Introduction

The President's Executive Order in regards to reducing cyber risks for critical infrastructures, and the subsequent publication of a Request for Information by the National Institute of Standards and Technology, highlight the growing concern in regards to cyber threat and attack in what has become a very interdependent system of systems that make up the critical infrastructure.

The definition of critical infrastructure itself is a challenging one as the advancements of technology have greatly altered how we communicate and has introduced new dependencies around these communications. A hundred years ago communications were based on person-to-person communications. Trust in this environment was maintained y the interpersonal relationship of the parties. Yes, we had eaves-droppers and what we now know as "social engineers" but fundamentally the system of systems in the early 20th century was largely reliant on people's actions based upon their interaction with another human entity.

In the latter part of the 20th century this interaction changed with the growth of the Internet, personal computers and computing devices, and machine-to-machine communications expanded. This altered the landscape in that now computing devices, or machines, were directly interacting with other computing devices, or machines. Similarly, people were interacting with machines more and more, whether it was a login to a local computer or remote mainframe or if it was the late 1990s and someone needed that last minute birthday gift from Amazon. These interactions changed how we developed and maintained trust. It is the basis of this idea that the comments towards the Framework for Reducing Cyber Risks to Critical Infrastructure are made.

Comments on Cybersecurity Framework

As described above, trust within the existing framework is one that is based around trust of the interaction of computing devices. These devices could be servers, personal computers/laptops, mobile devices, or automated machines such as industrial control devices. There are many ways to allow these devices to establish trust between each other but a common approach is through the use of digital certificates. These certificates are standards-based forms of digital identity that allow establishment of trust using common and standards-based protocols such as SSL/TLS, IPSec or SSH as examples.

These digital certificates are more commonly used than many people realize. A 2012 Research Study by Ponemon Research[1], which looked at over 2300 Global 2000 organizations in the US, Germany, UK, France and Australia, showed that an organization averaged 17,807 digital certificates within their organization. A more significant finding was that 51% of these organizations admitted to not knowing how many certificates were in use or where they were used. The fact that a large number of certificates are used within an organization but that a large percentage of those are not aware of where all of these certificates are create a unquantifiable cybersecurity risk. For this reason many large financial, retail and manufacturing organizations along with those in Government and the utility sector have begun to adopt a seven step best practice for managing their environment in regards to digital certificates, as well as for SSH and symmetric keys. These steps include:

1. Develop a comprehensive inventory of cryptographic assets, including
    - End entity digital certificates
    - Root and intermediate certificates that are trusted within the environment
    - SSH keys used within an organization and how these keys are implemented
    - Symmetric keys in use within the organization
2. Establish valid ownership of these identified assets
3. Monitor these assets for compliance
    - Alert owners to policy violations
    - Implement escalation plans to ensure action
4. Daily validation of the implemented assets
5. Comprehensive reporting to identify potential risks that either exist or can be projected
6. Automated enrollment and revocation of assets
7. Automated provisioning to devices and applications, ensuring automated testing to ensure proper implementation

In regards to the policy aspects, the largest concerns identified by organizations are in regards to:

- Certificate expiry, particularly for secure applications where expiry will result in loss of application or device availability
- Cryptographic weaknesses that expose the possibility of direct key attacks or attacks against a certificate, such as certificate replication.
- Certificate Authority (CA) Compromises which create potential risk due to the breadth of devices that possibly trust an internal or external CA that has had its trust breached
- SSH key theft or SSH attacks

[1] http://www.venafi.com/ponemon-institute-first-annual-cost-of-failed-trust-report/

All of these attacks create risk to an organization that have not identified its current assets and its current trust architecture.

Elements within the seven steps listed above fall into two categories: critical actions and; operational improvement. Steps 1 through 5 are critical for most organizations as without these steps implemented the potential attack vectors are unknown. An example of an unknown risk is:

- the case of printers that are shipped directly from a manufacturer with digital certificates that are signed using an MD5 hash. This issuance was still ongoing in May of 2012, many years after MD5 had been proven vulnerable to attack.

Within the area of policy compliance, identifying existing assets and evaluating them against existing policy is a critical part of continuous monitoring of the overall cybersecurity posture. This type of continuous monitoring would have quickly discovered the SSL certificate that currently protects the secure side of the White House website does not meet the Federal PKI policy.

These elements of cryptographic asset management are today key parts of guidelines such as Electricity Subsector Cybersecurity Capability Maturity Model, Reference section 4.3.3 and while there are general references to the need for continuous monitoring of the cryptographic assets in NIST SP 800-53 and specification for algorithmic use within NIST SP 800-57 there is not clear set of define processes for use of a system that would be built around NIST SP 800-152, which is still in draft form.

With these standards and special publications listed above, and guidelines such as the NIST ITL of July 2012 on CA Compromise recovery, highlighting the need for effective certificate and key management, organizations are looking for a more refined definition of the processes to put in place to effectively manage their cryptographic assets and thereby reduce risk in regards to key or certificate attack.