Homeland Security

National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE NOTE

May 22, 2018; 0900 EDT

CYBERSECURITY RISKS POSED BY UNMANNED AIRCRAFT SYSTEMS

KEY FINDINGS

The Department of Homeland Security (DHS)/National Protection and Programs Directorate (NPPD)/Office of Cyber and Infrastructure Analysis (OCIA) assesses that unmanned aircraft systems (UASs) provide malicious actors an additional method of gaining undetected proximity to networks and equipment within critical infrastructure sectors. Malicious actors could use this increased proximity to exploit unsecured wireless systems and exfiltrate information. Malicious actors could also exploit vulnerabilities within UASs and UAS supply chains to compromise UASs belonging to critical infrastructure operators and disrupt or interfere with legitimate UAS operations.

SCOPE NOTE: This Critical Infrastructure Security and Resilience note assesses cybersecurity risks to critical infrastructure associated with UASs. This product assesses the risks associated with malicious cyber actors utilizing UASs for offensive purposes, but does not assess the technical vulnerabilities associated with UASs or critical infrastructure systems. OCIA does not know of a confirmed incident utilizing a UAS for malicious cyber activity against critical infrastructure systems. This product provides situational awareness of potential current and potential future malicious actions, with malicious acts noted in this paper having occurred inside controlled environments. This product supports Federal, State, local, and private sector partners with UAS equities.

OCIA coordinated this product with the DHS/NPPD/Office of Infrastructure Protection, DHS/NPPD/Office of Cybersecurity and Communications/National Cybersecurity and Communications Integration Center, the DHS/Office of Intelligence & Analysis, DHS/Science & Technology Directorate, the Department of Transportation (DOT)/Federal Aviation Administration (FAA), the DOT/Office of the Secretary, the Federal Bureau of Investigation/Cyber Division, the National Counterterrorism Center, United States Army/National Ground Intelligence Center, the Northern California Regional Intelligence Center, the Aviation Information Sharing and Analysis Center (A-ISAC), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and Argonne National Laboratory.

BACKGROUND

The FAA defines UASs, also referred to as "drones," as "unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system."[1] The market for UASs has grown rapidly, and the FAA anticipates continued rapid growth in both the hobbyist and commercial UAS fleets between 2016 and 2021. For example, the hobbyist fleet of small UASs (sUASs)[i], which includes the vast majority of UASs purchased by the general public, is expected to triple in size by 2021, with the commercial sUAS fleet anticipated to grow tenfold by 2021.[2]

[i] A UAS weighing between .55 and 55 pounds is referred to as a small UAS (sUAS). Federal Aviation Administration. (2017). "FAA Dronezone." https://faadronezone.faa.gov/#/. Accessed March 12, 2018.

The overwhelming majority of commercially available UASs are operated through applications that run on a user's phone, tablet, or computer. These applications allow the user to manage a UAS, including establishing a route, piloting the aircraft, and receiving data from the aircraft. UASs also frequently come with memory sticks and USB ports to allow for the transfer of data, including images and video.

UAS capabilities will likely continue to improve based on consumer demand for greater payload, longer range, and autonomous operation. Additional anticipated UAS improvements include longer battery life, advances in route planning, and a reduced reliance on radio-frequency signals.[3,4,5]

UAS FACILITATE PHYSICAL ACCESS TO UNSECURED SYSTEMS

UASs provide malicious actors an additional method of gaining proximity to networks and equipment within critical infrastructure sectors. Malicious actors could then use the proximity provided by a UAS to wirelessly exploit unsecured systems and extract information from systems they cannot otherwise access remotely or may not be able to access due to range limitations. This includes networks and devices within secured buildings, as well as networks and devices behind fencing and walls.[ii,iii]

UASs can also allow a malicious actor to wirelessly exploit vulnerabilities from a distance (figure 1). The prevalent ownership and operation of UASs by the general public, the distance from which UAS can be operated, and a lack of tracking data can also provide malicious actors a level of anonymity that otherwise may not be available. UASs, in particular UASs, are typically more difficult to detect than a malicious actor attempting to trespass beyond physical barriers.

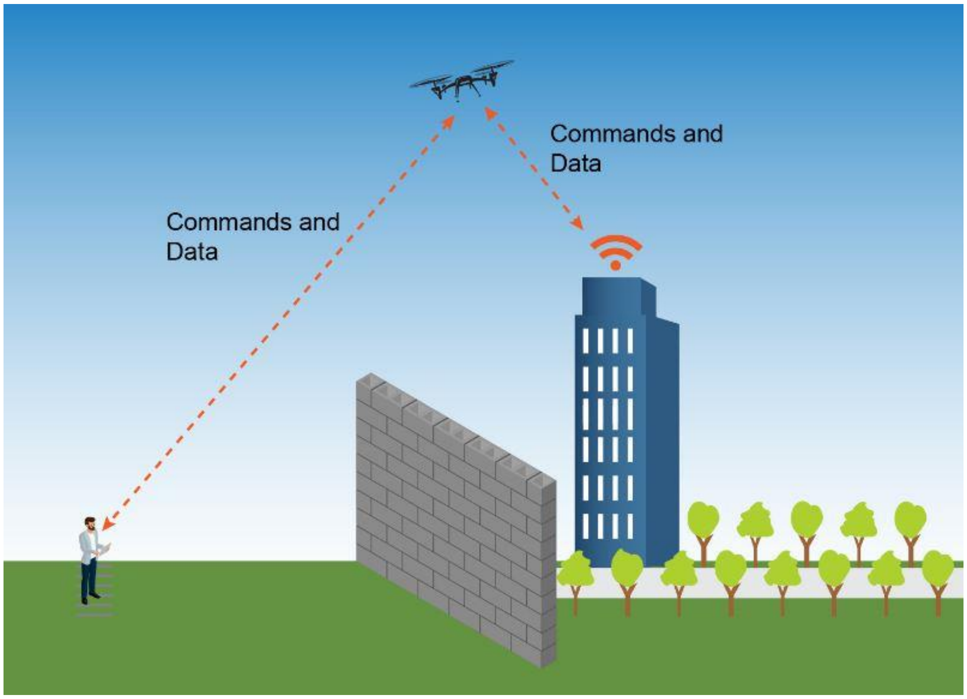

FIGURE 1—UAS OPERATOR EXPLOITING UNSECURED WIRELESS SYSTEM WITHIN SECURE FACILITY

[ii] Limitations on UASs, such as battery life and payload, may limit the ability of a malicious actor to carry out a cyber attack that requires persistent access; potential malicious cyber acts noted in this paper, however, do not necessarily require persistent UAS access and could be undertaken using commonly available UASs.

[iii] For more information on unsecured devices, see: DHS/NPPD/OCIA. (2017). "Why is the Internet of Things Insecure?"

UAS FOR WIRELESS SYSTEM EXPLOITATION

Malicious actors could utilize UASs in order to wirelessly exploit access points and unsecured networks and devices. This can include using UASs in order to inject malware, execute malicious code, and perform man-in-the-middle attacks. UASs can also deliver hardware for exploiting unsecured wireless systems, allowing malicious actors persistent access to the wireless system until the hardware is detected or runs out of power. While OCIA does not know of a confirmed incident utilizing UASs to exploit wireless systems, researchers have demonstrated this capability.

- In 2016, researchers in Israel flew a UAS outside of an office building and were able to compromise smart lightbulbs installed within the building using equipment attached to the UAS. The researchers were able to perform over-the-air firmware updates to take control of the lightbulbs at a range of 350 meters.[6,7]
- In 2015, researchers in Singapore attached a smartphone holding applications to a UAS to detect printers with unsecured wireless connections. The researchers flew the UAS outside an office building, had the phone pose as the printer, and tricked nearby computers to connect to the phone instead of the printer. When a user sent a document for printing, the phone intercepted the document and sent a copy to the researchers using a 3G or 4G connection. The document was then sent to the real printer so the user would not know the document had been intercepted.[8,9]

UAS FOR EXTRACTING INFORMATION

In addition to computer systems exploitation, UASs can be equipped to receive exfiltrated data sent through a visual or radio signal that a malicious actor may not otherwise be able to access due to physical barriers, heavily defended networks, and air-gapped systems.[iv]

- In 2017, researchers in Israel demonstrated the ability to exfiltrate data from an air-gapped computer[v] utilizing the computer's hard drive indicator LED light. Malware installed through separate means on the computer manipulated the LED light to blink rapidly, with information encoded and sent through the LED light. A camera attached to a UAS outside the window received the data transmitted from the LED light.[10]

While the use of UASs for information extraction is possible, the risk for infrastructure operators of this technique being used for the theft of large amounts of data is low. OCIA does not know of a confirmed incident utilizing a UAS to extract information, and the use of such a method would require a high level of sophistication in order to extract a limited amount of data. Such a method, however, could be used in order to steal small amounts of highly sensitive data to be used in future malicious actions, including information on critical infrastructure systems, administrative credentials, and encryption keys.

MALICIOUS ACTORS CAN EXPLOIT COMPROMISED UAS

While UASs can be used as a tool for an attacker, they are also vulnerable to exploitation. Many commercial UAS variations, for example, currently communicate with ground stations and operators using unencrypted feeds. This can allow a malicious actor to intercept and review data sent to and from the UAS.[11,12]

Malicious actors can target UASs belonging to critical infrastructure operators, using vulnerabilities within UAS software or firmware in order to compromise the systems and access sensitive networks and information.[13] Malware can also be pre-installed in a UAS application or in UAS software or firmware by a malicious actor with access to the UAS' supply chain. Likewise, embedded malware could compromise the computer, phone, or tablet

[iv] An air-gapped system refers to a system which is not directly connected to the Internet or connected to other systems that are connected to the Internet. Zetter, K. (2014). "Hacker Lexicon: What Is an Air Gap?" *Wired*. www.wired.com/2014/12/hacker-lexicon-air-gap/. Accessed January 16, 2018.

[v] While the researchers did not state how the air-gapped computer became infected with the malware, three potential methods were mentioned: supply chain attacks, social engineering, and hardware with pre-installed malware. Guri, M. et al. (2017). "LED-it-GO: Leaking (a lot of) Data from Air-Gapped Computers via the (small) Hard Drive LED." https://cyber.bgu.ac.il/advanced-cyber/system/files/LED-it-GO_0.pdf, p. 4. Accessed March 20, 2018.

where the application resides. A malicious actor can compromise any one of these systems to extract sensitive data, further infiltrate any networks the UAS interacts with, and take control of the victim's UAS.

- Security analysts have demonstrated the ability to hijack and take control of another user's UAS mid-flight, including UASs designed for commercial industry and first responder use.[14,15,16] Malicious actors hijacking another user's UAS could attempt to extract data from the UAS, including flight path and any images or video being taken. Malicious actors could also control the movements of the UAS, posing a physical danger to nearby aircraft and personnel.[vi,vii]

MITIGATION MEASURES

Organizations can update Emergency and Incident Action Plans to include UAS security and response strategies and know who has jurisdiction to take action in the air domain around the facility. Critical infrastructure operators can also contact the FAA to consider UAS restrictions in proximity to fixed site facilities and build partnerships with Federal, state, and local authorities for adaptation of best practices and response strategies.[17] If a suspicious UAS is detected in or around a facility, the incident should be reported to local law enforcement and other relevant officials immediately. Provide as much detail as possible, including the type of UAS, its size, shape, color, and the payload.[viii]

Securing wireless networks and devices can minimize the vulnerabilities that malicious UAS operators could exploit to compromise systems. Mitigation options include installing updates and patches in a timely manner, changing default passwords, restricting access, encrypting data, and installing host-based firewalls.[18] A "defense in depth" approach with layered[ix] physical[x] and network security measures allows victims more opportunities to slow, detect, and mitigate cyberattacks, including any attack utilizing UASs.

In addition to securing wireless networks and devices, UAS operators can also take steps to decrease risks to their UASs. This includes ensuring UASs and their components have the minimum necessary privileges, maintain minimal access to other networks and systems, and encrypt data while it is both at rest and in transit. Personnel utilizing UASs should also have adequate cybersecurity training, and critical infrastructure operators using UASs can perform cybersecurity risk assessments for their UASs to identify additional risks associated with the organization's UASs.

The Office of Cyber and Infrastructure Analysis (OCIA) provides analysis to support public and private-sector stakeholders' operational activities and effectiveness and to inform key decisions affecting the security and resilience of the Nation's critical infrastructure. All OCIA products are visible to authorized users at HSIN-CI and Intelink. For more information, contact OCIA@hq.dhs.gov or visit http://www.dhs.gov/office-cyber-infrastructure-analysis.

Prepared By: Operational Analysis Division

PDM17252

[vi] For more information on potential physical harm to aircraft from UAS, see: Alliance for System Safety of UAS through Research Excellence (ASSURE). (2017). "UAS Airborne Collision Severity Evaluation Executive Summary – Structural Evaluation." www.assureuas.org/projects/deliverables/a3/Volume%20I%20-%20UAS%20Airborne%20Collision%20Severity%20Evaluation%20-%20Structural%20Evaluation.pdf. Accessed April 9, 2018.

[vii] For more information on potential physical harm to a person from a UAS collision, see: Alliance for System Safety of UAS through Research Excellence. (2017). "UAS Ground Collision Severity Evaluation." www.assureuas.org/projects/deliverables/a4/ASSURE_A4_Final_Report_UAS_Ground_Collision_Severity_Evaluation.pdf. Accessed April 9, 2018.

[viii] For more information, please see the DHS pocket card on responding to UAS. DHS. (2017). "Tips in Responding to a UAS incident." www.dhs.gov/sites/default/files/publications/uas-ci-drone-pocket-card-112017-508.pdf. Accessed February 27, 2018.

[ix] For more information on layered network security, see: Shenk, J. (2013). "Layered Security: Why It Works." SANS Institute. www.sans.org/reading-room/whitepapers/analyst/layered-security-works-34805. Accessed February 12, 2018.

[x] For more information on layered physical security, see: Hutter, D. (2016). "Physical Security and Why It Is Important." SANS Institute. www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120. Accessed February 12, 2018.

END NOTES

[1] Public Law 112-95, Sec. 331. (2012). "FAA Modernization and Reform Act of 2012." www.congress.gov/112/plaws/publ95/PLAW-112publ95.pdf, p. 72. Accessed February 12, 2018.
[2] Federal Aviation Administration. (2017). "FAA Aerospace Forecast Fiscal Years 2017-2037." www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2017-37_FAA_Aerospace_Forecast.pdf, p. 31-32. Accessed January 5, 2018.
[3] *The Economist*. (2017). "Technology Quarterly: Taking Flight." www.economist.com/technology-quarterly/2017-06-08/civilian-drones. Accessed January 5, 2017.
[4] AZO Sensors. (2017). "The Future of Drone Technology - Autonomy, Collision Avoidance and Advanced Sensors." www.azosensors.com/article.aspx?ArticleID=782. Accessed January 5, 2017.
[5] iQ. (2017). "Drone Innovation Trends to Watch in 2017." Intel. https://iq.intel.com/drone-innovation-trends-watch-2017/. Accessed January 5, 2017.
[6] Ronen, E. et al. (2016). "IoT Goes Nuclear: Creating a ZigBee Chain Reaction." Weizmann Institute of Science. http://iotworm.eyalro.net/. Accessed January 2, 2018.
[7] Ricker, T. (2016). "Watch a drone hack a room full of smart lightbulbs from outside the window." *The Verge*. www.theverge.com/2016/11/3/13507126/iot-drone-hack. Accessed January 2, 2018.
[8] Zetter, K. (2015). "Hacking Wireless Printers With Phones on Drones." *Wired*. www.wired.com/2015/10/drones-robot-vacuums-can-spy-office-printer/. Accessed January 2, 2018.
[9] *Cyber Defense Magazine*. (2015). "Hacking enterprise wireless printers with a drone or a vacuum cleaner." www.cyberdefensemagazine.com/hacking-enterprise-wireless-printers-with-a-drone-or-a-vacuum-cleaner/. Accessed January 2, 2018.
[10] Greenberg, A. (2017). "Malware Lets a Drone Steal Data by Watching a Computer's Blinking LED." *Wired*. www.wired.com/2017/02/malware-sends-stolen-data-drone-just-pcs-blinking-led/. Accessed January 2, 2018.
[11] Glaser, A. (2017). "The U.S. government showed just how easy it is to hack drones made by Parrot, DBPower and Cheerson." *Recode*. www.recode.net/2017/1/4/14062654/drones-hacking-security-ftc-parrot-dbpower-cheerson. Accessed May 3, 2018.
[12] Federal Trade Commission. (2016). "FTC Fall Technology Series: Drones." www.ftc.gov/system/files/documents/videos/ftc-fall-technology-series-drones-part-1/ftc_fall_technology_series_drones_-_transcript_segment_1.pdf, p. 6. Accessed May 3, 2018.
[13] CybeRisk. (2017). "The Usage of Drones in Cyber Attacks – Both as Targets for Attack and as Potential Attack Vectors." www.cyberisk.biz/the-usage-of-drones-in-cyber-attacks/. Accessed January 5, 2017.
[14] Greenberg, A. (2016). "Hacker Says He Can Hijack a $35K Police Drone a Mile Away." *Wired*. https://www.wired.com/2016/03/hacker-says-can-hijack-35k-police-drone-mile-away/. Accessed January 16, 2018.
[15] Albanesius, C. (2013). ""SkyJack' Software Finds and Hijacks Drones." *PC Magazine*. www.pcmag.com/article2/0,2817,2427933,00.asp. Accessed January 16, 2018.
[16] Kamkar. S. (2013). "SkyJack." http://samy.pl/skyjack/. Accessed May 3, 2018.
[17] DHS. (2017). "Unmanned Aircraft Systems: Addressing Critical Infrastructure Security Challenges." www.dhs.gov/sites/default/files/publications/uas-ci-challenges-fact-sheet-508.pdf, p.1. Accessed February 12, 2018.
[18] United States Computer Emergency Readiness Team (US-CERT). (2016). "Securing Wireless Networks." Department of Homeland Security. www.us-cert.gov/ncas/tips/ST05-003. Accessed January 5, 2018.