Contribution ID: **204** Type: **oral**

Key Management Strategies for Safeguards Authentication and Encryption

Thursday 23 October 2014 09:50 (20 minutes)

Management of cryptographic keys for the authentication and encryption of safeguards data can be the critical weak link in the practical implementation of information security. Within the safeguards community, there is the need to validate that data has not been modified at any point since generation and that it was generated by the monitoring node and not an imposter. In addition, there is the need for that data to be transmitted securely between the monitoring node and the monitoring party such that it cannot be intercepted and read while in transit. Encryption and digital signatures support the required confidentiality and authenticity but challenges exist in managing the cryptographic keys they require.

Technologies developed at Sandia National Laboratories have evolved in their use of an associated key management strategy. The first generation system utilized a shared secret key for digital signatures. While fast and efficient, it required that a list of keys be maintained and protected. If control of the key was lost, fraudulent data could be made to look authentic. The second generation changed to support public key / private key cryptography. The key pair is generated by the system, the public key shared, and the private key held internally. This approach eliminated the need to maintain the list of keys. It also allows the public key to be provided to anyone needing to authenticate the data without allowing them to spoof data. A third generation system, currently under development, improves upon the public key / private key approach to address a potential man-in-the-middle attack related to the sharing of the public key. In a planned fourth generation system, secure key exchange protocols will distribute session keys for encryption, eliminating another fixed set of keys utilized by the technology and allowing for periodic renegotiation of keys for enhanced security.

Country or International Organization

USA

Primary author: CORAM, Michael (Sandia National Laboratories)

Co-authors: BROTZ, Jay (Sandia National Laboratories); MCDANIEL, Michael (Sandia National Laboratories); HYMEL, Ross (Sandia National Laboratories)

Presenter: CORAM, Michael (Sandia National Laboratories)

Session Classification: Equipment Security and Considerations for Joint Use