Securing Aeronautical Telecommunications
[Invited Paper]

Simon Blake-Wilson

Certicom Corp., 200 Matheson Blvd W, Mississauga, Ontario L5R 3L7, Canada

Abstract. The Aeronautical Telecommunications Network or ATN is the next generation network being developed by the international aviation community for providing voice and data communications between ground stations and aircraft. It is currently being trialed and will ultimately be used for applications such as air traffic control.

This talk will discuss recent work to add security provisions to the ATN to prevent threats like disruption of service, misdirection of aircraft, and disclosure of commercially sensitive data relating to aircraft operations. The talk will focus on the challenges faced when designing a security solution in this environment, how these challenges were addressed by the ATN security design team, and what the cryptographic community can do in the future to help designers of other solutions meet these challenges. Examples of the challenges include:

- providing security in a bandwidth-constrained wireless environment;
- balancing the conflicting needs of confidentiality, integrity, and availability in safety-critical applications; and
- minimizing the amount of mutual trust necessary between users with limited trust in each other.

The goal of this talk is to identify which areas will be the focus of future cryptographic research by investigating the problems facing cryptographic designers today.

M. Walker (Ed.): IMA - Crypto & Coding'99, LNCS 1746, pp. 243–243, 1999.