Autonomous Drones NIST Framework Assessment

Military Drone

Minhchau
Andre
Brennon
Paris
Dominic

This assessment is written primarily in the view of the use of drones in military organizations.

Asset Management Program

A well funded military with a drone program has many assets available to establish a management program with a purview of identifying cybersecurity threats. Since vulnerabilities in the drone are mainly software related, the military can hire more personnel and consultants to identify vectors of attack, especially with connectivity, drone maintenance, and software controls. Given the inherent hierarchical nature of the military, mechanisms are already in place to provide oversight of drone development and operation. A dedicated leader can be assigned specifically with the role of asset management to ensure oversight is constantly in use. Personnel can also be deployed to monitor and assess assets coming in from contractors, and implement screening processes to prevent vulnerabilities.

Business Environment

The Business Environment a military drone supports can be broken down into two categories. Surveillance and military combat. Within surveillance, drones have the crucial role of collecting information on subjects or geographical areas and the data they record is passed on in the supply chain. One use case would be to brief our military personnel engaged in combat. Another could be a more passive act of drones patrolling and merely acting as eyes in the sky. The data collected affects decisions made for tactics used in missions that later are played out during combat. Should a drone be compromised or hacked without knowledge, then either the information collected could be tampered with or it could be leaked out into the wrong hands which might lead to irreversible consequences. On the other end, drones can also play the role of engaging in combat missions with airstrikes. The importance of assuring the security of an unmanned, armed drone could never be overstated. If hacked by an enemy, it could lead to dire consequences that could affect much more than just the Defense Industrial Base Sector.

Governance

According to prominent cybersecurity news sources, the Department of Defense (DoD) is currently drafting an updated cybersecurity policy for their UAV systems. The current DoD IT governance addresses some generalized cybersecurity threat prevention practices. The document addresses the danger of insider attacks, which certainly pertains to drones, by either a pilot, engineer, or any other member who has access to the hardware or software. It is also noted that all devices which are connected over networks are susceptible to outsider attacks. This means that if a UAV is connected to a base station network or other communication systems, it is exposed to possible backdoor, eavesdropping, or access denial attacks, to name a few. The DoD IT department lists some high-level approaches to these vulnerabilities. These include using validated cryptographic identity credentials, detecting malicious software, unauthorized data movement, reducing the need to manually download information onto removable media to move it to another security domain, streamlining certification and accreditation, and using networks as a single information environments (DoD, 2011).

Citation: *Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap*. Department of Defence, 2011, dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf

Risk Assessment

The risk assessment of a drone is categorized by each component of the machine, and is reported by intensity of risk and amount of security needed. Each component is analyzed for its susceptibility to attacks of integrity, confidentiality, and availability, and the probability of an attack occurring. Additionally, UAV risks are dependent of the type of mission being carried out. The risk analysis is separated into five components. First is environment, which is assessed by geographical characteristics (affects availability) and political environment (ie. friendly or unfriendly territory). The main environmental threats are destruction, signal manipulation, or theft. The next component is communication links, mainly wifi connections. A possible threat to this software could result in a data breach, flight control takeover, or destruction of the drone. Another component is sensors. Drones are equipped with a multitude of sensors. Compromised sensors threaten a drone's ability to navigate safely, or use weapon/surveillance attachments. Additionally, drones send and receive massive amounts of sensitive data. Confidentiality and integrity are the primary concerns in this realm. UAV software must have state of the art encryption and signatures. Finally, drones must be equipped with fault handling mechanisms. These include fail-safe modes, redundancies, and even self-destruct which provide extra safety if certain aspects of a UAV are compromised. If these systems are hacked, the mission of a UAV could easily be altered.

Risk Management Strategy

The risk strategy used by an organization in the contexts of drones depends on the organization and the type of drone. The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. Risk management processes are established, managed, and agreed to by organizational stakeholders. The risk management processes for a military drone would most likely be established by a specialist and managed by a government or military official. Organizational risk tolerance is determined and clearly expressed. Once an organization decides what the risk tolerance of the drone they will make that information known and use it to manage risk. The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis. A military drone is going to have different risk management than the racing drone of a hobbyist. A sector like the military would need these drones to gather critical information while another sector would use drones to research AI. The risk management strategy will differ widely depending on the sector. In the context of the military the risk management is vital because the risk involved in a drone being compromised is very high.

Supply Chain Risk Management

Given the highly complex nature of drones, a comprehensive and thorough supply chain risk management strategy is a necessity to ensure cybersecurity risks are minimized. After identifying the risks associated with each component, the organization should traceback the development process of each component and the risks involved at each step, since the security of the whole supply chain is only as strong as its weakest link. The risk management strategy should prioritize working with the private sector contractors developing the drone and its systems to ensure their cybersecurity plan is just as thorough to ensure integrity throughout the entire development process, and choosing companies with both a proven track record and an appropriate plan for contracts. However, because of the reliance on these contractors, there is an inherent constraint in this risk management strategy. While military organizations have influence and some degree of power over contractors, there can only be so much oversight, meaning there is a reliancy on the contractors' abilities to manage their own risks. However, as long as they are vetted thoroughly, this can be within the acceptable risk tolerance, and through periodic evaluations of the contractors, the organization can assume that they are holding up their side of the risk management strategy.