Andrea Gibb

Continuous Assessment2

CS.996

Proposed UAV threats

The recent rise in small commercial drone availability has emphasised the potential threat posed by UAVs. The objective of this section is to investigate the five predominant vulnerabilities of an attacker gaining authority over a UAV system.

Falsified GPS signals

Once a UAV attacker has the ability to eventually specify the position and velocity estimates it is considered captured, thus meaning that post-capture attempts can be as equally damaging. An attacker could transmit falsified GPS signals allowing the behaviours of the UAV to be influenced, meaning the attacker could manipulate the true state of the UAV. During post capture the UAV could be manipulated to fly off route and even land without raising alarm. This type of spoofing technique could be used to land the UAV where and when the attacker desires, without having to crack the remote-control signals or communications from the original control centre. Furthermore, feeding fake GPS signals to the receiver so that it is believed to be somewhere it is not, is consider a seamless takeover as it a surreptitious alternative to jamming.

Land-to-Air attack

Land to air attacks could be extremely damaging, for example if an attacker has located the GPS coordinates and the direction of a UAV, then prediction of when the UAV may fly overhead. This kind of knowledge could allow the attacker to prepare, for example they could then shoot down the UAV successfully, costing large amounts of resources.

False information streaming

False information streaming, UAV’s provide live picture information to the control centre, this could be used for identifying, tracking and monitoring specific people and vehicles. If an attacker were to view this aerial video footage they could identify areas and people of, allowing …

Base Discovery

Base of discovery could be uncovered if an attacker were to capture a UAV, this would allow the attacker to find out information about the original control centre, for example who owns and controls the UAV, the location it came from, the purpose of the UAV and sensitive data.

POI discovery

Person of interest discovery, meaning the attacker capturing and uncovering a UAV containing data collected on an enemy (themselves). The attacker now has an in depth understanding of surveillance and reconnaissance information collection for combat purposes. This discovery could lead the attacker to the person of interest, allowing them to be cautioned and prompted into hiding.

Think about the network, obtaining the others, privilege escalation, group together, total control

As its designer, what precautions would you take in the high-level design

High level design precautions

An attacker will search for vulnerabilities that impose the highest threat, in much the same way a design architect goes about securing a system. The objectives of this section are to identify and eliminate the vulnerabilities by hardening the system with coping mechanisms. No system can be completely secured, the job of a designer is to make the system financially unprofitable to attack.

Software Update

A huge security risk that is very easily solvable is simply updating the software frequently, failing to do so can compromise all the security mechanisms set in place. Old software may have known bugs which attackers could exploit, this can become serious once an update has been sent out as the old version, with the known bugs often becomes public, meaning entry points are exposed.

Signal Encryption (TX)

Signal encryption is very important, one way to secure the signals sent to and from a UAV is TX signal encryption. The system ensures a high level of encryption against anyone that may try to capture the data being sent to the UAV, meaning even if the traffic were being monitored, only the correct recipient can read the data.

Firewall

* Encrypt signal tx (only correct recipient can read data sent by drone)
* Update frequently (update software on uav, patches)
* Firewalling
* Checksums (check only authorised commands accepted)
* Minimal implementation (message signature)
* Trusted hardware (Don’t use Chinese ~GPS for example)
* Kinds of attacks between policy and threats, relaunch, gaining control

Security policy for a university department

Who are the main actors and what are the assets (give a single line justification about why each asset is important from a security perspective)

The main actors are the people who are affected by the system, for example the students, staff and anyone that uses the system. The Assets are the physical parts of the system for example the server, a student’s personal laptop, Wi-Fi routers, university computers and devices connected.

Server

The universities data is stored on computers, the data is transmitted across the computer network, all of this data goes to and from a server. Having a centralised resource system means students can access their files over a whole network of computers, the blocking of untheorized entities can be maintained.

WIFI routers

Personal Devices

Network Computers

What are the main practical threats; i.e list who are the adversaries, what are their motivations, and what attacks are likely with appropriate justification.

The main practical threats:

* Spoofing Identity
* Tampering with Data
* Repudiation
* Information Disclosure
* Denial of Service
* Elevation of Privilege

Adversaries and motivation:

If the network security was compromised, the traffic between a student’s personal laptop or device and the server could become visible. This could lead to a number of information leaks, passwords and username for sites visited while connected via WIFI could be exploited. For example, if a student were on social media, the login detail packets could be monitored, and the account could be hacked, the information gained from social media conversations could be enough information to coerce the student into committed all kinds of illegal and dangerous acts. The student might then go on to visit sites like PayPal or Amazon, there often bank account and credit card details could be used to empty accounts or identity theft.

A student could be motivated to attack the university to gain access to information about another student, the information could be used against said student in order to gain cooperation. For example, a student with security experience and knowledge could be forced by intimidation to attack and hack into the system to gain information. There are a number of threats in this situation. The attacker might want to retrieve sensitive data to gain power, money or even destroy or corrupt. If an attacker had sensitive information on a teacher they use it gain coercion, for example they make demands and if these demands weren’t met then information could be leaked. This kind of attack could be motivated by money, if the attacker didn’t receive a payment then emails or personal information could be leaked.

If the university’s data were to be destroyed or corrupted the functionality of the education system could be damaged greatly, reputation would fall. The student data could be exposed, not only financial information but user names and passwords, this could link directly to email leakage.

3. How should information flow be restricted in order to prevent a leakage of personal information that compromises the privacy of the individuals at the centre of the matter? Do you think encryption mechanisms should be used? if so, how should the keys be set up between the various parties. If not, why not.

The objectives of this section are to identify the possible threats and provide security mechanisms to prevent such attacks. There are several ways in which information could be leaked or manipulated. Students grades could be compromised if an attacker were to hack into the sever once the grades had put up, an attacker could also hack the upload link between the teacher and the sever, this could also be done when the student downloads the grade, the download link could open to attack.

All users should have minimal privileges so that access to sensitive information cannot be gained, information must be classified according to appropriate availability, for example open, public and confidential. Information should be protected against unauthorised access, meaning only selected members of staff should have access to information combined with the responsibility to handle and maintain appropriately, in correspondence with classification. Group based access control should be in place to only allow certain people to view and append certain material, for example a teacher should be allowed to upload grades for their own students but shouldn’t be allowed to view student address or other grades from separate classes. Having minimal privileges restrictions set in place protects the system from having a large and easily attackable surface. Minimising all unnecessary access points prevents an attacker from having a wide range of targets. However, having data like grades flowing from teacher to sever and sever to student is a necessity, this data must be securely transferred between parties, there are several forms of encryption that could prove useful.

Public and private encryption could be used when sending sensitive information to the sever. This would protect against an attacker that may have intercepted the upload or download of the data when it is flowing from user to sever. This would stop the data from being read, even if captured. To obtain integrity the data could be hashed, ensuring things like the grades hadn’t been changed before reaching the server, using a digital signature ensures that the data hasn’t been manipulated in transit. To further protect, encrypt the data on the server so even if a breach occurs the data cannot be easily read.

Write more on encryption examples

However there are a few other methods that could be uses

Minimal implementation to the system, this means the system should be kept as simple as possible so that bugs aren’t introduced through needless complexity. If an attacker has limited ports to attack, they may see the system to as target not worth the time or effort. Another way to eliminate attack surfaces is to reduce software and network components. Limiting the devices, ports, cloud severs, systems, databases and operating systems exposed areas make the system more vulnerable by added weaknesses or deficiencies in the hardware, software and firmware.

Securing storage, having a demilitarized zone that students and staff can interact with but cannot store things directly. Having a gap between the demilitarized zone and the main systems means things like the internet and other untrusted networks are separate. This would provide the universities data with another layer of protection as the internal system remains unreachable from hackers directly access internal servers via the internet.

The universities computers are connected to the internet, this makes them a potential target to any attack, experienced or not. Keyloggers, Trojans or an attack through an unpatched hole are some of the many ways attackers can steal information. A firewall acts as a shield or barrier between the system network and cyber space. When a student is connected to the internet they are constantly sending and receiving information packets, a firewall is a way of filtering packets, according to a set of rules. The rules either allow the data or block potential harmful packets. Another way a server can reject known malicious sites is place an IP ban on certain IP addresses.

Conclusion.

* Encryption
* Least privilege
* Secure transfer

4. Second part: threat model

* Who is being attacked
* Who is attacking
* What are the valued assets
* Where am I most vulnerable
* What are the most relevant threats

Assets

This section implements a threat model policy for a university department, following the investigated sections previous it is important to understand the assets, threats and vulnerabilities of the system.

The most important step is to identify the assets, this could be exam questions or student and teacher information. For example, a list of names, addresses personal, medical history, current, recent grades and financial state. To protect these valuable assets an access category should be established, meaning trust levels should be set in place to ensure certain users can only gain access to certain data. Entry and exit points should be minimal and system assets and resources should be maintained. This means there should be data protection policy which users are aware of, understand and have access to. For example, the head of a particular department should be responsible for confidentially, integrity and availability of maintained information. IT support staff should be delegated authority from heads of departments, so that responsibilities are fulfilled.

Threats

Identifying the threats allows security staff to prioritise potential damage of security flaws, understanding what an attacker may do to the system. For example, a student with financial motivation may want to tamper with data, the changing of their own grades or another student. An attacker may want to disclosure teacher personal information for personal gain, to threat or intimidate or even leverage, for example if a student wanted a better grade than what was issued to them, they may hack into the system, gain person information on the teacher that issued the grade and use it to persuade or pressure said person into altering information. Financial motivation or the justification for revenge could result in a number to reasons to attack a system. A disgruntled teacher could elevate their own privileges or spoof identity, perhaps to demand a pay rise or influence job security. Another threat may be denial of service, if a student had been under prepared for an upcoming exam they might block the network system, stopping the exam from going ahead at that set time of day.

Threats can also be based on the severity of an attack, if a denial of service attack were to occur what is the damage potential, an hour, or several weeks. The affected users increase from a few hundred to a few thousand, if the network were down for several days this could mean the flaw exploited was highly discoverable and if not patched properly could be reproduced.

Vulnerabilities

The system vulnerabilities can be generalised down to the network, the host and application. A network vulnerability could be an attacker spoofing packets or injecting malicious packets. A threat to the host could be buffer overflow, an attacker could overload the system with more data than the memory can store, this could result in loss of data for example student records. A host could also be injected with malicious files which could result in loss of all data, and complete corruption of the system. An application threat could be a simple SQL injection, this kind of data injection can allow the attacker to spoof identity to tamper with data, destroy, make unavailable or even become the administrators of the sever.

It is important to consider discoverability, how easy was the flaw to find. Reproducibility, does the attack work every time, is there a timing window or does it rarely work. Exploitability, does the attacker need to be skilled, could anyone do it. Most importantly the damage potential, can the attacker retrieve sensitive data but do-little harm or could the data be corrupt and destroyed. In conclusion this threat model helps prioritise the university system so that threats can be establish and effective responses can be put in place.