THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics,
Security and Law

Volume 16

Article 2

3-2-2021

A Constructive DIREST Security Threat Modeling for Drone as a Service

Fahad E. Salamh
Purdue University, fsalamh@purdue.edu

Umit Karabiyik
Purdue University, umit@purdue.edu

Marcus Rogers
Purdue, marckrogers@gmail.com

Recommended Citation

Salamh, Fahad E.; Karabiyik, Umit; and Rogers, Marcus (2021) "A Constructive DIREST Security Threat Modeling for Drone as a Service," *Journal of Digital Forensics, Security and Law*: Vol. 16 , Article 2.
DOI: https://doi.org/10.15394/jdfsl.2021.1695
Available at: https://commons.erau.edu/jdfsl/vol16/iss1/2

A CONSTRUCTIVE DIREST SECURITY THREAT MODELING FOR DRONE AS A SERVICE

Fahad E. Salamh, Umit Karabiyik and Marcus K. Rogers
Purdue University
401 N. Grant St., IN 47906, Unites States
fsalamh,umit,rogersmk@purdue.edu

ABSTRACT

The technology used in drones is similar or identical across drone types and components, with many common risks and opportunities. The purpose of this study is to enhance the risk assessment procedures for Drone as a Service (DaaS) capabilities. STRIDE is an acronym that includes the following security risks: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges. The paper presents a modified STRIDE threat model and prioritizes its desired properties (i.e., authenticity, integrity, non-reputability, confidentiality, availability, and authorization) to generate an appropriate DaaS threat model. To this end, the proposed DIREST threat model better meets the overall security assessment needs of DaaS. Moreover, this paper discusses the security risks of drones, identifies best practices for security assessment, and proposes a novel software update mechanism for drones during their operations. We explore the best practices related to drone penetration testing, including an effective methodology to maintain the continuity of drone operations, particularly drones used for emergency, safety, and rescue operations. Moreover, this research raises awareness of DaaS and drone operation in general as well as in the forensic science community due to its focus on the importance of securely operated drones for first responders. Furthermore, we address various aspects of security concerns, including data transmission, software restrictions, and embedded system-related events. In order to propose a security assessment for drones, we incorporate digital forensics and penetration testing techniques related to drone operations. Our results show that the proposed threat model enhances the security of flying devices and provides consistency in digital forensic procedures. This work introduces modifications to the STRIDE threat model based on the current literature, drone images provided by the NIST program, and a firmware static analysis of a zino hubsan brand drone.

Keywords: UAV Security, Drone as a Service, Daas, Drone Forensic, Penetration testing, Firmware Analysis, Threat Modeling

1. INTRODUCTION

Drone as a Service (DaaS) adoption and use has been rapidly increasing in the professional and commercial sectors Buchholz & Richter (2019). As Figure 1 shows, it is estimated to be approximately 267,900 drones in use by professional sectors by 2025. The assessment and mitigation of software-related risks are essential to support the effective operational adoption of DaaS.

Firmware (i.e., low-level software) and embedded systems (i.e., high-level software) are omnipresent in most emerging technologies such as the Internet of Things (IoT), robotics, drones, 3-D printing, virtual reality, etc. These types of devices require continuous security testing to plug vulnerabilities Costin et al. (2014).

Firmware analysis and penetration testing of embedded devices are crucial in most technologies, making firmware security an essential factor, particularly in emerging devices such as drones. We address various aspects of security assessments conducted on several drones used by safety and rescue organizations. Our work focuses on the analysis of firmware to determine security vulnerabilities or misconfiguration that could expose threats to the activity of drones, software restrictions that could limit the operation of drones such as no-fly-zone (NFZ), and operational communication commands. Alternatively, other security risks could relate to the data architecture of flying devices. Threats such as remote access to the drone, mid-flight attack, or remote shut down during operation Valente & Cardenas (2017). The examination of the system architecture for unmanned aerial vehicles (UAVs) is an essential step to better address these security threats.

Another aim is to revise the STRIDE threat model and prioritize its desired properties (i.e., authenticity, integrity, nonreputability, confidentiality, availability, and authorization) to generate an appropriate DaaS threat model. STRIDE stands for security risks, namely, spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privileges. To this end, the DIREST threat model better meets the overall security assessment needs of DaaS. Moreover, this research raises awareness of DaaS and drone operations in general as well as in the forensic science community due to its focus on the importance of securely operated drones for first responders.

The analysis in this work is based on security measures and metrics such as the open web application security project of IoT Top 10 Miessler & Smith (2018), the National Fire Protection Association (NFPA) 2400, standards for Small Unmanned Aircraft Systems (sUAS) used for public safety operations NFPA (2019), and the national institute of standards and technology (NIST) security guidelines Initiative (2012).

In this paper, we use drone images provided by the NIST program for drone forensics *NIST: Drone Data Set* (n.d.) to reverse engineer specific files in the interest of confidentiality of data such as flight logs encryption. Also, we conduct firmware analysis on the latest firmware publicly available by drone manufacturers. To the best

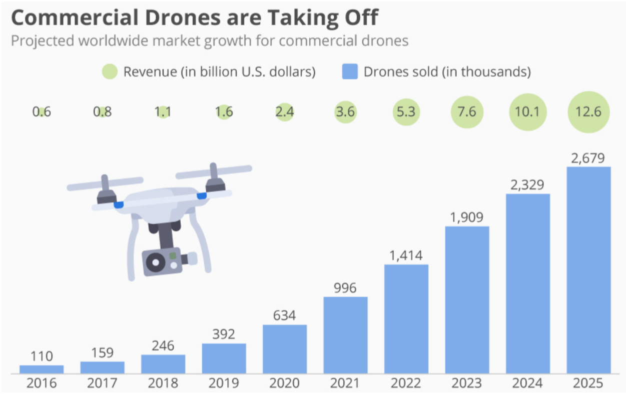


Figure 1. Market Growth of Drone as a Service Buchholz & Richter (2019)

of our knowledge, the incorporation between reverse engineering techniques on log files and firmware analysis has not been addressed by researchers; therefore, we concentrate on providing reliable measures and techniques in order to keep DaaS as operationally secure and resilient as possible.

Drone vulnerability is an emerging threat to the security field as the adoption of DaaS is going to impact the society as an investment into the drone space continues to grow. Drone adopters include operators in the fields of defense, emergency response, healthcare, agriculture, and transportation.

1.1 Contributions of the Paper

In this paper, we address security challenges related to the use of drones for first responders. The contributions of this paper are:

- We use various technical methods (i.e., penetration testing and reverse engineering) to address vulnerabilities that could be a threat to the operation of flying devices based on well-known security controls related to IoT devices.

- We present security controls related to the use of drones based on experimentation and a review of recent drone attacks.

- We propose the DIREST threat modeling process to enhance five aspects of DaaS security, including confidentiality, integrity, availability, and safety.

1.2 Organization of the Paper

This paper is structured as follows. In Section 2, we discuss the previous work carried out on simulated and actual unmanned aerial vehicle (UAV) hacking incidents, UAV incident response, and DaaS potential security threats. Section 3 addresses the approach we use to propose a threat modeling framework for DaaS. Section 4 presents a summary of our findings based on a literature review survey, technical experiments on Zeno Husban brand drone firmware, and a revisit of the STRIDE threat model. Finally, we conclude the paper with future research directions in Section 6.

2. LITERATURE REVIEW

The unprecedented outbreak of Coronavirus Disease-2019 (COVID-19) has boosted the implementation of drone technologies among different sectors. The integration of advanced technologies (e.g., artificial intelligence, networking, blockchain, and beyond visual line of sight Smoker et al. (n.d.); Chamola et al. (2020) has enabled DaaS businesses to utilize drone technology to respond to COVID-19 pandemic through numerous applications. Flying devices play an important role in government announcements, logistics services, detection, and monitoring Ruiz Estrada (2020). Alternatively, no standard security measures have been formulated to operate drones as secure as possible. Recently, the U.S. Department of Homeland Security is concerned about a potential risk from data collected by drones via cloud services Shortell (2019). Securing embedded devices requires manufactures to prevent access to software related data. Researchers in Watson & Dehghantanha (2016) suggested that developers of emerging technologies including drones should consider provocations faced by digital forensic practitioners when examining these devices. Architecture and implementation of IoT devices generate new security risks such as access to the device, maintenance, and software-update Van Oorschot & Smith (2019).

In our work, we take these security issues into consideration to intensify the challenges related to DaaS security. In Sections 2.1, 2.2, and 2.3, we discuss previous work related to general UAV security threats, UAV Incident Response, and potential security threats to DaaS, respectively.

2.1 Simulated and Actual UAV Hacking Incidents

A recent survey demonstrated a fair amount of simulated and actual cyberattacks on UAVs, discussing different vulnerabilities that targeted drones. The authors have summarized reported cyberattack incidents on both large and small size drones, where small size drones have experienced GPS jamming as an actual cyber incident; however, small UAVs are vulnerable to many other cyberattacks such as data leakage in communication protocols, and remote hijacking Krishna & Murphy (2017). Another work discussed the worthiness of drone security assessment, and conducted a security analysis on DJI Phantom 3 and drew the importance of software vulnerabilities that could lead to stealing sensitive data. Researchers recommended security measures such as a requirement to change passwords on the first use of the drone; prevent unauthorized access to the file system as a root user, and provide security for open ports while a UAV is in operation Trujano et al. (2016); F. Salamh et al. (2021). As we are targeting the security of DaaS, the study of interdiction attacks is important. A study on the security of DaaS cyber-physical formulated a zero-sum network ban game to avoid the interception of UAV by attackers when the drone is on a delivery mission Sanjab et al. (2017). This indicates that the adoption of DaaS needs a well defined and classified threat modeling system to achieve secure mitigation strategies which enhance the incident response plan.

2.2 UAV Incident Response

A recent research discussed drone incident response plans. It illustrated the importance of a 'lessons learned' phase where vulnerabilities and security threats are identified to improve the mitigation strategies (F. Salamh et al., 2019). On the other hand, a novel drone forensic investigation process has been introduced in F. E. Salamh et al. (2019), which provides an extra layer to the technical procedure of responding to drone hacking incidents. Works related to drone forensics can be beneficial in a post-incident stage; however, this paper focuses on the pre-incident stage to enhance the security of flying devices. A comprehensive work in Prathap & Rachumallu (2013) illustrated the penetration testing of electronic control units (ECUs) in vehicles. ECUs are known as embedded systems to operate a device in an automated approach. For instance, ECUs are effective for vehicles to perform actions requested through different sensors; however, UAVs use multiple control systems to perform specific actions (e.g., an Electronic Speed Controller), which deals with the motor speed and directions.

2.3 DaaS Potential Security Threats

Lack of research in the area of DaaS security assessment creates challenges for the future of emerging technologies. The advancement of technology is moving very fast. This requires scientists to focus investigative research on sociotechnical systems (STS) development. Adopting new technologies as a solution to current problems does not prevent the occurrence of significant issues; therefore, in this research, we carefully address this challenge by combining all principals of STS. For instance, Noy et al. (2018) discuss challenges posed in the cyber-physical realm, including UAVs. Researchers have identified the lack of research on the implications of dealing with complex systems issues from a security lens as a potential safety threat, and they have proposed two principles of STS. These proposed core principles are provided to enhance the overall security of systems. This would increase the overall functionality of the systems when they are connected through hierarchical feedback control loops, considering all subsystems.

We consider the STRIDE threat model to support our security risk assessment model for emerging technologies, specifically DaaS, because we believe an in-depth technical analysis should be conducted to enhance the theoretical methodology; while the proposed model could be implemented on other technologies, however, measuring the risk assessment of other emerging technologies are out of the scope of our research. STRIDE Shostack (2008) is a well-known threat model that is used in this research to study potential threats of Unmanned Aerial Systems (UASs). Drone GPS spoofing controls the functionality of flying devices, and there are several incidents related to maldrone and GPS spoofing attacks for weaponizing purposes.

A proof of concept has been presented in Braga (2015), where a programmed drone controls another drone and hacks into it. Vulnerabilities such as unnecessary open ports increase the risk of drones being hacked. In terms of using drones as a service, it is essential to avoid data being tampered with, including, for instance, using drones for crime scene mapping in the performance of public safety services Mendis et al. (2016). One aspect of data tampering on drones is the modification of sensitive data such as secure features implemented on the drone's firmware. Modification to the NFZ is out of the scope of this research; however, the ability to modify such a restriction feature poses challenges to the environment of DaaS.

The concentration of this paper is to enhance the overall security of DaaS implementation. A proof of concept design for data tampering has been presented in (F. Salamh et al., 2019), where it is possible for an attacker to modify metadata that is critical to the digital forensic community. Repudiation in DaaS mainly deals with performing unauthorized access and being able to deny the perpetration of actions He et al. (2017); Baldini et al. (2013); Humphreys et al. (2008). Researchers discussed issues related to information disclosure by initiating an eavesdropping attack. An experimental Denial of Service (DoS) attack was presented in Vasconcelos et al. (2016). The DoS attack performed on an AR drone 2.0 illustrated the malfunctioning of live streaming data using tools such as lioic, netwox, and hping3. A privilege escalation vulnerability such as the nvidia tegra processor, which is known as the cold-boot attack Bhatia (2019), illustrates the impact and threat that DaaS implementers need to address, preferably through a program of secure patch management. The complexity of drone technology and its system components raise a security issue when it comes to the protection of these systems against attackers.

A lack of proper security assessment leads to the rapid diffusion of DaaS. For instance, these flying devices rely on GPS technology, which can be spoofed by an attack, potentially resulting in the weaponization of a drone. Researchers classified GPS spoofing attacks as the main security threat to flying devices INFOSEC (2013); therefore, in this research, we take the severity level of security threats into consideration. GPS spoofing impacts the security component of drone operations, namely availability Choudhary et al. (2018) and might lead to data being tempered. This type of attack imposes anti-forensic challenges to the drone forensic investigation process (F. Salamh et al., 2019). An experimental evaluation of GPS spoofing was performed on a Hornet Mini civil UAV, resulting in digitally dispositioning the UAV geo-location of approximately 0.62 kilometers Shepard et al. (2012). UAVs cyber threats include GPS spoofing, DoS, hardware/software trojans, and unauthorized access to telemetric signals. Researchers in Altawy & Youssef (2016) proposed security requirements to mitigate these by enhancing the encryption of telemetric channels, regular system update, and system monitoring.

Another security threat to DaaS is a malware attack Storm (2015), where a drone can be injected with an exploit targeting a specific backdoor in the system to take full control. Firmware is considered to be a major risk to drones, mainly when companies aim for low-cost maintenance Kvarda et al. (2017). The traditional process of firmware updates has several unsecured processes and steps, where a vulnerability has been identified, and a manufacturer distributes the updated firmware over the internet to let customers update their drones. In this case, attackers have easy access to the entire firmware image file, which can be reverse-engineered. In Atmel (2013), researchers presented the flow process of firmware update security as shown in Figure 2.

A study in Egham (2013) emphasizes on the importance of updating firmware remotely, Jurkovic & Sruk (2014) researchers proposed an updated solution for firmware update transmitted over a transport layer security with a unique certificate. In our research, we particularly study the security aspect of firmware updates associated with DaaS. We look into strategies that could enhance the secure firmware update to avoid operational and security risks. An introduction to the three update strategies has been presented in Jurkovic & Sruk (2014). The presenters demonstrated a live demo where they updated the camera's software while the drone was operational and airborne Imreh (2017). Software update while in mid-flight is crucial to the field of DaaS. Suppose a significant bug was discovered while thousands of drones are on an active delivery mission. This indicates the need for a live software update with zero-downtime, as presented in Jurkovic & Sruk (2014); Imreh (2017). The presented system relies on creating smart contracts for a new firmware update, which is distributed via top-reputation AVs Baza et al. (2019). In DaaS, the case is entirely different since we can not implement drone to drone communication, which might result in more risks; therefore, our proposed firmware update strategy combines the work presented by Jurkovic & Sruk (2014); Imreh (2017); Baza et al. (2019) to match the objectives of the DIREST threat model proposed in this research.

3. METHODOLOGY

The technical experiment of this research involves different classes within the firmware. The firmware is the brain of flying devices in terms of effective operation in the sky; therefore, we conduct security testing on zino hubsan brand firmware and drone images to generate a threat modeling process that could mitigate security threats to drone operations, especially when adopting the technology as a service. For instance, a built-in camera attached to the drone has firmware that should be securely programmed to avoid unauthorized access to media files and data tampering. Safety and reliability of flying devices are linked to the firmware security. These products should have a constant security scanning of embedded systems as drones operate on built-in software.

Firmware can be found and downloaded through the vendor's website, which is not recommended as the newly released update can be distributed by attackers using a modified infected version of the software. For DaaS, it seems that most well-known companies have started to avoid public distribution of firmware; however, this does not effectively work when it comes to DaaS because it is difficult to update the system while the drone

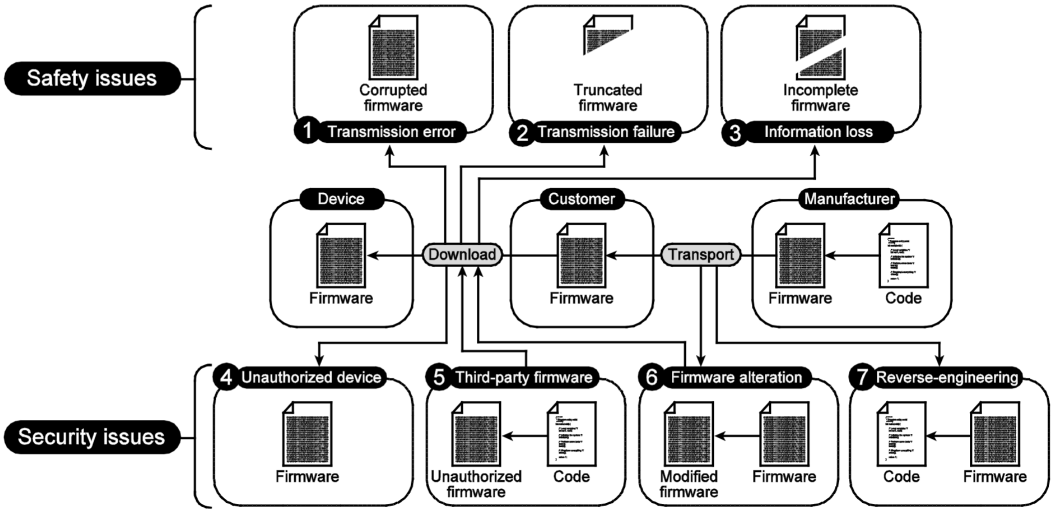


Figure 2. Firmware Update Security Issues Atmel (2013)

engaged in a flight operation. It is crucial that a drone should be updated in the air to avoid possible threats. In this paper, we perform technical analysis (i.e., penetration testing and reverse engineering) to discover possible vulnerabilities and misconfigurations related to the selected firmware. Our analysis includes decompression of firmware, entropy analysis, and system fingerprinting (see Section 4).

Also, we propose an enhanced DIREST Threat Model Method (DIREST-TMM), which is an acronym of ***D****oS,* ***I****nformation disclosure,* ***R****epudiation,* ***E****scalation of privilege,* ***S****poofing GPS protocol, and* ***T****ampering* as a result of a new prioritized view of the STRIDE threat model will be used as a methodology to deal with UASs and propose a developed threat model for DaaS. We developed the DIREST threat model taking the priority of different attacks related to drones into consideration.

4. RESEARCH FINDINGS

The scope of this paper is to integrate most well-known security standards and frameworks to propose a comprehensive threat model based on the following measures:

- A literature review of recent incidents related to drones.
- Technical experiments on a Zeno Hubsan firmware.
- A revisit to the STRIDE threat model and a proposed enhancement that is a better fit for DaaS.
- A proposed risk assessment framework specifically for DaaS.

Since we covered most of the drone cyber incidents in Section 2, it is essential to validate the security weaknesses of drones and tackle the studied issue from technical and theoretical sides.

4.1 Technical experiment on Zeno Hubsan drone

Firmware analysis is a crucial pen-testing technique to avoid security holes that can be exploited as a vulnerability. Penetration testers capture the firmware of the device through packet sniffing, reverse engineering the mobile app, or dumping it from the flash storage chip. These are commonly used methods for testing for software security; however, recently, some well-known drone companies have deployed over-the-air (OTA) firmware updates. OTA updates are a good practice to update software bugs automatically. Unfortunately, manufacturers focus on the lowest cost production and firmware update mechanisms, which often creates a major security issue. Continuous update to the firmware of a flying device is important as the device heavily relies on programmed features that can be vulnerable anytime.

A proof of concept (PoC) in (F. Salamh et al., 2019) illustrated a security issue related to a software bug that failed to encrypt flight logs while on flight mode, which leaves the flight logs in plaintext format. Furthermore, we unpack and reverse engineer three firmware assemblies belonging to the mentioned UAV in this research. The main goal of the technical experiment is not to suggest additional techniques in firmware analysis; however, we do check the security strategy used in implementing the firmware. The unpacking process starts using binwalk on Kali Linux to get a deeper understanding of the firmware heterogeneity. The presented technical PoC on the firmware update strategy in Imreh (2017); Baza et al. (2019) used a hand over update strategy as shown in Figure 3. The handover update strategy has a zero-downtime update as it starts with downloading the new firmware image while the old firmware is active. The old firmware image is rendered inactive when the new firmware update is completed and notifies the old version. This strategy reduces the risk of relying on client-side updates and provides a faster and more efficient approach to fix vulnerabilities.

In this paper, we conduct a static analysis of zino hubsan firmware as a proof of concept, which will enhance the overall threat model of flying devices. We analyze the code for known vulnerabilities; measure entropy level, and look into the data transmission methodology. Our purpose is to have both technical and theoretical aspects in place, using best practices. Figures 4, 5, and 6 show the decompression and unpacking of the firmware. We looked at compressed files, which include the kernel binary image. Running the 'strings' command provides more details about the readable text inside the image.

Figure 6 illustrates the first ten readable strings, which include the version of the Linux operating system. This information can be helpful and harmful at the same time. Attackers might get an advantage by fingerprinting the firmware and target these devices. We looked at vulnerability databases to determine the type of attacks associated with this particular version of the Linux operating system. As shown in Figure 7, this version is highly affected by DoS (43.8%) with 192 vulnerabilities during the last five years. This presents the lessons to be learned by DaaS adopters. All systems should be up to date to avoid risks. From our analysis, we found that the firmware is updated; however, the version of the operating system is about three years old.

Entropy analysis is a technique used to measure data randomness of a binary file. The technique was derived by Claude Shannon Shannon (1948) and is computed as:

$$H(X) = -\sum_{i=1}^{n} p(X_i) log_2 p(X_i)$$

A computation of entropy measurement was performed on four training sets including plaintext files. The expected 99.99% confidence interval (CI) for encrypted or packed data ranges from 4.941 - 6.369, 6.677 - 7.267, and 7.174 - 7.312 for native, packed, encrypted executables, respectively Lyda & Hamrock (2007). Alternatively, the highest 99.99% CI on plaintext files on all training

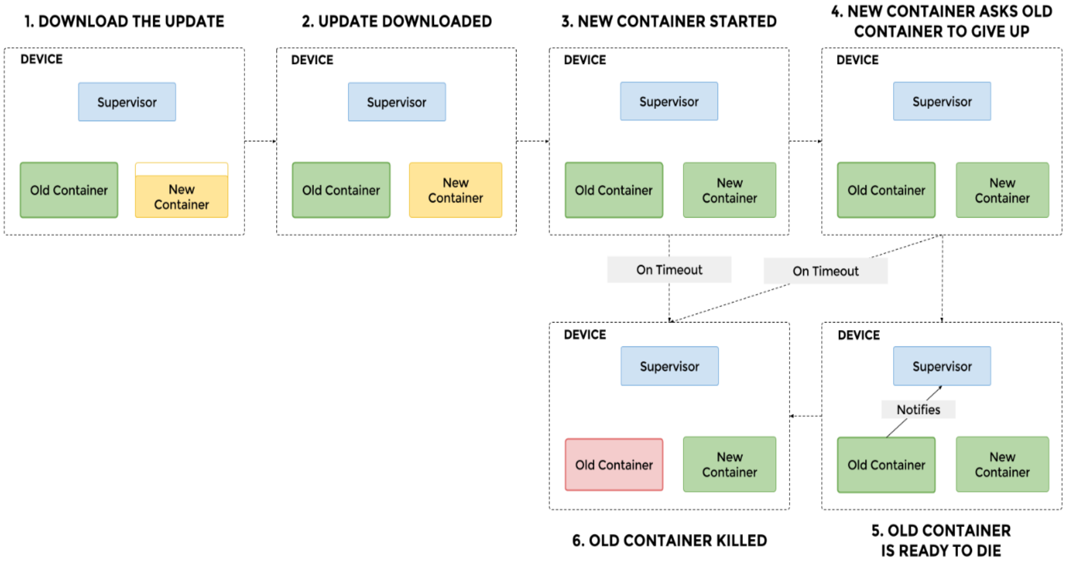
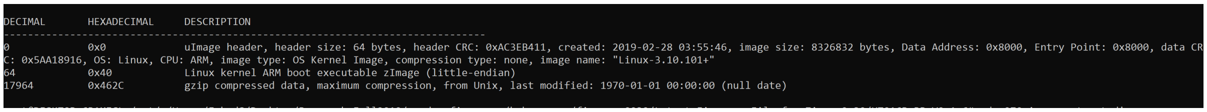


Figure 3. Firmware hand over update strategy Baza et al. (2019)

sets was 5.030, indicating that an entropy above 0.6 is likely to be compressed or encrypted. We delved into a static analysis of the software code and the entropy level of the Zino firmware, as shown in Figure 8. The performed entropy analysis illustrates a low level of encryption or compression in some regions of the binary file. These blind spots can divulge sensitive confidential information related to the firmware content.

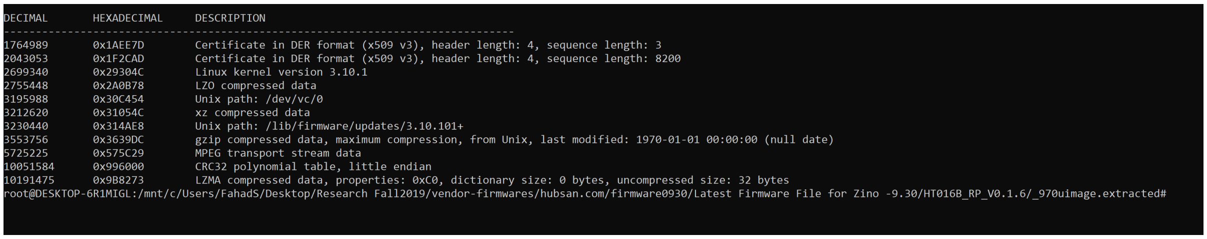
4.2 A revisit to the STRIDE threat model and a proposed enhancement that fits DaaS

Earlier, we provided a piece of introductory information on the STRIDE threat model. In this paper, we build a threat model based on the STRIDE acronym; however, we named it the DIREST threat model because it is based on the priority of each risk factor. On the other hand, we carefully considered the hardware and software components of drones in three instances when data is at rest, in motion, and in use. DaaS organizations must achieve appropriate security levels and protections for these categories. Data at rest contains data stored within the firmware, memory cards, and logs. The security of these components is important to avoid data being tampered with or stolen. More importantly, for the transmitted data, drones have different communication protocols, and it is very important to secure this transmitted data properly. For instance, (F. Salamh et al., 2019) presented a vulnerability in the storage mechanism of Typhoon H drone, where it does not encrypt live streaming data. Similarly, with data in use, most of the activities between the server and the client should be secured. When it comes to drone security for DaaS, we prioritize *DoS* as the most critical risk factor because disruption of drone service is an issue for most companies that adopt drones. Second, *Information Disclosure* is critical because these devices are equipped with sensitive customer information, which might result in cyber profiling and identity theft. *Repudiation* is considered as the third risk factor in our model. It has been proven in (F. Salamh et al., 2019) that the integrity of data is a concern when dealing with flying devices. The reason is that they operate on



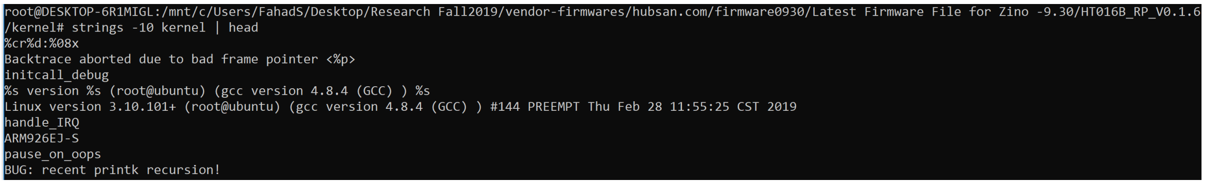
```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             uImage header, header size: 64 bytes, header CRC: 0xAC3EB411, created: 2019-02-28 03:55:46, image size: 8326832 bytes, Data Address: 0x8000, Entry Point: 0x8000, data CR
C: 0x5AA18916, OS: Linux, CPU: ARM, image type: OS Kernel Image, compression type: none, image name: "Linux-3.10.101+"
64            0x40            Linux kernel ARM boot executable zImage (little-endian)
17964         0x462C          gzip compressed data, maximum compression, from Unix, last modified: 1970-01-01 00:00:00 (null date)
```

Figure 4. Decompression of Firmware



```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
1764989       0x1AEE7D        Certificate in DER format (x509 v3), header length: 4, sequence length: 3
2043053       0x1F2CAD        Certificate in DER format (x509 v3), header length: 4, sequence length: 8200
2699340       0x29304C        Linux kernel version 3.10.1
2755448       0x2A0B78        LZO compressed data
3195988       0x30C454        Unix path: /dev/vc/0
3212620       0x31054C        xz compressed data
3230440       0x314AE8        Unix path: /lib/firmware/updates/3.10.101+
3553756       0x3639DC        gzip compressed data, maximum compression, from Unix, last modified: 1970-01-01 00:00:00 (null date)
5725225       0x575C29        MPEG transport stream data
10051584      0x996000        CRC32 polynomial table, little endian
10191475      0x9B8273        LZMA compressed data, properties: 0xC0, dictionary size: 0 bytes, uncompressed size: 32 bytes
root@DESKTOP-6R1MIGL:/mnt/c/Users/FahadS/Desktop/Research Fall2019/vendor-firmwares/hubsan.com/firmware0930/Latest Firmware File for Zino -9.30/HT016B_RP_V0.1.6/_970uimage.extracted#
```

Figure 5. Unpacking compressed data



```
root@DESKTOP-6R1MIGL:/mnt/c/Users/FahadS/Desktop/Research Fall2019/vendor-firmwares/hubsan.com/firmware0930/Latest Firmware File for Zino -9.30/HT016B_RP_V0.1.6
/kernel# strings -10 kernel | head
%cr%d:%08x
Backtrace aborted due to bad frame pointer <%p>
initcall_debug
%s version %s (root@ubuntu) (gcc version 4.8.4 (GCC) ) %s
Linux version 3.10.101+ (root@ubuntu) (gcc version 4.8.4 (GCC) ) #144 PREEMPT Thu Feb 28 11:55:25 CST 2019
handle_IRQ
ARM926EJ-S
pause_on_oops
BUG: recent printk recursion!
```

Figure 6. Human Readable Strings in Kernel Image

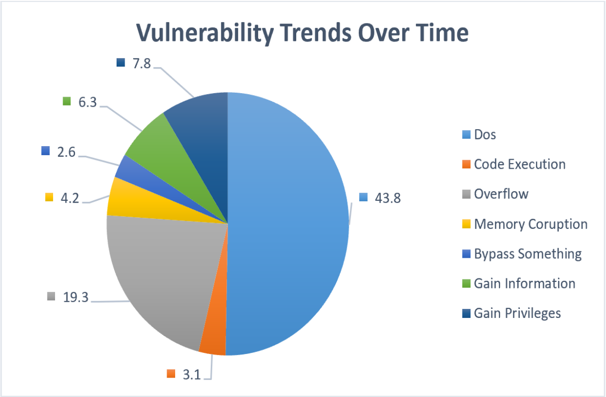


Figure 7. Vulnerabilities Associated with Linux V.3.10.101

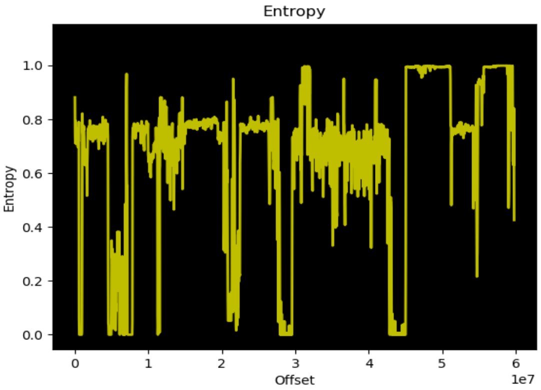


Figure 8. Entropy Analysis of Firmware

different communication protocols and even multiple system components; therefore, it is important to properly certify these digital communications and consider it as a risk factor that might lead to other security risks.

In Section 4 we present a technical proof using a reverse engineering technique that touches on issues related to security best practices and software update mechanisms. For instance, when we unpacked the firmware (see Figures 4, 5, and 6) we discovered that the operating system was seriously outdated while the firmware was the latest version. Furthermore, the old-fashioned style of providing firmware to be downloaded from the vendor website is considered a notable threat, which could lead to a targeted cyber attack on these devices. *GPS Spoofing* is categorized as a level five threat because it relates to countermeasures that should be secured in the first four risk factors, including, for example, the hardening of navigation systems. The *Tampering* risk factor is key since it is crucial for DaaS to be able to carry reliable data and be tamper-proof to comply with the Federal Aviation Administration (FAA) drone operator guidelines. Our proposed threat model supports the design of a comprehensive risk assessment framework for DaaS.

4.3 Proposed DIREST Threat Model Method (DIREST-TMM)

The model proposed in this paper (see Figure 9) concentrates on the prioritization of security threats. In regard to DaaS, the availability of the service is a primary and driving principle of the model. Mitigating DoS attacks to DaaS is crucial to avoid service disruption. DIREST-TMM is categorized in an ascending order based on the level of security risk. We determine the security threats based on recent publications related to drone cyber attacks and technical experiments conducted in this research. Next in priority comes the information disclosure element, which should be assessed on different stages of data storage, including data at rest, data in motion, and data in use. These three types of data should be transmitted and kept securely by implementing proper encryption mechanisms.

5. SUMMARY OF FINDINGS

Our study and the experimentation completed in this research has led to a novel risk assessment framework that should be implemented in most DaaS organizations. Currently, the hype of drones as a service is rapidly increasing without any security assessment plans. Moreover, most research efforts lack threat modeling and threat analysis tailored for drone operations. We studied software/hardware-related security threats, weak communication protocols, and data flow in transmitting data to generate a standard risk assessment framework.

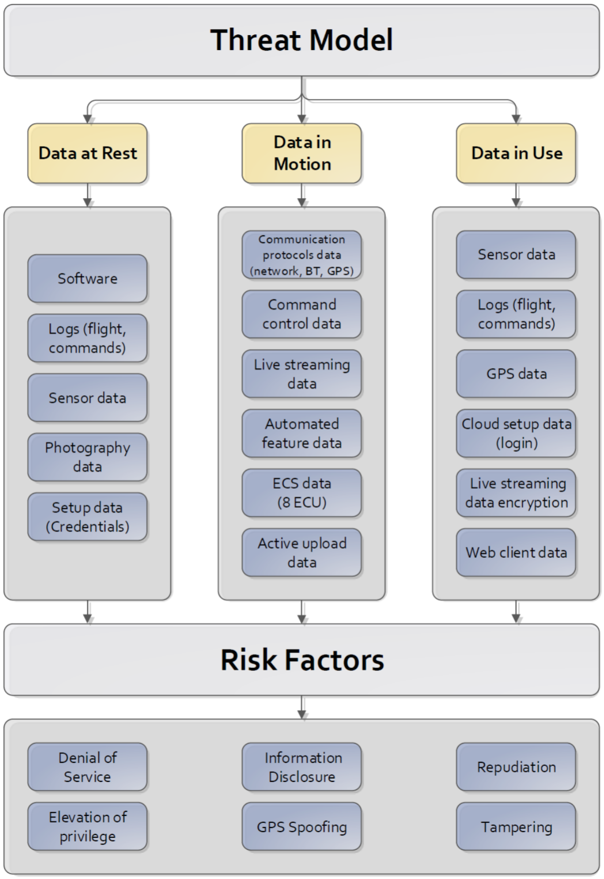


Figure 9. DIREST-TMM

5.1 Proposed risk assessment framework designed for DaaS

We took the OWASP IoT top 10 list Miessler & Smith (2018) into consideration to develop this framework, which is designed for flying devices with no restrictions on the different automation levels. Ultimately, securing drones from cyber threats are crucial. We developed a comprehensive framework that enables DaaS organizations to consider security risks, particularly since when the number of flying drones increases, there will be an increase in non-cyber threats; however, discussing non-digital risks is out of scope for this paper. Hence, we focus only on digital risks. As shown in Figure 10, our proposed threat assessment framework enables organizations to adopt drone technology more safely. We categorize the threat assessment framework based on four phases (i.e., assess, identify, evaluate, and treat) and each phase deals with a specific category of risk that includes

1. Assessing application and link risks,
2. Identifying accessibility risks,
3. Evaluating perceptional risks, and
4. Treating data security risks.

This is done based on the data flow architecture of flying devices illustrated in Figure 10, which illustrates the proposed DIREST-TMM that comprises sixteen risk factors related to the security measurement of DaaS operation. For instance, we recommend assessing application and link risks by securing streaming data and connected communication protocols; however, to achieve secure operation and maintenance, our proposed framework insists on identifying accessibility risks (i.e., system monitoring, update management, secure ecosystem, secure network services and credentials).

DaaS businesses must evaluate perceptional risks such as autonomy, human trust, and efficiency. Doing so would target a better measurement and evaluation – lastly, the treatment of data security risks. The adoption and deployment of secure cryptography of data would enhance data governance and reduce potential privacy issues.

Security risks of these devices come from weak communication protocols, unpatched software, and the use of unneeded network services. In our framework, we consider all these aspects, mainly where application and data link risks dictate measures to prevent data leakage while in motion; therefore, weak communication protocols and insecure data streaming should be well managed to avoid leakage of these data. Researchers (F. Salamh et al., 2019; F. E. Salamh et al., 2019) demonstrated how data transition can be an issue to drone operators, mainly when drones are used as a collector of and collection point for sensitive data. Furthermore, it is crucial for DaaS implementers to manage the risk of accessibility to drone devices.

The management of encryption and network services deployed on drones are essential to operate and maintain flying devices securely. Soon, drones will carry and transmit invaluable data. For instance, data leakage of gas thermal imaging or any other critical infrastructures becomes a potential immediate critical infrastructure risk. With the increased advancements in drone technology, we will see more incidents related to data or service disruption. The previous work discussed in this research indicates that hacking drones is not a significant challenge because of the weak software and communication protocols used. Furthermore, most of the drone adopters are not concentrating on the security of DaaS, focusing instead on the advancement of the technology and functionality of these devices. That is why we classified risk Perception as an important factor in our proposed threat assessment framework.

Risk Perception deals with the safety and security of sensors and actuators, targeting a higher maturity level of measurement and evaluation. From a human perspective, human trust in automation is still in its early stages, which is a function of the autonomy and efficiency of insecure technologies. From a technology perspective, data and geolocation pose a threat to these flying devices.

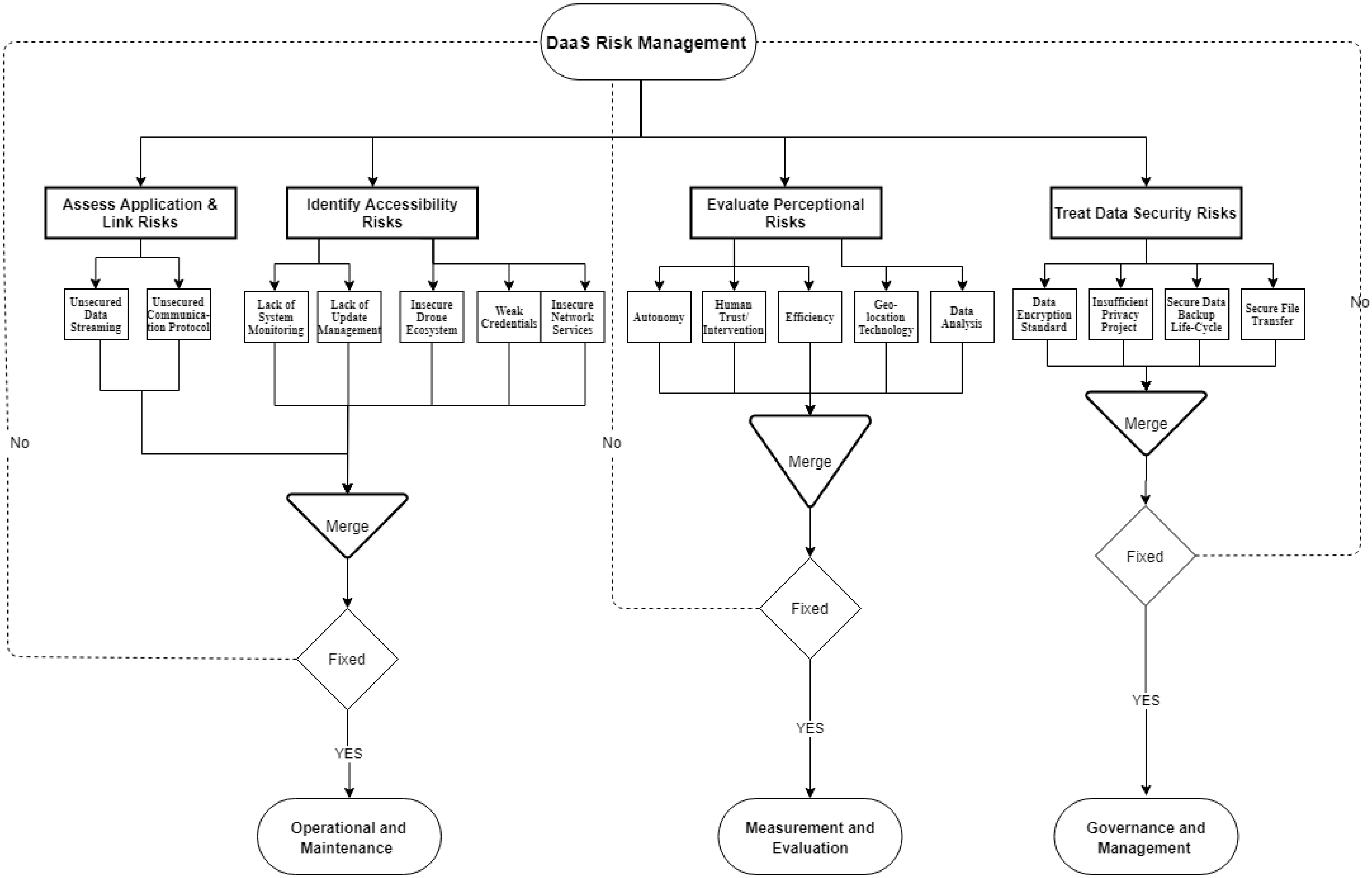

DaaS Risk Management
Assess Application & Link Risks
Identify Accessibility Risks
Evaluate Perceptional Risks
Treat Data Security Risks
Unsecured Data Streaming
Unsecured Communication Protocol
Lack of System Monitoring
Lack of Update Management
Insecure Drone Ecosystem
Weak Credentials
Insecure Network Services
Autonomy
Human Trust/ Intervention
Efficiency
Geo-location Technology
Data Analysis
Data Encryption Standard
Insufficient Privacy Project
Secure Data Backup Life-Cycle
Secure File Transfer
Merge
Merge
Merge
Fixed
Fixed
Fixed
No
No
No
YES
YES
YES
Operational and Maintenance
Measurement and Evaluation
Governance and Management

Figure 10. Threat Assessment Framework for DaaS

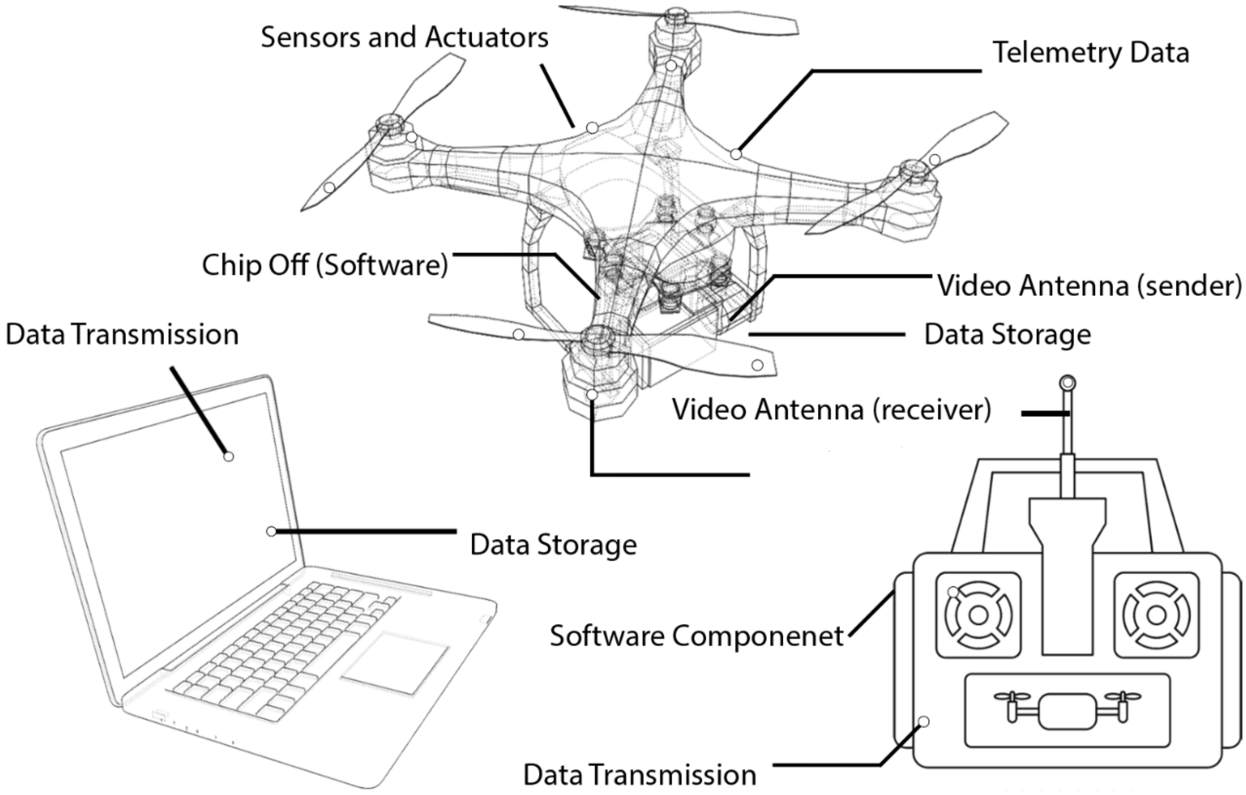


Figure 11. Drone Data Flow and Components

It is a balanced equation when sensors and actuators are performed securely, resulting in an increase in safety and efficiency through measurement and evaluation of perceptional risks.

Data risks are covered in most of the previous work; however, in this last category, we insist on the importance of adopting secure encryption mechanisms based on well-known standards along with data policy for each DaaS provider. Having clear policies on data transmission will enhance the overall governance and management of data risks. Also, the methodology of data backup used for drones plays an important role in governing data risk. In Figure 11, we illustrate the data flow and the important components of a drone. These components along with cloud-based data storage and transmission of data should be assessed using the proposed threat assessment framework to improve the overall security of drones.

6. CONCLUSION

Companies offering DaaS are growing rapidly without taking proper security measures into consideration. COVID-19 pandemic played an important role in testing drone technologies and could be considered as an excellent excellent opportunity for researchers to evaluate drone security from different angles. We discussed various technical techniques that could potentially be security threats to drone operations.The proposed DIREST threat model and threat assessment framework will aid in improving the security of these flying devices. In this research, we have demonstrated a number of security vulnerabilities and presented the weaknesses of drone systems. Also, we discussed the previous work related to drone hacking incidents due to weak communication protocols and network services ensuring a proper security measure of drone operations. DIREST threat model comprehensively appraised measures such as confidentiality, integrity, availability, and safety to satisfy minimum security requirements related to drone operations.

As for future work, we plan to develop an operational drone security center where all software components and communication protocols are automatically scanned for vulnerabilities. This would enhance the adoption of DaaS and the secure monitoring of drones on both critical and noncritical missions. Regarding the automation of secure firmware updates, we would like to work on integrating the proposed technology in this research with block-chain technology to enhance the integrity and authentication of scalable firmware update distribution on a large scale.

REFERENCES

Altawy, R., & Youssef, A. M. (2016). Security, privacy, and safety aspects of civilian drones: A survey. *ACM Transactions on Cyber-Physical Systems*, *1*(2), 1–25.

Atmel. (2013). *Safe and secure bootloader implementation for sam3/4.* http://ww1.microchip.com/downloads/en/AppNotes/Atmel-42141-SAM-AT02333-Safe-and-Secure-Bootloader-Implementation-for-SAM3-4_Application-Note.pdf. Retrieved from http://ww1.microchip.com/downloads/en/AppNotes/Atmel-42141-SAM-AT02333-Safe-and-Secure-Bootloader-Implementation-for-SAM3-4_Application-Note.pdf (Accessed: 2020-05-22)

Baldini, G., Karanasios, S., Allen, D., & Vergari, F. (2013). Survey of wireless communication technologies for public safety. *IEEE Communications Surveys & Tutorials*, *16*(2), 619–641.

Baza, M., Nabil, M., Lasla, N., Fidan, K., Mahmoud, M., & Abdallah, M. (2019). Blockchain-based firmware update scheme tailored for autonomous vehicles. In *2019 ieee wireless communications and networking conference (wcnc)* (pp. 1–7).

Bhatia, R. (2019). *New vulnerability at nvidia allows remote code execution.* https://www.securitynewspaper.com/2019/07/23/new-vulnerability-at-nvidia-allows-remote-code-execution-and-privilege-escalation/. Retrieved from https://www.securitynewspaper.com/2019/07/23/new-vulnerability-at-nvidia-allows-remote-code-execution-and-privilege-escalation/ (Accessed: 2020-05-22)

Braga, M. (2015). *New malware gives hackers another way to crash your drone.* https://www.vice.com/en_us/article/wnj744/new-malware-gives-hackers-another-way-to-crash-your-drone. Retrieved from https://www.vice.com/en_us/article/wnj744/new-malware-gives-hackers-another-way-to-crash-your-drone (Accessed: 2020-05-22)

Buchholz, K., & Richter, F. (2019, Feb). *Infographic: Commercial drones are taking off.* https://www.statista.com/chart/17201/commecial-drones-projected-growth/. Retrieved from https://www.statista.com/chart/17201/commecial-drones-projected-growth/

Chamola, V., Hassija, V., Gupta, V., & Guizani, M. (2020). A comprehensive review of the covid-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact. *IEEE Access*, *8*, 90225–90265.

Choudhary, G., Sharma, V., Gupta, T., Kim, J., & You, I. (2018). Internet of drones (iod): Threats, vulnerability, and security perspectives. *arXiv preprint arXiv:1808.00203*.

Costin, A., Zaddach, J., Francillon, A., & Balzarotti, D. (2014). A large-scale analysis of the security of embedded firmwares. In *23rd USENIX security symposium. usenix security 14* (pp. 95–110).

Egham, U. (2013). *Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016.* https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 (Accessed: 2020-05-22)

He, D., Chan, S., & Guizani, M. (2017). Drone-assisted public safety networks: The security aspect. *IEEE Communications Magazine*, *55*(8), 218–223.

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner, P. M. (2008). Assessing the spoofing threat: Development of a portable gps civilian spoofer. In *Radionavigation laboratory conference proceedings.*

Imreh, G. (2017). *How we updated a drone while flying - and how you can too!* https://www.balena.io/blog/how-we-updated-a-drone-while-flying-dockercon2016/. balena. Retrieved from https://www.balena.io/blog/how-we-updated-a-drone-while-flying-dockercon2016/

INFOSEC. (2013). Hacking drones ... overview of the main threats. https://www.securitynewspaper.com/2019/07/23/new-vulnerability-at-nvidia-allows-remote-code-execution-and-privilege-escalation/. Retrieved from https://www.securitynewspaper.com/2019/07/23/new-vulnerability-at-nvidia-allows-remote-code-execution-and-privilege-escalation/ (Accessed: 2020-05-22)

Initiative, J. T. F. T. (2012, Sep). *Guide for conducting risk assessments.* https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Jurkovic, G., & Sruk, V. (2014). Remote firmware update for constrained embedded systems. In *2014 37th international convention on information and communication technology, electronics and microelectronics (mipro)* (pp. 1019–1023).

Krishna, C. L., & Murphy, R. R. (2017). A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In *2017 ieee international symposium on safety, security and rescue robotics (ssrr)* (pp. 194–199).

Kvarda, L., Hnyk, P., Vojtěch, L., & Neruda, M. (2017). Software implementation of secure firmware update in iot concept.

Lyda, R., & Hamrock, J. (2007). Using entropy analysis to find encrypted and packed malware. *IEEE Security & Privacy*, *5*(2), 40–45.

Mendis, N., Dharmarathne, T., & Wanasinghe, N. (2016). Use of unmanned aerial vehicles in crime scene investigations-novel concept of crime scene investigations. *Forensic Res Criminol Int J*, *4*(1), 00094.

Miessler, D., & Smith, C. (2018). Owasp internet of things project. *OWASP Internet of Things Project-OWASP*.

NFPA. (2019). *Standard for small unmanned aircraft systems (suas) used for public safety operations.* `https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=2400`. Retrieved from `https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=2400` (Accessed: 2020-05-22)

Nist: Drone data set. (n.d.). `https://www.cfreds.nist.gov/drone-images.html`. Retrieved from `https://www.cfreds.nist.gov/drone-images.html`

Noy, I. Y., Shinar, D., & Horrey, W. J. (2018). Automated driving: Safety blind spots. *Safety science*, *102*, 68–78.

Prathap, V., & Rachumallu, A. (2013). *Penetration testing of vehicle ecus* (Unpublished master's thesis).

Ruiz Estrada, M. A. (2020). The uses of drones in case of massive epidemics contagious diseases relief humanitarian aid: Wuhan-covid-19 crisis. *Available at SSRN 3546547*.

Salamh, F., Karabiyik, U., Rogers, M., & Al-Hazemi, F. (2019). Drone disrupted denial of service attack (3dos): Towards an incident response and forensic analysis of remotely piloted aerial systems (rpass). In *2019 15th international wireless communications & mobile computing conference (iwcmc)* (pp. 704–710).

Salamh, F., Karabiyik, U., Rogers, M. K., & Matson, E. (2021, January). Unmanned aerial vehicle (UAV) kill chain: Purple teaming tactics. In *2021 ieee 11th annual computing and communication workshop and conference (ccwc) (ieee ccwc 2021).*

Salamh, F. E., Karabiyik, U., & Rogers, M. K. (2019). Rpas forensic validation analysis towards a technical investigation process: A case study of yuneec typhoon h. *Sensors*, *19*(15), 3246.

Sanjab, A., Saad, W., & Başar, T. (2017). Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game. In *2017 ieee international conference on communications (icc)* (pp. 1–6).

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell system technical journal*, *27*(3), 379–423.

Shepard, D. P., Bhatti, J. A., Humphreys, T. E., & Fansler, A. A. (2012). Evaluation of smart grid and civilian uav vulnerability to gps spoofing attacks. In *Radionavigation laboratory conference proceedings.*

Shortell, D. (2019). *Dhs warns of 'strong concerns' that chinese-made drones are stealing data.* `https://www.cnn.com/2019/05/20/politics/dhs-chinese-drone-warning/index.html`.

Shostack, A. (2008). Experiences threat modeling at microsoft. *MODSEC@ MoDELS, 2008*.

Smoker, A., Lundberg, J., Polishchuk, V., & Woltjier, R. (n.d.). Transportstyrelsen risk assessment for bvlos category 5c uav operations.

Storm, D. (2015). *Drones infected with malware can drop from the sky or be hijacked for surveillance.* https://www.computerworld.com/article/2876912/drones-infected-with-malware-can-drop-from-the-sky-or-be-hijacked-for-surveillance.html. Retrieved from https://www.computerworld.com/article/2876912/drones-infected-with-malware-can-drop-from-the-sky-or-be-hijacked-for-surveillance.html (Accessed: 2020-05-22)

Trujano, F., Chan, B., Beams, G., & Rivera, R. (2016). Security analysis of dji phantom 3 standard. *Massachusetts Institute of Technology*.

Valente, J., & Cardenas, A. A. (2017). Understanding security threats in consumer drones through the lens of the discovery quadcopter family. In *Proceedings of the 2017 workshop on internet of things security and privacy* (pp. 31–36).

Van Oorschot, P. C., & Smith, S. W. (2019). The internet of things: Security challenges. *IEEE Security & Privacy*, *17*(5), 7–9.

Vasconcelos, G., Carrijo, G., Miani, R., Souza, J., & Guizilini, V. (2016). The impact of dos attacks on the ar. drone 2.0. In *2016 xiii latin american robotics symposium and iv brazilian robotics symposium (lars/sbr)* (pp. 127–132).

Watson, S., & Dehghantanha, A. (2016). Digital forensics: the missing piece of the internet of things promise. *Computer Fraud & Security*, *2016*(6), 5–8.