ADVANCED CYBER SECURITY CONCEPTS

**Physical Security Development Environment Task**

Omar Salih

horizontal line

# 20140620_Drones3.jpg

### Facility location in dangerous locations 3

### Facility Security 5

### Media Security 6

### Intelligence, Surveillance, and Reconnaissance (ISR) 8

### Biometrics 11

### 

### Facility location in dangerous locations

In 2014 Nigeria became the largest economy in Africa. Nigeria is half the size of the United States population, 170 million to be exact. These are alluring facts to foreign consumer-facing companies’ and investors. Kano, the capital of Kano State in northern Nigeria, is the second largest city in terms of population, after Lagos. Lagos tends to be a great place to enter the Nigerian market, because of its population of 20 million with a more developed infrastructure for its business ecosystem to rely on. The problem with entering the Nigerian business scene in Lagos is that you will be entering as a market saturated with wolves, meaning you will be a sheep among wolves. Lagos business scene is more competitive compared to Kano's.

The Northern Nigeria region does have great potential outcomes for cash and carry wholesale style businesses, as well. Shoprite, A South African retailer, opened its first outlet in Kano in early 2014. Shortly after, Massmart did the same as well, despite potentially imposed security risks by Islamic militants that have a stronghold of the region, as Mark Turner the Massmart Africa director stated. He was quoted by Reuters when he was at the Africa Summit saying that he thinks that really “you can’t be in Nigeria without being in Kano.” Further supporting doing business in Northern Nigeria is the fact that the African Development Banks report that is entitled *Tracking Africa’s Progress in Figures*, reveals Kano to be one of Africa’s fastest-growing cities. Nigeria is notorious for violent and non-violent crime, such as economic crime, financial crime, advance fee fraud, money laundering, terrorism, cybercrime, rape, police brutality/hostility, high way robbery, bribery and finally corruption. Therefore, Northern Nigeria does sound like a robustly active in many aspects and sounds like a very exciting and lucrative place for a team to operate.

One thing that is a must to consider, is the safety of all company property, physical and none, as well as the safety of all personnel, as well. To ensure employee safety some sort of multipronged security protocol would be necessary for such an environment. A security team would be necessary always, they would have the sole responsibility for implementing and enforcing security protocols. One of the best ways to approach such a chore is to think about how someone would have to protect a high-value entity from the way of out-to-in. The first line of defense would have to consist of the facility physical location itself. Depending on the type of business, it might be very limiting to where you can consider.

For our current purpose of conversation, let’s consider a huge data center that houses valuable, sensitive and highly confidential data, that happens to be in Northern Nigeria. The facility would best be situated on the outskirts of Kano, to ensure the facility is situated in favorable clear visibility in all directions of the facility. Ideally, the facility would be situated so that it has at least a couple miles of clear visibility in each direction radiating from all walls, to ensure that there aren’t any visual impairments.

The security team should be required to implement, as a first line defense, a multi-high wall defense with limited, monitored and controlled entrance(s) access to the facility. The walls, driving up, needs to be constructed with reinforced concrete, that is sufficient to withstand the impact of a heavy vehicle, it should be utilized to guide cars thru a 24-hour manned security checkpoint. The inner wall should consist of an electrified chain link fence with barbed wire at the top, to run around the perimeter of the facility walls, with one gate for entering and exiting the premises. The security team should consist of former soldiers, if possible, for security details. They will be armed and stationed at all entrances with snipers, or watchtowers, at the corners of the facility. Towers will also be equipped with anti-drone and human population neutralizing technology(s) to immobilize any unfriendly activity. Additionally, drone surveillance will be active all day, 24 hours 365 days, to protect from any chance of clandestine activity, such as tunneling beneath the data center. There needs to be ground penetrating radar (GPR) surveillance that constantly monitors the ground for such activity, as well.

For the security of the facility VIP Nigerian and any non-Nigerian employees, they will be required to be housed within the walls of one of the data center village condo complexes. These complexes will have the same security protocols as the facility itself. All employees will be transported to and from work in an armored chauffeur-driven SUV. Drivers will be well versed in all the company security protocols. All others that choose to live beyond the data center property will be required to abide by the company personnel private residences policy, which requires they always have an activated and monitored company-approved security system. All personnel will be accompanied by an armed plain-clothed security officer when leaving from or entering the facility, as they certainly would be high-value targets for kidnappers looking to collect ransom or access to the facility.

All personnel will be strongly authenticated with facial recognition, a fingerprint scan, ID cards and entry of a personal identification number code (PIN). All personnel will be required to wear a company issued ID, plainly visible attached to the front of the chests or worn around the neck always, except when they are in their own personal living space. These ID’s will have chips embedded in them so that the facility managers are able to locate employees, monitor productivity, as well as monitor work ethic.

### Facility Security

The ability that IoT HVAC devices offer is to be able to continuously monitor conditions which allow for the quick response by technicians, engineers, and system managers, should equipment misbehave. Maintaining a constant temperature and humidity is crucial to the functionality of electronic equipment, including servers housing data within the facility. A connected system detects any unapproved change(s), defects or issue(s) that may arise, and signal the appropriate personnel to resolve the task that has derived from the original plans. As well as, offers the opportunity to run diagnostics remotely using a mobile device, saving on costs, time and energy. To help mitigate the threat of malicious hacking, by a competitor, employee, a foreign government or a malicious person(s) attempting to sabotage the server farm, any IoT systems utilized on the premises will be required to be connected to an encrypted secure wireless or wired communications.

One of the first prongs of security, devices functionalities shouldn’t be on always, unless it is being actively used. When it comes to IoT, many people perceive just because something is an IoT device, that it must be connected to the internet. If you aren’t utilizing the online functionality of that device, then that function should always be in the off position. It is good practice to create a separate network for your IoT devices to separate them from your day to day traffic and even your guest traffic as well. This way guests can’t connect to the same network as the companies traffic, therefore keeping that traffic on par with any proprietary data being communicated to the secured connected signals at the farm. Thru firewall segmentation, guests cannot gain access to any of the companies shared files, documents or devices that are on the network. This kind of separation also works well for IoT devices that have questionable security. To go a step further, it is always in everyone’s interest to have a firewall, and a Virtual Private Network (VPN) as well, after the modem but before the rest of the intranet, so that device(s) are protected from outside “bad” elements. Another way to secure your IoT devices, most importantly your network, is by implementing a good strong password system.

It is very good practice to give every device a different very strong password that’s to be changed every few weeks. Traditionally, when a hacker gets ahold of one password, they try it on all devices and accounts associated with that user, company or entity to penetrate them. Therefore, reusing passwords is not a good idea. Since most people have too many passwords to remember, it is strongly urged that people start using an encryption and passkey secured password management system. Turning off Universal Plug and Play (UPnP), making sure to have the latest firmware, be wary of how cloud services are being utilized, keep personal devices out of the workplace, track and assess devices are some of the other good practices that should be considered, to keep all IoT and work ecosystems copasetic and secure.

### Media Security

As for how to manage the risk of data storage, media should always be well labeled with what data is being stored there, and when media is stored it should contain some form of code that explains data’s range of confidentiality level. If data is stored electronically, the data file will require a level of permissions to be set as well. Setting permissions levels should be done once it is determined what level of security is required. This will eliminate any risk of improper viewing of the media by people who shouldn’t have access to the data. Confidentiality should range from being public domain to being top secret. Encryption of the data will be required for any data that is labeled secret or top secret. Those type(s) of data should be locked with some form of not easily hackable form of a lock. The lock can check identity and access control requirements, for personnel to gain access to the data. If data requires being stored behind physical controls, depending on the confidentiality level of that data, the lock should require different levels of security. It is strongly urged that each data be required to be scrutinized by the facility faculty along with the client if it is appropriate to consider whether to use facial, retinal, finger scan, FOB, passkey or require a combination of one or multilayered authentications required, to enter the physical premise of the secured stored data. People that have access to the data that requires such measures to secure it, should go thru the same style of vetting before gaining any access to any secured areas of the datacenter. The datacenter physical control policy, of media, also includes requiring conducting inventory checks. It is important to know exactly what inventory is available when implementing a media library system for individuals to check in and out media.

Transport of media containing sensitive information would require a strict protocol. Designated personnel will be allowed to transport sensitive data after being susceptible to record keeping and possibly transport of the media in a locked container. It is easy to erase data, but it is tasking. To destroy stored data will require overwriting the media multiple times. By overwriting the data once, it is possible to patch the information again, by recovering what’s left behind. Therefore, to fully sanitize the storage medium it is necessary to overwrite the media multiple times to ensure there is no way any of the data leaves fragments that can be harmful if leaked. An easier way to make sure nobody can gain access to sensitive data is by encrypting the storage and get rid of any public key that has access to the data. There are other ways to make sure that sensitive data doesn’t leak out using equipment, software, and procedures that can be implemented for media sanitization. The most important thing though is to test it first, to ensure data containment.

Authentication, the key to verifying someone’s identity on the internet, is the process of determining an entities identity and if they are who they claim to be. The most popular version of authentication today is the process of two-step authentication, meaning identification is the first step followed by authentication. There are three basic methods to authenticate factors. The first method, to authenticate the person in question would require possessing something they know, such as a password. The second method, something they have in their possession, such as a hardware token. Finally, something they are or something they do, such as fingerprints, palm scan, facial recognition and eye iris patterns, or where they are, such as the location of an individual. Some utilize a fourth method to verify an individual. IP address authentication reveals what machine is attempting to connect or enter into the system. Strong authentication consists of requiring the authenticating entity to provide two factors at a minimum. It is important to remember, never to require two of the same type of factors to verify, such as a password and PIN, iris and fingerprint, FOB and mobile device, because they are not strong authentications. The reasoning is since two of the same form factors cause security flaws in the physical security protocol.

Public and private organizations utilize multiple prongs of open source security solutions and standards that can be implemented to authenticate entities identities. UMA, SAML, Shibboleth, and OpenID Connect all enable strong authentication. For example, OpenID Connect is one of the standards out there that enables strong authentication thru 0Auth 2.0. It is an extension used for authentication. As for SAML 2.0, it enables single sign-on and UMA provides access management. Thousands of organizations worldwide, currently use one of the most widely used identity solutions called Shibboleth. The upside is that Shibboleth is free for organizations to use on top of being open source. Finally, there is the Gluu server, that is a free service, that implements and integrates all the standards mentioned so far, as well as multiple others open source standards.

Two-factor authentication sounds too good to be true, which is true, it does have problems. Authentication integration into the day to day work life can be complex. With complexity comes the high cost of running, maintaining and implementing strong authentication. If someone is unqualified and is designing a complex security implementation, it can lead to further holes in security, therefore allowing outside perpetrators access to the company’s sensitive media. Also, integration with the existing IT infrastructure of an organization may cause difficulties. An organization may have a false sense of security leading to less vigilance for data security breaches when using two-factor authentication. If an organization utilizes strong authentication system(s), may end up with the loss, damage, and theft of the smart card, USB tokens or other ‘possession’ authentication. There will be some degree of a learning curve with the implementation of strong authentication and humans are inherently resistant to change, therefore it can be costly to train security personnel.

### Intelligence, Surveillance, and Reconnaissance (ISR)

The YouTube video in our current discussion, showed in detail, the use of weaponized Remotely Piloted Aircrafts, aka RPAs or Drones, by the CIA throughout the Middle East and West Asian countries such as Afghanistan, Pakistan, Iran and Iraq, and highlighted several issues concerning their use. The emergence of weaponized drones seems to have led an even more decentralized and dehumanized style of warfare, in comparison to what already exists today. It is nice, in today's United States Army, a pilot, or the RPA drone operator, comes to work, “war”, from his own home, in his own car, living with his family in the US, while fighting a war on the other side of the world.

Today’s US pilots, drone operator, are fearless because there is no risk of being killed or injured while on duty, anymore. The reasoning is that the physical action of neutralizing an enemy happens in a virtual world for our soldiers. The VR represents the physical actual world that is located thousands of miles away from the pilots’ actual location.

The lax environment that most drone pilots fly from allows for mistakes to happen routinely. For example, an operator at any of the numerous command centers, located all over the world even here at home, can be sitting in a comfortable chair, in an air-conditioned room, login online onto any drone tasked for the job that could be located anywhere in the world, while remotely piloting the drone that’s thousands of miles away from their actual physical location above the any harsh and hard to reach environments of the Afghan mountains, Iraqi deserts, Russian Siberia or any remote no road access or harsh weather locations. That’s not the perk though, the best part is that pilot gets to sleep in their own bed, as well as enjoy all the worldly creature comforts, at the end of the day.

The days of a ‘gentleman’s war’ are long gone. People are getting accustomed to the experience of fighting proxy virtual wars. Where robots kill robots, humans or go on missions for us. There is always the fear of tying in AI with these machines when they start to make their own decisions, will they decide to go rogue? People no longer fight by coming face to face with predetermined rules for warfare. Since war has become what it has when mistakes happen they may become so routine that they become over-sought routinely because the aftermath of attacks is so far away and not felt. When the fact is, we are speaking about real human lives that are being affected on the other end of pilot’s day to day ‘job’ tasks.

This leads to the concern that drones facilitate indiscriminately, or worse, discriminate killing disguised as indiscriminate killing, part of ‘the job’. The CIA uses ways to determine if the target is a threat, the actual positive target, that is being sought. These are known as “signatures” or the details of the enemy. They are used to determine when a drone will fire a missile at a person or group of people. Now, who made the CIA the knows all be all. It seems that they are running these programs with little to no accountability for the way they determine to use the drones, how they use the drones or to decide to go after one of their qualified pre-screened targets.

Naturally inciting videos of reports of the innocent civilians, including women, children, handicapped and the elders, are on the receiving end of these drone strikes. These videos bring a great deal of anger and hatred among the local populace towards us. What has been witnessed, it has resulted in a call to arms, thus creating an enemy instead of a hero of the United States for the time being. Drone strikes are making a more global terrorist, rather than mitigating the problem, by promoting negativity towards the U.S. Making our problem with militant terrorist organizations worse. Allowing for them to easily recruit members and keep existing.

Even though actionable intel is available, that Intel should still be subject to vetting, especially when it comes to the matter of someone’s life. Vetting could have avoided the killing of the innocent kid life that attend the conference at the beginning of the story. A drone hit should not be allowed just on the word of a spy alone. There should be a level of professionalism in battle, there should be agreed upon true gentlemen rules for the battle, and that was how the war was fought. Back in the day of when the war was fought on a horse using a sword, that’s what war was known to be like. It is evident that it is necessary to develop new standards of war for identifying and verifying threats.

Drones indeed have many, many, many peaceful real-world applications, and are not just for military purposes. As of today, drones are starting to find an application where it would be most beneficial, in different applications, for all parties that are using the drone. Rather than any other mode of transportation, drone medical supply delivery has emerged most useful for medications and health lifesaving products shipments to remote villages, in underdeveloped nations across Africa. The drones are faced with basically no obstacles, like difficult terrain, long distances travel or any of the high cost encountered by other modes of transport. The cost of sending supplies by a drone is minuscule compared to that of conventional vehicles or current possibilities to send courier packages.

One retailer, Amazon, has been on the road to full drone implementation for its drone delivery technology, since it has been testing unmanned delivery in the last few years, that as soon back as March 2017, Amazon demonstrated its first concept publicly. Shortly after, July 2017, Amazon filed for its first drone patent. The patent stated that Amazons drone delivery service will also scan the delivery area. Meaning, after delivering a customer’s order, Amazon might also conduct a scan of the recipient’s address, residence or business, for an Amazon marketing tool/service. A roof defect, garage door broken, tall grass, broken window, theoretically will trigger Amazon in recommending a service.

For the past 40 to 50 years, remotely operated machines have been used to dispose of bodily injuring threats. One that comes to mind is the explosives disposal robots. These search and rescue devices afford the operators their safety, by allowing remote operation of these machines from a safe distance. Which is the most obvious benefit, especially when the hazard ends up discharging during disposal, and the use of the drone technologies end up saving human lives in the process? This leads us to think of the ethical ramifications regarding the use of robots with artificial intelligence (AI). Will humanity ever allow robots to make the ‘kill’ decision? Or can humanity accidentally gives the ‘kill’ decision making capability to the robots? Is vetting of ground intel necessary? Is double vetting of intelligence required? Should there be new vetting techniques & policies?

Search & Rescue drones are revolutionizing the science of drone application usage. Search & Rescue drones have been utilized in the past in warfare, hazard rescue and inclement weather rescue. Remotely controlled robots can search through collapsed rubble to locate and rescue trapped survivors, deliver food, water and medicine as well. The current convenience that pilots have, the ability to log in, online, to take control of the remotely controlled object, whether it be a drone or other type of robot, to do the task at hand. This is a huge advantage in comparison to the current ‘traditional’ piloting style, where the pilot must be physically present to pilot.

Drone piloting allows for the same capabilities as traditional physical piloting a plane, but it saves time, lives, space and most importantly money. Today, an available pilot, near or across the world, can login to the internet and take control of any drone anywhere necessary for the job. Allows for cheaper costs for employers, the pilot and in turn the consumer saves at the end. The job will be taken care of faster because the response will be quick. No travel time is necessary for pilots, as soon as a pilot is available globally with internet access they can start the task straight away. No human is onboard, therefore all involved are safe. Only threats, in this case, is in case of if malfunctions happen, and people on the ground get struck by something falling off the drone. Due to all these facts and savings, the operator will save and earn the most money at the end of the day.

### Biometrics

The Crossover Error Rate (CER) is a quantitative comparison measurement of the accuracy of the biometric authentication method(s), which measures the success for the overall precision of the solution(s), application(s) or device(s) and of its usability. CER represents the value when sensitivity is configured so that the False Rejection Rate (FRR) equals the False Acceptance Rate (FAR). The Crossover Error Rate is the value of [FAR](http://www.biometric-solutions.com/glossary.php?term=FAR) and [FRR](http://www.biometric-solutions.com/glossary.php?term=FRR) crossing points at the axes of the graph. The values of Type I & II, FAR & FRR, curves represent the number of errors as well as sensitivity level values. The x-axis crossing point represents sensitivity levels, where the higher the sensitivity of the biometric, the higher the FRR and the lower the FAR. Just the same, the number of errors value is the crossing point on the y-axis.

Small and midsize organizations must consider the same risk factors as large organizations when it comes to implementing biometric authentication. Some of the many factors that need to be considered when implementing biometrics applications throughout organizations are facts of error rates and reporting, cost(s), security, spoof-ability, scalability, identity protection, system integration and hardware interoperability. Consideration of false acceptances is an important concern of biometrics, no matter the size of the organization. False acceptance, also known as Type II error, is a mistake occasionally made by biometric security systems where an unauthorized person is identified as an authorized person. Most small and medium organizations don’t have equivalent financial resource capabilities as large organizations; therefore, implementing and maintaining cost(s) would be a primary concern for implementing costly biometrics within struggling small to mid-sized organizations.

For a small to midsize company, practical uses of biometrics at the workplace would include: DPI (Dots per Inch) to identify unique fingerprint identity within the organization, liveness detection aka spoof detection will help control unmanned access to the organizations premise or building(s), and False acceptance rate (FAR) and false rejection rate (FRR) are two parameters used by vendors to rate the accuracy of fingerprint-based biometric devices. Biometrics authentication applications could be implemented methods using a signature, fingerprint, iris, voice or facial scan, to secure or open a computer, software application, folder or document. Biometrics is used to control access to facilities or rooms within a corporate building.

Strong Authentication should be the goal always when anything is connected online, especially if the goals are to be secure. Strong Authentication is any method of verifying the identity of a user, or device, that is unique enough to ensure the security of the system it protects by withstanding any attacks it is likely to encounter. Often, Strong Authentication is confused with two-factor or multi-factor authentication. However, Strong Authentication is not necessarily multi-factor authentication. Since there are always the possibilities of errors, the fear is they happen while connected online, allowing the end-user to be vulnerable. To mitigate possible occurrences of false acceptance error(s), use retinal, finger or a facial biometric scan(s) in combination with either “something you have”, such as a smart device, FOB or a phone or secondly, “something you know”, such as a pattern/sequence design, username, passkey.

The loss of biometric data may have very severe ramifications. Where the loss of a password means, that a couple moment is lost due to the time necessary to click “forgot password” and creating a new one. whereas the loss of someone’s biometrics can lead to someone being framed for murder. A loss of a password or a key FOB isn’t as dire of a loss as if one’s retina, facial, fingerprint or voice data being stolen. The problem with biometrics is that it is truly identifying the individual. Biometrics are so unique, that two forms of biometrics are truly authenticating pieces of data when two are used in conjunction with the other to verify authentication. Like many people of the world, American’s value their identity, security, and privacy, and biometrics afford criminals the ability to steal all the above. Within there lies the reluctance of Americans.

**REFERENCES**

Alex, Remmy. (2016, July 1). Metro 10 Most Common Crimes Committed in Nigeria [LIST]. https://www.nigerianbulletin.com/threads/10-most-common-crimes-committed-in-nigeria-list.215978/

Amazon Prime Air. https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011

Chiaberge, [Marcello;](https://www.tandfonline.com/author/Chiaberge%2C+Marcello) Silvagni, [Mario;](https://www.tandfonline.com/author/Silvagni%2C+Mario)  Tonoli, [Andrea;](https://www.tandfonline.com/author/Tonoli%2C+Andrea)  & Zenerino, [Enrico. (2016, October 7).](https://www.tandfonline.com/author/Zenerino%2C+Enrico) Multipurpose UAV for search and rescue operations in mountain avalanche events. Pages 18-33. <https://doi.org/10.1080/19475705.2016.1238852>. <https://www.tandfonline.com/doi/full/10.1080/19475705.2016.1238852>.

# Douglas, Kate. (2014, May 30). Moving outside of Lagos: Five Nigerian cities with business potential. <https://www.howwemadeitinafrica.com/moving-outside-of-lagos-five-nigerian-cities-with-business-potential/39927/>.

# Fletcher, [Pascal. (2014, April 9). Retailers chase reward in booming but volatile Africa.](https://www.reuters.com/journalists/pascal-fletcher) <https://www.reuters.com/article/us-africa-summit-retail/retailers-chase-reward-in-booming-but-volatile-africa-idUSBREA371MP20140409>

# Hernandez, Steven. Official (ISC)2 Guide to the CISSP CBK, Second Edition Page(s) 73-75.

# Hotz, Robert Lee. (2017, December 1). In Rwanda, Drones Deliver Medical Supplies to Remote Areas. <https://www.wsj.com/articles/in-rwanda-drones-deliver-medical-supplies-to-remote-areas-1512124200>.

# Lin, Connie A.; Mauntel, Cherie; Shah, Karishma; and Shah, Sachin A. (2017, December). Drone delivery of medications: Review of the landscape and legal considerations. <https://doi.org/10.2146/ajhp170196>. <http://www.ajhp.org/content/early/2017/12/08/ajhp170196?sso-checked=true>.

# Lockhart, [Bob. (](https://www.tractica.com/about/team)2015, June 23). In Biometrics, Which Error Rate Matters? <https://www.tractica.com/biometrics/in-biometrics-which-error-rate-matters/>

# LUCKWALDT, ADAM. (2017, October 6). Career Profile: Army Unmanned Aerial Vehicle Operator. <https://www.thebalance.com/career-profile-army-unmanned-aerial-vehicle-operator-2356463>

# NIST. (2010, June). USB thumb drive security best practices spelled out. https://searchsecurity.techtarget.com/USB-thumb-drive-security-best-practices-spelled-out-by-NIST

# Oxford Brookes University. Information Security Working Group. Portable Devices and Removable Media Acceptable Use Policy ­ v1.0. <https://www.brookes.ac.uk/WorkArea/DownloadAsset.aspx?id=2147555201>.

# Schneider, [David. (2014, April 11).](https://spectrum.ieee.org/author/schneider-david) Why Are Search-and-Rescue Drones Grounded? The FAA says model airplanes can't fly when the purpose isn't just good fun. <https://spectrum.ieee.org/automaton/robotics/drones/search-and-rescue-drones-grounded>

# UC Berkeley. Data Encryption on Removable Media Guideline. <https://security.berkeley.edu/data-encryption-removable-media-guideline>.

# West Point. (2012, December). Biometrics Metrics Report v3.0 Prepared for U.S. Military Academy (USMA). <https://www.usma.edu/ietd/docs/BiometricsMetricsReport.pdf>

# <https://www.igi-global.com/dictionary/crossover-error-rate-cer/6294>