OVERVIEW OF SECURITY OF UNCREWED AIRCRAFT SYSTEMS (UAS)

A SURVEY OF EXISTING WORK

Michaela Vanderveen, Ph.D., Principal 5G Security Architect, MITRE

Contents

SUMMARY

This document is a high-level survey of cybersecurity for Uncrewed Aircraft Systems (UAS). It examines security evaluations and threat taxonomies for the UAS, as gathered from published guidelines, best practices, research literature, and existing surveys. The aim of this document is to clarify the UAS threat space in order to inform the selection of security measures for the design and deployments of UAS.

The scope of this paper is cybersecurity aspects, including physical security, and privacy issues for Uncrewed Aircraft (UAs) and their associated components—including communication links and traffic management.

Introduction: UAS Basics

An Uncrewed Aircraft System includes an Uncrewed Aircraft, a UA Controller—also referred to as a "Ground Control Station" (GCS)—and (traditionally) communication links between the UA and the GCS.

A UA is a flying device of moderate complexity. Also known as a drone, the UA encompasses sensors, hardware, and software/firmware (e.g., Flight Controller), as well as a communication module. The UA's onboard sensors (e.g., accelerometer, Global Positioning System (GPS) receiver, and camera) feed data into a Flight Controller. The Flight Controller uses these measurements to guide the drone's propulsion system. The Flight Controller also sends telemetry data to the operator's (either human or drone pilot) ground-based GCS through a communication channel. The operator—also via the GCS—can then send operational commands back to the UA Flight Controller. The data transferred between the UA and the GCS can be of two types:

- **Command and control (C2)** refers to communications related to the operation of the drone and includes data on both ways, i.e., GCS-UA commands (e.g., to send commands to the drone) and UA-GCS control and telemetry (e.g., transmission of sensor data, surveillance data, video supporting remote piloting, etc.).
- **Mission payload** refers to data exchanged between the UA and GCS that is not related to drone operation, but rather to the drone's mission. For instance, for an infrastructure-inspection mission, the video stream collecting images in the field is part of "mission payload."

Other types of communications include messages for identification sent from a UA to another UA, or from UA to network via regular cellular connectivity.

The communication channel uses a wireless technology such as Wi-Fi, Bluetooth, or cellular. Since mission payload data, C2 signals, and identification data are transmitted via wireless, the security of these wireless channels is a key aspect of the UAS's overall security.

Another part of the UA ecosystem is the UAS Traffic Management (UTM). The UTM is an industry-led capability that comprises a set of functions and services for managing a range of autonomous vehicle operations. The UTM concept was born out of the need to manage airborne traffic given the evolving flight modes from line of sight to beyond visual line of sight, across multiple environments and airspaces.

A noteworthy UAS feature has to do with identification. In the United States, the Federal Aviation Administration (FAA) regulates civil aircraft operations. The FAA has a issued the final rule (14 CFR part 89) for remote identification to "address safety, national security, and law enforcement concerns". While the FAA has determined that a broadcast-based remote identification will be adequate for the purposes of part 89, they also acknowledge the UAS industry's need for "developing the network-based UTM ecosystem". Network-based sharing of aircraft identification and state on secure cellular networks will be an important capability to allow for future high-traffic volume Beyond Visual Line-of-Sight (BVLOS) flight operations.

The FAA provides air traffic management to traditional airspace users, such as crewed aircraft. As the FAA provides traditional air traffic control support directly to large scale UAS operations, the FAA will support UAS operations conducted in low altitude airspace using UTM, leveraging the industry-led capabilities, under FAA's regulatory authority.

The FAA UTM Pilot Program Final Report (2021) [1] describes the UTM as:

[…] a community-based, cooperative traffic management system in which the [UAS] operators and entities providing operation support services (i.e., UAS Service Suppliers [USSs]) are responsible for the coordination, execution, and management of operations, with rules established by the FAA [1].

The UTM concept includes a wide range of services for UAS operators. A provider of UTM services is called a "UAS Service Supplier" (USS). The USS is an organization that provides services to support the safe and efficient use of airspace, with services to the operator of a UAS to assist in meeting UTM operational requirements. For instance, a USS gathers weather and air traffic information from various sources and then analyzes and provides service to UAS operators to help ensure the safety of flight.

Security of Drones—Brief Introduction and History of Research

The American National Standards Institute/ Consumer Technology Association cybersecurity standard ANSI/CTA-2088 [2] defines security as:

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide—

(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;

(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, which means ensuring timely and reliable access to and use of information.

The earliest research on UA systems started around 2009 and focused on mobility models. The UAS security issues only started drawing attention from the research community around 2013. Between 2013–2016, several academic attacks with drones were published, whereby the drones were used for spying activities (e.g., intercept Wi Fi data).

A fair amount of research into drone security was conducted from 2016 to 2020. Research papers tended to view the drones as connected Internet of Things (IoT) devices, with some referring to the UAS as an "Internet of Drones" (IoD) and a "Flying ad hoc network" (FANET). Others viewed the UAS as another type of cyber-physical system. With this type of system in mind, security challenges of ad hoc networks were re evaluated, for example, secure (e.g., encrypted) communications between a group of drones.

Starting around 2019–2020, communication link security and information technology (IT) system security started to become the focus of drone cybersecurity research. The envisioned use cases were no longer small groups of drones needing covert communication, but rather the entire community of flying drones securely sharing clear-text identification and intended trajectory data with neighboring drones. In addition, given the increased complexity of the software running on the Flight Controller and cameras, security threats inherited from the IT world (e.g., malware) were drawing attention—along with their already known mitigations, such as Intrusion Detection Systems (IDS).

The Introduction of 5G

5G-based cellular technology can support the communication links between UA and GCS, as well as between UA and UTM via the 5G network (see **Figure 1**). Cellular enhancements for UA were designed in 5G, starting with Third Generation Partnership Project (3GPP) Release 17 [3]. As 5G cellular standards matured, the UAs' communications via cellular networks began to gain the attention of UAS-related research and experiments.

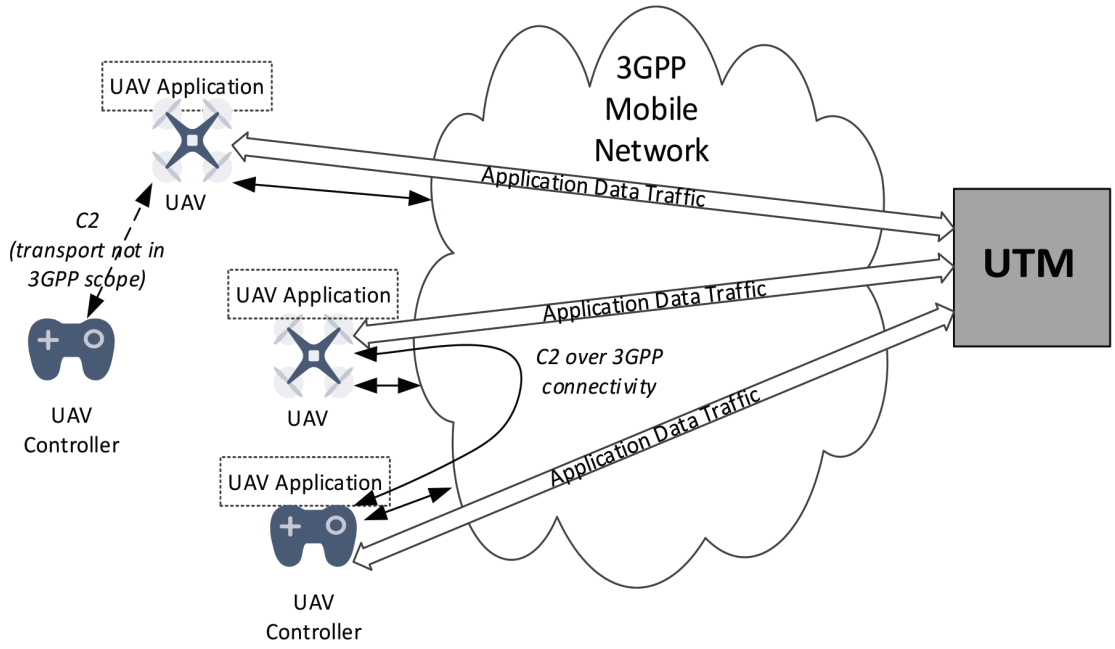

FIGURE 1. 3GPP DEFINED CELLULAR LINK SUPPORTING UA COMMUNICATIONS [3]

From the perspective of security, 5G has been recognized as having the benefit of stronger security compared to 4G/LTE (Long Term Evolution). Additionally, the FCC's Technological Advisory Council (TAC) examined [i] the communications options for UAV, concluding for the superior robustness of cellular compared to Wi-Fi or Bluetooth. As such, 5G technology is considered suitable for the C2 communication link and to carry mission payload traffic.

[i] FCC TAC document https://transition.fcc.gov/oet/tac/tacdocs/meeting12419/TAC-Presentations-12-4-19.pdf.

Notably, 5G- and even 4G-related security challenges for the UAS have not received much research attention so far. That said, there are security-related benefits for communication via 5G in general that are applicable to the UAS-generated traffic, as shown in **Table 1**.

5G Security Aspect	UAS Component Benefiting
Subscriber identifier privacy (Subscription Concealed Identifier (SUCI))	UA and GCS cellular identifier protection
Updated key establishment procedures (Authentication and Key Agreement (AKA))	Strong authentication of UA and GCS to the network
Data integrity and confidentiality protection over the air interface	Security of the traffic exchanged between the UA and the radio and core network, and the GCS and the radio and core network
Increased home network control	Security of roaming UAs
Detection of false base stations	Security of the UA attaching to the network
Secondary and additional authentication to third-party providers	Authentication/authorization of UA to the UTM
Use of millimeter wave radio	UA communication jamming resistance (closer proximity is required)

TABLE 1

It is well-recognized that 5G since Release 15 has had its security challenges [4]. These threats are well-understood, and their mitigations—which are not covered by subsequent releases—have been proposed by the industry, by operator forums such as the Global System Mobile Association (GSMA), and by various researchers.

In addition, there is a set of 5G-related threats that are not expected to affect the UAS significantly. For example, fraud (accessing services without paying for them)—which makes up the bulk of the negative financial impact on mobile operators from 2G, 3G, and 4G—is not a major concern for the UAS communications or the UA accessing the 3GPP data services. Similarly, Short Message Service (SMS) security threats (e.g., spoofing of second-factor authentication/one-time passwords) for financial fraud are also not applicable to the UA (assuming SMS is not used to transmit C2 or mission payload data).

The 5G-related security challenges most applicable to UAS are location tracking, Denial of Service (DOS) attacks via the network, radio jamming, call/data interception, and routing attacks. An investigation on the references that propose mitigations to these threats is out of scope for this document version.

Threat Models for UAS

Threat modeling, which is a formal process to identify threats and analyze vulnerabilities of a system's assets, uses communications and information processing as well as associated risk levels to each threat. The purpose of threat modeling is to inform system design and deployment, and guide mitigation measures. A system is considered secure or not, depending on how well it meets the security objectives of Confidentiality, Integrity and Availability, also known as the "CIA triad."

Threat models or frameworks can be constructed from the point of view of the attacker or of the defender.

Some commonly used threat modeling approaches are the Microsoft STRIDE method and the Lockheed Martin Cyber Kill Chain® (see **Figure 2**). Both are considered "high-level of detail" threat modeling approaches, with the former having the defender perspective and the latter having the adversary perspective. Mid-level abstraction threat taxonomies include MITRE ATT&CK® and MITRE FiGHT,™ as well as the National Institute of Standards and Technology (NIST)/National Cybersecurity Center of Excellence (NCCoE) Mobile Threat Catalogue, which are all constructed with an adversarial perspective. Finally, detailed threat modeling approaches include the MITRE Common Vulnerabilities and Exposures (CVE®), the NIST National Vulnerability Database (NVD), the MITRE Common Weakness Enumeration (CWE™), and the Common Attack Pattern Enumerations and Classifications (CAPEC™).

The attack tree method is another threat modeling tool that has been used for many years and is suited for cyber-physical systems. In this method, an adversary's goal is depicted as the root of a tree of various paths, with steps towards achieving the goal. Attack trees can then feed into the threat modeling frameworks mentioned above.

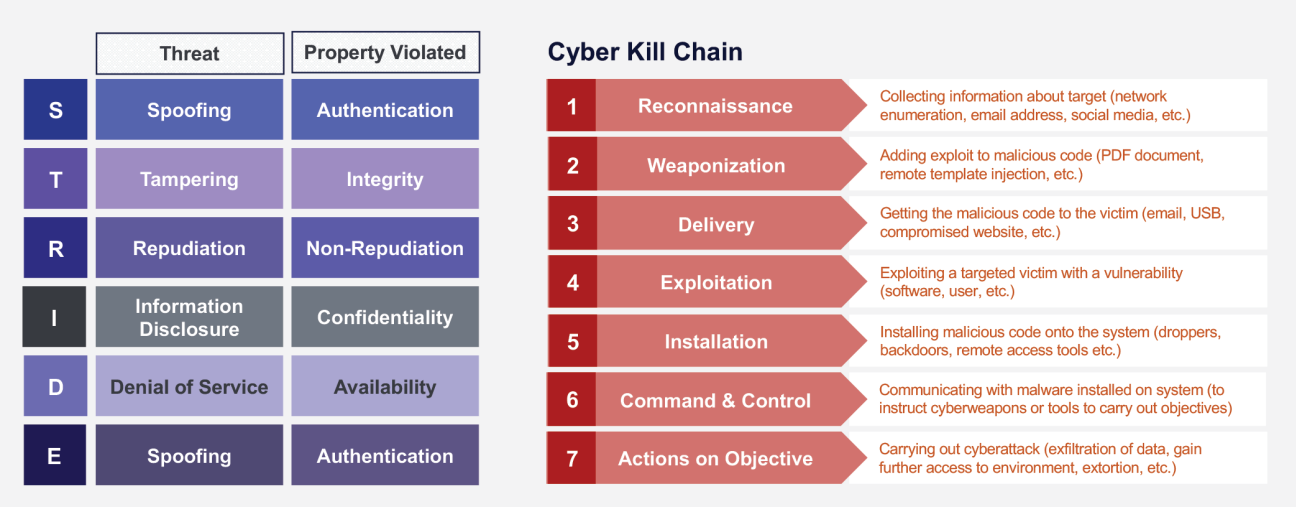

FIGURE 2: STRIDE AND CYBER KILL CHAIN THREAT MODELS

Terms and Definitions

Formal definitions for security-related terms can be found in the NIST Computer Security Resource Center (CSRC) resource https://csrc.nist.gov/glossary [5]; for example, for "threat," see: https://csrc.nist.gov/glossary/term/threat [6]. Informal definitions (based on [7]) are given below:

- **Asset:** anything that has value to the organization, its business operations, and its continuity.
- **Authentication:** ensuring that the identity of a subject or resource is the one claimed.
- **Availability:** property of being accessible and usable on demand by an authorized entity.
- **Confidentiality:** ensuring that information is accessible only to those authorized to have access.
- **Impact:** result of an information security incident, caused by a threat, which affects assets.
- **Integrity:** safeguarding the accuracy and completeness of information and processing methods.
- **Mitigation:** limitation of the negative consequences of a particular event.
- **Non-repudiation:** ability to prove an action or event has taken place, so that this event or action cannot be repudiated later.
- **Risk:** potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.
- **Threat:** potential cause of an incident that may result in harm to a system or organization. A threat consists of an asset, a threat agent, and an adverse action of that threat agent on that asset.
- **Threat agent:** entity that can adversely act on an asset.
- **Vulnerability:** weakness of an asset or group of assets that can be exploited by one or more threats.

Survey of Existing Guidelines, Recommendations, and Policies

This section contains a summary of existing guidelines for UAS security as output by various national and international bodies (standards, regulatory, or industry).

International Civil Aviation Organization (ICAO) developed an interoperable International Aviation Trust Framework (IATF) [8], which is a set of policies, requirements, and best practices to enable trusted, resilient, and secured ground-ground, air-ground, and air-air exchange of digital information. ICAO established the Trust Framework Study Group (TFSG) in 2019 to develop the work through three working groups: operations, digital identity, and network. These groups are reviewing the concept of operations, defining use cases, developing a digital certificate policy, and identifying the security and access control requirements for a Global Resilient Aviation Interoperable Network (GRAIN). The concept of operations for GRAIN contains a cybersecurity and network policy.

American National Standards Institute (ANSI)/ Consumer Technology Association (CTA) published the ANSI/CTA-2088 (2020) [2], which sets forth some very basic cybersecurity guidelines for consumer devices such as IoT. The standard calls for device identifiers security, secured access, protection of data in transit and data at rest, use of industry standard protocols for communication and cryptography, data validation and event logging, ability to patch vulnerabilities, and reprovisioning capabilities. ANSI/CTA also released a version for drones, namely ANSI/CTA-2088.1 [9] (2022), to "address the cybersecurity requirements and recommendations relevant to the unique capabilities, uses, and applications of small UAS."

Cybersecurity and Infrastructure Security Agency (CISA), as a U.S. federal agency under the Department of Homeland Security (DHS), published "Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems" (2019) [10]. This brief paper covers secure use of UAS software/firmware, secure UAS operations, security of data storage and transfer, and use of information/ vulnerability sharing.

Civil Air Navigation Services Organization (CANSO), a European Air Traffic Management system industry consortium, published the "Standard of Excellence in Cybersecurity" (2020) [11]. This document contains high-level UAS security recommendations, such as asset management, information sharing, risk assessments, supply chain risk management, protective technology, response planning, and others.

FAA issued a final report on the UTM Pilot Program Phase 2 [12]. This document contains a section on message security (Section 4.5), whereby they recommend securing the UTM node to the Flight Information Management System link via OAuth 2.0 for authorization and TLS for link security. Their main recommendation is rather broad (e.g., use of digital signatures).

Survey of Existing Published Research and Findings

This section contains a survey of the survey-style publications that address more than one aspect of UAS cybersecurity. The papers are listed in order of publication, and a brief summary of each is given. The purpose of this exercise is to observe how thinking about security for drones has evolved along with the UA technology itself, and to highlight findings to identify what threats seem to be more prominent—and by extension—should be prime candidates for which to prioritize mitigation efforts within a given deployed system.

Special attention is given to a recent survey by The RAND Corporation, "How to Analyze the Cyber Threat from Drones," as it is closely related to the scope of this paper and is a recent, comprehensive, and government-funded effort to show both history and future trends.

The RAND Corporation Survey

Reference [13] is a comprehensive analysis of drone security, funded by the Department of Homeland Security (DHS) and performed in 2020. It explores the security implications of the rapid growth in UAS technology, looking at both current and future trends. The RAND report outlines a conceptual approach to enable the identification and categorization of UAS cyber threats, both for drones compromised for malicious purposes ("UAS as cyber-targets") and for drones used specifically as attack vectors ("UAS as cyber weapons"). It uses the two well-known and high-level threat modeling approaches to categorize threats found in the literature (up to 2020): STRIDE and Cyber Kill Chain.

In this survey, the authors examine published works that describe historical, proof of concept, or hypothesized attacks and categorize them based on attack type, UAS role (target of attack or cyber weapon), and access points. Most of the attacks found are where UAS is a target, and fall under DOS attacks, and spoofing for hijacking of UAS; the most common access points used are communication links based on Wi-Fi or cellular networks.

A few examples of demonstrated attacks are categorized according to STRIDE and Cyber Kill Chain: GPS spoofing to take control of a victim drone, use of a drone to anonymously capture vulnerable devices in a city to form a botnet, and use of a drone to get close enough to inject malware into Zigbee light bulbs in a large building.

As for future trends (at the time the paper was written in 2020), the authors note that the pace of technology advancements (e.g., from UAS patents filed) has increased, and so cybersecurity professionals are "left playing catch-up." The trends they saw at that time were: increased flight automation, UTM development, "swarming," increased hardware and supply chain complexity, use of machine learning (ML) and artificial intelligence (AI) to detect cyber intrusions, and the use of blockchain to log flight data for security. The authors point out how some advancements have both benefits and risks—for example, increased automation supports more advanced use cases but exposes bystanders to several risks. Automated tools can be employed to detect aberrant system behavior.

The summary of UAS key features and trends is shown in **Table 2** on the next page.

Trend	Key UAS Feature	STRIDE Taxonomy Threat	Vulnerabilities and Attack Vectors
Simplified Control and Operation	Camera view-based flight; following target on camera	Repudiation and Information Disclosure	Third-party monitoring of user activities
	Gesture and speech-directed flight control	Elevation of Privilege and Tampering	Alteration of factory- installed configurations
Self-Operation and Vigilance	Location or sensor-based payload manipulation (e.g., crop spraying, medical supply delivery)	Elevation of Privilege	Intercept of payload usage or delivery
	Swarm drone maneuvers; multi-UAS operations	Elevation of Privilege and Tampering	Scaled-propagation of operational errors
	Preplanned hovering; patrol routines	Spoofing or Tampering	Override of authentic GPS signal or uploaded navigation files
Self-Maintenance and Protection	High-speed obstacle avoidance	Spoofing and Denial of Service	Sensor saturation or interference for obstruction of "view"
	Auto-docking; recharge; return to home	Repudiation and Information Disclosure or Spoofing and denial of service	Third-party monitoring of user activities and sensor interference for failure to register "home" state

TABLE 2. SUMMARY OF UAS KEY FEATURES AND TRENDS [13]

Survey Papers with Threat Taxonomies or Models

This section lists and briefly summarizes selected surveys, threat taxonomies, and security and privacy evaluations of UAs in chronological order of publication, to show the evolution of the cybersecurity efforts in the research community.

2013–2017

[14] describes the first approach to a UA-specific risk assessment, addressing susceptibility to attacks on the integrity, confidentiality, and availability of each UAS component, including communication links. The authors then apply this scheme to two drone products.

[15] classifies threats into several (mid-level of abstraction) categories and proposes general guidance for attack response––to the effect that the UAS should be constructed with defensive capabilities allowing for automated response to deliberate attacks or accidental malfunction events.

[16] surveys the main security, privacy, and safety aspects associated with the use of civilian drones in the national airspace. The paper looks at both physical and cyber and outlines deployment challenges in terms of scalability and safety of people and property. The paper describes a set of threats that can be combined to take over a drone and crash it, making the point that the functional safety of civilian drones requires cyber physical security. The paper also outlines security requirements (mitigations) and privacy considerations.

[17] presents a modified taxonomy to organize cyber-attacks on UAs by attack vector and target. The survey points out the gap in research on attacks on the data communication, showing that UA-related research to counter cybersecurity threats had focused so far on GPS jamming and spoofing.

2018

[18] describes a "security framework" for detecting and mitigating cyber-attacks on airborne networks. The framework is based on intrusion monitoring and modeling to monitor the behavior of devices. The intrusion detection and prevention systems are used to prevent and detect malicious activities.

[19] organizes sixteen relevant published research articles based on the "attack vector" and the "proposed countermeasure" that each article considers and introduces. One point that the authors bring up is the potential for "adversarial attacks on the employed machine learning techniques." It makes sense that if a particular ML or AI technique or tool is widely used to detect intrusions, then attackers may develop strategies for deceiving the technique or tool itself.

[20] proposes a taxonomy to classify attacks based on the threats and vulnerabilities associated with the connectivity of the drone to existing cellular networks. The authors extend the CIA triad to include privacy and trust, listing attacks in each category.

[21] is a brief article studying the IoD architecture and its security and privacy requirements. It outlines potential solutions for identity/location privacy protection, and for security, accessibility, and privacy of data moved from the drone to the cloud to be stored and accessed.

2019

[22] describes new societal threats to security and privacy created by drones, and current academic and industrial methods used to detect and disable drones.

2020

[13], the RAND paper, is discussed separately above.

[23] is a very comprehensive survey (over 400 references examined) that analyzes drones' vulnerabilities pertaining to communication links (cellular, satellite, Wi-Fi), as well as to smart devices and hardware (that control them). It presents a detailed review on UA usage in multiple domains (i.e., civilian, military, terrorism, etc.) and for different purposes. It also contains a list of UAS regulations in various countries. Most importantly, this survey shows a table with twenty-one drones/counter-drones cyber-attacks along with their mitigating cryptographic and non-cryptographic security measures. These threats are categorized in a taxonomy with attack types, targets, and countermeasures.

[24] analyzes a few potential threats in the UA system, pertaining to sensors (for spoofing), Wi-Fi communications, multi-UA networking security, and privacy disclosure caused by aerial photos.

2021

[25] focuses on the UAS threats that arise from cellular connectivity. It provides insights into the 3GPP standardization efforts with respect to authentication and authorization, location information privacy, and C2 signaling to identify remaining research and standardization opportunities.

[26] contains possibly the most comprehensive recent literature review and UA security and privacy research (over 180 works cited). The threats are classified in four categories ("levels"): sensor, software, hardware, and communications. For communications, the authors examine all used technologies: Wi-Fi, Bluetooth, ZigBee, LoRa, Sigfox, Narrow Band IoT (NB-IoT), WiMAX, and cellular (4G, 5G).

[27] assesses the recent trends in security and privacy issues that affect the IoD network. It also addresses a purported neglected area of research, namely secured IoD architecture, including cloud-based systems. The authors propose a comprehensive taxonomy on the drones by type and a taxonomy of the attacks on IoD, along with mitigations and performance evaluation methods.

2022

[28] is a very detailed survey of security and privacy threats for drones in FANETs and IoD. The paper proposes to categorize threats based on type of communications between the drones, GCS, and personal pilot devices. The impact on the tenets of security (Confidentiality (C), Integrity (I), Availability (A), and Privacy (P)) is assessed. Defense mechanisms are reviewed, along with limitations of current UAS standards.

The Assets, Threats, and Mitigations for UAS

This section outlines the assets, threats, and mitigations related to UAS—the key elements of threat modeling—as gathered from the literature search in the section above.

Assets

Assets pertaining to the UAS can be categorized as follows:

- **Physical assets:** receivers, optical sensors, controllers.
- **Software assets:** flight control software/firmware, navigation apps.
- **Communication assets:** all communications links.
- **System assets:** UAS C2 link, remote identification data, UAS payload data, cloud-stored UAS data, configuration of the system.
- **Privacy-related assets:** GCS operator identity, GCS location, UA location.

Threats

The threats and vulnerabilities pertaining to UAS, as evident from the body of literature in the section above, are listed below. There are several ways to categorize them in the literature, as detailed in the section above, and each method has its own merit depending on the perspective taken. Therefore, we simply list them here and give three example pictures of their categorization from the literature.

We note that UTM-related threats have not been thoroughly examined in the literature yet, to our knowledge. The well-known communication link security threats apply to the UAS-to-UTM communication. In addition, there is the issue of intended UTM/USS, i.e., that UAS should be assured to communicate only with the correct UTM/USS.

- GPS signal spoofing.
- Sensor output spoofing.
- Spoofing of data transmitted to/from drones.
- Jamming of radio communications.
- Interception of data transmitted to/from drones.
- Denial or degradation of service (capability disruption) for drone operation, including de-authentication.
- Remote ID spoofing.
- Unauthorized flying—at wrong time/wrong place.
- Onboard sensor control application hijack.
- Unauthorized Flight Controller software modification (e.g., to allow entry into airspace where/when flights are not allowed).
- Malware.
- Location tracking.
- False location reports.
- Traffic analysis.
- Supply chain threats.

A few examples (**Figures 3,4,5**) of threat classifications are given on the following pages from the sources examined.

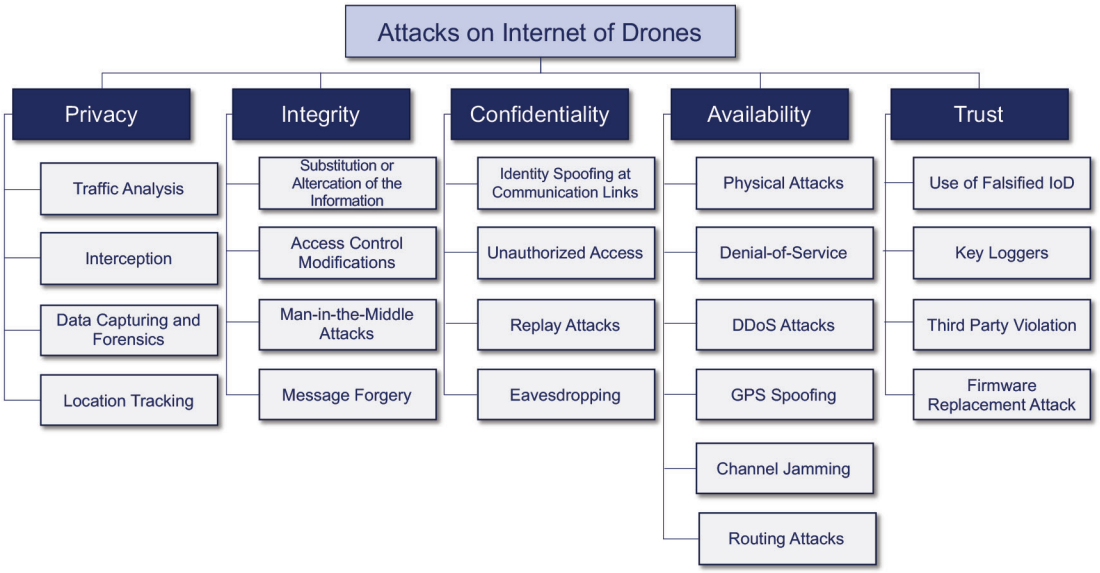

FIGURE 3. EXAMPLE IN [20]

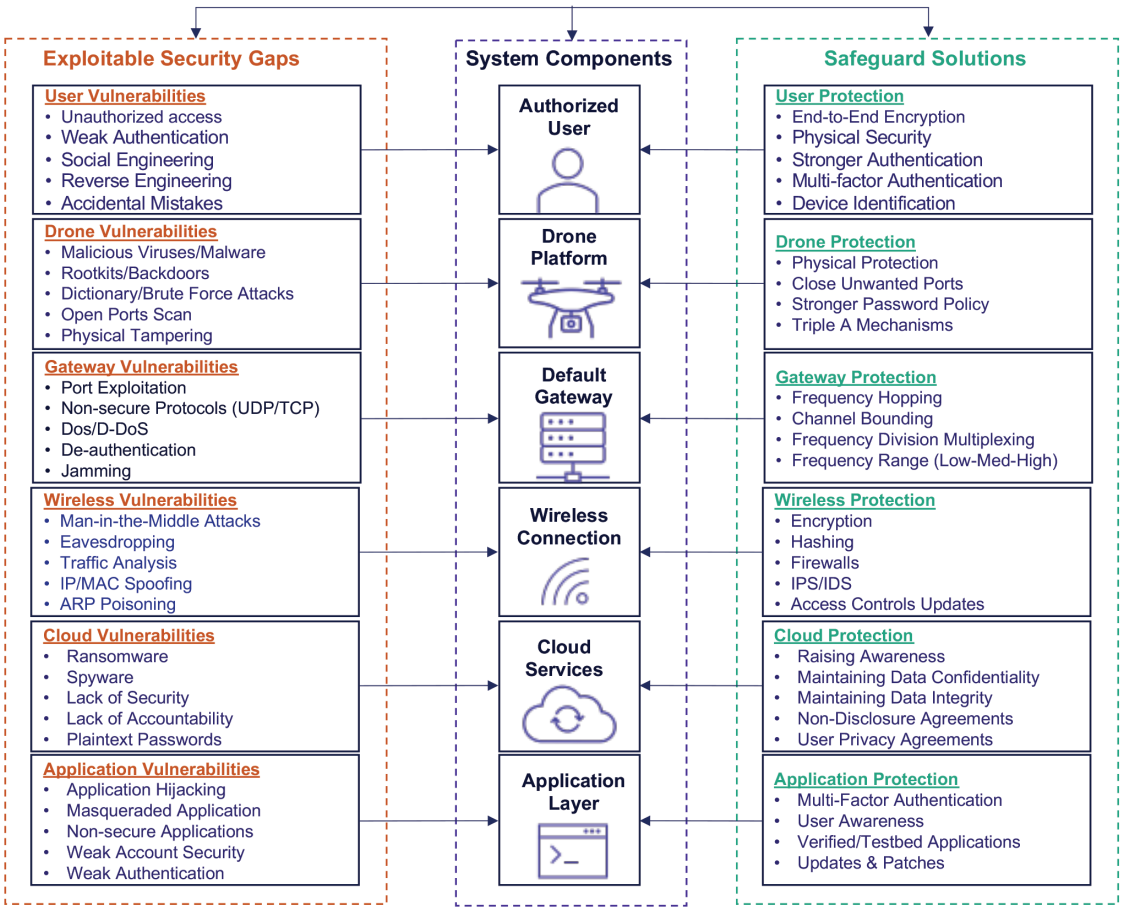

FIGURE 4. EXAMPLE IN [23]

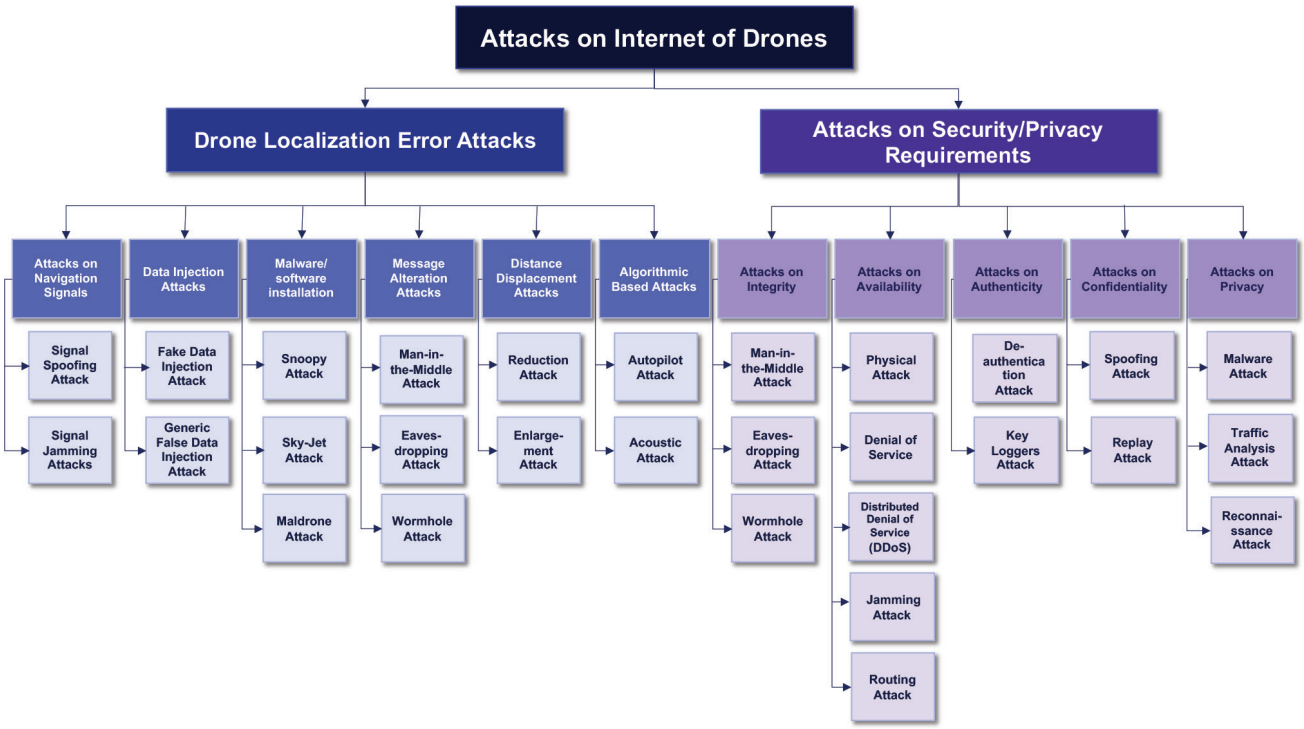

FIGURE 5. EXAMPLE IN [27]

Risk

In order to assess risk, the likelihood of a given threat (i.e., probability of that vulnerability being exploited) has to be multiplied by the impact (i.e., the severity of the consequence). This document version does not include a risk analysis.

Mitigations

Regarding mitigations, we start with the existing recommendations from various standardization and policy bodies, both U.S. and international, as well as those proposed in some of the survey papers examined. Typically, mitigations are listed along with their threats, but this also involves a categorization exercise, which we do not attempt here.

A list of mitigations proposed in the literature can be summarized as follows:

- Confidentiality and integrity protection of all communication links.
- Securing data at rest (including stored data on the drone or in the cloud), data in transit.
- Intrusion Detection Systems (IDS).
- Software supply chain security.
- Software testing and patching security.
- Software and hardware assurance (being able to testify to the integrity of running software and the hardware it is running on).
- Logging of all received C2, payload metadata, and access attempts.
- Authorizing all parties with access to any part of the system, per local policy.
- Non-repudiation for commands issued by the drone operator.
- Tracking of drones to detect unauthorized flying (in space/time).

Conclusions and Future Work

This paper gives an overview of published works on the security of UAS. Although historically in many systems, security lags behind design improvements (for example, as has been the case for the IoT), in the case of drones, many researchers and even regulatory/standards bodies have recognized the importance of security (physical and cyber) fairly early on. The UAS is a complex cyber-physical system, and this complexity increases the attack surfaces and the security challenges associated with protecting from these attacks. We highlight that the focus of security challenges has shifted over the years from routing security and covert communications to communication link security and software security. Signal jamming (e.g., GPS) remains a constant threat.

This paper does not provide a formal threat analysis of the UAS, although we recommend a threat analysis to inform system design and deployments in a system—simple or complex. Others have attempted this in recent years, and those results have been cited herein. Even so, we note that threat analysis and incorporation of security controls within a system is a continuous lifecycle evolution and not a one-time process. The set of known threats should be updated as they arise, and the affected system components (e.g., node, interface) should be updated as required. In this process, the cost of mitigation is often a factor, and sometimes a conscious decision may be made to accept the newly identified risk, given a cost-benefit analysis result.

It is worth noting that new technologies may be incorporated in UAS as an evolution: AI/ML, blockchain, Fog/Edge computing, zero-trust architectures, and Software-Defined Networking (SDN).

A future version of this document could contain a threat model for the UAS ecosystem. The threat modeling for the UAS could be at the high-level or mid-level of abstraction, or even detailed, and could leverage existing UAS threat models published to date. Enumerating possible future attacks requires a thorough investigation of the threat space.

An example of such a threat modeling effort would be an update to the STRIDE method as well as the cybersecurity Kill Chain used in [13] given any new vulnerabilities that have come to light since its publication in 2020. A more heavyweight approach would be based on the well-known Common Criteria (ISO 15408) and encompass a thorough threat, vulnerability, and risk assessment of the UAS. On the practical side, a report on penetration testing or "pen-test" would provide additional analysis of the cyber posture of a real-life deployed UAS.

References

1. Federal Aviation Administration (FAA), *FAA UTM Pilot Program Final Report*, 2021.
2. ANSI/CTA, ANSI/CTA-2088, *Baseline Cybersecurity Standard for Devices and Device Systems, Consumer Electronics Association*, 2020.
3. Third Generation Partnership Project (3GPP), "Uncrewed Aerial System (UAS) support in 3GPP; Stage 1, 3GPP TS22.125, V17.6.0".
4. ENISA, "ENISA Threat Landscape for 5G Networks Report," ENISA, [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/. [Accessed 13 April 2021].
5. National Institute of Standards and Technology (NIST), "Glossary," NIST, 20 September 2022. [Online].
6. National Institute of Standards and Technology (NIST), "Glossary: Threat," NIST, 20 September 2022. [Online].
7. European Telecommunications Standards Institute (ETSI), TS 102 165-1, CYBER; Methods and protocols; Part 1: *Method and pro forma for Threat, Vulnerability, Risk Analysis* (TVRA).
8. International Civil Aviation Organization, 2022. [Online]. Available: https://www.icao.int/airnavigation/Pages/IATF.aspx.
9. ANSI/CTA, ANSI/CTA-2088.1, *Baseline Cybersecurity for Small Unmanned Aerial Systems, Consumer Technology Association*, 2022.
10. Cybersecurity & Infrastructure Security Agency (CISA), *Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems (UASs)*, CISA, 2019.
11. Civil Air Navigation Services Organization (CANSO), *Standard of Excellence in Cybersecurity*, 2020.
12. Federal Aviation Administration, "UTM Pilot Program Phase 2 Final Report," 29 July 2021. [Online]. Available: https://www.faa.gov/sites/faa.gov/files/uas/research_development/traffic_management/utm_pilot_program/FY20_UPP2_Final_Report.pdf.
13. K. L. Best, J. Schmid, S. Tierney, J. Awan, N. M. Beyene, M. Holliday, R. Khan and K. Lee, "How to Analyze the Cyber Threat from Drones," RAND Corporation, 25 April 2020. [Online].
14. K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber-attacks - An approach to the risk assessment," in *2013 5th International Conference on Cyber Confilct (CyCon)*, 2013.
15. Z. A. Aktaş, C. Gemci and E. Yağdereli, "A study on cyber-security of autonomous and unmanned vehicles," *Journal of Defense Modeling and Simulation*, vol. 12, no. 4, October 2015.
16. R. Altawy and A. M. Youseff, "Security, privacy, and safety aspects of civilian drones: A survey," ACM *Transactions on Cyber-Physical Systems*, vol. 1, no. 2, pp. 1-25, 2017.
17. C. G. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in *2017 15th IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR) Conference*, 2017.
18. H. Sedjelmaci and S. M. Senouci, "Cyber security methods for aerial vehicle networks: Taxonomy, challenges and solution," *Journal of Supercomputing*, vol. 74, no. 10, pp. 4928-4944, Oct. 2018.
19. Shakhatreh, H. et al., "Unmanned Aerial Vehicles: A Survey on Civil Applications and Key Research Challenges," 2018. [Online]. Available: https://arxiv.org/abs/1805.00881.
20. G. Choudhary, V. Sharma, T. Gupta, J. Kim and I. You, "Internet of Drones (IoD): threats, vulnerability, and security perspectives," in *3rd International Symposium on Mobile Internet Security*, 2018.
21. C. Lin, D. He, N. Kumar, K. K. R. Choo, A. Vinel and X. Huang, "Security and privacy for Internet of Drones: Challenges and solutions," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 64-69, 2018.
22. B. Nassi, A. Shabtai, R. Masuoka and Y. Elovici, SoK - Security and privacy in the age of drones: Threats, challenges, solution mechanisms, and scientific gaps, 2019, pp. 1-17.

23. J.-. P. Yaacoub, H. Noura, O. Salman and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things*, vol. 11, p. 100218, 2020.

24. Y. Zhi, Z. Fu, X. Sun and J. Yu, "Security and privacy issues of UAV: A survey," *Mobile Networks and Applications*, vol. 25, no. 1, pp. 95-101, 2020.

25. A. S. Abdalla and V. Marojevic, *Security Threats and Cellular Network Procedures for Unmanned Aircraft Systems*, 2021.

26. Y. Mekdad, A. Aris, L. Babun, A. E. L. Fergougui, M. Conti and R. Lazzeretti, "A Survey on Security and Privacy Issues of UAVs," 2021. [Online]. Available: https://arxiv.org/abs/2109.14442.

27. M. Yahuza, M. Y. I. Idris, I. B. Ahmedy, A. W. A. Wahab, T. Nandy, N. M. Noor and A. Bala, "Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges," *IEEE Access*, vol. 9, pp. 57243-57270, 2021.

28. K.-. Y. Tsao, T. Girdler and V. G. Vassilakis, "A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks," *Ad Hoc Networks*, vol. 133, no. C, August 2022.

As MITRE's tech foundation for public good, MITRE Engenuity collaborates with the private sector on challenges that demand public interest solutions, to include cybersecurity, infrastructure resilience, healthcare effectiveness, microelectronics, quantum sensing, and next-generation communications.

MITRE ENGENUITY™

mitre-engenuity.org