Position Paper: Executive Order on Improving the Nation’s Cybersecurity

Chris Miyata (chris.miyata@microfocus.com) & Luther Martin (luther.martin@microfocus.com)
Representatives from Voltage, a division of Micro Focus

Date: 5/26/2021

This position paper addresses Section 4(e)(i)(E) of the May 12, 2021 “Executive Order on Improving the Nation’s Cybersecurity,” in particular its requirement to secure software development environments by “employing encryption for data.”

There has been much work done in the past few years that supports the goal of enhancing software supply chain security. To support this, NIST has published several documents, including at least these:

- NISTIR 8276, “Key Practices in Supply Chain Risk Management”
- NISTIR 7622, “Notional Supply Chain Risk Management Practices for Federal Information Systems,” NISTIR 8272, “Impact Analysis Tool for Interdependent Cyber Supply Chain Risks”
- NIST Special Publication 800-161, “Supply Chain Risk Management Practices for Federal Information Systems and Organization,”
- NIST Special Publication 800-37, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy”
- NIST Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations”
- “NIST Framework for Improving Critical Infrastructure Cybersecurity.”

The CERT division of the Software Engineering Institute has also been active in this area, and its members have written multiple papers on the topic, while CERT has organized and run workshops on it. There is even an ISO standard on the topic, ISO/IEC 27036-3:2013, “Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for Information and communication technology supply chain security.” In short, many of the issues around how to improve the security of the software supply chain are already well-understood, but these approaches have not yet been widely implemented. Thus, we instead focus on an area that has not yet received much attention: the use of encryption as EO 4(e)(i)(E) requires.

Federal agencies and their supporting contractors use of encryption to protect both data at rest and in transit as required by Federal Information Security Modernization Act of 2014 (FISMA). This is typically accomplished by using Transport Level Security (TLS) and transparent disk encryption (TDE). While both of these technologies are useful and are very effective at countering certain threats, they do not protect against the most serious attacks at all: often collectively called “advanced persistent threats (APTs),” these operate at the Application layer of the TCP/IP protocol stack.

TLS operates between the Application and Transport layers. TDE operates below the Network Access Layer. Encryption relative to a particular layer of the TCP/IP stack only protects against threats that operate at that layer or below, so that APTs that operate at the Application layer are unaffected by these uses of encryption. At the Application layer, the protection provided by TLS or TDE is not present, so threats that work at that level simply do not have to worry about cracking the encryption or bypassing it. From their point of view, the data is not protected by encryption at all.

The commercial world strongly follows what NIST does. Although FIPS 140-3, “Security Requirements for Cryptographic Modules,” is only required to be followed by Federal agencies, it has become the *de facto* standard for encryption for the entire world. The ISO standard “ISO/IEC 19790:2012 Information Technology - Security Techniques - Security Requirements for Cryptographic Modules” is essentially a reformatted version of FIPS 140-3. Even the Chinese Commercial Cryptography Scheme is largely a translation of FIPS 140-3 into Chinese. In short, NIST is in a leadership role for the world for the standardization of encryption technology. But their cautious approach in this area has had some unfortunate consequences.

As Section 6.8 of the "National Cyber Leap Year Summit 2009 Participants' Ideas Report" noted, the Federal government has been slow to adopt innovative approaches to encryption, which has, in turn, led to the slow adoption of innovative approaches to encryption everywhere. And the Federal government has actually made it more difficult for Federal agencies to test a new encryption technology over time by making it more difficult to get the necessary Interim Authority to Operate these new technologies. This is a step in the wrong direction.

The National Cyber Leap Year report recommended the following:

> **6.8.4 Action Plan**
>
> NIST should determine a way to quickly approve provably-secure technologies for Federal use and should review existing regulations and identify ways to allow provably secure technologies within them. This should involve, as a minimum, granting a blanket IATO to new encryption technologies with peer-reviewed proofs of security, and adding provably-secure public-key encryption technologies to the list of techniques that are allowed by FIPS 140-2. In the long run, standards and policies should be changed to allow the rapid adoption of new technologies that are provably secure.
>
> **6.8.5 Jumpstart Plan**
>
> Within 90 days, NIST should define and implement a way to approve provably secure technologies for Federal use. Within 180 days, a pilot of one of these technologies should be started at a Federal agency.

It looks like these recommendations were not acted upon. This should change. By following these recommendations, NIST would be actively encouraging the adoption of the newer encryption technologies that have proven useful in protecting data at the application layer, which is exactly what is needed to protect against the APTs that are currently a danger to the nation's software supply chain. The current common uses of encryption are not protecting against the most serious threats that the software supply chain currently faces. TLS and TDE are not enough to address today's serious threats. What FISMA requires is not enough. One critical vulnerability with the current TLS and TDE deployment model is that it is overly reliant on a very narrow level of accountability for security around data in flight. To mandate a secure tunnel for data to travel between components, but not mandate data be encrypted as it enters and leaves a TLS connection leaves data vulnerable to attacks in the sending and receiving applications. Data should be encrypted as close to the point of data origination as possible and maintain that encrypted state until the exact moment when the original plaintext data is required for use. NIST should act quickly to address this issue by encouraging the use of useful innovative encryption technologies. The result would be a greatly improved level of security against APTs in general, and against those that target the software supply chain in particular as the NIST guidance gets adopted, initially by the Federal government, and subsequently by the US private sector.