremely lightweight publish/subscribe messaging transport that is ideal for connecting remote devices with a small code footprint and minimal network bandwidth. MQTT today is used in a wide variety of industries, such as automotive, manufacturing, telecommunications, oil and gas, etc. The Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained networks in the Internet of Things. The protocol is designed for machine-to-machine (M2M) applications such as smart energy and building automation. From the perspective of UAV applications, both protocols are applicable as centralized as well as decentralized cybersecurity awareness connections. This, for example, can be applied to stand-alone drones or federated drones operation and networks. Moreover, from the hardware platforms used in this project, we can see that such higher OSI stack protocols allow transmission over a variety of commonly used drone control and telemetry exchange protocols such that 2.4Ghz (WiFi), 433Mhz or even Infrared (IR).

To ensure efficient and responsive **cyber security awareness protocol**, it has to be established application-level transfer of the OS state and artefact data transmission over the air to the operation control panel and dashboard. While it is not the case with GHz band drones, the 433Mhz band drones have a limited bandwidth throughput of up to 4,800bps. Therefore, it is of utmost importance to use as few resources as possible on transferring. To achieve this, we are using several components for efficient cyber security awareness protocol composition. First, the data from KPI 1 have to be processed and embedded in object-like structures to be able to reflect the complexity of each measurement. Second, the object-like structures need to be self-contained and deployed using either JSON (JavaScript Object Notation) or Protobuf [6]. In such a way, the data objects use the least possible explanatory fields to contain all variables. Third, the data needs to be put in a universal transferable format such that using *serialization*, which is a universal conversion of data objects into a stream of bytes. Fourth, the final data need to be encrypted before the transfer is made through CoAP/MQTT protocols to ensure the confidentiality and integrity of

Co-funded by the Horizon 2020
Framework Programme of the European Union

the cyber security awareness information. One of the prominent libraries available for the low end IoT devices is ArduinoLibs [7] which works at the MHz-wise microcontroller and fits the purpose of operator-drone communication well. We chose to focus on JSON format, which does not require a pre-defined scheme as in the case of ProtoBuf. Moreover, JSON is also applicable to transfer parameters of the AI model to be used to detect viruses as shown in the Figure 1.

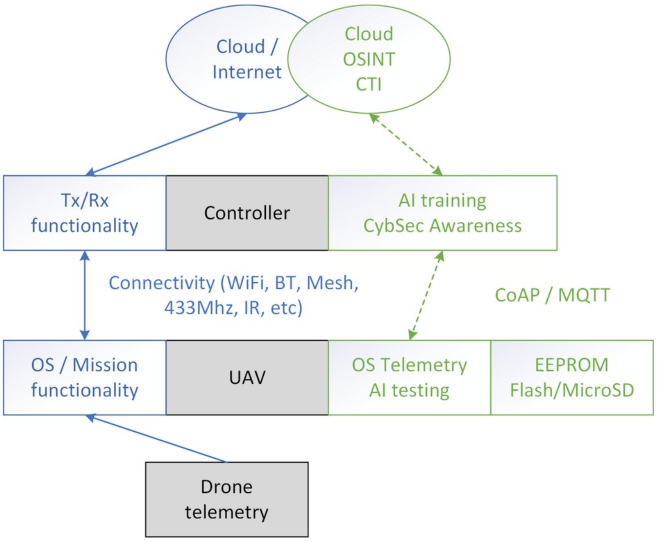

Figure 1: An example of the SecureUAV implementation on the OS-based drone platforms

For example, the cybersecurity awareness information can be transferred in such format:

{“cpu load” = “0.9” , “average load 1min” = 0.5, “rkhunter”=”no issues”}

KPI 3: Realistic energy consumption and computing overhead analysis. Adversarial actors constantly discover previously unseen vulnerabilities and attack vectors that impact both on personal and national levels such that SolarWinds attack. It becomes critical in a smart infrastructure ecosystem with limited resources such that modern UAVs. Therefore, we need novel models to evaluate the cost of cyberattacks, protective measures and new ways of selecting relevant energy-friendly cyber response scenarios. To start with, a community-accepted measure of computer architecture efficiency is co-called *Performance per Watt* or FLOPS (Floating Point Operations Per Second). Another commonly used measure of Central Processing Unit (CPU) speed in Linux Operating System is expressed in the number of internal busy-loops in so-called *bogomips* (“bogus” millions of instructions per second). And there are tremendous differences between desktop machines and smaller IoT platforms used as drones' main boards when it comes to this measure. A modern laptop with 11th Gen Intel Core i7-1165G7 @ 2.80GHz has eight cores (5606.40 bogomips each), while the latest Raspberry Pi 4 with Cortex-A72 CPU @ 1.5Ghz has four cores (108 bogomips each). It is reasonable to see several magnitudes of difference in overall performance indicators. However, the first CPU consumes 28 Watts according to Intel specifications, while the

Co-funded by the Horizon 2020
Framework Programme of the European Union

second - up to 10 Watts. Therefore, an average IoT board (used for UAV) is tens of times less energy efficient than a desktop or server station when it comes to computational capabilities. While privacy, confidentiality, availability and integrity issues are of utmost importance in drone operations, one can see also an increased need to evaluate the energy footprint of such use cases. Therefore, the perspective of this project is tight to the following two aspects: (i) energy consumption of ARM-based drone components under malware infection and cyber-attacks on UAVs and simulation on general-purpose microcomputers, (ii) energy consumption of deployed AI model and cybersecurity awareness agent. Both need to have a clear baseline of attack indicators. The utilization of SecureUAV protection mechanism should not create a significant delay in drone operation and drain the battery at a higher speed than required.

Originally planned hardware devices for drone energy consumptions were *Nordic Semiconductor Power Profiler Kit II* and *Uni-T UT658D USB-tester.* However, due to the internal limitations (current measurement experiments with 1 Amp current limitation), the experiments faced issues with booting Raspberry Pi boards because the board consumes 3 Amps at the initial booting. Because of this, we have purchased a bench multimeter PeakTech P4090 that will be used in the follow-up conference paper and journal particle to be published based on the results of the SecureUAV project.

Experimentation summary:

- Most of the platforms use Wi-Fi/2.4Ghz-based drone communication, which is well-documented and many tools help to evaluate the cyber security aspects of the communication protocols as well as to easily simulate attack scenarios and monitor bandwidth with standard tools.
- Operating System (often Linux)-based platforms offer a wide range of indicators and system metrics that can be used to capture possible indicators of compromise and perform basic malware triage.
- We have used several datasets (IoT23 dataset and Edge-IIoTset dataset) that consist of malware attacks also applicable to OS-based drone platforms.
- To simulate real-world drone operations, it was used Raspberry PI 4B and Raspberry Pi Zero with the envisioning the following experimental parts: **E1** – Communication protocols, **E2** – Relevant cyber viruses data, **E3** – Software components, **E4** – Performance and energy consumption. The same System-on-a-Chips are used in larger drones as was supported by the US partner environment and knowledge that resulted in the following scenario: Raspberry PI 4B - Navio2 board and Raspberry Pi Zero - Flight Controller FM250 kit / PixHawk as the most feasible connection.
- In addition, DJI Ryzer Tello platform offers a ready-to-deploy drone platform that can be controlled over WiFi using a command line interface. However, this is a firmware-based drone platform that does not offer to deploy custom agents to the device. Nevertheless, it offers a range of possible indicators that can be collected according to documentation. Therefore, it is possible to integrate the SecureUAV solution on

Co-funded by the Horizon 2020 Framework Programme of the European Union

the controller side as well as to fetch OSINT data from the cloud, however, offering the limited possibility to deploy on the drone itself.

- Among all available AI models, Neural Network is considered to be the most generalizable and applicable to most of the data in cybersecurity. TensorFlow Light AI library has been developed for IoT applications and therefore is used in SecureUAV project as the most applicable implementation. Based on the experiments, the Neural Network initialization on Raspberry Pi 4 can take up to 35% CPU load to initialize, while it adds only 2% to idle mode on average, which is not a large load. Moreover, there is an average increase from 0.421 Amps to 0.469 Amps in current consumption by the Raspberry Pi 4 board while running a model.

Hardware platforms used for the project and to be further analysed in dissemination activities beyond project:

1. Drones (drones assembled and tested already)

- 2 x DJI Ryze Tello drone (WiFi communication - active)
- ZMR250 250 Carbon Fiber quadcopter kit + X-Racer Xracer V3.1 F303 Flight Controller V3.1 DSHOT (WiFi communication to be used)
- F450 Quadcopter Frame Kit + APM2.8 Controller board + Flysky FS-i6 RC controller (2.4MHz controller - active)
- DJI Phantom 3 main board
- Smaller drone with 433Mhz communication

2. Flight controllers

- Navio2 – autopilot HAT for Raspberry Pi + GPS/GNSS
- Pixhawk PX4 PIX 2.4.8 32 Bit Flight Controller Autopilot kit
- CRIUS SE V2.5 MWC Mega 3.0 MegaPirateNG Flight Control

3. Radio Frequency Equipment

- RF Explorer Digital Handheld Spectrum Analyzer 6G Combo Plus (bandwidth usage monitoring)
- Comidox CC2531 Sniffer USB Dongle Protocol Analyzer+Bluetooth 4.0 CC2540 Zigbee CC2531 Sniffer (traffic analysis)
- Flipper Zero (sub-Ghz and WiFi dev board for replay attacks)
- WiFi Pineapple MARK VII+AC TACTICAL (Man-in-the-Middle attack in WiFi)

It was found that for the proper utilization of the RF equipment and experimentation, there is a need to do such experimentation in a complete radio silent environment such that a Faraday cage or remote location. Otherwise, there is too much noise from any devices working in 2.4Ghz* frequency range. Moreover, ideally, it is needed to enable a larger fleet and test on tens of devices to record possible abnormalities and irregularities caused by cyber attacks.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Overview of the software components employed in the project:

- Python 3.9
- Python Libraries: TensorFlow, Keras, Numpy, Pandas, Matplotlib, etc.
- Arduino IDE
- Arduino Third Party Libraries: TensorFlowLite, AlfES for Arduino, EloquentTinyML, etc.
- Neptune API

Data collection dimensions applicable to UAVs:

- Analysis of RF spectrum, e.g. by using sniffers or RF Spectrum Analyzer together with Flipper Zero capabilities to create a raw signal repay attack.
- Analysis of the 2.4 GHz / WiFi communication channel using WiFI Pineapple and Linux tools such that Wireshare and Nmap.
- Protocol communication (MAVLink) offers capabilities to analyze and gather necessary communication and concurrency-related data, besides system artefact information.

Considering these two aspects, for the AI-based model deployment, we are focusing on the following platforms that control UAVs over WiFi and are capable of supplying cybersecurity awareness information and possible viruses' detection:

- Raspberry PI 4B -> Navio2 board
- Raspberry Pi Zero -> Flight Controller FM250 kit / PixHawk

5 Present and Foreseen TRL

At the beginning of the project, we assess the TRL of the cross-disciplinary results to be used in the project are at level **3** (basic principles analysed, formulated technology concept and built experimental AI for IoT cybersecurity proof-of-concept).

During the execution of the project and with achieved results, the TRL has been increased to **5** based on the technology validated in the relevant UAV environment using open-source hardware and software components. Moreover, together with US partner, we anticipate getting funding and applying the proposed cybersecurity and AI model in the context of larger drones, a possibility developed by international companies and used in large-scale applications.

Co-funded by the Horizon 2020
Framework Programme of the European Union

6 Exploitation, Dissemination and Communication Status

The project resulted in a unique hardware and software testbed being built at EU partner as well as a similar setup used by US partner. Thankfully to fruitful cooperation, there an overwhelming results that can be achieved also after the SecureUAV project ends in December, 2022. The plan is to continue working on the results to be able to submit one conference and one journal article (MDPI Drones) during Spring 2023. Furthermore, we plan to release some of the source code used during the project together with data simulating real drones cyber security-enabled use cases.

In August, 2022 EU and US partners held bilateral visits and presented the overall problem and ambition to be solved in SecureUAV and shared results of their previous NGI Pointer- and NSF-funded projects. At the moment, both partners are working on a conference paper that will describe the data-driven aspect of cybersecurity in UAVs. Moreover, two relevant workshops are being chaired by the partners that have been in use to promote the project and describe its ambition. Prof. Houbing Song chaired the Ninth IEEE International Workshop on Security and Privacy for Internet of Things and Cyber-Physical Systems (IoT/CPSSecurity 2022) within 2022IEEE 95th Vehicular TechnologyConference: VTC2022-Spring: https://events.vtsociety.org/vtc2022-spring/conference-sessions/call-for-workshops/w22-the-ninth-ieee-international-workshop-on-security-and-privacy-for-internet-of-things-and-cyber-physical-systems-iot-cpssecurity-2022/ and IEEE SmartData 2022 - The 8th IEEE International Conference on Smart Data, August 22-25, 2022, Espoo, Finland http://www.ieee-cybermatics.org/2022/smartdata/. Associate Professor Andrii Shalaginov is the main chair of *"The 6th International Workshop on Big Data Analytic for Cyber Crime Investigation and Prevention 2022"* (https://smartseclab.com/bdaccip2022/) to be held in December, 2022 and hosted a speech on the results of SecureUAV.

The outcome of the project will be elaborated in the journal article, and selected source code/datasets will be released to support relevant international research efforts. During the 2nd visit to ERAU in November 2022, EU partner has delivers lectures and presentations on the preliminary results of the SecureUAV project.

Thankfully to the overwhelming project results and built prototypes, EU partner has also submitted several proposals to the Norwegian Research Council as well as European Research Council. All project results also will be used in teaching activities of 200+ bachelor students in cyber security at Kristiania University College (Oslo, Norway) as a part of the Internet of Things / Operational Technologies Security course in 2023.

Co-funded by the Horizon 2020
Framework Programme of the European Union

7 Impacts

Impact 1: Enhanced EU – US cooperation in Next Generation Internet, including policy cooperation.

SecureUAV international cross-disciplinary project consortium gives access to a unique set of research environments, industrial collaborators, SME partners, and future applications for joint funding projects in this area both in EU and US. The collaboration ensembles building an experimental platform will bring global diversity towards a common goal through the synergy of the industrial-oriented differences in innovation and research strategies. Increased digitalization and globalization, will help to ensure better and more resilient cybersecurity practices. Moreover, the mission is to make some of the results of the SecureUAV project public and enable reproducibility of the results, so that other research environments can utilize and deploy AI models for malware detection as well as cyber security awareness mechanisms to be incorporated not just on the OS-based drones, but also firmware-based drones.

Impact 2: Reinforced collaboration and increased synergies between the Next Generation Internet and the US Internet programmes.

Technologically, there will be enhanced exposure to EU- and US-based innovation and research practices in securing UAVs by using lightweight Artificial Intelligence models with a particular focus on energy efficiency and mission-critical tasks. Energy efficiency first EU strategy with the objective of 32.5% reduction in energy consumption towards 2030 defines the importance of such energy-related aspects, both in cybersecurity and UAV operations domain. US NSF program has granted US partner for SecureUAV project with the following grant:

- Title: SaTC: EDU: Collaborative: Bolstering UAV Cybersecurity Education through Curriculum Development with Hands-on Laboratory Framework
- Sponsor: National Science Foundation (Grant No: 1956193)
- Amount: $472,060
- Period: May 1, 2020-April 30, 2023
- URL: https://www.nsf.gov/awardsearch/showAward?AWD_ID=1956193

Impact 3: Developing interoperable solutions and joint demonstrators, contributions to standards.

Following joint EU-US research activities, SecureUAV project will include the development of AI-based cybersecurity solutions protecting UAVs from cyberattacks, viruses and bringing forward improved awareness and training. Moreover, we will seek industrial validation of the cybersecurity "telemetry" model in real-world scenarios. At the end of the project,

Co-funded by the Horizon 2020
Framework Programme of the European Union

selected results will be published that will serve as a stepping stone in developing new standards and building new synergies based on the achieved results.

Impact 4: An EU - US ecosystem of top researchers, hi-tech start-ups / SMEs and Internet-related communities collaborating on the evolution of the Internet

Through decades, both UAV development and cyberthreat analysis communities have been developing in US and EU, following their own paths defined by needs, application areas, national strategies, and industrial applications. This project and the support from NGIAtlantic bring together EU and US lab working on interdisciplinary research and following innovation regional and national innovation needs. As a result of this synergy, it is expected to achieve not just international-quality experimentation results but also to promote and expose the advantages in structure and approach to experimentation. EU partner will be contacting major UAV producers and operators in Norway towards the end of the project regarding possible validation of the project results. Furthermore, together with US partner we are planning to apply for NGI Enrichers program through Spring 2023, which will be an extension of the existing work. Furthermore, we are currently working on the extension of the SecureUAV solution for the joint US-EU Horizon cooperation project proposal (HORIZON-JU-SNS-2023).

8 Conclusion and Future Work

To summarize the overall conclusions of the project:

- Communication in consumer UAVs spans over RF protocols: 2.4Ghz, 433, WiFi that can be analysed/intercepted by used RF / WiFi devices, where multiple toolkits are available.
- Firmware/OS-enable platforms have different capabilities and require own approach.
- Telemetry measurements (set: battery, time, altitude, temp, barometer) are available in every platform and can enrich cyber security awareness information.
- OS telemetry (CPU, RAM, I/O stat, filesystem, avg.load 1,5,10 min) gives direct indicators of malware infection using standards tools available in Linux
- IoT23 and Edge-IIoTset datasets are the most applicable datasets to be integrated with AI agents to be embedded in UAV, also to cover various types of applicable malware attacks (backdoor, password, Mirai, etc)
- OS data artefacts for malware analysis: MD5 has sums, log files, process lists, etc

Future work:

- Need to perform a comparison to Linux-based Anti-Virus solutions VS SecureUAV approach both in terms of energy and load using precise energy profiling.

- Cooperation with major drones manufacturer, presentation at the Unmanned Aerial Vehicle conference in Norway.
- Release of the relevant source code to GitHub
- One journal article from early 2023
- At least one conference paper in 2023
- A considerably wider range of applicable experiments.

9 References

1. Jiang, Y., & Yuan, J., & Sun, L., & Song, H. (2021, July), Development of a Laboratory Platform for UAV Cybersecurity Education Paper presented at 2021 ASEE Virtual Annual Conference Content Access, Virtual Conference. 10.18260/1-2–36958.

2. ENViSEC: Artificial Intelligence-enabled Cybersecurity for Future Smart Environments, https://smartseclab.com/envisec/ (December 2022)

3. Ferrag, Mohamed Amine, et al. "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning." IEEE Access 10 (2022): 40281-40306.

4. MISP Threats Sharing https://www.misp-project.org/

5.https://medium.com/@rkone1552000/rootkit-detection-chkrootkit-rkhunter-f52394116861

6. https://developers.google.com/protocol-buffers

7. https://github.com/rweather/arduinolibs

8. Shalaginov, Andrii, and Muhammad Ajmal Azad. "Securing resource-constrained iot nodes: Towards intelligent microcontroller-based attack detection in distributed smart applications." *Future Internet* 13.11 (2021): 272.

10 Glossary

AES-256	Advanced Encryption Standard (256 bit)
AI	Artificial Intelligence
ARM	Advanced RISC Machine – popular embedded devices architecture
AV	Anti-virus

Co-funded by the Horizon 2020
Framework Programme of the European Union

CPU	Central Processing Unit
CoAP	Constrained Application Protocol
DoS	Denial of Service attack
GPS	Global Positioning System
IDS	Intrusion Detection
IoC	Indicators of Compromise
IoT	Internet of Things
I/O	Input / Output interfaces
MQTT	Message Queuing Telemetry Transport protocol
NGI	Next Generation Internet
NSF	National Science Foundation
TRL	Technology Readiness Level
UAV	Unmanned Aerial Vehicles

Co-funded by the Horizon 2020
Framework Programme of the European Union