Title: AN OPEN FRAMEWORK FOR LOW-LATENCY COMMUNICATIONS ACROSS THE SMART GRID

Author:John A. Sturm-PhD Candidate, Indiana State University, j.sturm@sbcglobal.net

Technology Space: Sensor and Building Networks
Class of Cryptographic Requirements: Performance of Cryptographic Services

ABSTRACT

The recent White House policy paper for the Smart Grid that was released on June 13, 2011, *A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future*, defines four major problems to be solved and the one that is addressed in this paper is Securing the Grid. Securing the Grid is referred to as one of the four pillars to be built on an open technology framework and cybersecurity practices must provide the special, low-latency communications needed for real-time automation control. NIST is tasked with development of the cybersecurity communication standards through establishment of the Cybersecurity Working Group (CSWG). This paper highlights some of the critical Smart Grid communications issues, tests an initial set of open technology solutions (i.e. OpenSSL, OpenVPN, OpenHIP, etc.) that address low-latency automation control file transfers, and recommends an open framework for the future that is capable of evolving over time as new demands and technologies become available. Among the requirements for real-time control are high speed file transfer capability to provide low-latency; strong security with Identity Management for trustworthy communications including Denial of Service (DoS) resistance to reduce delays/outages; and a reliable communications transport protocol per the Guidelines for Smart Grid Cyber Security (NISTIR-Volumes 1-3, 2010). Security is further defined as end-to-end trust (E2E trust) that implements cryptographic means of authentication at each end-point and also seamless security across all the protocol layers and routers, proxies, etc. between user interfaces and/or other devices. The solution tested in this paper provides low-latency file transfers through a system of open protocols that incorporate HMAC key processing (Hashed Message Authentication Code) and strong cryptographic identification for real-time automation control across the Smart Grid. Ultimately the payoff of the SmartGrid should be the creation of global wealth that benefits all people