Spring 5-3-2021

Cybersecurity Considerations with the Increasing Uses of Small Unmanned Aircraft Systems (sUAS) or Drones

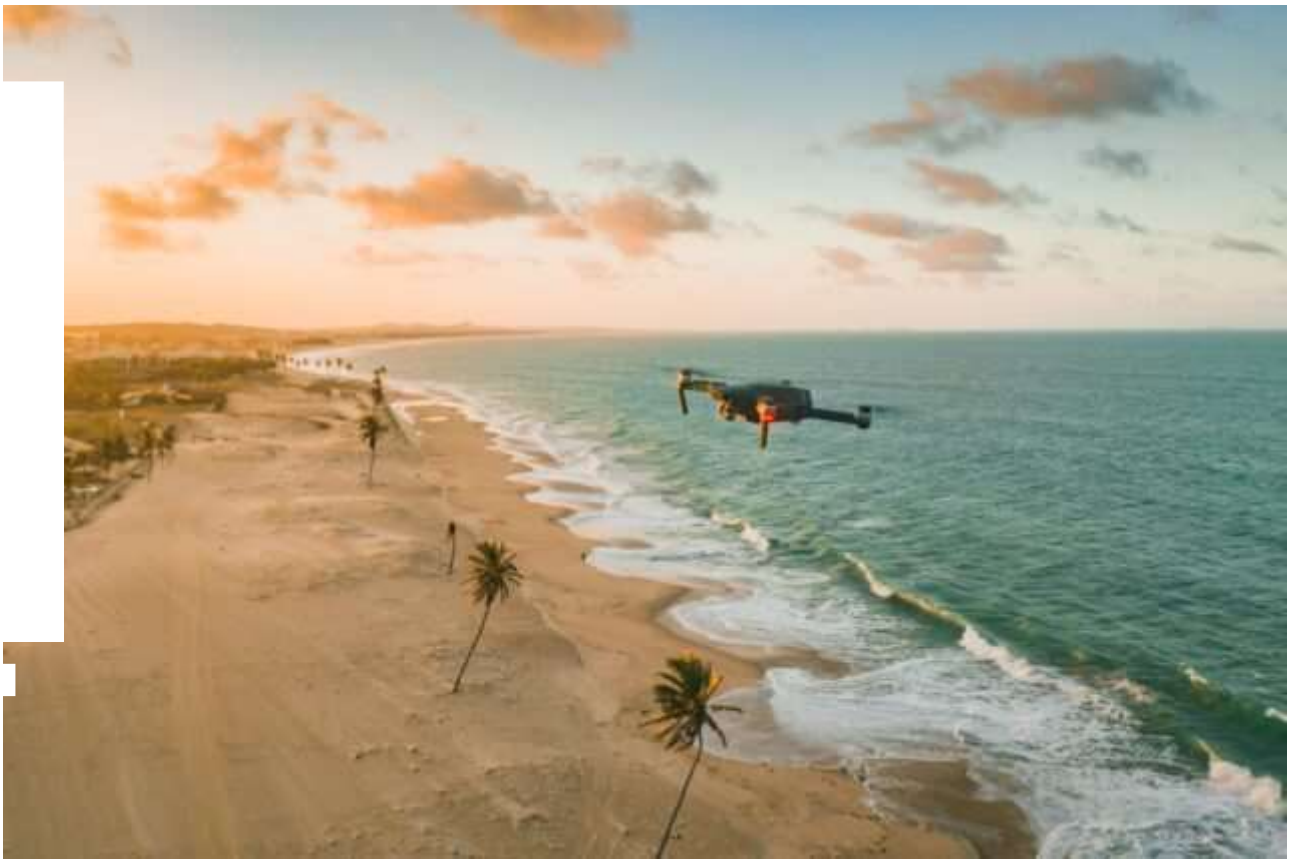
Matthew Kucharek
Bergen Technical High School, mkucharek03@gmail.com

Stanley Mierzwa
Kean University, smierzwa@kean.edu

Cybersecurity Considerations with the Increasing Uses of Small Unmanned Aircraft Systems (sUAS) or Drones

The use of Small Unmanned Aircraft Systems (sUAS), otherwise less formally known as drones, is expanding in use cases throughout work and commercial environments and personal and recreational purposes.

By **CISOMAG** - May 3, 2021



The effort to produce this information resource results from a collaborative effort between the Bergen County Technical Schools (high school), through the advisor Andrea Buccino, and a cybersecurity expert mentor. High school senior members of this learning partnership are provided with an interactive learning experience. They gain an increase and knowledge in a particular area of study while under the topical guidance of a mentor. In this example, the high school senior is pursuing coursework in Aerospace Engineering, and this was combined with the focus of cybersecurity to expand the students' cross-discipline knowledge. This collaborative work was done virtually, given the current pandemic situation.

By Matthew Kucharek, Senior, Aerospace Engineering Program, Bergen County Technical High School; and Stan Mierzwa, M.S., CISSP, Director and Lecturer, Kean University Center for Cybersecurity

Introduction

The use of Small Unmanned Aircraft Systems (sUAS), otherwise less formally known as drones, is expanding in use cases throughout work and commercial environments and personal and recreational purposes. One industry and critical infrastructure area expanding its use into drones include emergency services. The Emergency Services Sector is considered by the United States Cybersecurity and Infrastructure Security Agency (CISA) as one of the sixteen critical infrastructure sectors (Cybersecurity & Infrastructure Security Agency, 2021). Within this sector are housed fire stations, local town public works departments, police departments, and medical service providers. The use of technology drones is beginning to complement the emergency services sector's response
ts. With this, a greater demand to ensure the use of the devices remains free from cyber
ats.

show of support of protecting drones, the National Science Foundation has funded the creation
drone cybersecurity curriculum (Targeted News Service, 2020). Creating such a curriculum will
train students on cybersecurity concerns and ways of assessing such risks. The need is
anted, given the U.S. Federal Aviation Administration (FAA) expects the growth of registered
es to reach 3.8 million by 2022 (Federal Aviation Administration. 2019; Tezza, Andujar, 2019).

short article will outline the general growth and increasing use cases of drones, provide
ground to understand the blocks or components of a drone solution, and finally, detail awareness
of the cybersecurity concerns to be aware of.

Background on Growing Uses of Small Unmanned Aircraft Systems (sUAS)

Concerning the use of drones, some common commercial areas include inspection of industrial facilities, real estate and aerial photography, agriculture, state and local government, including emergency management services (Tezza, Andujar, 2019). In addition, growing research is being done in such sectors as product delivery; consider the research and work going on at Amazon via their PrimeAir that permits for 30-minute deliveries in certain areas using unmanned aerial vehicles or drones. Other emergency services, including medical services, are investigating the prototypes of drones to provide logistic services and hospital deliveries for remote or rural areas (Nenni, M., et al. 2020). The use cases for drones seem endless and time will tell how far the technology may venture.

Understanding the sUAS Components

Actual Physical Drone

There are several Components in a drone. Some of the components are used to fly the drones, while others are tasked to collect data. Two essential components are used in flying the drone: A small computer, and this is used to collect information from the satellite and the user. The second is the GPS chip. The GPS chip, which is connected to the computer, collects info from the satellite for the drone to know where it and it relays the information back to the user. Two components used in a drone to collect data are the camera and the microphone. If the malicious aggressor manages to get in, they can tap into and see/collect the data (Craiger, 2020).

Controller (Smartphone or Tablet) Application

: drones use a software application on the device used to control the drone. These applications nstalled on a smartphone or tablet, and then the smartphone or tablet is connected to another ce that has controllers to fly the drone. As the people move the controllers to fly it, it sends a sage to the application and the drone.

nectivity/Communication

way information is sent to and from the drone is with the use of satellites. With significant or big ı areas where it is hard to connect to the Wi-Fi, drones use one of 4 civilian bands to relay mation. These networks can be unsecured and unencrypted (Craiger, 2020).

Cybersecurity Concerns with sUAS Devices

Like any computing device, there are several different cybersecurity concerns with sUAS or drone devices. A malicious aggressor can attack drones via diverse methods to gain access to the drone or the information that the drone is collecting or that the drone contains. To bring attention to these cybersecurity concerns, several different vectors are outlined below.

Connectivity

Before delineating the different attacks on drones, there needs to be an explanation of why some of these attacks can happen in the first place. The biggest reason is that drones are connected, for the most part, to a network, whether a private or public connection. Citizens who have drones can only use one of 4 civilian bands. The problem with them is that they are not encrypted, not authenticated, and have weak signals. These three problems help hackers get into the drone to either fly it or acquire data that the drone is collecting (Craiger, 2020).

Denial of Service (DOS)

With very similar components to computing devices, several different ways, and approaches would pertain to Denial of Service against drones. In essence, a drone is essentially a flying computer. As such, this means that they are subjected to similar attacks as your desktop computer. One such attack is Denial of Service (DOS). In one scenario, if the drone operator is connected to an unsecured Wi-Fi, the malicious aggressor can connect to a proxy system and attack the drone. The attacker may have an opportunity to run as an administrator-level account through a proxy, such as "root" under Linux or "administrator" under Windows. Once the malicious aggressor gets into the drone, an attacker can use several destructive common Linux commands to cause damage to the drone or the user.

De-Authentication Attacks

:her attack against a drone is called a de-authentication attack. De-authentication can be pared to the act of hanging up or disconnecting from a telephone. In one method, this attack : the drone's Media Access Control (MAC) address. The malicious aggressor uses a modified drone another computer from a stationary position and scans to certain MAC addresses. Once it tifies a MAC address, the address is compared to known MAC identifications to find out the dor, such as DJI or Parrot, two very popular drone manufacturers (Craiger, 2020). If the malicious essor decided they want to target the drone, they send a hang-up package and disable the drone the user. In one example of sending a de-authentication or disconnection attack to a flying e, a young 13-year-old person demonstrated such an attack at a cybersecurity and drone erence hosted in South Africa. This demo was valuable in bringing awareness to such attacks approaches that are not extensively sophisticated (VOA News, 2019).

GPS Spoofing

Two other possible attacks against drones include Global Positioning System (GPS) spoofing and GPS jamming. GPS spoofing can include the process when a malicious aggressor creates a stronger signal that overrides the weak signal from the satellite GPS and targets the drone (Craiger, J. P. 2020). As a result, the drone does not know where it is and has a false GEO location. In such a case, the drone could fly aimlessly or even fall and crash to the ground. GPS jamming is when the malicious aggressor can create a stronger signal on the same communication frequency that is being used by the civilian GPS satellite; then the drone is unable to receive that GPS location information.

Suggestions to Guard Against Cyberthreats with Drones

Updates

Ensure that the devices (drones and applications) are kept up to date with security and other related software and firmware patches (Threat Report, 2019). Oftentimes these updates are designed by drone companies to fix any bugs or security gaps with the drone. To stay abreast of the updates, similar to how this is approached with other devices such as computer operating systems and software applications, timely patching to protect systems against vulnerabilities in drones needs to be undertaken. Routine checks with the drone manufacturer to determine the most up-to-date firmware and software are suggested.

Secure connection

Refrain from connecting to insecure Wi-Fi with the controller or drone device. Insecure Wi-Fi can lead malicious aggressors to infiltrate your drone quicker and easier. Connect only to a secured Wi-Fi if possible. Consider using a Virtual Private Network (VPN) if connecting to Wi-Fi to ensure the communications cannot be hacked via such techniques as Man-In-The-Middle attacks.

swords

isswords are utilized for connection or login to the drones or applications, use Multi-Factor ientication (MFA) or Two-Factor Authentication (2FA), where possible (Hinkle, S. 2020). Use a sword where it is possible since it adds an extra layer of protection to your drone. As is the case other network-connected devices, refrain from using identical passwords in other services and ems to minimize the ease of a hacker gaining access.

nclusion

nes are essentially flying computers. This means they are assessable to cyber-attacks. From Denial-of-Service attacks to GPS Spoofing, drones have vulnerabilities that pose threats to itself or to the user. In this short article, the author's aim was to bring attention and cybersecurity situational awareness to both drone professionals and hobby enthusiasts regarding cyber threats to drones. A focus was placed on the components and operations of the drones. It should also be noted that drone-related information can be housed within such repositories of drone manufacturer websites, where user accounts, address information and other personal-related knowledge may reside and need to be protected from threat actors.

The use of drones is expected to grow in various professional and personal interests, and the malicious potential of these platforms is inevitable and can no longer be avoided (Edwards, B. 2021). There is the possibility that drones could become as commonplace as the cellphone, which was not the norm not too long ago (Seqrite, 2019).

> ***An unabridged version of this article appears in the May issue of CISO MAG.***

References

Craiger, J. P. (2020). NYCTE Center An Introduction to Small Unmanned Aerial Systems (sUAS) Cybersecurity. As retrieved from: https://www.youtube.com/watch?v=vE3TDmsYrvg

Craiger, P., Kessler, G. & Rose, W. (2018). uUAS: Cybersecurity Threats, Vulnerabilities, and Exploits. *National Training Aircraft Symposium (NTAS)*.

Cybersecurity & Infrastructure Security Agency. (2021). Critical Infrastructure Sectors. Retrieved from: https://www.cisa.gov/critical-infrastructure-sectors

ards, B. (2021). Cybersecurity and Drones: A Threat From Above. *Forbes*. Retrieved from: s://www.forbes.com/sites/forbestechcouncil/2021/02/25/cybersecurity-and-dronesa-threat-from-ve/?sh=66e4e4627b0d

eral Aviation Administration. (2019). Unmanned Aircraft Systems Forecast. Retrieved from: s://www.faa.gov/data_research/aviation/aerospace_forecasts/media/Unmanned_Aircraft_System f

le, S. (2020). Drones and Cybersecurity – Smart Eye Explains How Cybersecurity Extends to ne Operators. Retrieved from: https://mavicmaniacs.com/drones-and-cybersecurity

Nenni, M., Di Pasquale, V., Miranda, S. & Riemma, S. (2020). Development of a Drone-Supported Emergency Medical Service. *International Journal of Technology*. 11(4).

Seqrite. (2019). Consequences of cyberattacks on UAVs: The cybersecurity threats drones face and how to mitigate them. Seqrite Blog. Retrieved from: https://www.seqrite.com/blog/cybersecurity-threats-drones/

Targeted News Service. (2020). National Science Foundation Funds Development of First-of-Its-Kind Drone Cybersecurity Curriculum at Embry-Riddle. Washington, DC.

Tezza, D. & Andujar, M. (2019). The State-of-the-Art of Human-Drone Interaction: A Survey. IEEE Access.

Threat Report, (2019). Drone Technology a Rising Threat to Cybersecurity. As retrieved from: https://www.youtube.com/watch?v=h_GwkFOZHKI

VOA News. (2019). 13-Year-Old 'CyberNinja' Hacks Drone to Show Cyber Threat. As retrieved from: https://www.bing.com/videos/search?q=cybersecurity+threats+to+drones&&view=detail&mid=D444D976FAE65D92E304D444D976FAE65D92E304&&FORM=VRDGAR&ru=%2Fvideos%2Fsearch%3Fq%3Dcybersecurity%2Bthreats%2Bto%2Bdrones%26FORM%3DHDRSC4

About the Authors

Matthew Kucharek is a Senior at Bergen County Technical High School in New Jersey and currently partaking in a cybersecurity mentoring program collaborating with the Kean University Center for Cybersecurity. Kucharek possesses a black belt in Tae Kwon Do martial arts.

Stanley Mierzwa is the Director, Center for Cybersecurity at Kean University in the U.S. He lectures at Kean University on Cybersecurity Risk Management and Foundations in Cybercrime. He is a peer reviewer for the Online Journal of Public Health Informatics journal, a member of the FBI Infragard, IEEE, ISC(2), and a board member of the global pharmacy education non-profit, Vennue Foundation. Mierzwa received his MS in Management of Information Systems at the New Jersey Institute of Technology and his BS in Electrical neering at Fairleigh Dickinson University. Mierzwa is also a Certified Information Systems urity Professional (CISSP), a member of the FBI Infragard, and currently pursuing a Ph.D. rmation Technology with a specialization in cybersecurity.

Disclaimer

Views expressed in this article are personal. The facts, opinions, and language in the article do not reflect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same.

CISOMAG

https://cisomag.com/