ADVANCED CYBER SECURITY CONCEPTS

Physical Security Development Environment Task

Henry Post, hpost@hawk.iit.edu

Introduction to assignment

In this assignment you are to critically think and analyze what physical security means. These set of tasks are to challenge your way of thinking as it relates to current topics that affect our societies. Once this assignment is complete we will discuss this in an open forum.

Tasks

Below are the following tasks for this assignment.

Facility location in dangerous locations

In 400-600 words provide a justification how a site could be located in the following areas; Northern, Nigeria; Tijuana, Mexico; and Pretoria, South Africa. Select only one location. What are the actual physical security threats that pose a danger to your selection? What mechanisms would you put in place to ensure the safety of the people and business operations? Hint: Guns, gates, and guards.

Provide answer below this line

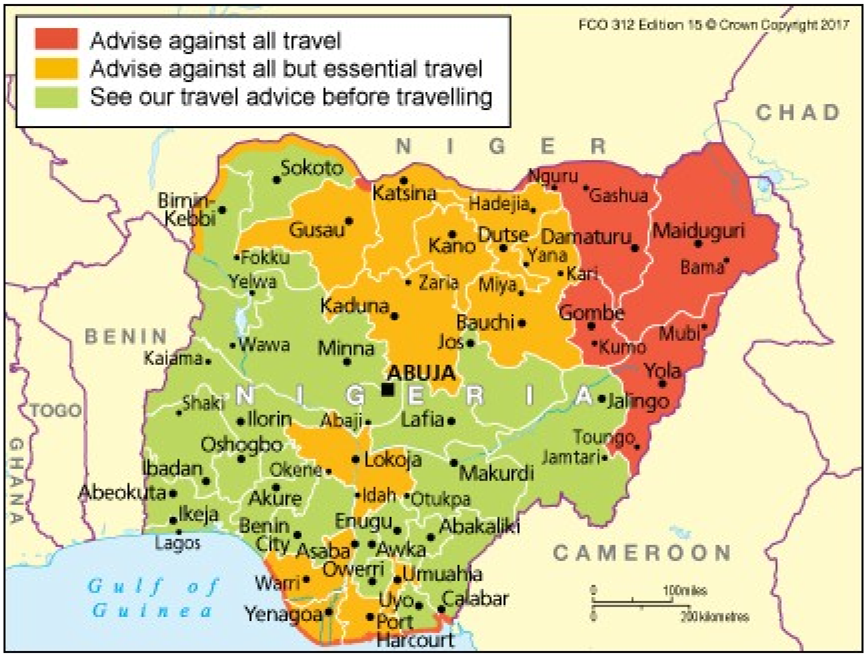
I am choosing Northern Nigeria as my location. Tijuana and Pretoria's landscapes are far too urban and restrict our defensive as well as offensive strategies too much to work in an urban environment.

In an urban environment, there are large amounts of people moving around at all times. This aids attackers in espionage, confusion, and concealment. This increases the amount of surveillance required to establish total situational awareness, the amount of security cameras needed, dead zones, personnel to man the cameras, and the amount of armed guards. In short, it is a logistical nightmare compared to large, open areas in low-population areas.

In addition to this, certain surveillance tactics and strategies cannot be used in cities for sociopolitical reasons.

Northern Nigeria is primarily farmland, villages, and shrubland. There are cities on the major roads, but there are still a lot of farmland and villages. The main physical threats that would be considered are terrorist groups, bandits, and rioters.

The site `state.gov`, operated by the U.S. Government, currently recommends strongly against traveling to Northern Nigeria. Also, the site `gov.uk` maintains a terrorism map for Nigeria at `https://www.gov.uk/foreign-travel-advice/nigeria`:



Most areas in northern Nigeria are in states of unrest, and `state.gov` estimates that ~2,000,000 Nigerians have been displaced as a result of terrorism and violence.

So, terrorist groups are our largest issue. Establishing a facility in a city is not an option as the land availability will be low and visibility will be poor. The threat of suicide bombers or armed terrorists is very high, so visibility must be high in order to neutralize potential terrorists.

Terrorists may acquire military vehicles, civilian vehicles, firearms such as long rifles, automatic rifles, rocket-propelled grenade launchers, IEDs, mortars, potentially tanks, and potentially aircraft.

The plan is to secure a flat piece of land, approx. 50,000 sq. feet with about 1 mile visibility in all directions. There shall be a perimiter double-walled barbed wire fence approx. 700 meters away in all directions from the facility sufficient to stop on-foot subjects but not necessarily vehicles.

Staggered at the perimiter, every 25 feet or so shall be infrared wireless perimiter alarms that are connected via encrypted wired connection as well as encrypted cellular to the facility.

These infrared perimeter alarms shall be automated in their monitoring, to prevent the need for security personnel to monitor them. These infrared alarms shall sound an alarm if their connection is disabled for more than two seconds or if they are tripped.

Atop the facility shall be a series of eight night-vision cameras manned by 16 guards who will rotate shifts. Two guards will man one screen. These cameras must be able to identify humans, vehicles, and aircraft for at least 0.75 miles.

Anywhere from 10 to 20 autonomous thermal imaging drones shall monitor the edge of the facility, approximately 100 to 800 feet away from the outer perimiter, for ground and air anomalies. These drones shall rotate in a round-robin fashion for repairs and for recharging to ensure minimum loss of coverage.

There shall be a series of eight armed guard towers located in a circular pattern approximately 200 feet from the edges of the facility. These towers should be supported by the autonomous drones, perimiter alarms, and night-vision cameras.

There shall be a ground-penetrating radar operating continuously to detect tunnels that may be dug by terrorists. The radar shall be operated around the perimiter every 30 minutes, at a different location.

There shall be two trucks armed with machine guns and supporting troops to provide direct fire support. There shall be one truck armed with an artillery cannon to provide long-range fire support.

Missile launchers shall be employed to provide ground-to-air fire.

One THAAD shall be stationed in a concealed part of the facility, to neutralize long-range missile threats.

All facilities shall have back-up power for at least 48 hours.

P.S.: The price of this as well as geopolitical impact of this amount of firepower may prove impractical. This is a very ‘loud’ approach. It may be salient to locate this base underground in a fenced-off area with the same amount of firepower, but concealed. However, I don’t want to rewrite this text.

Facility security

In at least 600 words to address the following questions. [1] How does one secure a HVAC system that has Internet of Things (IoT) capabilities? [2] What Risk Management Framework (RMF) requirements should one use to store media, protect media, and degauss/erase media? [4] How do you implement strong authentication? Are there open source possibilities? What are the problems associated with the implementation of strong authentication into facilities?

Provide answer below this line

[1] Securing an HVAC system

Any IoT system is essentially one that transmits information and allows control over internet protocols such as IP, DNS, TCP, HTTP, etc.

Using a HVAC system, one which undoubtedly collects and transmits sensor information as well as accepts remote controls, must have controls in place to restrict the transmission of data as well as the processing of remote commands only to authorized parties.

First, to prevent MITM attacks, all communications must occur under an asymetrically encrypted communication where a public key exchange. HTTP/S is an extremely well-documented use case for this. We must use an asymmetric encryption algorithm because of **the key exchange problem**. How do we exchange initial secrets *in plaintext* if we're being listened to? Asymmetrical encryption solves this by having both parties keep their secrets secret and only exchange public keys.

After MITM attacks and snooping is mitigated, a framework of authentication must be established. When a measurement device wishes to submit a datum to an aggregation device, it must prove that it really is a measurement device. This can be done with X.509 Certificates. Upon installation of a new temperature sensor or moisture sensor, each temperature measurement device must be given a new certificate distributed by an aggregation device.

This distribution of certificates shall apply to all actors and devices that communicate with eachother. If I, an HVAC technician, wish to turn off the AC in my room remotely, It must be determined that I:

- Am proving who I am by authenticating myself, and

- I am authorized to perform actions on that specific AC unit.

This permission information must be stored in a central location that will establish access control for actors who wish to manipulate devices.

[2] RMF Requirements for storing, protecting, and erasing media

There is no one-size-fits-all answer for the appropriate controls to securing data in an organization. Some information should be public (facebook events, giveaways), some information should be somewhat hidden (company picnic dates, meeting notes), some information should be classified depending on who **needs to know** that information (internal emails, company plans, internal project blueprints), and some information should only ever be known by a single entity (private keys, passwords, certificate files).

Access to media should be controlled depending on its classification level. If a piece of data is top secret, if it must be stored, it should be stored using multiple layers of protection that require the party attempting to view or transmit to authenticate themselves.

This can be done through controlling access (i.e. a software program), but should be done through hardware encryption as this cannot be defeated by physical disassembly of the storage medium, as encryption irreversibly transforms the data.

Erasing data is also something that depends on the sensitivity of the data being stored on the medium. If a public flier is stored on a hard drive, it may not even need to be erased. However, if an employee is fired and they worked on a top secret blueprint, their hard drive must be wiped in such a way that leaves no recognizable trace of the data.

[4] How do you implement strong authentication? Are there open source possibilities? What are the problems associated with the implementation of strong authentication into facilities?

Authentication is the act of proving that you are a specific entity. The most common form of this is a username-password based authentication scheme, such as logging into msnbc.com to view the news. This authentication scheme assumes only you know the password and username combination, thus proving that you are the person who originally opened the account.

Strong authentication is achieved by the combination of different authentication schemes to reduce the risk of a different, likely malicious, entity attempting to impersonate you, being able to authenticate itself as if it were you.

For example, having both a password AND a fingerprint reader to unlock your phone requires the entity authenticating itself to both have your fingerprint as well as know your password. However, this still does not protect you against extortion or torture, or physical capture. However, you must be physically forced to put your thumb against the phone. Assuming hardware and software have no flaws, there is one extra layer of authentication that makes it more difficult for malicious entities to authenticate themselves as you.

There are many open-source possibilities for implemeting strong auth.

One could use fingerprint and face biometric authentication code that the Android project uses.

A rotating hardware key fob could be used, or a physical key fob with a crypto key.

A rotating code on your mobile phone could be used.

Security questions could be used.

Bio auth data is PII, and this data can be exfiltrated and analyzed to perhaps find out information about the users who authenticate themselves, or to exploit weaknesses in your bio auth scheme.

The more authentication is required for users, the higher the chance that they will be unable to authenticate themselves at a certain point will be. People can lose eyeballs, fingers, hands, the ability to speak, or can obtain facial deformities. People lose keys, wallets. People forget passwords. Software and hardware platforms like phones can be bugged, stolen, hacked, or lost/destroyed. The more checks there are, the harder it can be to authenticate yourself.

However, people generally lose more phones than fingers, so bio auth is less susceptible to the loss of the identifying feature.

Intelligence, Surveillance, and Reconnaissance (ISR)

Watch Unmanned: America's Drone Wars • FULL DOCUMENTARY FILM • BRAVE NEW FILMS

https://www.youtube.com/watch?v=mpzk7OdbjBw. Provide at least 300 words regarding the ethical considerations of using drones in physical security.

Watch Attack of the Drones: Is war becoming a video game? https://www.youtube.com/watch?v=msHJLwYWX30. Provide 300 words regarding drones are not only used for war but use of drones domestically. You also have the ability to discuss the use of the Unmanned Ground Vehicle (UGV) created by iRobot and its applications to physical security.

Provide answer below this line

Ethical considerations of using drones in physical security:

Using drones in physical security poses ethical issues whether they are remotely-operated, semi-autonomous, or fully autonomous.

The first largest question is, do you have a right to record, surveil, and store audio, video, thermal imaging, and other data about a specific person, esp. against their knowledge or will? What procedures exist to regulate the type of data, who it is disseminated to, and how long it is stored? This question can be applied to overseas use of drones as well as the domestic use of drones.

The next question is: In terms of lethal drones, or drones armed with weapons, what are the acceptable rules of engagement or rules for the use of force when engaging a target? What information must be certain to be known about the target? How much of that information is inferred? Can inferred information be used to support the reasoning for engaging a target?

Is wearing traditional muslim attire and moving in and out of a large building at a specific time enough to cause a drone operator to reasonably terrorist activity?

That being said, the effects that remotely piloting a lethal vehicle and engaging targets can have on operators can also be negative. Being disconnected from the battlefield by both distance and sensory feedback can cause a rift between the battlefield situation and the actions of the operator. Operators of these vehicles may not be realistically affected by the reality of their actions. Some suffer mental health issues as a result of their time spent remotely operating these drones.

Is war becoming a video game?

Military remove-operated drones provide the ability for the military to extend its power without putting humans directly in harm's way. This applies both to foreign and domestic situations.

However, as we have seen in the previous videos, accountability and the emotional connection normally provided by soldiers is absent when piloting a drone remotely. This causes intelligence and decision-making deficiencies.

Soldiers cannot interrogate people, interact with civilians or detained terrorists, observe their environment fully, or gather any intel past the drone's visual/NV/IR sensors.

This emotional detachment and intelligence deficiency brought on by the void between the remote drone operator and the battlefield does not apply to combat robots that are operated by soldiers on the battlefield. These can include quadriped, biped, flying, and tank-tread-style robots. These robots can be used in tactical situations to gather intelligence, traverse hazardous terrain, and neutralize threats.

When you are in a safe steel container flying a drone that is thousands of miles away, you have no risk of being shot at, making an emergency landing, or having any kind of bodily harm inflicted upon you. You don't need to gather intelligence on the ground, talk to civilians, or interrogate civilians. This will very likely change your behavior.

Biometrics

What is the important of the Crossover Error Rate (CER)? How can a small or midsize corporation implement the use of biometrics in their organization? Should strong authentication be implemented for the use of biometrics? Why are American citizens reluctant to the use of biometrics? Provide at least 300 words on this topic.

Provide answer below this line

The Crossover Error Rate is the point at which the FAR (false acceptance rate, incorrect entity is auth'd) and the FRR (false rejection rate, correct entity is rejected) are equal. This metric is usually used to measure the average accuracy of a biometric system.

A small or midsize corporation should realize that there must be a nonzero crossover error rate because biometrics measure a non-quantitative object: your skin, DNA, or physical features. They cannot be perfectly digitized!

This means that corporations should not rely on **only one** biometric auth option, and that **individuals should be allowed to fail one or more, but not all, biometric auth tests**. The thresholds for these values should depend on how difficult it should be to authenticate yourself, and how strict the biometric authentication should be.

In addition to this, biometric auth **must not** be the only form of authentication because it **can always be spoofed**. Through physical seizure of biological materials, impersonation, hacking, force, or blackmail, these authentication methods can be defeated by a large enough or determined enough threat. Strong authentication is a must when using biometrics, not only to fix the problems inherent in using a biological system to authenticate, but also because people's physical features can change.

To be able to authenticate yourself using a physical feature means that the physical feature must be stored in a digital representation in some way. This means that your fingerprint scanner on your phone must store a digital representation of the features of your finger in some way, and a person could recreate a series of thumbprints that authenticate as if they were your thumbprint. This is very similar to cracking an MD5 hash through a brute-force attack.

This is why Americans are afraid of bio auth: It stores an inherently reversible representation of their biological features. Data breaches can expose these and can be used by people to profile them based off of these features.

More importantly, once people have these biological signatures, they can be used to impersonate other bio auth systems! It’s password breaches all over again, but with faces and fingerprints!

Graduate Students Only:

The Most Dangerous Town on the Internet - Where Cybercrime Goes to Hide https://www.youtube.com/watch?v=CashAq5RToM Provide an 500 word response analyzing this video. Response can include the physical security surrounding various bunkers which should include physical access. Explain why secure places like this are in use and why they

Read the following article: Weingart, S. H. (2000, August). Physical security devices for computer subsystems: A survey of attacks and defenses. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 302-317). Springer, Berlin, Heidelberg. Write a 500 word overview of his article. You may focus on any of the items contained in article. Read full article at https://link.springer.com/content/pdf/10.1007/3-540-44499-8_24.pdf