Probleem:

De drone moet vanuit een GUI kunnen worden gevolgd en commandos verwerken. Deze gui draait op een van de computers aanwezig bij het bedrijf. Momenteel kan iedereen de data van de drone uitlezen en commando’s uitvoeren, hiervoor is alleen een verbinding nodig met het draadloze netwerk. Dit is niet wenselijk. Daarom is het de bedoeling dat de verbinding tussen de GUI en de drone beveiligd wordt. Hierdoor is het niet meer mogelijk voor 3e partijen om de drone commando’s te sturen of om mee te luisteren met de data stream.

Oplossing:

De standaard voor het versleutelen van een verbinding is Secure Sockets Layer (SSL). SSL werkt door middel van public en private key encryption. Dit houdt in dat er een public key is waarmee de data versleuteld wordt, vervolgens kan deze alleen ontsleuteld worden met de private key, die alleen in het bezit is van de ontvanger.

Certificaten

SSL werk doormiddel van certificaten. Een SSL certificaat bevat wat informatie over het ‘subject’. Dit gaat over de eigenaar van het certificaat, zoals de website van het certificaat.

Certificaten kunnen vertrouwd worden door een client, dat betekend dat ze er vanuit gaan dat de source van het certificaat betrouwbaar is.

Een certificaat kan vertrouwd worden door dit op de client zelf aan te geven dat het certificaat vertrouwd is.

Het is ook mogelijk om je als client aan te melden bij bijvoorbeeld de certificaten ‘service’ van google. Google zal dan bepalen welke certificaten vertrouwd worden. Dit word in praktijk veel gebruikt.

Voor de drone is alleen een self-signed certificaat nodig. Dit is dus niet vertrouwd door bekende services zoals google. Dit is niet nodig omdat het certificaat alleen lokaal gebruikt wordt. En dus niet in het world wide web.

Bij het communiceren middels dit certificaat kan de client een waarschuwing krijgen dat het certificaat niet vertrouwd is. Deze waarschuwing kan genegeerd worden.

Voor de veiligheid van de verbinding is het wel belangrijk dat gecontroleerd word of het certificaat echt hoort bij de drone, en niet bij een ‘fake server’.

Bij de drone wordt er gebruik gemaakt van OpenSSL. Dit kan als volgt worden geïnstalleerd op linux:

sudo apt-get install openssl

Het genereren van een self signed certificaat op linux:

openssl req -new -newkey rsa:2048 -nodes -keyout yourdomain.key -out yourdomain.csr

Het genereren van een certificaat op MAC.

open Keychain Access

navigeer Keychain Acces > Certificate Assistant > Create A Certificate…

Kies dan de optie Self Signed Root.

Vul bij de andere velden de informatie naar wens in.

Nu is er een beveiligde verbinding mogelijk. Bij het leggen van de verbinding tussen de client en de drone is het wel belangrijk dat er gecontroleerd wordt of de client wel gemachtigd is om verbinding te maken met de drone. Hiervoor zal het wachtwoord gebruikt worden waarmee ingelogd wordt via in de GUI