Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

InIT Institut für angewandte
Informationstechnologie

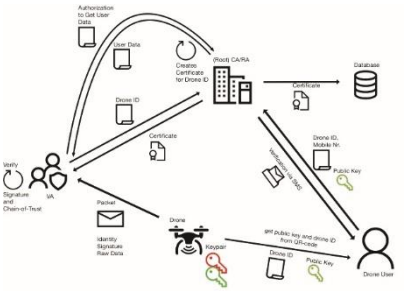
Infrastruktur für sichere Identifikation, Verfolgung und Management von Drohnen

Diplomierende
Linda Helen Bödi
Valentin Bossi

Dozierende
Bernhard Tellenbach
Kevin Lapagna

In den nächsten Jahren wird erwartet, dass die Zahl der Drohnen, die herumschwirren, stetig zunehmen wird. Um die Sicherheit und Effizienz des Flugverkehrs zu gewährleisten, müssen Drohnen zuverlässig identifizierbar und lokalisierbar sowie gegen Manipulationen geschützt sein. Das derzeit verwendete ungesicherte Datenprotokoll erlaubt verschiedene Angriffe auf das System, die Flugobjekte sogar zu gefährlichen Manöver verleiten können.

Diese Arbeit gibt eine Antwort auf die folgende Frage, ob es möglich ist, eine sichere Public-Key-Infrastruktur für Drohnen zu entwerfen. Ein Prototyp dieses Systems wurde mit Unterstützung der FLARM Technology AG in Form einer Web-Applikation realisiert. So ist es möglich, Datenpakete von Drohnen, die das Protokoll 'FLARM UAS Electronic ID' verwenden, über eine REST-Schnittstelle zu verifizieren, Drohnen und deren Benutzer mittels Public-Key-Verfahren (EdDSA) zu registrieren und die Benutzerauthentifizierung per SMS zu simulieren. Zusätzlich werden die aktuellen Validierungszustände der Drohnen sowie deren Positionen während des Fluges in Google Maps visualisiert. Es wird gezeigt, wie dieser Prozess in die Infrastruktur integriert werden kann, damit die Chain-of-Trust funktioniert.



Das Public-Key-Infrastrukturmodell des Prototypen

Um den Prototyp zu entwerfen, wurden verschiedene Infrastrukturmodelle analysiert und der geeignetste Ansatz gewählt. Alle am System beteiligten Einheiten wurden evaluiert und ihre Architektur sowie die Hauptprozesse, wie die Registrierung einer Drohne oder die Verifizierung von Datenpaketen, bestimmt. Schliesslich wurden die Schwachstellen des gewählten Infrastrukturmodells und die daraus resultierenden möglichen Angriffe herausgearbeitet. Die Infrastruktur des Prototyps besteht aus einer Root-Zertifizierungsstelle mit internem Intermediate-Zertifikat, Validierungsstellen, den Drohnen und den Anwendern. Bis auf wenige Ausnahmen funktioniert der Prototyp wie erwartet.

Diese Arbeit zeigt, dass die Public-Key-Infrastruktur des Prototyps funktioniert und in die Praxis umgesetzt werden kann. Die Sicherheit des Luftverkehrs ist zu einer unvermeidlichen Frage geworden und das diskutierte Modell ist ein Beitrag zur Lösung für dieses Problem.

Bild klein 2.