Security for Robotics - Design Document

Emily Longman, Zach Rogers, and Dominic Giacoppe

CS461 Capstone

11/30/2016

Abstract

In drones and other networked robotics there is a broad array of security vulnerabilities that can be leveraged in an attack. We will evaluate the ROS to find as many of these security holes as we can and document them. The different vulnerabilities find will be categorized into malware, sensor hacks, network and control channel attacks, and physical breaches. For some of these exploits we may be able to implement solutions, which will also be documented. These findings and any solutions will be added to an ongoing academic effort to make robotics more secure.

Drone OS

For the purposes of the OS, it is not so much it's design as it is it's execution. We will be using ROS Indigo, which is the recommended version of ROS for our setup on top of some board-specific software builds. The control station, AKA a desktop or laptop computer running Ubuntu 14.04 for it's own operating system, will have a trivial install and setup procedure. It is detailed here[1] but boils down to about 8 commands total and waiting for apt-get to finish. We forsee little trouble with the process.The more involved process will be flashing the drone with the correct software. To start, we will need to flash the beaglebone black itself with a specific image found at this link along with instructions for the flashing process[2]. The general idea here is to flash a SD card with the given image, then get the beagle bone black to boot off it. After that, we'll need to build the associated kernel with instructions on the same page and insert that into the beagle bone black so that it can operate the pixhawk. That is much the same process except we'll have to install some specific packages for cross compiling. Once that is complete, then we can build the pixhawk specific libraries for autopilot with instructions found on this page[3]. We would need to follow the advanced instructions at the bottom of the page, but they are no harder than command line git is and should not be too difficult for our team. Once this is all done, our drone will be using a version of arduPilot for our flight systems and a custom Debian-based Linux build for the underlying operating system on the beagle board black.

Network Setup

Wired communications shouldn't be any harder than inserting the Ethernet cable into the appropriate slots on the drone and the control station laptop. We may need to configure the debian install on the drone to recognize the Ethernet connection but it should be automated as part of the debian install, if it is anything like what a normal live installation media is like. The wireless connection will be more involved, but should not be any different than a regular setup of wireless connectivity for an debian system. If the need arises many guides for setting up wireless connections on linux systems exist, like this [4]. It should not be a big issue. Actually setting up the wireless card so that the board recognizes it and can use it is a different matter, and will be covered later on in this document. The control station wireless shouldn't be any different than the drone's, and may infact be pre-configured for us as part of the initial installation.

ROS v SROS (or rather ROS)

Once we have Ubunutu installed on both the station and debian on the drone, we can follow[1]. The gist of it is that's it isn't much different than a regular desktop install; setup your sources, your keys, do some apt-gets, and ROS will be installed. The better question is what ROS packages we will install outside of the base ones for testing, but that is a question for later on as we explore our options.

Drone Communication Channel

The two drones that we have use a 2.4Ghz data-link between the drone and the receiver ground-station unit. That receiver unit then uses a Bluetooth connection to connect to the user's controller, which is a physical controller or device such as a laptop or tablet.[5] With this in mind, there are two communication channels that can be targeted; the connection from the drone to the ground-station unit, and the connection from the ground-station unit to the controller[5].

The 2.4Ghz frequency is commonly used by most Wireless Access Points, following the IEEE 802.11a/b/g standard. Bluetooth is another protocol that operates within the 2.4Ghz RF (radio frequency) spectrum[6]. This means that communication packets for the drone are being sent and received out in the open, which can be can be intercepted and analyzed with the right tools.

Each drone will be using a BeagleBone Black with a PixHawk Fire v1.6 Cape, making our drones Linux powered, running Ubuntu Snappy Core, enabling us to use ROS[7]. The PixHawk is a flight control system, similar to the Naza-M2, which comes standard on the Flame Wheel ARF F550. It handles the drone's flight system, and includes a cluster of sensors (GPS, Gyroscope, etc) to keep track of vital information in order to maintain control over the drone while in flight. The PixHawk also handles telementry communication between the drone and the ground-station. As stated before, 2.4Ghz is the operating frequency between the drone and the ground-station, though the PixHawk also supports a RFD900 900Mhz Telemetry Radio, for longer operating distances[8]. This opens up an additional communication channel that could be targeted. In order to intercept and analyze 900Mhz RF communications, we would need additional tools, seperate from what would be needed to intercept and analyze communications on the 2.4Ghz frequency[9].

What should now be clear is that there are a lot of data transmitted in the open air in order to have a successful drone system. This means that there are a lot of different ways that communications can be intercepted and even altered, in an attempt to gain control over a drone's flight plan. Knowing which communication channels to target is only a small part of getting to the ultimate goal of intercepting drone data; consider that the Research and Development phase. The next step is to explore how exactly to capture that data.

Methods of Data Capture

Capturing communication data between the user flying the drone, and the drone itself, will allow us to reverse engineer the communication protocols being used. Being able to capture that data also presents the possibility of doing a Man-In-The-Middle (MITM) like attack, enabling an attacker to intercept and spoof commands being sent to the drone in real time.

In order to capture this data, we need hardware that can recieve RF on the 2.4Ghz and 900Mhz band. There are many, many options out there, some of which can be quite costly. Since the primary method of communication is through the 2.4 Ghz band, we can use a standard wireless radio that can run in permiscuous mode[10]. Permiscuous Mode enables us to capture wireless packets without associating with an access point. This is how a lot of wireless attacks are performed[10]. With this, we can use the Aircrack-NG suite of wireless auditing tools to attack the wireless communication channel that the drone uses[11].

While running in permiscuous mode a popular packet capturing tool known as Wireshark will also be helpful. Wireshark is a very powerful application that will allow deep packet inspection, which will aid in reverse engineering the communication channel[10].

With these tools we will be able to capture communication between the drone and the drone ground control station, allowing us to leverage that data to develop drone attack methods, relating to our communications threat model.

Leveraging Captured Data to Develop Attack Methods

Wireshark will also assist with analying the unknown communication protocol that the drone uses. Following the packet streams, and looking at the raw packet data, will allow us to form a concrete understanding of how the drone and ground control system associate with each other, and how commands are sent to the drone[12].

If reverse engineering proves to be unsuccessful, or difficult, we will still be in a poisiton to attack the drone communications, using MITM style attacks, and possibly some fuzzing related attacks[13].

References

[1] R. Project. Installing ros indigo. [Online]. Available: http://wiki.ros.org/indigo/Installation/

[2] A. Project. Building ardupilot for beagle bone black. [Online]. Available: http://ardupilot.org/dev/docs/building-for-beaglebone-black-on-linux.html#

[3] ——. Building ardupilot for pixhawk. [Online]. Available: http://ardupilot.org/dev/docs/building-px4-for-linux-with-make.html

[4] Linux.com. How to configure wireless on any linux desktop. [Online]. Available: https://www.linux.com/learn/how-configure-wireless-any-linux-desktop

[5] DJI. Naza-m2 flight control system. [Online]. Available: https://www.dji.com/naza-m-v2

[6] B. Barnett. Hacking at the 2.4ghz spectrum. [Online]. Available: http://www.grymoire.com/Security/Hardware.html#TOC

[7] BeagleBoard. Pixhawk fire cape: Linux drones with the beaglebone black. [Online]. Available: http://beagleboard.org/project/pxf/

[8] A. Project. Pixhawk overview. [Online]. Available: http://ardupilot.org/copter/docs/common-pixhawk-overview.html

[9] B. Barnett. Hacking the 900mhz spectrum. [Online]. Available: http://www.grymoire.com/Security/Hardware.html#Hacking_the_.3C1Ghz_Range_.28900Mhz_.29_Spectrum

[10] Wireshark. Wlan ieee 802.11 capture setup. [Online]. Available: https://wiki.wireshark.org/CaptureSetup/WLAN

[11] A. NG. Getting started with aircrack-ng. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=getting_started

[12] Polynomial. How do you analyze an unknown network protocol. [Online]. Available: https://security.stackexchange.com/questions/17344/how-do-you-analyze-an-unknown-network-protocol

[13] H. Bck. Network fuzzing with american fuzzy lop. [Online]. Available: https://blog.fuzzing-project.org/27-Network-fuzzing-with-american-fuzzy-lop.html