Developing a Framework to Improve Critical Infrastructure Cybersecurity

Comments submitted 8 April 2013

Bill Worley PhD
CTO, Secure64 Software Corp.

Unless critical cyber infrastructure is built from system components that integrate essential security and defense capabilities from the ground up, no body of policies, best practices, standards, and procedures will be able to protect it sufficiently. The vicious cycle of vulnerability-exploit-patch will persist.

Experience deploying massively complex COTS systems lacking such integrated security and defense capabilities, then attempting to secure them with additional protective software and external bodyguard systems such as firewalls, intrusion detectors, etc., as well as operational standards, practices, and polices has:

- Shown itself unable to stem the still growing tide of bot formation, compromised systems, and successful cyber attacks. Systems continue to lose more and more cyber attack battles. It is clear that new thinking and approaches are needed.
- Produced no solid evidence that refinement of this current approach can be expected to succeed in the long run.
- Led to increasingly complex and expensive bodyguard systems, which are themselves often ineffective, vulnerable, and capable of being highjacked and used in attacks.
- Confirmed Albert Einstein's observation that "Insanity is doing the same thing over and over and expecting different results."

Cyber infrastructure components with the required capabilities for the core of our cyber infrastructure in fact exist today in DNSSEC systems used both by NIST and by the Department of Commerce. The hardware is commonly available from Hewlett Packard, is based upon Intel processors, and could quickly and cost effectively be deployed to far better effect than today.

Secure64's DNSSEC product family has been specifically architected for the heart of a critical cyber infrastructure. It produced the first fully automated DNSSEC signing server (partially funded by DHS). It embodies hardware and software architecture that is immune to malware injection and resists DDoS attacks at line speed with little latency. The full line of DNS servers built upon this secure architecture are now widely deployed on five continents, including important US Governmental agencies and large communication carriers. No client using Secure64's DNS severs has been disrupted by a DDoS attack. The design principles for this product family have evolved and are broadly applicable throughout all levels of a cyber infrastructure.

It is becoming increasingly clear to many that the cryptographic chain of trust established by DNSSEC can be leveraged to expand the core security of the cyber infrastructure significantly. Such expanded solutions, in turn, lead to important second-order security benefits for multitudes of application systems that rely upon the cyber infrastructure. This makes it practical and effective to begin now, at the heart of the critical cyber infrastructure, then incrementally deploy step-by-step extensions to expand strong security properties for communication and transaction protocols, benefiting SCADA, banking, and other critical systems. A workable sequence of initial priorities and steps could be:

1. Full DNSSEC deployment - a top priority.
   Step 1: Mandatory deployment in all critical cyber infrastructure.
   Step 2: Require integrated security and defense capabilities in all new DNSSEC server products.
   Step 3: DNSSEC system diversity to phase out vulnerable DNSSEC hardware and software over time.
2. Leverage DNSSEC to solve problems of:
   1. Route highjacking (working prototype today).
   2. Malicious Site Blacklisting.
   3. SSL/TLS Target site certificate validation (DANE)
   4. Trusted public key publication repository
   5. Effortless encrypted email, sender authenticated email, email-based malware attacks, SPAM, strong multi-factor authentication.
   6. Creative juices active in many quarters.

Secure64 welcomes the opportunity to engage with and contribute to NIST's critical cyber infrastructure framework process.

--