Unmanned Aircraft Systems: Information Security Threats Within the Cyber Domain

The Aerosonde® Mk. 4.8 Hybrid Quad UAS at Redstone Arsenal, Alabama. Courtesy photo: Program Executive Office, Aviation.

**By Company F, 227th Aviation Regiment, "Godfathers"
Fort Cavazos, Texas**

Information security (INFOSEC) applies to all information, regardless of its domain. Technological advancements challenge the security of information, especially within the cyber battlefield. Security considerations must be applied based on the protected data's value. Information that should be secured may include proprietary rights, information sent across networks, or system accessibility. The three fundamental tenets of INFOSEC are confidentiality, integrity, and availability (Figure) (LBMC, 2022). Threat nations, especially pacing threats such as China or Iran, will aggravate those security measures to leverage strategic advantage. Since unmanned aircraft systems (UAS) operate exclusively within the cyber domain through network communication, it is imperative to understand the capabilities threatening UAS INFOSEC.

> **"The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government [2001] to protect classified information"**
>
> **(Awati et al., n.d.).**

Confidentiality of information pertains to the measures emplaced to permit only authorized users access during storage or operational use. Additionally, confidentiality does not include attacks that intend to alter or modify. Exploits to breach confidentiality protocols may include methods that attempt to receive or access information through unauthorized methods. Security protocols that emphasize physical components are the most widely used for retaining confidentiality. "The universal technique for providing confidentiality for transmitted or stored data is symmetric encryption" (Stallings & Brown, 2015, p. 41). Threat actors may breach the confidentiality of information in a variety of schemes. For simplicity and applicability purposes, focusing on threats that take advantage of network infiltration is paramount.

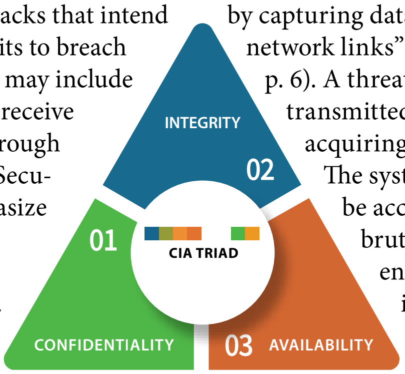

Figure. The three fundamental tenets of INFOSEC. "Together, they are called the CIA Triad" (LBMC, 2022). Triad drawing courtesy of LBMC.

Bharat B. Madan, Manoj Banik, and Doina Bein, Department of Modeling, Simulation, & Visualization Engineering professors at Old Dominion University, USA, express concerns with information confidentiality stating, "An attacker can also compromise the confidentiality of an *[sic]* UAS by capturing data communicated over network links" (Madan et al., 2016, p. 6). A threat actor may extract transmitted data packets by acquiring access to the network. The system acquisition may be accomplished through brute force hacking the encryption system or using social engineering methods. Conversely, brute force hacking is infrequent due to the sophistication of the embedded Advanced Encryption Standard.

> **The Data Encryption Standard is a symmetric block cipher adopted in 1977 by the National Institute of Standards and Technology. The AES "is intended to replace DES and DES with an algorithm that is more secure and efficient"**
>
> **(Stallings & Brown, 2015, p. 645).**

An additional attack process may entail exploiting human negligence through social engineering (Stallings & Brown, 2015). Phishing e-mails, physical tailgating, or deceptive interviews are all used to retrieve information that can be utilized to gain unauthorized access. Afterward, attackers may install malware to manipulate protocols to create a bypass directed into the system (Madan et al., 2016).

The Data Encryption Standard and

Advanced Encryption Standard are two critical principles that fortify symmetric encryption (Stallings & Brown, 2015, pp. 643-645). These standards utilize block ciphers, which are fundamentally a password-based authentication. However, security protocols are generally irreversible by end-users without authorization from a privileged user. As such, all Soldiers, Department of Defense (DoD) contractors, and DoD Civilians are the first line of enforcement when protecting information. Army Regulation 25-2, "Army Cybersecurity," establishes policies for securing data from unauthorized users (Department of the Army, 2019). First, the enforcement of physical security will deter unwanted threats. Secondly, users must comply with the appropriate handling or storing procedures dependent on the information classification. Lastly, end-users should spread awareness of cybersecurity threats and those measures used to prevent attacks.

The integrity of information involves the accuracy and validity of data during transmission. Security measures used to protect the integrity of information share semblance to those in confidentiality. However, unlike confidentiality, integrity encompasses modifying data or the origin of data provided to the user. The act of altering data can be just as catastrophic as having no data at all. Since viable strategies derive from unerring information, an attack on integrity may lead to poor decisions and judgment. Protecting information integrity ensures that the information retains its authenticity for accurate and timely decisions. In our opinion and combat experience, one of the biggest threats to information integrity of UAS operations is Global Positioning Systems (GPS) spoofing through modification or masquerading.

Global Positioning System spoofing is employed to tamper with the integrity of GPS information. Generally, GPS spoofing transmits broad-ranging signals to deceive GPS receivers within proximity. These transmissions then cause the receivers to display arbitrary locations. However, a new technology developed in China allows GPS spoofing to be used in a calculated method to alter GPS locations into a fixed pattern. The technology, which enables spoofers to deploy GPS attacks deliberately, was inconceivable until now. Todd Humphreys, the head of Radionavigation Laboratory at the University of Texas, states, "To be able to spoof multiple ships simultaneously into a circle is extraordinary technology" (Trevithick, 2019). Global Positioning System spoofing, now coupled with new technology, is a developing threat that sends UAS operations into disarray.

Accurate GPS information is critical in mission planning and execution; therefore, it requires security measures to ensure validity. Successful spoofing entails three components: a transmitter, frequency, and a receiver (McAfee,™ 2020). Identifying the weakness in those components will aid in avoiding deception. The transmitter and frequency are threats based on their locality, and as such, may be avoided through evasive procedures.

The Valiant UAS at Redstone Arsenal, Alabama. Courtesy photo: Program Executive Office, Aviation.

If those threats are unavoidable, the receiver is now an active threat. Typically, receivers have embedded anti-spoofing modules within their encryption systems (e.g., Selective Availability Anti-Spoofing Modules). However, if those modules are compromised, maneuvering through "map to video" correlation is required. Security measures focused on information integrity will help guarantee all information is valid for use in the decision-making process.

Information **availability** consists of the user's ability to perform actions when required. In some cases, denying information availability may permit unauthorized users to breach confidentiality and integrity. Since availability threats indicate a form of system denial, the same security measures designed for the other tenets may not work. Additionally, common system protocols are embedded, and monitoring their effectiveness may be restricted. A common way to combat an availability threat is to develop redundancies into a system. These may include alternate ways to perform actions or a contingency plan to execute during denied service. Unmanned aircraft system operations should be primarily concerned with Denial of Service (DoS) attacks devised to deny communications or seize access and control of the aircraft.

Denial of Service[1] attacks deploy interferences through frequency overflow that overburden the bandwidth or resources (Stallings & Brown, 2015). Denial of Service methods cited within Stallings' & Brown's book express direct concerns for UAS operations. Furthermore, though it may not originate from DoS attacks, commandeering may be a form of availability denial that is utilized. Threats against system unavailability were demonstrated during an incident that involved the hijacking of an RQ-170 stealth drone by Iran in 2011. Iran cyber experts seized control over the aircraft and used reverse engineering to gather proprietary schematics (Opall-Rome, 2018). This event revealed the devastating cause and effects of an attack on system availability.

Military + Aerospace Electronics published an article that inferred the results of the RQ-170 incident caused the Pentagon to advocate the need for higher levels of cybersecurity (Keller, 2016). Keller's article emphasizes how disastrous this attack was on cybersecurity and the Pentagon's determination to make cybersecurity a top priority. The necessity for securing availability presents several concerns. In terms of technology, systems already have internal defense mechanisms to protect against attacks through wireless assaults. However, the DoD emphasizes the importance of the human factor in cybersecurity by analyzing the Navy's nuclear-propulsion program designed by the "Father of the Nuclear Navy," Admiral Hyman Rickover (Winnefeld et al., 2015). The program's cybersecurity process enforces the technical development of all users to provide maximum results. As UAS experts, all users need to understand and apply security methods that the system employs to protect information availability.

Information security is paramount for successful operations against pacing threats that dominate the cyber domain. Decision-makers should consider the three tenets when performing operations or planning engagements. Confidentiality of information must be established to ensure only authorized users have access to confidential information. Information integrity is accomplished by allowing only authorized users to modify data. In our experience, the foundation of information availability is preventing, identifying, and reacting to attacks that may deny system access. However, this is easier said than done. The cyber domain is a vast and unpredictable realm that is hemorrhaged by technological advancements. Human due diligence is essential if technologies were ever to fail. Information security requires attention from all users to prevail against opposing forces.

Biography:

The F/227th is a UAS company assigned to the 1st Air Cavalry Brigade, 1st Cavalry Division, at Fort Cavazos, Texas. The unit's last combat deployment was to Al-Asad, Iraq, in October 2021—June 2022. For composition, the F/227th is comprised of Six Platoons: Headquarters, Ground Vehicle Maintenance, Air Vehicle Maintenance, and three Flight Platoons. There are two commissioned officers, 10 Warrant Officers, 43 noncommissioned officers, and 72 Troopers, totaling 127 service members. The F/227th is currently deployed in support of operation Atlantic Resolve in the European Command area of responsibility.

[1] "A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users" (Cybersecurity & Infrastructure Security Agency, 2021).

References:

Awati, R., Bernstein, C., & Cobb, M. (n.d.). Advanced encryption standard (AES). *TechTarget*. https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard

Cybersecurity & Infrastructure Security Agency. (2021). *Understanding denial-of-service attacks*. https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

Department of the Army. (2019, May 4). *Army cybersecurity* (Army Regulation 25-2). https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN37506-AR_25-2-003-WEB-4.pdf

Keller, J. (2016, May 3). *Iran-U.S. RQ-170 incident has defense industry saying 'never again' to unmanned vehicle hacking.* Military + Aerospace Electronics. https://www.militaryaerospace.com/computers/article/1675072/iranus-rq170-incident-has-deffense-industry-saying-never-again-to-unmanned-vehicle-hacking

LBMC. (2022, May 23). *Three tenets of information security.* https://www.lbmc.com/blog/three-tenets-of-information-security/

Madan, B. B., Banik, M., & Bein, D. (2016, February 23). Securing unmanned autonomous systems from cyber threats. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 16*(2), 119-136. https://doi.org/10.1177/1548512916628335

McAfee.™ (2020, August 25). *What is GPS spoofing?* https://www.mcafee.com/blogs/consumer/what-is-gps-spoofing/

Opall-Rome, B. (2018, February 12). *Israel Air Force says seized Iranian drone is a knockoff of US Sentinel.* Defense News. https://www.defensenews.com/global/mideast-africa/2018/02/12/israel-air-force-says-seized-iranian-drone-is-a-knockoff-of-us-sentinel/

Stallings, W., & Brown, L. (2015). *Computer security: Principles and practice* (3rd ed.). Pearson Education, Inc. https://www.cs.unibo.it/~babaoglu/courses/security/resources/documents/Computer_Security_Principles_and_Practice_(3rd_Edition).pdf

Trevithick, J. (2019, November 19). *New type Of GPS spoofing attack in China creates "crop circles" of false location data.* The War Zone. https://www.twz.com/31092/new-type-of-gps-spoofing-attack-in-china-creates-crop-circles-of-false-location-data

Winnefeld, J. A., Jr., Kirchhoff, C., & Upton, D. M. (2015, September 09). Cybersecurity's human factor: Lessons from the Pentagon. *Harvard Business Review*, 86-95. https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon