Establishing a Safe and Secure **Municipal Drone Program**

SECURING SMART CITIES

cloud security alliance®

The permanent and official location for *Cloud Security Alliance Internet of Things Working Group* is **https://cloudsecurityalliance.org/group/internet-of-things/**.

Authors

Brian Russell
Chief Engineer, Leidos

Mohamad Amin Hasbini
Senior Security Researcher, Kaspersky Lab

Martin Tom-Petersen
Client director and partner, Smart City Catalyst

Contributors

Sabri Khemissa
Drew Van Duren
Brian Daly
Paul Lanois
David Jordan
Jonathan Petit
Sandeep Singh
Alan Seow
Vish Rao
Raghavender Duddilla

Table of Contents

Executive Summary

According to a **report from Tractica in 2015**, the interest in utilizing drones for commercial applications will drive commercial-grade UAV shipments from 80,000 units in 2015 to more than 2.6 million annually by 2025. The market intelligence firm forecasts that annual revenue from commercial drone hardware sales will reach nearly $4 billion within the same timeframe. However, the more significant revenue opportunity will be in commercial drone-enabled services, which Tractica forecasts will grow to $8.7 billion annually by 2025.

Drones are expected to play a key role in the smart city environment, providing support for a range of use cases: medical, transport and agriculture. These civil implementations can also be used for emergency management use cases such as critical infrastructure protection and inspection, forest fire fighting, police augmentation, coastal monitoring, and identifying changes in urban vegetation. Drones will also be used to support telecommunication services in the handling of capacity surges and the restoration of services following a disaster.

The implementation of drones in the smart city will involve multiple drone platforms that operate simultaneously to run missions. These drone systems must be safely deployed and operated, and protected against compromise. They also need to be highly available and ready to be called upon when required for a mission.

The main drone system challenges are:

- The need for drone manufacturers to improve security by integrating methodical security practices into their development and manufacturing efforts.
- Identifying and addressing the multiple points of integration within a city-wide drone system that can be used as attack vectors, including cloud-based software service.
- Establishing stabilized and standardized regulations to recognize possible measures to deal with rogue drones, evidence collection options, no fly zones, etc.
- The use of new, as yet unproven, algorithms to support automated operations and cooperation between drones.
- The fact that drones will eventually be authorized for widespread Beyond Line of Sight (BLOS), operations and security engineers are expected to plan now to protect against future threats of integrating drone systems into national airspace.

Many indicators still show vendors consider security as an added cost and prefer to offer more features over protection. It is the responsibility of vendors to establish a safe and secure environment for drones' operational quality and stability, if urbanized environments are to adopt them and benefit from their potential. It is also important for governments to implement regulations to enforce safe security standards and disallow the implementation of weak cyber security measures in live environments.

Implementing these guidelines will ensure that citizens and municipal employees are safe when drones are used. Drone use must adhere to citizen imagery and information privacy policies, safeguarding this information from disclosure and maintaining compliance with all applicable rules and regulations. Drones should be kept in a "State of Readiness" to be available to operate when needed (24x7) and, at the same time, they should be secured from physical theft during operation, maintenance and storage. This includes electronic tampering and "hijacking" over the command and control link.

Conventions

The term 'drone' has been used synonymously with Remotely Piloted Aircraft System (RPAS), Unmanned Aerial Vehicles (UAVs) and Unmanned Aerial Systems (UAS).

According to the International Civil Aviation Organization (ICAO), a RPAS is "a set of configurable elements consisting of a remotely piloted aircraft, its associated remote pilot station(s), the required command and control links and any other system elements as may be required, at any point during flight operation."

According to ICAO, an UAS is "an aircraft and its associated elements which are operated with no pilot on board". UAS can be considered as automatic aircraft, which can be programmed to fly to coordinates in support of mission parameters. In this document, we focus on the use of UAS within municipalities.

Purpose

This paper provides guidance on the safe and secure introduction and operation of a municipal "drone" program. This paper will try to analyze the drone's role and impact on future metropolitan areas, with a focus on information security threats caused by the mainstream utilization of the drone, the impact drones could have on the main municipal aspects, such as performance, efficiency and national security, and the measures that need to be taken to protect, monitor, respond to and recover from cyber security threats. We will also describe how drones can be used as an effective cyber security tool in the monitoring of a smart city environment.

Introduction

In spite of being relatively new technology, drone systems are actively being developed and utilized. They vary in size and type (air, ground, marine or mixed), which include delivery drones, hobby drones, news drones, sightseeing and surveillance drones. As UAS platforms continue to proliferate across the business and civil landscape, care must be taken by the integrators that assemble complex drone systems and the operators that rely upon them, to safeguard the public from both intended and unintended consequences. Municipal implementations require more diligence in the design and implementation of drone systems.

There are also confidentiality requirements that should be imposed upon municipal drone operations, to guard against leakage of captured private information as well as to protect against the ability for adversaries to gain access to critical system functionalities. For example Unmanned Aerial Systems (UAS) provide imagery and other sensor data to organizations that operates them across diverse industries, in the United States, the Federal Aviation Administration (FAA) has provided Certificates of Authorization (COAs) to film makers, aerial photographers and even municipalities such as the **city of Hannover, MD**. Data integrity must also be protected to guard against redirection of routes and injection of false sensor/camera data. These requirements denote security controls that should be incorporated into a drone program and its corresponding systems from the beginning, and those controls should be continuously evaluated to ensure they are functioning accurately.

Compliance mandates should also be tracked and continuously complied with - within a municipal drone implementation, operators must adhere to rules and regulations to comply with national-level legislations that restrict things like altitude and location, and requires drone operator qualifications.

In the end, securing a municipal drone system requires a similar engineering process to that required to secure other computing based systems and airplanes. Unique challenges associated with drone systems require that security practitioners be flexible in their approaches to achieving their goals.

Drone System Challenges

Drones are expected to bring many benefits to the smart city economy. Unfortunately, however, a number of challenges are delaying the large scale deployment and operation of drones, such as:

1	Drone manufacturers do not always incorporate methodical security practices into their development and manufacturing efforts.
2	There are multiple points of integration within a city-wide drone system that can be used as attack vectors, including cloud-based software services.
3	Regulations are not yet stabilized and standardized, making it difficult to recognize possible measures to deal with rogue drones, evidence collection options, no fly zones, etc.
4	New, as yet unproven, algorithms will be used to support automated operations and cooperation between drones.
5	Drones have and will continue to proliferate at an accelerated pace. This introduces new strains on municipal governments that will be required to operate in the same airspace as consumer drones.
6	Drones will eventually be authorized for widespread Beyond Line of Sight (BLOS), operations and security engineers are expected to plan now to protect against future threats of integrating drone systems into the national airspace.
7	Drones pilots can operate with a level of anonymity. It can be difficult to locate the operator as well as to identify the drone itself through visual cues.

Privacy Considerations

This paper focuses on securing drones and drone systems from unsafe or unwanted actions and activities. It is also important to note that drones can introduce privacy concerns among the public.

For example, it appears that the Singapore-based company AdNear is already using a fleet of commercial drones **to determine user locations and deliver hyper-targeted ads**. As such, municipalities should consider establishing ground rules for the collection, storage and processing of potentially sensitive data in order to alleviate concerns.

Some examples of drone equipment that could have an impact on privacy and data protection include:

- Visual recording equipment: the drone may contain equipment capable of storing or transmitting videos, live images and sound, regardless of visibility conditions (through the use of thermal cameras, etc.) and may feature facial recognition capabilities which may be used to identify and track specific individuals;
- Radio-frequency equipment: the drone may be fitted with equipment allowing the capture and eavesdropping of Wi-Fi access points or cellular stations, including the reading of transmitted text messages. The risk is no longer theoretical since researchers at the London-based Sensepoint security firm have designed software named Snoopy that **allows a drone to steal data from a nearby mobile device, including usernames and passwords for Amazon, PayPal and Yahoo**.
- Specific sensors may be used, such as optical-electronic sensors, thermal cameras, infrared scanners, synthetic aperture radars (SAR) and inverse synthetic aperture radars (ISAR) to identify objects and vehicles and obtain information on their position and course even behind walls, smoke and other obstacles.

Drones could be abused - not only for surveillance purposes; they could also be hijacked or destroyed by attackers, causing the interruption of the service they were meant to provide. Like any device, drones may be hacked and controlled by hackers. According to reports, a hacker has already released the information needed **to build a drone that can hunt and hack others as it flies - creating an army of drone zombies along the way**.

Municipalities may also be well served by evangelizing neighborly drone use among their residents, as laid out in the National Telecommunications and Information Administration (NTIA) report that details **Voluntary Best Practices for UAS Privacy, Transparency, and Accountability**.

Threats to Drone Systems

Drone systems are unique in that, because they are new technologies, they will likely be targeted frequently in attempts to cause some physical effect on the platform (e.g., forced landing, throwing off course, etc.). This significantly increases the pool of potentially malicious actors that will target these platforms. As tools are inevitably developed that make the compromise of these systems easier to achieve, those tools will find a ready set of people to make use of them.

Regarding tools, researchers and enthusiasts have already begun assembling tools that can either take control of a drone mid-flight, or perform a denial of service attack on the platform. Some of these tools have been aided by the purposeful configuration of weakened security controls - for example turning off encryption to reduce latency for command and control data. Other tools introduce efficient and effective ways to turn the infrastructure against the drone, such as GPS-spoofing attack tools.

Aside from the curiosity factor involved with drones, the ability to impact city operations will be a lure for more focused attackers aimed at causing disruption or harm to citizens and services. Drones therefore must be designed with safeguards against a wide range of threat actors and associated skill sets. Table 1 provides a view into the types of threats that municipal leaders must consider and guard against using defense-in-depth approaches.

Table 1

Item	Threat	Impact
1	Privacy zealot with gun, etc	Drone shot down
2	System error, unexpected shutdown	Drone flies off course, potentially into restricted zone (no fly), posing a threat to airlines safety, urban safety, etc.
3	Attackers man-in-the-middle (mitm) attack the Command and Control (C2) link (no encryption/authentication applied)	Drone may be hijacked and used for a variety of purposes
4	Attackers compromise the transmission security applied to the C2 link	When no additional cryptography employed on C2 link, drone may be hijacked and used for a variety of purposes
5	Weak security (encryption, authentication, unique-key for all devices) allows attackers to compromise device	Drone may be hijacked and used for a variety of purposes
6	Attacker/Rogue drone platform or large bird flies in front of drone	Assuming Collision Avoidance (CA) software, drone re-directed to new location (herded). Otherwise, drone crashes
7	Attackers spoof GPS geolocation signals to confuse drone platform	Drone will travel to a false waypoint and potentially cause harm/damage or theft of the drone and/or its payload

8	Ground Control Station (GCS) software is compromised through identified vulnerability	Drone may be hijacked and used for a variety of purposes
9	Denial of Service against C2 link	Drone paralysed and uncontrollable from command center
10	Denial of Service against Cloud link	“Connected drone” loses database access
11	Smart Charging systems are compromised	Drones are not charged and cannot be ready for flight
12	Municipal maintenance systems compromised	Drone platform compromised when connected to maintenance system
13	Drone flight controller (on-board) software is compromised through local or remote exploit	Full control of drone once taken off
14	Drone payload sensors are compromised	Bad data sent to relying systems
15	Theft of drone platform(s)	Unavailable for service
16	Identity spoofing	Drone spoofs identity of another drone to collect data, items, use charging stations or other hidden operations
17	Data leakage due to software error or misconfiguration	drone leaks data related to communication encryption, mission data, etc.
18	Drone silent compromise	Drone compromised but operations kept stable, used for spying and data collection purposes
19	Design Flaws	Attacks against insecure bootloaders, insecure firmware, etc.
20	Insecure Protocols	Protocols implemented are sometimes not secure which can allow attackers to install malicious software on the ground station.
21	Drone firmware update mechanism is compromised (e.g., attacker forces flash of malicious firmware update)	Potential to take complete control of drone platform and disrupt mission.

Examples of drone incidents

The following are examples of drone incidents over the past few years. Although this seems like a large number of examples, it is important to remember that small drone sales in the United States alone **totaled 2.5 million** in 2016. The below incidents represent a small fraction of the overall drone population, however they do signal a need to securely engineer drones and drone systems as they become more relied upon for business and mission purposes.

1 **Drone crashes near the White House**
On Monday, January 26, 2015, a drone crash landed on the White House lawn. The White House does have its own specific flight restrictions, but the drone wasn't easy to detect. Immediately after the incident, the White House went into lockdown. The US attorney decided not to charge the drone operator, Shawn Usman, after determining the drone was not under his control at the time of the crash.

2 **Drone "attack" on German Chancellor Angela Merkel**
During a Christian Democratic Party campaign in September 2014, a Parrot AR drone crashed in front of German Chancellor Angela Merkel. The drone was piloted by a German Pirate Party member as a government surveillance protest. No one was harmed, but the situation raised concerns over similar experiences with weaponized drones.

3 **Drone cuts off tip of photographer's nose**
What started out as goofy holiday promotion ended terribly when a drone crashed into the face of Brooklyn Daily photographer Georgine Benvenuto, clipping the end of her nose and cutting her chin. The drone was a promotion by TGI Fridays called "Mobile Mistletoe," and it carried mistletoe above diners prompting them to kiss.

4 **Drone injures Australian triathlete**
At the Geraldton Endure Batavia triathlon in Australia, a drone was being used to photograph competitors when it crashed into triathlete Raija Ogden, causing a minor head wound, which required stitches to close. The drone operator, photographer Warren Abrams, claims that the drone crashed after someone in the audience stole control of it from him.

5 **Drone injures bystanders in Virginia crowd**
In the fall of 2013, spectators gathered at the Virginia Motorsports Park for the Great Bull Run, a festival with live music, drinking, a tomato fight, and a bull run similar to the Running of the Bulls in Spain. During the festival, a drone being used to record video crashed into the stands, injuring several people in attendance.

6 **Drone flies too close to a news helicopter**
One major concern for consumer drone use is the potential for operators to pilot drones into occupied airspace. In Washington, a news helicopter was covering a fire when the pilot noticed a drone flying too close for comfort. Nothing happened in this particular incident, but the FAA said it receives 25 reports a month of drones flying too close to manned aircraft. Recreational drone flights are supposed to be kept below 400 feet.

7 **Drone nearly crashes into Airbus A320**
In July 2014, a drone narrowly missed colliding with an Airbus A320 as it was taking off from London's Heathrow airport. The plane was at about 700 feet when the incident occurred and the BBC reported that the Civil Aviation Authority (CAA) rated the incident as a "serious risk of collision," the top rating it can give.

8	**Drone caught carrying drugs near the border** On Tuesday, January 20, 2015, a drone carrying methamphetamine crashed in Mexico near the US border. The drone was transporting more than six pounds of crystal meth when it crashed in a supermarket parking lot in the Mexican city of Tijuana. According to the DEA, drones are becoming a common means to transport drugs over the border.
9	**Drone flies over Bank of America Stadium** Unsuspecting fans and players alike were surprised when a drone flew over Bank of America Stadium during a Carolina Panthers football game in Charlotte, North Carolina. The drone caused no harm or damage in its operation, but its operator was detained and questioned afterwards. This incident, along with similar situations, prompted the FAA to criminalize drone flight in certain areas.
10	**Drone flies over Comerica Park** The Detroit Tigers were playing against the Baltimore Orioles in a Major League Baseball game when a drone went buzzing by overhead. Being that professional sporting events usually attract fans in the tens of thousands, a weaponized drone could cause serious injury. Drones are difficult to detect and make security harder to enforce at such events.
11	**Drone crashes into Grand Prismatic Spring** A Dutch man crashed his drone in the Grand Prismatic Spring, a famous hot spring in Yellowstone National Park. At the time, park rangers were concerned that the downed drone, as well as attempts to remove it, could hurt the spring.
12	**Drone attacked by hawk** In the ultimate case of nature fighting back against man-made machines, a drone met its demise at the talons of a red-tailed hawk flying in a Cambridge, Massachusetts park. The drone caught the skirmish on its attached camera and the ensuing video went viral. While this probably won't be a common occurrence, the argument can be made that drones still pose a threat to wildlife.
13	**A series of unexplained drone sightings were reported flying over multiple areas in France overnight** In 2015, France registered some 60 drone sightings near nuclear plants and, in central Paris, over the Elysée Palace, the residence of France's president, the US embassy, the Eiffel Tower, the Place de la Concorde, the Invalides military museum and around the Paris ring road.
14	The Federal Aviation Administration (FAA) released an updated list of pilot, air traffic controller and citizen reports of possible encounters with unmanned aircraft systems (UAS). The latest report covers August 22, 2015 through January 31, 2016. Reports of unmanned aircraft have increased dramatically since 2014. Safely integrating unmanned aircraft into the national airspace system is one of the FAA's top priorities, and the agency wants to send a clear message that operating drones around airplanes and helicopters is dangerous and illegal. (**http://www.faa.gov/uas/resources/uas_sightings_report/**)

Municipal Drone System Operational Security Goals

Security goals drive the controls that must be put in place to defend a system. Smart Cities should strive to achieve the following goals for any drone support system.

1	Keep citizens and municipal employees safe from harm caused by drones
2	Keep citizen imagery and information private and safeguarded from Disclosure
3	Keep drones in a “State of Readiness” to be available to operate when needed (24x7)
4	Secure drones from physical theft during operation, maintenance and storage
5	Secure drones from electronic tampering and “hijacking” over the command and control
6	Maintain compliance with all applicable rules and regulations
7	Maintain understanding of latest threats and vulnerabilities and keep systems up to date
8	Maintain stable operations through incident response and contingency planning

Drone System Cyber Security Needs

Drone systems are similar in concept to many other types of Information Technology (IT) systems in that there are endpoints, communications channels, messaging constructs and backend systems that process and store data. Smart cities that are working towards establishing a drone program will need to incorporate security activities throughout the life-cycle of that program - from planning to operations. Figure 1 provides a view of the activities that those implementing an integrated drone system will need to consider across the lifecycle of that system.

Figure 1

Planning	System Design	Acquisition	Integration/Test/Deployment	
Establish Governance Framework	Threat Model	Platform Security Verification	Authentication & Authorization	Assure Availability
Policy & Compliance Management	Privacy & Safety Impact Assessment	Service Provider SLAs	Secure Communications	SF/WF/Patch Management
Establish HR Security & Personnel Security Guidelines	Operational Data Flow Protection Model	Software Selection	Secure Data at Rest	Logging, Monitoring, & Auditing
Establish Change Control Board (CCB)	Drones Control Data Protection Model	Inventory Management	Quality Control	System-Wide Penetration Tests
	Drones Misbehavior Alerting/Incident Response Model		Funcional Security Tests	Incident Isolation & Response
	Resiliency		Funcional Security Tests	Incident Isolation & Response

Planning

At this stage, city leaders are establishing the specific use cases for their drones and creating guidelines by which those drones must operate. A key aspect of this planning is identifying and documenting the national level regulations that drone programs must adhere to during operations. The regulations that apply are based on the location of the city.

At a global level, the UN International Civil Aviation Organization (ICAO) establishes standards for unmanned aerial systems. The US, EU and other regulators can incorporate these standards into enacted regulations.

Within the United States, the Federal Aviation Administration (FAA) provides rules that must be followed - specifically the small UAS (sUAS) rule, part 107 which became effective 29 August 2016. The Federal Communications Commission (FCC) Technological Advisory Council (TAC) is also working on **documenting the implications for Mass Deployment of Aeronautical / Space Transmitters**.

In Europe, it is the EU agency EASA (European Aviation Safety Agency) that is responsible for the work with harmonizing the flight safety rules and standards. It is the task of EASA to transform the existing JAR rules (Joint Aviation Requirements), adopted in the JAA, into EU Regulations which will become directly binding on the citizens of the EU member states. Furthermore EASA prepares rules in the areas that are not yet covered by JAR rules. Finally, the European organization EUROCONTROL is preparing harmonized guidance for the use of the European airspace. EUROCONTROL provides advice and guidance while the EU Commission drafts standards in this space.

Table 2 provides a summary of other national rulemaking.

Table 2

Country	Regulation	Link
United States	sUAS rule, part 107	https://www.federalregister.gov/articles/2016/06/28/2016-15079/operation-and-certification-of-small-unmanned-aircraft-systems
Denmark	Amendment to Law on Aviation, effective 1 September 2016	http://www.trafikstyrelsen.dk/da/~/link.aspx?_id=20BA60F4CC044ADDACFCE16F1359D230&_z=z
European Union (EU)		https://www.easa.europa.eu/system/files/dfu/A-NPA%202015-10.pdf
France	17 December 2015 from Ministry of Ecology, Sustainable Development and Energy	http://www.developpement-durable.gouv.fr/IMG/pdf/jo_pdf_frame-conception.pdf http://www.developpement-durable.gouv.fr/IMG/pdf/jo_pdf_frame-condition.pdf
Netherlands		https://www.ilent.nl/onderwerpen/transport/luchtvaart/dronevliegers/
United Kingdom	Article 94	

Establish Governance for the Drone Program

The appointment of a senior government employee as the Drone Security Officer (DSO) and providing that role with the resources required to carry out the activities identified in this document is a first step. The Drone Security Officer should be accountable for the safe and secure operation of all drones in the municipal fleet. The governance principles of the drone program should be established to sufficiently assure the protection of privacy and defense against cyber threats. If the need arises for drone take down, the party involved should provide the necessary reasons and seek approval from the DSO before taking action. The same governance needs to be established for the adoption and development of technologies, maintenance fulfilment and human resource security.

Agencies within a geographic area should also focus on cross collaboration should an emergency arise. This can be accomplished by agreeing on governance standards at the executive levels of the municipalities.

Establish a Policy Management Framework

The city leaders must establish policies for drone system operations that flow down from the applicable regulations and are used as the basis for configuring safety controls, and mission management systems as well as training drone pilots and other stakeholders on proper operation and incident handling. Rules and regulations developed at national level are sometimes augmented by local rules as well, so these should be considered when identifying regulatory authorities. Mission management software used for route planning often provides the ability to configure parameters that will be obtained from those rules and regulations. For example:

- Setting a flight ceiling at x feet,
- Setting geofence areas that drones are not allowed to enter,
- Actions to take upon a lost link, etc.

As these regulations often flow down into configuration settings within the drone systems, the implementation of proper change control procedures is critical to ensuring that configurations are not mistakenly or maliciously changed. The modification of some safeguards within the system could result in the drones not operating in the intended manner.

Establish Personnel Security Guidelines

Insider threats are a significant concern within a drone system, given the ability of drone platforms to inflict damage or harm to citizens and property. Guarding against insider threats is possible through monitoring activities, establishing processes (e.g., CCB, etc), mandating two-person integrity for flight operations, in addition to threat awareness training for the corresponding personnel.

Establish Configuration Control Board (CCB)

One of the best ways to ensure high level policy frameworks are adhered to is to review and approve all changes to the configuration of drone systems. As such, a Configuration Control Board (CCB) should be established to:

- Review and assess any proposed configuration changes
- Direct updates to configurations, based on modified or new regulations

Maintaining compliance with regulations requires that configurations be reviewed on a regular basis. Configurations should be reviewed prior to every flight (e.g., Pre-flight checklists) and any identified anomalies should be recorded and reported immediately to the drone security officer.

Integrated System Design

Municipal drone systems can become quite complex with multiple drone platforms (from different vendors), flight management software, charging systems, communication links and interfaces to/from various data systems. Systems such as this must be designed prior to integration and security activities must feature prominently within that design.

Threat Model

Threat modeling activities will assist in identifying the unique threats to your city's implementation. This is critical to understanding the mitigations that must be applied to keep the drone systems safe and secure.

Privacy Impact Assessment

Drones are essentially flying cameras. However they also provide a platform for the use of other sensor technology. It is important that citizens are made aware what the uses for imagery and other data captured by drones flying over them or their property are. Notification is essential for a municipal drone program - provide notification through as many means as possible.

Defining what data (e.g., imagery) can be used for is also important, as is outlining any data sharing agreements and disposal procedures for data.

Municipalities may also want to consider citizen concerns regarding encroachment on their private spaces. For example, municipal drones flying over rooftop pools, near home windows or over backyards.

Safety Impact Assessment

Drones are considered a Cyber Physical System (CPS) because of the integration of the physical and electronic world. This means that someone who takes control of one of these platforms can use it to fly into a victim, a car, etc. in an attempt to cause havoc or destruction. Additionally, having an adversary take one of the drone platforms offline (e.g., denial of service) could also have safety ramifications if the intended mission cannot be accomplished.

Therefore it is important to conduct a safety impact assessment to define what could go wrong from a safety perspective and, if necessary, design redundant safety controls into various aspects of the drone system.

Resiliency

Resiliency supports the ability to continue operations even in degraded modes. For municipal drones, continued operations should be achievable for short periods of time, in order to support return to launch or other designated waypoints. If a drone detects, for instance, that a failure is imminent, the drone is programmed to return to a designated coordinate. The same should be possible if the drone or some other component within the drone system detects a potential cyber-attack.

Acquisition Security

The protection and validation of new devices is a necessity for the protection of the whole drone platform. Devices need to be monitored while being shipped, and mechanisms should also be utilized to verify against tampering and implants upon arrival.

Platform Security Validation

Work with drone platform vendors to understand the security controls that were put in place during the development and testing of the platforms. Give preference to vendors that have:

- Established secure development methodologies for their drone offerings
- Incorporated FIPS 140-2 approved cryptographic libraries to support encryption, authentication and integrity controls
- Incorporated 3rd party testing services to validate the security posture of their systems
- Made available software/firmware/patch management services to quickly update purchased drones

It is also a good idea to understand what open source libraries may have been employed within a drone platform. This allows security administrators to keep up to date on vulnerabilities that may affect modules within the drone and patch them as necessary.

Service Provider Security Level Agreements

Work with any cloud service providers (SaaS) to create security level agreements. Depending on the nature of the provider, agreements may include topics such as:

- Availability expectations
- Access to data for monitoring purposes
- Provision of support during incident response activities

Software Selection

Technology and application selection is when organizations want to find a solution that will be implemented on a metropolitan scale. The software selection phase is important for the operational stability of the drones program, as technology should be chosen with proper cyber security controls and defenses in mind, when municipalities consider the desired functionalities and features, they also need to consider attack and damage possibilities.

More on technology selection for smart cities can be found in a previously published document "**Cyber Security Guidelines for Smart City Technology Adoption**."

Inventory Management

Municipalities are faced with additional cyber security challenges due to the requirements of transparency in the procurement process. The procurement process discloses the architecture of the technology base publicly and available for all to study in detail (for example, requirements that the municipality post the RFP/RFQ to a website). This means that potential attackers can study the technologies employed and operational schedules in drone systems, to be include the drone platforms themselves. Municipalities must be able to act quickly when new vulnerabilities in their installed base are discovered, as attackers will be able to quickly capitalize on vulnerabilities that are exposed in technologies that are prevalent within an organization.

Municipalities should establish drone tracking programs that break out the different technologies associated with each individual platform. As new vulnerabilities are discovered, this inventory database should be consulted to determine whether new updates/ patches to the drones or associated technology are required.

Municipalities should also consider having spare drones with fresh batteries available in the case that an operational drone is lost or unable to complete the mission. These hot spare drones should be managed by the municipality and held at a secure location.

Integration / Test / Deployment

Establish Authentication and Authorization Procedures

A drone system is a complex integration of hardware, software and cloud based services. Flight Management Software provides route planning while interfacing to services that may provide navigation databases (e.g., latest geofencing databases), weather information and other data. Implementers must guard against the ground controller being spoofed (e.g., GCS/ Flight Management Software), which, without proper authentication controls on the drone platforms, would enable an attacker to take complete control of the drone. It may also be feasible to install immobilizers that re-route rouge drones.

Data collected by drones may be offloaded post-flight to cloud-based services that provide 2D/3D modeling, data analytics and other services. Even charging systems that may be spread throughout a city are vulnerable to theft-of-service if they do not properly authenticate the drone that is requesting a charge.

Each of these interfaces should require authentication and authorization controls. Methods for achieving this through PKI-based certificates (e.g., X.509) would support the implementation of two-way Transport Layer Security (TLS) between the system, ideally with two-way authentication (client and server both present certificates for verification). Protocols such as OAuth 2.0 can also be used to establish token-based authentication through a system such as this, and this approach is well suited when dealing with 3rd party cloud providers.

It's important to understand any potential configuration weaknesses within authentication/ authorization schemes and work to mitigate those weaknesses. Storing secrets/private keys associated with authentication transactions securely is critical, and it is essential to consider how this could be accomplished on each server, workstation and drone platform involved with the drone system.

Whichever technical approach is implemented for a particular drone system, it is important to integrate the authentication and authorization techniques within existing Identity and Access Management systems whenever possible. Also note that this applies to both physical and logical access requirements, and for certain roles should require two-person integrity controls to be put in place. Ideally, the integration of Physical Access Control Systems (PACS) with Logical Access Control Systems (LACS), tied into a Security Information Event Monitoring (SIEM) system would provide a foundation for monitoring the actions of anyone involved with the drone program.

Monitoring should also include the recording of anyone that has logged into any of the drones or drone systems.

Flexible Policy Management

Drone systems are dynamic in nature, with many people involved in the operation and maintenance of the platforms and supporting infrastructure systems. In addition, new capabilities and features will be developed to allow drones to communicate with each other (e.g., platooning) and with new cloud services. Municipalities must implement flexible policy management capabilities to support dynamic authentication and access control decisions.

Secure Communications

Drone communications are often segmented between command and control data, telemetry and video, with different security mechanisms applied to each. This is often because of the larger bandwidth needed to support the transmission of video. Drone C2 data is transmitted at various frequencies depending on the country of operation. Within the United States, drone C2 is often conducted at 915 MHz or 2.4 GHz. Telemetry data is often transmitted from the drone, and video is often transmitted from the drone at 5.8 GHz.

In the case of the link between a pilot and a drone being taken offline, drones should be programmed prior to flight with lost link procedures. These procedures, often programmed into the flight management software, should give the drone the information it needs to return home (or to some waypoint) safely in the event that communications are lost.

Note that in many cases the drones may fly semi-autonomously, relying on location tracking (e.g. GPS) to navigate towards the next programmed waypoint. GPS plays a vital role in drone operations. Procedures for what should occur when access to GPS satellites is no longer accessible should also be programmed pre-flight, alternative location tracking solutions should also be considered.

4G/LTE and in the future 5G cellular networks will be used to support drone command and control. Although drones may make use of the security features enabled by these networks, it is the responsibility of the drone manufacturers to ensure that make efficient use of the network security services. APIs between Flight Management Software and various 3rd party support services will also be implemented. Services that provide data for consumption by the flight management software often provide critical information to be used in route planning.

Encrypt all interfaces within the drone system using acceptable cryptographic algorithms for your country. It is advisable to encrypt data using the public keys of the municipality systems to restrict access to that data from unauthorized sources.

Municipal Drones Database

Drone systems need to be well monitored and controlled, a national database needs to be established to document and record all drones inventory, serial numbers, hardware and frequency channels, historical activities and operations. For example, in the United States the **sUAS Registration Service** exists for registration of aircraft that weigh between 0.55 lbs and 55 lbs. All this information needs to be consolidated to ensure the responsibility and accountability of drone operators. The database could be actively utilized to find vulnerabilities, anomalies and incidents, but also used in investigations as evidence. The database should

be able to store tracking and operational data sent by the drones themselves and also from external monitoring systems such as radars, which could be used to detect the misbehavior caused by cyber-attacks or firmware manipulation.

Secure Data At Rest

Operational data, and imagery data can be stored on the drone (e.g., SDCard, etc.) and should be encrypted in case the drone is lost and seized by someone. Encryption could be based on asymmetric encryption algorithms requiring the involvement of Command and Control centers in the decoding of the corresponding data upon startup, which would enforce drone data to be accessed only after communication with command center, supporting the program safety.

Functional Security Tests

Security engineers should identify a set of functional security requirements to apply to the municipal drone system at the planning stage. The output of the threat model will provide an opportunity to establish these functional security requirements (e.g., encrypt transmissions, authenticate messages, etc.). For each security requirement, create a set of tests that can be run (preferably automatically) once the system is integrated. Run these tests on a regular basis to ensure system security controls are functioning as expected.

Review 3rd Party Code

3rd party modules may be installed upon drone platforms and these could be used to perform additional functions and provide features. Performing a test and security assessment of each code-base prior to installing it on drone platforms is important to verify the drone's stability and to identify risks. Additional features could be useful for the drone program, but might introduce vulnerabilities and threats. It is also important to regularly keep track of new threats and vulnerabilities being introduced in 3rd party codes and mitigate them in order to avoid security risks.

Assure Availability

Drones are expected to offer services to satisfy urban, municipal and commercial needs, substituting other services that require more time and cost. To succeed, these services require sustainability and resilience for the stakeholders to trust the service, knowing that problems can arise, but solutions and readiness are available to recover and sustain a certain quality of service. Ensuring and assuring availability in drone systems is critical for the survival and adoption of any drone program.

Location Tracking Assurance

Signals such as GPS and GLONASS, commonly utilized for location tracking are not secure or authenticated, therefore easily spoofed. In the case of municipal drone systems, alternative location tracking techniques need to run in parallel. Examples include tracking through cellular networks (e.g., mobile tower IDs), WIFI signals database, Geographic Information Systems (GIS), RFIDs or even custom solutions with location towers distributed over a metropolitan area.

Safeguarding against Communication Channels Disruption/Jamming

Jamming signals could be the cause of service disruption and denial of service for drone systems relying on wireless communication. The monitoring of jamming signals could be performed by systems planted in the regions where drones are operational. The same could be done by drones themselves, but could be limited, requiring additional instruments such as backup frequencies or communication equipment, emergency backup routes, etc.

Maintain Integrity Controls and Guard against Malware

Integrity controls are a core feature of any modern digital system. They represent the measures in place to promote, monitor and maintain integrity, protecting the quality and sustainability of drone system operations, thus minimizing compliance and policy violations. There is much utilization of integrity controls in the context of drone systems. Examples include the integrity protection of navigation databases (e.g., route planning, geofence instructions, no fly zones, emergency routes). Another example of integrity controls is the monitoring of drone platforms and flight management systems for rogue system modifications, malicious applications or updates, 3rd party compromised plugins.

Software/Firmware/ Patch Management

The drone program and the systems belonging to it are all operated by software, programmed to control, manage and protect the different aspects of the program. Software integrity is vital to make sure a drone program is safe and trustworthy. Integrity verification controls should be in place and part of drone program routines, to make sure drone program data, assets, operators, and control centers are all well protected and safeguarded. Integrity verification controls could be applied to device firmware, update sources, and patch management functions. Proper change management functions should be in place when applying any change in software/firmware.

Monitoring

Monitoring for drone system security events requires blending both physical and logical analysis.Monitoring should alert security administrators to activities such as:

- Performing reconnaissance of the drone system, both electronic and physical, to identify potential weaknesses in system design
- Changes to configurations within Flight Management Software
- Changes to configurations on the drone platforms
- Additions/deletions of user accounts on drone (including cloud) systems
- Changes in privileges associated with any accounts within the drone system
- Log-ins to the drone and mission planning systems

It is expected that municipalities will make heavy use of cloud services (SaaS) associated with drone operations. Whenever possible, gaining access to instrumentation data from the cloud service provider to correlate with events occurring locally will provide the greatest degree of situational awareness within the system. Work with your cloud provider to identify what data can be exported via API to your SIEM system for monitoring.

Further research may be required in the area of misbehavior detection for drone systems. Similar systems to those being developed for Connected Vehicles should be considered for sUAS.

System-wide Penetration Tests

Prior to deployment, and once deployed, penetration testing can thoroughly identify weaknesses in the security controls, procedures, training and staffing within the drone program. Perform penetration tests at least annually after operations commence.

Incident Response

Establish Incident Management Procedures

Information services development and propagation requires cyber security issues to be monitored. Information security incidents, should they occur, should be reacted to appropriately to control, contain and mitigate threats. Establishing incident management for the municipal drone program, requires the development and legal adoption of city wide policies and procedures for identifying the corresponding teams that manage, assess and respond to cyber incidents, examples of such include cyber-attacks on the infrastructure and compromise of drone machines. Monitoring and reporting procedures also need to be formalized, reporting on incidents could be done through device management solutions (reachability, integrity checks, controllability, etc.) or by citizens reporting misbehavior that they witness.

Incident Planning

An incident response is usually guided by a plan that aims to manage the cyber security incident in such a way as to limit damage and reduce recovery time and costs.
An incident response plan is expected to:

- Defining roles and responsibilities for the planning and integration of the incident-response efforts across the program technologies and geographies. Ensure that all staff members understand their roles and responsibilities in the event of a cyber incident
- Ensure staff is well trained and best prepared for incident response. Extensive training and simulation of real-world scenarios will enable the fine tuning of staff capabilities and performance
- Ensure redundancy among the incident response staff, especially for critical roles
- Develop a classification of risks, threats, and potential failure scenarios, to be continuously updated
- Train the relevant teams on incident scenarios, especially the most common ones
- Establish clear guidelines for making major decisions, such as when to isolate compromised drone systems or even areas of the network
- Maintain service-level agreements and relationships with external providers, vendors, experts and law enforcement
- Ensure the continuous development and availability of the response plan documentation to the relevant parties

Establish Citizen Alerting System

As drones will be enabled and operational inside urban environments, the implication of misbehavior or incidents can affect urban and human safety. All the city stakeholders are expected to be involved in the monitoring of incidents or suspicious behavior related to drone activities and will need efficient tools to report these issues as soon as they happen.

Incident response capabilities

Drone programs will need advanced tools to enable the response against incidents with drone systems, including, but not limited to the following:

- Backup routes: in case of disconnection from the command center due to cyber-attack or hardware/software issues, the drone needs a backup route, where it can go back to its source station without the need for communication with the command center.
- Incident response drones: in the case of an incident, special drone systems should be ready for the isolation and identification of the threat type and source. Drones should also have enforcement capabilities such as the ability to take down a drone, through jamming, or physical isolation (drone catchers).

Contingency planning

A contingency plan is an organized effort involving plans, procedures, and technical measures that enable the recovery of systems, operations, and data after a disruption. This is required in drone programs, as the drone mission quality, safety and availability are essential for the adoption of these platforms. A contingency plan for drone programs includes the following components:

- Conduct impact analysis, to identify and prioritize information systems and components critical to the survival of the drone program mission and functions
- Identify preventive measures which could be taken to reduce the effects of the drone system disruptions, increase availability and reduce costs
- Create contingency strategies, to ensure that the systems and missions can be recovered quickly and effectively following a disruption
- Develop a contingency plan with detailed guidance and procedures for restoring an affected system, a function or a mission
- Plan testing, training and exercises, to validate capabilities and ensure readiness of systems and staff
- Plan maintenance, with continuous updates to reflect on new threats and organizational changes

Contingency planning is especially important in drone based programs. Since they act as links between the digital world and the physical world, their missions could be critical for urban safety, economic and ecological stability. A contingency plan generally includes one or more of the following approaches to restore disrupted IT services:

- Restoring operations through staff intervention
- Restoring operations through alternate locations
- Recovering operations and missions through alternate equipment, technologies and routes

Delivering cyber security through drone systems

One of the major challenges in modern regions and smarter cities is the sustainability of secure environments where systems are patched and devices are controlled. Monitoring large numbers of sensing devices cannot be done manually, it has to be automated.

Another benefit of establishing a secure drone system is the utilization of its features to drive other advantages, such as dealing with cyber security issues and incident response. The use of different drone sensors would also be highly efficient for mapping issues with location data, and photos. This must be done in collaboration with assigned information security teams in the city, such as the Computer Emergency Readiness Team (CERT) or similar.

The following issues could arise in future cities with large numbers of sensing systems:

- **Rogue systems:** a rogue tower or access point is usually set up by an attacker for the purpose of sniffing wireless network traffic in an effort to identify interesting information or gain unauthorized access. This would include low range signals such as Bluetooth or Wi-Fi, or longer range such as mobile tower transmissions (2G, 3G, 4G, etc.).
- **Rogue drones:** a rogue drone is one that is compromised or facing operational disruption, leading to random or rogue behaviour that could be of danger.
- **Jamming systems:** a jamming device is usually set up by an attacker for the purpose of disrupting wireless signals; they could operate using a portable source of power such as batteries. In the case of modern or smart cities, jamming signals could cause total blackouts in regions fully dependent on wireless signals, and this could be compared to a denial of service, or, in cases where attackers place multiple devices around the city, to a distributed denial of service.
- **Vulnerable systems:** misconfigured, unpatched or obsolete systems could be the cause of damage, including data sniffing, manipulation or unauthorized access to secure networks. As sensor systems get distributed, monitoring these in an effective way is essential to maintaining the overall stability of city operations.

Municipal drone programs are highly beneficial for the monitoring of city sensing operations. While unmanned aerial systems fly over large regions for targeted missions, their sensors could be actively utilized to drive other advantages, such as identifying cyber security issues. Drones could have sensors for ranges of frequency that are commonly utilized by the city services such as Wi-Fi, mobile, and the military.

Drone systems could help in identifying **rogue signals** while hopping around regions and report these to connected command centers (direct send or stored and then uploaded upon arrival), such data could be also be matched with geolocation data. Command centers are then expected to correlate signals and their geolocation data using predefined databases, to identify unknown/rogue sources.

Rogue drones need more attention. An unknown drone could be utilized to cause damage or spy on facilities. They need to be identified through specialized radars that are connected to a municipal drone system and able to identify and correlate drone systems, helping in the identification of unknown/new devices. On the other hand, rogue drones could also be compromised devices, where the identification and isolation could be more difficult. Such devices first need to be identified as compromised by the municipal drone system (unresponsive and unknown behavior). Then, an alert is sent to the corresponding unit to initiate incident response.

The **rogue drone** issue can also be addressed with so-called black-out zones. Black-out zones are special areas nearby public places (stadiums, elected official inaugurations, parades, travel portals such as airports, train stations, bus stations, ports, etc.). In some city areas, smart city administration should require the capacity to deploy mobile black-out units that can be quickly provisioned to secure events or incident sites.

That said it may not always be best to use RF black-out technology as a shield. An anti-drone system could be a sensor, based upon a software defined radio architecture, which can map out the RF environment of the protected area and then look for anomalies, very much like sensors today (IDS, IPS, etc.) create logs and send them to a SIEM for correlation.

The SIEM would then generate an alert which would lead to action – this could include initiating RF black-out transmissions, surgically targeting the intruder drone's telemetry channel with RF jamming, or launching an observation or defense drone, etc. A smart city needs to not only authorize planned drone traffic, it must also be able to police that drone traffic including rogue drone deterrents and interdiction in a similar way that land based traffic management and policing takes place.

In the case of **jamming signals**, they could also be proactively identified and located by drones, a challenge in this case would be the ability to report findings to command centers while staying connected and receiving instructions through the network.

In the case of **vulnerable systems**, drones could be used proactively to track down misbehaving sensors to identify possible issues such as jammers. Reactively, signals broadcasted by the sensors or wireless transmitting devices can also be correlated with geolocation to identify weak configurations (such as in Wi-Fi), or outdated devices that could cause abuse by attackers.

Drones can also support incident response for other connected systems. For example, drones could be dispatched as a result of a misbehavior investigation performed for connected vehicles (e.g., in order to check signal/GPS at location before dispatching a human team).

Overall, utilizing a municipal drone program is beneficial for cyber security. It identifies and locates issues, validating and verifying the overall status of the city's sensors and systems.

Conclusion

Drones are expected to play a major role in future smart city environments. For the municipalities to adopt large scale drone programs, and for society to embrace them, drone systems need to be safe, stable, resilient and sustainable. Many indicators still show that vendors consider security as an added cost and prefer to offer more features over protection. It is the vendors' responsibility to establish a safe and secure environment for the operational quality and stability of drones, it urbanized environments are to adopt them and benefit of their offerings. It is also important for governments to implement regulations to enforce safe security standards and disallow the implementation of weak cyber security measures in live environments.

The future of drone systems is highly promising, with soaring expectations, the proper development of drone systems will empower its trust and adoption by society, enabling functions and benefits that no one thought of, just few years back.

This paper provides guidelines on the safe introduction and operation of a municipal "drone" program, analyzing the drones' cyber security role and impact on future metropolitan areas, with a focus on information security threats. The document also addresses the role drones could play in delivering cyber security capabilities.