Assessing the Cyber Risk of Small Unmanned Aerial Vehicles

Dillon Pettit, Scott Graham

Chapter 1

CYBERSECURITY RISK ASSESSMENT FOR SMALL UNMANNED AERIAL VEHICLES

Dillon Pettit and Scott Graham

Abstract The ever growing market for Commercial-off-the-shelf Unmanned Aerial Vehicles has brought with it innate vulnerabilities and rising rewards. The aerial technology presents unique Information Technology risk characteristics that must be managed in new ways. A key stage of the risk management process is completing a risk assessment; the earlier in the life-cycle this is completed, the more security can be designed into the operational environment. In this work, a quantitative risk assessment is defined based on qualitative cybersecurity measures and requirements of an unmanned aerial vehicle and its corresponding ground controller to capture the dynamics of probability and severity. The assessment uses 14 sub-metrics covering device securities, time dynamics, and mission environment to encapsulate the risks imposed into a single score from 0 to 10. Through ten case studies using three currently popular models and three mission-environment scenarios, the assessment is shown to meet the objectives of ease-of-use, breadth, and readability. By allowing risk assessment at or before acquisition, organizations and individuals can accurately compare and choose the best aircraft for their mission.

Keywords: Cybersecurity Risk Quantifiable Assessment Unmanned Aerial Vehicles

1. Introduction

Applications of small Unmanned Aerial Vehicles (UAVs) have grown considerably in the current century. While the military sector may have had near exclusive use of the devices previously, the commercial sector has also recognized the benefits of the small and inexpensive unmanned aircraft to meet a multitude of needs. Infrastructure, defined as "The framework of interdependent networks and systems...that provide a reliable flow of products and services essential to the defense and economic

security of the United States...", whether critical or non-critical [2], increasingly employ small UAVs. Each of the sectors of critical infrastructure have been growing their use of small UAVs related to Geo-spatial and Surveying, Civil Surveillance, Traffic and Crowd Management, Natural Disaster Control and Monitoring, Agriculture and Environmental Management, Urban Security, Big Data Processing, and Coordination between heterogeneous systems [15]. Mapping and inspections of buildings, distribution, and inaccessible terrain monitoring [12] have utilized small UAVs for most of the critical infrastructures, but all sectors need to trust their tools due to their intrinsic importance to the nation. Small UAVs are designed as both an operational aircraft and functional computer, with combined vulnerabilities. Operational risks include collision with buildings and other aircraft as well as uncontrolled landings [1]. Cyber risk however arises from various methods through which an attacker may compromise any component of the system. Unlike in the operational risk arena, there is no lead agency or tool to manage the growing UAV cyber risk to critical infrastructure [17]. With the Federal Aviation Administration (FAA) and other regulatory bodies lagging with respect to mitigating cyber risk with small UAVs [13], organizations and customers have little guidance in determining the amount and type of risks accepted when purchasing new fleets. Acquisition teams are ill-equipped to analyze the complex cyber ramifications of components that may or may not be installed within UAVs and therefore require a tool to compare the risk between various brands and models to accomplish their organization's mission.

This paper introduces a cyber risk assessment tailored for small UAVs and analyzes the tool for the types of aircraft, missions, and environments common in the field. Section II provides background to the UAV field, including a brief history of UAV use, definition and scope for this tool, and related work in assessing risk of the aircraft. Section III explains the mechanisms of the proposed risk assessment tool. Section IV presents several case studies to clearly demonstrate the application of the tool across the spectrum of use. Section V provides analysis of the case studies and discussion into how well the tool met the defined objectives. Section VI concludes the paper with open issues and future work.

2. Background and Related Work

Historically built for military applications, UAVs use has expanded by hobbyist enthusiasm. By definition, UAV includes any device that can sustain flight autonomously, with similar sub-cultures of Remotely

Piloted Vehicles (RPVs) and drones [6]. UAVs are usually able to either maintain a hover or move completely via computer navigation, whereas RPVs require control instructions throughout flight and drones have even more limited mission and sophistication. The exact definitions between sizing tiers have not been standardized between countries, though practically they consist in some format of very small, small, medium, and large. Very small UAVs exist at a miniaturization of aerodynamics that result in very low Reynolds numbers and are usually less than 20 inches in any dimension. Small UAVs tend to be a range of popular model aircraft used by hobbyists and have at least one dimension greater than 20 inches. Medium and Large UAVs are too large for an individual to carry and may even use full runways like light aircraft, which allows for greater on-board securities and more regulations. Their internal architecture differs greatly by removing the human pilot directly from the vehicle and are controlled by varying degrees of autonomy of their autopilot [9].

Quantitative risk assessments are not unique to computers and have existed within the field of commerce since the start of civilization. The most generalized description of risk is well-known as the product of Cost and Likelihood. Cost is the loss or recovering price tag in the event of a failure. Likelihood is the probability of failure over time or the rate of failure in a specific time frame. The field of risk management with UAVs is a multi-dimensional issue with related research presented in the following paragraphs, moving from operational to acquisition.

Operational risk assessment for small UAVs has been delegated to the National Aeronautics and Space Administration (NASA) for development and testing, then to be fielded by the FAA within the National Airspace System (NAS) [14]. In response to commercial requests, NASA began development of the UAV Traffic Management (UTM) system in 2014 with the publication of a 15 year plan, with initial deployment planned for within five years [14]. Connection to this new UTM would involve approximately ten new communication protocols as standard on all UAVs, enabling receipt of flight plan constraints for individual UAV autopilots to avoid (navigate around) in real-time [14]. The UTM's risk modelling software is device agnostic, except for size and weight, which means that the system in no way quantifies cyber risk threat for these UAVs, though such efforts would cause "off-nominal trajectories" [1] which NASA and the FAA are attempting to reduce. While regulation of small UAV production to meet the communication requirements of the NAS may incidentally provide some level of cyber risk reduction, failure to design for cyber objectives will mean that any improved cyber risk posture will be undocumented and ineffective.

Today's most utilized quantitative vulnerability severity assessment tool is Cyber Vulnerability and Scoring System (CVSS) [18], maintained by Forum of Incident Response and Security Teams (FIRST) Inc. As an "open framework for communication of the characteristics and severity of software vulnerabilities" [8], CVSS provides data points to the National Vulnerabilities Database (NVD) and Common Vulnerabilities and Exploitations (CVE) databases, which are in turn utilized by risk frameworks to define vulnerability of networks. The most current version, 3.1, calculates a Final score from 0.0 to 10.0 through 15 sub-metrics seen in Figure 1. The Base metrics are split into three sub-categories, and the Environmental metrics split into two, based on commonalities and use within the algorithms, as will be shown in the next section. An Extensions Framework optionally allows for the manual adjustment of constants for specific fields (There is no published framework yet for UAVs). CVSS is specific to a vulnerability of a component and therefore does not fully define a system, its mission, or its environment, all of which are of critical value to UAVs [10]. CVSS does provide the most robust, utilized, and therefore practical scoring system for cyber devices on the market.

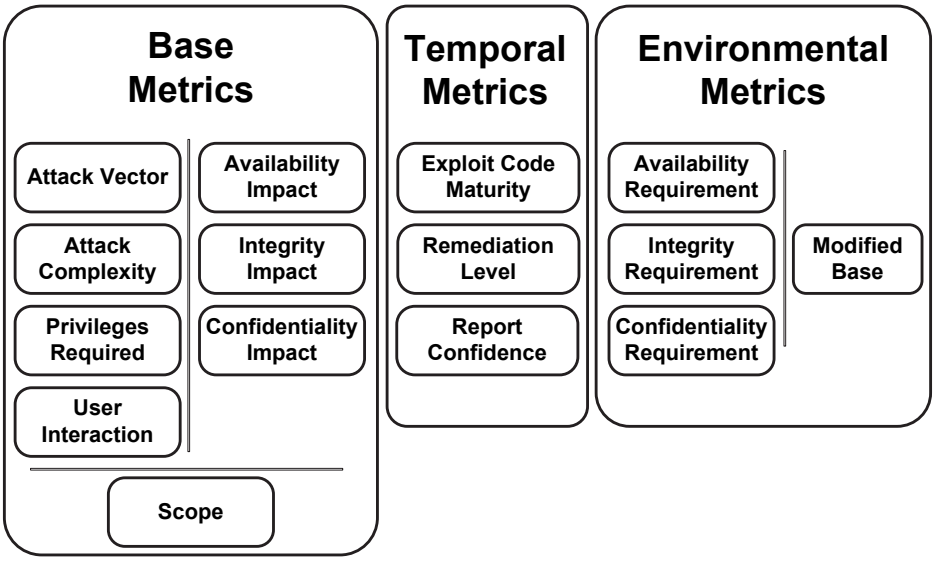

Figure 1. CVSS v3.1 Metrics [8]

Within the healthcare field, only 61% of organizations are currently using cyber risk management [4]. Since cyber flaws were only being

treated as device flaws that were corrected through long-term regulations by the Food and Drug Administration (FDA),, Stine proposed a medical device risk assessment that would allow for understanding of risk in hospitals, prioritization of devices requiring additional protection, and ease of calculation for the low cyber awareness of general healthcare practitioners [19]. Stine created a cyber risk scoring system through two steps: severity of worst case scenario and the amount of security features present. While Stine met the self-set goals of Ease of Use, Low Cost, and Understandable Results [19], the use of manually crafted constants to define the risk of an attribute's severity to the overall risk of the device requires significantly more application.

Within the UAV community, Hartmann and Steup's scoring system shows the current threshold for a quantifiable cyber risk score, though with significant shortcomings. The authors define the general internal network of UAVs with the most vulnerable components as communication links, sensors, data storage, and autopilot configurations [11]. By defining the hardware and software of each of these components through a survey of the market, corresponding attributes were defined with the autopilot being simplified to its fail-safe state and the sensors being increased to four configurations and 3 combinations. The attribute of Environment was also added in with the imperative that any risk assessment for UAVs must include the risk inherit to the operational environment and the mission set [11]. Lacking in categorization of risk and what values are acceptable, this simple calculation lacked detail describing what its risk value meant. Though stating that mission sets must be included, the authors did not create any attribute for calculation or factoring.

3. Risk Assessment Design

The basis of this proposed risk assessment is CVSS which provides common nomenclature for cyber risk managers currently administrating networks and strong quantification constants in their functions proven over time and extensive use. The model of Base metric modified by Temporal and Environment metrics provides a vehicle currently used today which may aid adoption rate. As described in Section 2, CVSS does not score risk, but severity of vulnerabilities, so significant changes are required to shift the focus to device risk and UAVs in specific. A simple extensions framework, as provisioned in CVSS Version 3.1, would not update the original scoring system to rate any metric outside of severity of vulnerabilities as the extensions framework merely tweaks constants within the equations. This new framework redefines all sub-

metrics to some extent, while maintaining as much of the CVSS structure as possible. Figure 2 shows the full structure of the assessment which will be described by sub-metric next.

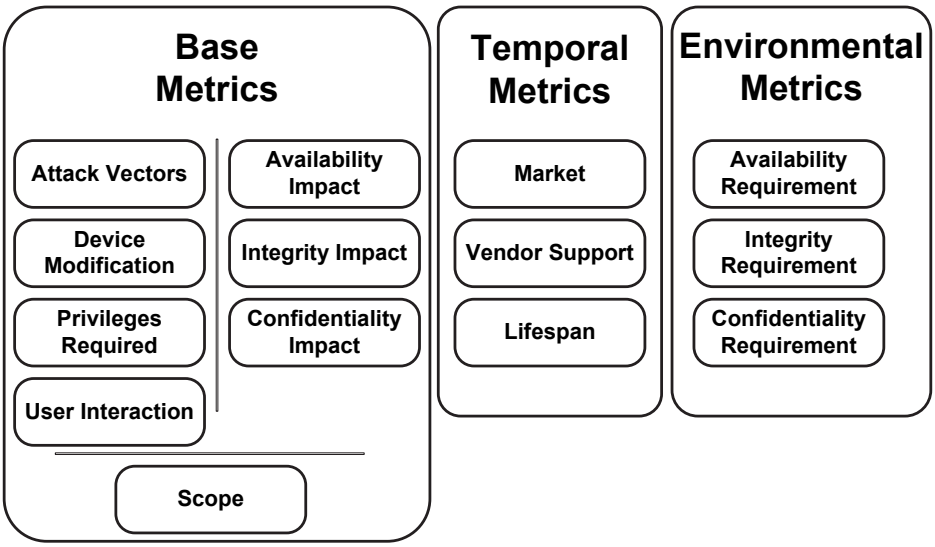

Figure 2. New Proposed Metrics.

3.1 Base Metrics

As the first sub-metric of the new assessment, Attack Vector (AV) is the sub-metric of the connection of the device to potential attackers. Similar to Information Technology (IT) networked devices, the required logical location of an attacker directly correlates to the risk of the device being attacked due to size of audience and increased automation of scanning and exploiting, as shown in Table 1. The larger the logical separation between the set of potential attackers and the system, the less risk of cyber-based compromise is assumed. For all new sub-metrics, the numerical value listed is directly from CVSS [8].

The second sub-metric of the Base Score is Device Modification (DM), which analyzes how standard the device is to its brand's advertising or specifications, and is shown in Table 2. The most common Commercial Off The Shelf (COTS) UAVs purchased have a base-line model with few (if any) variations, and all of the variations represent a higher level of risk since the attacker has less discovery required and more confidence in repeatability between the same models. The other extreme is a complete

Table 1. Attack Vector Values.

Base Level	Description	Value
Direct	System is often termed "remotely exploitable" and can be thought of as being exploitable at the protocol level one or more network hops away.	0.85
Ground Controller	The UAV is indirectly bound to the entire Internet through the ground controller.	0.62
Air-Gapped	The UAV is not bound to the network and the attacker's path is via persistent read/write/execute capabilities on the ground controller.	0.55
None	An attack requires the attacker to be physically present to manipulate the vulnerable component. Physical interaction may be brief or persistent.	0.20

Do-It-Yourself (DIY) UAV that has no standard configuration and is close to being unique.

Table 2. Device Modification Values.

Base Level	Description	Value
Low	Specialized modifications or extenuating circumstances do not exist. An attacker can expect repeatable success when attacking the UAV.	0.77
High	One or more custom modifications or extenuating circumstances exist, requiring the attacker to invest in some measurable amount of preparation.	0.44

Privileges Required (PR) is the sub-metric that defines the software design of components implementing appropriate privilege delineation, as shown in Table 3. Unlike common IT networks, UAVs typically have the assumption that the connected user, whether physically or wirelessly, is the administrative user with the only other privilege level being a kernel variety that is used by the Operating System (OS). Authentication for communication and commands, and authentication prior to access at rest show High levels of separation. If the communication protocols allow any signal received to be executed or valuable flight data and commands are accessible physically by any user with a cable, then the level of privileges required is None.

The next sub-metric of the Base Score is Scope (S), which is an evaluation of risk associated with an attack on the device spreading to other devices. While many UAVs are operated within a one user / one device model, ad hoc networking and swarm technologies are gaining viability, with the risk levels shown in Table 4. The addition of trust connected

Table 3. Privileges Required Values.

Base Level	Description	Value
None	The attacker is unauthorized prior to attack and therefore does not require any access to settings or files of the vulnerable system to carry out an attack.	0.85
Low	The attacker requires privileges that provide basic user capabilities.	0.62 (0.68 if Scope Changed)
High	The attacker requires privileges that provide access to device-wide settings and files.	0.27 (0.5 if Scope Changed)

agents to a targeted UAV increases the risk associated to others and increases the likelihood of an attack on the device in question, extremely similar to IT networks. The connection can vary from command signals to simple navigational directions, but a single vulnerable device has the potential to infect or somehow affect others in the network or compromise a mission. Scope level changes the equations used in the algorithms to associate all of the sub-metrics, increasing the score potential for a Changed value.

Table 4. Scope Values.

Base Level	Description	Value
Unchanged	An exploited UAV can only affect resources local to that device or ground controller.	N/A
Changed	An exploited UAV can affect other devices beyond the local scope.	N/A

The next sub-metric of the Base Score is User Interaction (UI), which is the evaluation of the risk associated with not including a human in the loop, with the risk levels shown in Table 5. Architectures range from fully autonomous, to inject only, to full control. When a UAV has complete control of its flight, assuming some preset mission parameters, the user does not have the ability to override incorrect decisions made by the system. With any amount of user interaction, errors or compromises to the mission may be counteracted, such as Global Positioning System (GPS) spoofing being counteracted with new waypoints or direct first-person control.

The next three sub-metrics of the Base Score are related to the impact of an attack on the device. The first is the Confidentiality Impact (C), which analyzes the securities in place on the device to lessen the threat

Table 5. User Interaction Values.

Base Level	Description	Value
None	The vulnerable system can be exploited without interaction from any user.	0.85
Required	Successful exploitation of this system still allows for the intended user to send commands or otherwise control the flight.	0.62

of a confidentiality breach. Confidentiality being the security objective of keeping access to information at appropriate pre-determined levels, securities enforcing this include encryption of data at rest and Over-The-Air (OTA), as explained in Table 6. Not all data on or transiting a UAV may be considered sensitive information by the user, and as such lower coverage or levels of encryption may be considered sufficient security and therefore less risk.

Table 6. Confidentiality Impact Values.

Base Level	Description	Value
None	There is no confidentiality security in place, resulting in all resources within or transmitting from the impacted UAV being divulged to an attacker.	0.56
Low	There is some confidentiality security in place. The information unsecured does not cause a direct, serious loss to the user.	0.22
High	There is no loss of confidentiality within the impacted UAV or in its communications due to proper security.	0

The next impact sub-metric is Integrity Impact (I), which analyzes the securities in place on the device and on its communication links to enforce integrity, as shown in Table 7. Integrity is the security objective of verifying that information present is the correct or intended information, and the information has not been tampered with by an attacker. These securities usually are included based on the type of protocols used for communication with check sums, cryptographic methods, or through self-diagnostics.

The third impact sub-metric and last sub-metric of the Base Score is Availability Impact (A), and the levels are shown in Table 8. Availability Impact analyzes the level of security providing for continued availability of communication links, whether from an attack or from non-malicious electromagnetic interference. Availability is most commonly secured through multi-channel communication and is important for both the command and data signals. Multi-channel communication may be

Table 7. Integrity Impact Values.

Base Level	Description	Value
None	There are no protections of integrity in place on the UAV. The attacker is able to modify any/all files.	0.56
Low	There are some protections in place, but modification of data is possible. However, attacker does not have control over the consequence of a modification, or the amount of modification is limited.	0.22
High	There is no loss of integrity within the impacted UAV or in its communication links.	0

built into a wireless protocol or be present via hardware in multi-protocol communications.

Table 8. Availability Impact Values.

Base Level	Description	Value
None	There is no availability security, resulting in the attacker being able to fully deny access to resources of the impacted UAV; this loss is either sustained or persistent.	0.56
Low	The resources in the impacted UAV are either partially available all the time, or fully available only some of the time, but overall there is no direct, serious consequence to the impacted component.	0.22
High	There is no impact to availability within the impacted UAV's communication or there is no threat to availability.	0

3.2 Temporal Metrics

A significant aspect of cyber risk is its ability to change over time. The temporal sub-metrics each represent aspects of the risk of the device that are evaluated at some instance in time and are also understood to change over a period of time.

The first sub-metric of the Temporal Score is Market (M), which is an assessment of how common the device is around the world and potentially how valuable the UAV is to attackers. Taking directly into account an attacker's motivation, risk is increased if the reward to effort ratio is greater, as shown in Table 9. This metric is constantly changing as the market morphs due to country relations, large organizations make trade deals, and new regulations impact the viability or marketability of UAVs. For value of a UAV, the key players in the UAV industry include, but are not limited to, first-world military inventories, distribution companies, and other large companies that may use UAVs to provide services.

Table 9. Market Values.

Temporal Level	Description	Value
High	50% or more of the market is held by the UAV brand or the UAV is used by more than one major customer.	1
Medium	More than 25% but less 50% of the market is owned by the UAV brand or the UAV is used by exactly one major customer.	0.97
Low	Less than 25% of the market is held by the UAV brand and the UAV is not used by any major customer.	0.94
None	The UAV is either non-standard or homemade, and therefore holds near 0% of the market share.	0.91

The next sub-metric of the Temporal Score is Vendor Support (VS) which evaluates the rate or quality of updating a UAV's software and is defined in Table 10. Often termed "patches", the vendors of computer products still within marketability will release updates in code in response to discovered vulnerabilities or new features. Cyber risk is significantly reduced when time, money, and people are invested to secure released software. Vendors are not the only parties interested in securing software; the user or research communities often step up to release optional patches when vendors refuse and there is user interest.

Table 10. Vendor Support Values.

Temporal Level	Description	Value
Unavailable	There is no vendor support and no active community support for the UAV.	1
Low	There is no official vendor support, but there is active community support providing updates or workarounds to vulnerabilities.	0.97
Medium	There is occasional official vendor support and there is active community support for the UAV.	0.96
High	There is active official vendor support and active community support for the UAV.	0.95

The third and last Temporal Score sub-metric is Lifespan (L) which is the evaluation of the expected time of device service life remaining. Risk is increased when more time is available for the device to be discovered and attacked, as shown in Table 11. While individuals or smaller organizations may not have concrete decisions in place at acquisition, most large organizations determine a life-cycle management plan where a mission life is expected. Different than normal IT equipment in some ways, the life expectancy of a small UAV is most likely less than the planned

life-cycle for an organization, so when new models will be purchased needs to be taken into account.

Table 11. Lifespan Values.

Temporal Level	Description	Value
High	The expected lifespan of the UAV for missions is greater than the expected support of the device by the vendor or greater than 2 years.	1
Normal	The expected lifespan of the UAV for missions is within the expected support of the device or between 1 and 2 years as a normal lifespan.	0.96
Low	The expected lifespan of the UAV is less than 1 year and is expected to be discontinued soon.	0.92

3.3 Environment Metrics

Vital to any UAV risk assessment, mission risk is rated within the Environment Score. The mission requirements are similar to the original CVSS definition due to the whole device or system being rated for mission requirements, instead of an individual vulnerability. The whole device, here the UAV platform, may be designed for multiple mission sets and therefore must be rated for the highest requirement in each sub-metric. The mission metric is divided into Confidentiality Requirements (CR), Integrity Requirements (IR), and Availability Requirements (AR), following the basic definition for cyber security. Each sub-metric is rated from three possible levels which are defined in Table 12 and are as follows: High, Medium, Low. Unlike CVSS, which includes a Not Defined level, this framework requires a determination of mission requirements, with Medium level being the default by having a neutral modifying effect on the Base metric.

Table 12. Environment Sub-Metric Values.

Requirement Level	Description	Value
High	Loss of {Confidentiality — Integrity — Availability} is likely to have a **catastrophic** adverse effect on the organization or the mission.	1.5
Medium	Loss of {Confidentiality — Integrity — Availability} is likely to have a **serious** adverse effect on either the organization or the mission.	1.0
Low	Loss of {Confidentiality — Integrity — Availability} is likely to have a **limited** adverse effect on either the organization or the mission.	0.5

Included within the Environmental Score of CVSS is the Modified Base Metric Scores, which are duplicates of the Base Score sub-metrics that are adjusted for the specific situation of the device in question. CVSS Base Score sub-metrics are expected to be analyzed as network and mission agnostic for the vulnerability in question, such that the metrics would then be static for any customer using a device that would be vulnerable. This assessment analyzes each device with its prospective mission and environment in the Base Score, such that no new information would be gleaned in the Modified Base Score. Removing the Modified Base Score sub-metrics from the scoring system is simple as the CVSS default is to use the original Base Score sub-metrics. In the future, should a risk assessment of an UAV be beneficial separate from mission and environment, then this assessment is simply reverted by using Modified Base Score sub-metrics in the Environmental equations instead of the Base sub-metrics.

4. Scoring System

The risk scoring system is designed to incorporate each of the metrics defined in the previous section to calculate an overall risk score. For ease of use, the score is limited to values between 0.0 and 10.0, which should provide close to 101 possible risk states based on the 14 sub-metric values. The values of sub-metrics are drawn directly from the open-source values of CVSS, leveraging the long-term value of testing and refining that CVSS placed into their vulnerability severity assessment. Due to the design of each of this framework's sub-metrics in line with CVSS's sub-metrics, the values of severity should be close and directly related to values of risk. The equations also are directly borrowed from CVSS due to the direct connection between their assessment and this assessment.

4.1 Base Score

The Base Score is calculated using the first eight sub-metrics that consider device design and securities. This score is not necessarily accurate for any future assessment or for a different customer since the use cases, configurations, and payloads are considered. Using the Base Score values as defined, the Base Score is then calculated using Algorithm 1. Scope is used as a modifier to both intermediaries using constants used by CVSS. The influence of each metric has been balanced over time and testing by CVSS for their vulnerabilities and directly relate to this framework's risk metrics.

Algorithm 1 Base Score Calculation

$ISS = 1 - [(1 - C) * (1 - I) * (1 - A)]$
if $S = Unchanged$ **then**
  $Impact = 6.42 * ISS$
else
  $Impact = 7.52 * (ISS - 0.029) - 3.25 * (ISS - 0.02)^{15}$
end if
$Exploitability = 8.22 * AV * DM * PR * UI$
if $Impact <= 0$ **then**
  $BaseScore = 0$
else
  if $S = Unchanged$ **then**
    $BaseScore = Roundup(Min[Impact + Exploitability), 10])$
  else
    $BaseScore = Roundup(Min[1.08 * (Impact + Exploitability), 10])$
  end if
end if

4.2 Temporal Score

The Temporal Score is calculated next after the Base Score using the three sub-metrics associated. The Temporal Score is the new score for the device as the Base Score of risk is potentially reduced by factors relating to time. The highest risk values could be considered the default as it assumes the worst case temporal state for each sub-metric and does not have an effect on the Base Score. The calculation of the Temporal Score is shown in Algorithm 2.

Algorithm 2 Temporal Score Calculation

$TemporalScore = Roundup(BaseScore * M * VS * L)$

4.3 Environmental Score

The Environmental Score uses the assessed sub-metrics in relation to requirements of the device in its required or proposed mission sets. The process to determine the Environmental Score is shown in Algorithm 3. The "Modified" terminology is used to separate these terms from the Base Score and do not use actual modified values as in CVSS per the explanation earlier in this section. The Environmental Score is then calculated using the sub-metrics of the Temporal Score and Base Metrics.

With the Environmental Score calculated, this value is the Final Score representing the cyber risk associated with a particular UAV and a particular mission-environment set. Ranging from 0.0 to 10.0 with rounding

Algorithm 3 Environmental Score Calculation

$//EnvironmentalScore \leftarrow$ {C,I,A Requirements , Modified Base Metrics}
$MISS = Min\{1 - [(1 - CR * C) * (1 - IR * I) * (1 - AR * A)], 0.915\}$
if $S = Unchanged$ **then**
  $ModifiedImpact = 6.42 * MISS$
else
  $ModifiedImpact = 7.52 * (MISS - 0.029) - 3.25 * (MISS * 0.9731 - 0.02)^{13}$
end if

$ModifiedExploitability = 8.22 * AV * DM * PR * UI$

if $ModifiedImpact <= 0$ **then**
  $EnvironmentalScore = 0$
else
  if $S = Unchanged$ **then**
    $EnvironmentalScore = Roundup(Roundup[Min([ModifiedImpact + ModifiedExploitability], 10)] * M * VS * L)$
  else
    $EnvironmentalScore = Roundup(Roundup[Min(1.08 * ModifiedImpact + ModifiedExploitability), 10)] * M * VS * L)$
  end if
end if

up to the nearest tenth, scores are designed to be easy to use by non-cyber focused personnel and vary enough to see subtle changes based on the sub-metrics. All changes to the CVSS model have now been explained and the new information relating directly to UAV risk have been correlated to the original well-established model.

5. Case Study Build and Scoring

To demonstrate and analyze this risk assessment methodology, two models of UAVs and three mission-environment scenarios will be used. By scoring across the total of six case studies, the objectives of ease of use, readability, and breadth should be made evident. To accomplish this, the two models are first defined with their relevant specifications, then the mission-environments are defined. This section concludes by presenting the finished matrix of scores.

Model 1: The first model to be used in this case study is one of the highest rated consumer UAVs currently on the market: the Chinese-made DJI Sciences and Technologies Limited (DJI) Mavic 2 Pro. The Mavic 2 Pro was released in mid-2018 and rivaled the best of its competitors for "camera performance, video transmission, fight time, flight speed, less noise, omnidirectional obstacle sensing, intelligent flight modes

and its unique Hyperlapse feature" [3]. The Mavic 2 Pro quad-rotor has a maximum flight time of 31 minutes, maximum speed of 45 mph, and hover at windspeeds up to 25 mph, all while being sold for under $2,000 [3]. The Mavic 2 Pro is controlled via the DJI GO 4 app from a user's phone connected to a DJI controller, which commands and receives data over Wifi protocol standards and both frequencies by default [5]. The DJI brand is well-known for their autopilot obstacle avoidance of which the Mavic 2 boasts 360 degree vision. The user is always in control of the UAV per FAA regulations, and the Mavic 2 Pro features multiple control failure protocols such as returning to a home waypoint. DJI is known as a brand for their closed systems and protocols with the data being encrypted with AES-256 standard [5]. DJI is plagued by rumors of supply chain vulnerabilities with epartment of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) placing the company on an industry alert [20]. While DJI has officially denied all allegations to the United States (U.S.) Senate sub-committee on Security, some industries are taking precautions with acquiring new UAVs from this manufacturer [20].

Model 2: The second model to be used for case studies in this paper is the well-publicized U.S.-made Falcon 8+, of which the Shooting Star version is most known for its light displays at Disney Parks [12]. The Intel-produced Falcon 8+ model was released in 2015 and is meant for missions of mapping structures and terrain [12]. The Falcon 8+ is an octo-rotor design, unlike the Shooting Star which features only four rotors, and boasts a maximum flight time of 26 minutes, maximum speed of 22 mph, and hover at windspeeds up to 27 mph [12]. Engineered specifically for Intel's waiver with the FAA to allow the Intel Cockpit to operate upwards of 1,500 UAVs at one time, the individual price tag of $30,000 is a bit misleading since they are contracted by mission and not purchased one-off [7]. The Falcon 8+ is controlled exclusively through the single Intel ground controller Cockpit, sending commands and receiving data through both Wifi frequencies with manual control of a single device possible for emergencies [12]. The Falcon 8+ runs off of open-source Linux OS and only uses Wifi encryption for data transmission and no encryption published for data at rest [12]. While operating multiple UAVs, all mission data is processed at Intel data centers since missions have been clocked at generating over 18TB of data [7].

Model 3: The third model is the French-made Parrot Anafi, which represents the cheaper yet capable UAV models for comparison. Produced by Parrot who is known for the under $1,000 market, the Anafi ($600 currently in the U.S.) represents the professional tier for Parrot while being accessible by hobbyists. The Anafi is a quad-rotor model

and is clocked at 25 minutes of flight time, 33 mph maximum horizontal speed, and hover control up to 31 mph [16]. Parrot utilizes a unique controller that the user's smartphone attaches into for navigation and the standard software build requires full control during missions with a few pre-programmable fail-safe controls [16]. The controller utilizes both Wifi frequency standards for control and data, and features no security for data at rest or over the air. The smartphone app is the ground controller and, while usually connected to Parrot servers, can operate away from network [16].

Mission 1: As the simplest of mission scenarios, an individual user purchases a single UAV for their agricultural business to monitor crops and livestock. Since video streaming is the only mission, and lacking ability to modify, the device bought will only be used in a standard out-of-the-box configuration. The terrain is almost completely flat with no buildings or very few trees within the operating area. The user plans to operate the UAV manually only to fly first-person video capture with no data storage. The user plans to utilize the aircraft for only a single season to test out its effectiveness. As an independent farmer, the user does not consider data captured to be confidential. With full access to the area and a low operating ceiling, manual recovery after losing signal is easy. The user plans to utilize a tablet as the ground controller without access to the Internet while operating.

Mission 2: The user organization is purchasing a fleet of UAVs for their delivery and distribution business. The devices will require modification in-house to allow the carrying and releasing of small packages. To meet regulations, each UAV will be controlled by individual ground controllers and the devices will not be interfaced. The delivery area is a 10 minute radius around the distribution center and is comprised of sub-urban home communities with no nearby airports. The organization plans on utilizing these aircraft for three years, at which point they plan to purchase a new fleet. The flight data stored on each device is considered sensitive to the company due to research plans to expedite deliveries. The delivery area has many civilians and homes, so uncontrolled landings are highly dangerous. The ground controllers are computers that are networked directly to the Internet for data processing off-site.

Mission 3: The last mission scenario is a military organization purchasing a fleet of UAVs to map potential enemy positions. The UAVs require a separately procured camera-sensor suite, though the software will remain standard. The fleet will be pre-programmed with mission data from a stand-alone ground controller and only interface with mission-partnered UAVs as a swarm, meaning the scope will change if one is compromised. The military organization plans a life cycle of two years

Table 13. Mission Scenario Sub-metrics and Scores.

	Scenario 1			Scenario 2			Scenario 3		
Model	1	2	3	1	2	3	1	2	3
AV	0.55	0.55	0.55	0.62	0.62	0.62	0.2	0.2	0.2
DM	0.77	0.77	0.77	0.44	0.44	0.44	0.44	0.44	0.44
PR	0.27	0.62	0.62	0.27	0.62	0.62	0.5	0.68	0.68
UI	0.62	0.62	0.62	0.62	0.62	0.62	0.85	0.85	0.85
C	0	0	0.56	0.22	0	0.56	0.56	0	0.56
I	0.22	0.22	0.56	0.22	0.22	0.56	0.56	0.22	0.56
A	0.22	0.22	0.56	0.22	0.22	0.56	0.22	0.22	0.56
M	1	0.97	0.97	1	0.97	0.97	1	0.97	0.97
VS	0.95	0.95	0.97	0.95	0.95	0.97	0.95	0.95	0.97
L	0.92	0.92	0.92	1	1	1	0.96	0.96	0.96
CR	0.5	0.5	0.5	1.5	1.5	1.5	1.5	1.5	1.5
IR	0.5	0.5	0.5	1	1	1	1.5	1.5	1.5
AR	0.5	0.5	0.5	1.5	1.5	1.5	0.5	0.5	0.5
Base	3.1	3.9	7.3	3.8	3.4	6.8	6.8	3.4	7.0
Temp	2.8	3.4	6.4	3.7	3.2	6.4	6.3	3.1	6.4
Final	1.7	2.3	4.7	4.4	3.7	6.4	6.4	3.1	6.4

for the fleet before replacing aircraft. Since all data captured is stored on the device until mission is complete, all mission data is extremely sensitive.

Table 13 is the scoring matrix for each of the pairings of model to mission scenario using only the provided information. The Base, Temporal, and Environmental sub-metrics are spaced apart, along with the calculated scores for each at the bottom. Scenarios represent the Mission-Environment pairing described above and the Model numbers correlate to the described models in order.

Table 13 does not include the worst case scenario which is simply setting each individual sub-metric to the highest risk value. This is scenario is used for analysis to show breadth and calculate the amount of lost potential scores due to CVSS algorithms' maximum values.

6. Analysis

Below we discuss the presented implementation's benefits and challenges. The risk assessment tool is rated against the three objectives of Breadth and Variability, General Applicability, and Ease of Use. These are suggested by related research in cybersecurity risk assessments [19, 11]. The scope of this paper does not analyze the assessment

against any live situations or historical information, which may provide additional and different insights for adjustments.

6.1 Benefits

The first observation of the case studies is the spread of scores based on the limited number of examples. Even with just ten total example scenarios including the worst case, the scores cover 83% of the possible scores. Best case scenarios were specifically not built as one of the examples as they present trivial information, that can easily be achieved by a number of vectors. A UAV with high securities within Confidentiality, Integrity, and Availability Impact sub-metrics will force the overall Base, Temporal, and Environmental Scores to 0.0 without variations. The objective of reaching breadth of the scoring range to allow for maximum variations of risk scores is therefore achieved. Across the three scenarios where risk to the buyer was increasing, the scores for almost all models increased as well. Additionally, between models, the DJI and the Intel models provided more security than the Parrot, which is factored into the cost of the UAV, and their scores were noticeably lower for the majority of missions. One exception to this was in Scenario 3 where the DJI's rumored supply chain risk is heavily factored for a non-Chinese military organization and that risk is shown by scoring the Mavic 2 Pro close to the unsecured Anafi. Scenario 2 had a buying organization only slightly influenced by this possible risk, and the Mavic 2 Pro showed significantly better final scores compared to the Anafi. The objective of the risk assessment showing variability and general risk correlation is therefore achieved.

For General Applicability, the tool was successfully able to apply to all of the models and scenarios without having a sub-metric being inapplicable. This is in sharp contrast to the direct CVSS sub-metrics which has several that do not apply based on the scope of component versus system level view and assuming traditional network setup. The models were limited to similar copter designs, so further case studies are required to prove.

The last proposed objective, Ease of Use, is a more subjective characteristic, but is determined to be achieved in this risk assessment based on the required documentation to complete the scores in the case studies. For all three models presented, all of the sub-metrics were determined from the specification documentation that is published online and from other easily accessible advertisements. This means that nearly anyone, with the risk assessment's guide, could determine their organization's or their personal scores with some amount of accuracy. There is no

in-depth cyber forensics or testing utilized for any of the sub-metrics, though research into vulnerabilities can still be taken into account, as seen with the supply chain risk of DJI.

6.2 Drawbacks & Challenges

The spread of scores is seen to be limited by CVSS's built in caps to make sure that the scores do not go above 10.0, which it may in the worst case. Running the algorithm for the worst case found that a number of possible high ranged risk values are lost, such as those to 10.8 for Base Score (if Scope Unchanged, then no values lost) and those to 10.9 on the Final Environmental Score. These caps result in lost variability between scores at the top end of the risk spectrum by setting them equal at the maximum 10.0 score. CVSS accepts this loss with the assumption that any risk framework utilizing their assessment will make strides to reduce and cover this glaring vulnerability to the network [8]. Working with system risk here, the same assumption can be made for this risk assessment that few systems will actually achieve an above maximum score and the users will put forward effort to lower that score through security features or by choosing another available model.

Another drawback of this risk assessment through the case studies is the actual level of usability by potential users. By focusing on the acquisition phase, the level of cybersecurity knowledge is expected to be low, but the translation done by the assessment of cyber principles is expected to bridge that gap. To fully verify this objective may require human studies or live production level results, which are outside the scope of this paper. The analysis of documentation required for accessibility and legibility shows promise, but does not prove the objective.

7. Conclusion and Future Work

The current field of small UAVs lacks a tool to compare and subsequently reduce cybersecurity risks within an organization's risk frameworks. The risk assessment proposed here is grounded in the well-known CVSS model for network vulnerabilities and calculates a risk score based on 14 sub-metrics. These sub-metrics encapsulate the range of risks presented from the cyber realm to compromise UAVs and are weighted to provide an easy-to-use metric for acquisition decisions. The included ten case studies provide fuller description and implementation of the risk assessment, and show the preliminary achievement of all three original objectives for a small UAV risk assessment.

Further study is required for risk assessments focusing on UAVs. This risk assessment requires additional data points to validate claims of vari-

ability and breadth with current market data. The weights and submetric definitions also require additional study to verify that they meet the requirements specific to UAVs. The ease-of-use objective may also require human studies with expected users to validate the proposed tool's questions as a bridge between cyber knowledge and risk determination at the earliest point in the life-cycle management. For risk assessments in general, while quantitative assessments are preferred mode of calculation for risk, a true quantitative assessment for UAVs requires a better understanding of what criteria are able to be directly measured and rated.

Disclaimer: The views expressed in this paper are those of the authors, and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government. This document has been approved for public release; distribution unlimited, case #88ABW-2019-6089.

References

[1] E. Ancel, F. Capristan, J. Foster and R. Condotta, Real-time risk assessment framework for unmanned aircraft system (UAS) traffic management (UTM), *Seventeenth AIAA Aviation Technology, Integration, and Operations Conference*, 2017.

[2] B. Clinton, Executive Order 13010: Critical Infrastructure Protection, The White House, Washington, DC (`www.hsdl.org/?abstract&did=1613`), 1996.

[3] F. Corrigan, DJI Mavic 2 Pro and Zoom Review of Features, Specs with FAQs, *DroneZon* (`www.dronezon.com/drone-reviews/dji-mavic-2-pro-zoom-review-of-features-specifications-with-faqs/`), 2019.

[4] Dimensional Research, Trends in Security Framework Adoption: A Survey of IT and Security Professionals (`static.tenable.com/marketing/tenable-csf-report.pdf`), 2016.

[5] DJI, Mavic 2 Pro/Zoom User Manual v2.0 (`https://dl.djicdn.com/downloads/Mavic_2/20190417/Mavic_2_Pro_Zoom_User_Manual_v2.0_en.pdf`), 2019.

[6] P. Fahlstrom and T. Gleason, *Introduction to UAV Systems, 4th Edition*, John Wiley and Sons, West Sussex, United Kingdom, 2012.

[7] J. Feist, Intel's drone business explained - Falcon 8+, Shooting Star and Insight, *Drone Rush* (`www.dronerush.com/intel-drone-business-12568`), May 8, 2018.

[8] Forum of Incident Response and Security Teams (FIRST), Common Vulnerability Scoring System SIG (`www.first.org/cvss`), 2020.

[9] J. Gray, Design and Implementation of a Unified Command and Control Architecture for Multiple Cooperative Unmanned Vehicles Utilizing Commercial-off-the-Shelf Components, M.S. Thesis, Department of Systems Engineering and Management, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, 2015.

[10] K. Hartmann and K. Giles, UAV exploitation: A new domain for cyber power, in *Proceedings of the Eighth International Conference on Cyber Conflict*, N. Pissanidis, H. Rõigas and M. Veenendaal (Eds.), NATO CCD COE Publications, Tallinn, Estonia, pp. 205–221, 2016.

[11] K. Hartmann and C. Steup, The vulnerability of UAVs to cyber attacks - An Approach to the risk assessment, in *Proceedings of the Fifth International Conference on Cyber Conflict*, K. Podins, J. Stinissen and M. Maybaum (Eds.), NATO CCD COE Publications, Tallinn, Estonia, 2013.

[12] Intel Corporation, Intel Falcon 8+ System (`www.intel.com/content/www/us/en/products/drones/falcon-8`).

[13] P. Kopardekar, Unmanned Aerial System (UAS) Traffic Management (UTM): Enabling Civilian Low-Altitude Airspace and UAS Operations, NASA/TM—2014–218299, NASA Ames Research Center, Moffett Field, California, USA, 2014.

[14] P. Kopardekar, Unmanned Aircraft Systems Traffic Management, U.S. Patent No. 0275801 A1, September 22, 2016.

[15] F. Mohammed, A. Idries, N. Mohammed, J. Al-Jaroodi, and I. Jawhar, UAVs for smart cities: Opportunities and challenges, *International Conference on Unmanned Aircraft Systems*, pp. 267-273, 2014.

[16] Parrot, Anafi (`www.parrot.com/global/drones/anafi`), 2018.

[17] D. Pettit, R. Dill and S. Graham, Zero Stars: Analysis of cybersecurity risk of small COTS UAVs, in *Proceedings of the Thirteenth International Conference on Emerging Security Information, Systems and Technologies*, S. Rass and G. Yee (Eds.), IARIA, Wilmington, DE, USA, pp. 90–95, 2019.

[18] K. Scarfone and P. Mell, An analysis of CVSS version 2 vulnerability scoring, *Third International Symposium on Empirical Software Engineering and Measurement*, pp. 516–525, 2009.

[19] I. Stine, A Cyber Risk Scoring System for Medical Devices, M.S. Thesis, Department of Electrical and Computer Engineering, Air

Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, 2017.

[20] D. Sullivan, Drone Security: Enhancing Innovation and Mitigating Supply Chain Risks, U.S. Senate (www.commerce.senate.gov/2019/6/drone-security-enhancing-innovation-and-mitigating-supply-chain-risks), June 18, 2019.