A Key Generation System (KGS) Suitable for Sensor and Building Networks

David McGrew mcgrew@cisco.com and Brian Weis bew@cisco.com
September 26, 2011

Submission to the Workshop on Cryptography for Emerging Technologies and Applications

Emerging Technologies and Applications: Sensor/Building Networks, Smart Objects, Internet of Things
Cryptographic Requirements: Key establishment for nodes with limited computation and communication

Abstract

A sensor network is an ad-hoc network, possibly with dynamic topology, that includes nodes with limited computation and communication abilities. Key establishment in such networks requires special techniques. Much work has been done over the last decade on efficient key pre-distribution schemes, in which each device is populated with a distinct set of symmetric keys, each pair of devices can compute a pairwise secret, and the system is secure against the collusion of devices (up to some threshold). Flexible and compact key management systems for sensor networks have been described by Eschenauer and Gligor, Perrig and Song, Stinson and Lee, and many others.

This presentation focuses on a particular technique that is a good fit for the NIST cryptographic toolkit. The technique is based on the foundational works in this area: the Key Generation System (KGS) of Blom and Blundo et al, who presented information-theoretic bounds and efficient algorithms for achieving those bounds using polynomial functions over finite fields. This KGS can be used as an efficient key management system for sensor networks, or it can be used as a building block in other keying methods. Interestingly, the computations in the KGS of Blundo et al have much in common with the polynomial math used in the Galois/Counter Mode (GCM) of operation. In this presentation, we show how this KGS can be efficiently implemented using the mathematical primitives in GCM. This reuse of components is ideal for a sensor node with limited computational resources. We also review KGS designs, and describe how the KGS can provide security in the concrete model through the use of key derivation functions.