Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

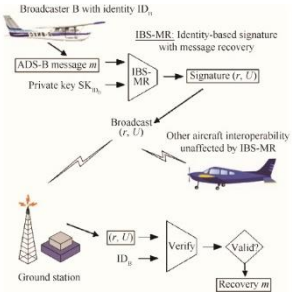
InIT Institut für angewandte
Informationstechnologie

Authentifizierte Langstrecken-Kommunikation - Konzept und Umsetzung

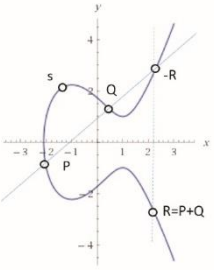
Diplomierende
Larissa Frei
Marc Iseli

Dozierende
Bernhard Tellenbach
Karl Rege

Hintergrund der vorliegenden Bachelorarbeit sind die in der jüngeren Vergangenheit vermehrt diskutierten Sicherheitsprobleme im Zusammenhang mit verschiedenen Aviatik-Funkprotokollen zum direkten Datenaustausch, wie z.B. FLARM und ADS-B. Diese Arbeit zeigt auf, wie das Problem der fehlenden Prüfung von Authentizität und Integrität der ausgetauschten Nachrichten für das FLARM-Protokoll gelöst werden kann. Der vorgestellte Lösungsansatz kann prinzipiell für beliebige, meldungsbasierte (Broadcast-) Kommunikationsprotokolle verwendet werden.
Für die Konzipierung der Lösung wurden verschiedene Signatur-schemen wie digitale Signaturen mit elliptischen Kurven und X.509 Zertifikaten sowie Hash- und identitätsbasierte Signaturen analysiert, wobei insbesondere auf entsprechende Lösungsvorschläge aus verwandten Arbeiten zurückgegriffen wurde. Dabei galt es, insbesondere die limitierte Rechenleistung der FLARM-Hardware und die geringe Bandbreite der Langstreckenkommunikation zu berücksichtigen. Zudem sollten weitere Aspekte, wie zum Beispiel eine gewisse Zukunftssicherheit oder die Rückverfolgbarkeit der zu einer digitalen Identität gehörenden Person, gewährleistet werden.
Die gewählte Lösung basiert auf dem für ADS-B vorgeschlagenen Signaturschema «EBAA: An efficient broadcast authentication scheme for ADS-B communication based on IBS-MR». Die Implementation von EBAA erfolgte in C++ mit der Library MIRACL Crypto SDK. Zusätzlich wurde eine mit dem RELIC Toolkit for Cryptography erstellte Referenz-implementation hinzugezogen. Die abschliessende Analyse der Umsetzung zeigt, dass für ein Sicherheitslevel von rund 110 Bits die zu Beginn definierte maximale Nachrichten- bzw. Signaturgrösse um knapp 50% überschritten wird.



EBAA mit IBS-MR



Beispiel einer elliptischen Kurve:
y^2=x^3-3x+3