Response to NIST RFI: 81 FR 52827

Information on Current and Future States of Cybersecurity in the Digital Economy

By:

Jackrabbit Consulting

R. W. Stavros, Ph.D.

Ian Stavros

Bryan Turek

The following are in response to the NIST RFI 81 FR 52827 named Information on Current and Future States of Cybersecurity in the Digital Economy. Specifically, this response covers the topics mentioned in the RFI.

1. Critical Infrastructure Cybersecurity

One of the biggest stumbling blocks confronting the transition to digital economy is providing an infrastructure that works with existing hardware and software technologies and yet can offer assurance for the security of the transactions and the ledger used to store the results. The infrastructure must be standards based versus product based. For example, the infrastructure must work on Microsoft, Apple, Android, Linux, and UNIX operating systems and work on the major browsers. Apple Pay is an example or a product which offers reasonable cybersecurity but it requires an entire Apple ecosystems and does not run on Android or Windows based Operating Systems. This does not mean that Google Wallet, Samsung Pay, Android Pay or Current C do any better with regards to this [13a] All of these "Pay" methods only provide a fronted to existing financial instruments denominated in as currency such as credit cards and bank accounts.

There are standards such as Object Management Group's (OMGs) [16] Data Distribution Service [8] family of standards that cover critical infrastructures cybersecurity, however, these standards only cover critical infrastructure cybersecurity in Local Area Networks (LANs) versus being available on Wide Area Networks (WANS). Several companies that have implemented products that are compliant with the DDS standards that work over WANs, but the solutions are not standards based. There is also no standard way to hook "Pay Technologies" up to the secure infrastructure.

2. Cybersecurity Insurance

Cybersecurity Insurance, as with all insurance, is based on actuarial tables which assign risk to a failure in some component or portion of the digital economy. As a general rule, the more components in a system, the higher the risk of failure. If there is a high degree of interdependence of the components, then the risk becomes multiplicative versus additive [2]. Examples of dependent components in the cybersecurity in the digital economy would be "the build" of the components required to comprise a working component. If any of the components has risk, then the risk is cascaded multiplicatively throughout the digital economy since all the components are dependent on each other. Risk can be reduced if each component is independent of the other. For example, the marshaling/de-marshaling are independent of the encryption/decryption which is independent of the transport protocol.

For example, one of the biggest risks to insuring/ensuring bitcoin would be the spoofing of a transaction [20], or a double spend [17a]. Block-chains are the implementation methodology for bitcoins, and have spent a considerable amount of effort on solving these two issues, although there is more work that needs to be done.

Other issues might be the delay of a transaction, the knowledge that a transaction is underway or the speed at which a transaction can be made [27]. Protecting the metadata surrounding a transaction is as important as protecting the transaction data itself. This generally requires multiple layers of encryption. For example, the data required to route the transaction through the network needs to be free and clear on the internet. However, the information about the participants of a transaction needs to be encrypted independently from the information held within the transaction. For example, the bank or brokerage house might need to have information about the participants, but the details of the transaction are to remain "out of sight" to the network and administrative staff [18].

3. Cybersecurity Research and Development

As fast as the cybersecurity community can evolve to protect cyber data and assets, the nefarious element is moving to find new ways to break it [3]. The use of the word nefarious is not unintended. Not all nefarious activity is necessarily criminal [19] and can have a broad range of purposes.

Lately, because of the poor choice of passwords made by many users (i.e., "password" and "123456"), the use of passwords is being frowned upon.[24] in favor of biometrics such as fingerprints, retinal scans and even facial and voice recognition. The need for middleware involvement in the IA is essential. [4].

DDS Security [10], as an example, cleanly separates the marshaling/un-marshaling and the encryption/decryption from the Identification and Authentication (IA) through the use of a standardized interfaces. This allows the IA aspects of security to evolve independently from the rest of the middleware. The only requirement is that all participants in the secure DDS infrastructure are in sync with respect to IA and encryption/decryption. That is why secure DDS has security "baked in" rather than applied like frosting.

4. Cybersecurity Workforce

According to the Bureau of Labor Statistics, the rate of growth for jobs in information security is projected at 37% from 2012–2022—that's much faster than the average for all other occupations [22]. With this kind of demand, it will be almost impossible to meet the need. One way to mitigate this demand is to have clear and well defined boundaries between the infrastructure required to support digital economy and the cybersecurity requirements. This separation allows the companies and consequently people that provide middleware and infrastructure to do what they do best and allow the cybersecurity companies to focus on what they do best without having to duplicate efforts or compete.

To accomplish this clean separation, there needs to be well defined unbreakable interfaces as the bond between the two groups. DDS Security [10] provides that separation by defining an interface that facilitates loose coupling [25] between the security and the middleware components. The interface design also foster cohesiveness within the components [7].

5. Federal Governance

At the Federal level, the digital economy governance needs to prescriptive not descriptive [6]. Descriptive governance describes an actual hardware and software architecture which is great for the companies that own the products or the components captured within the descriptive architecture, but will fall short of the rigor required to not only implement the architecture but to provide a dynamic, responsive digital economy that is not subject to vendor lock-in and provides a plethora of responses to the ever evolving threats to the digital economy. The federal governance needs to be prescriptive in nature and provide actionable requirements and guidance. The resulting implementations need to be measurable for compliance to the governance. This is accomplishable using very rigorous methods for capturing the requirements and guidance using governance models similar to those described by Net-centric Enterprise Solutions for Interoperability (NESI) . [15].

6. Identity and Access Management

Built into the DDS Secure standard is Identity and Authentication (IA) which meets some of the toughest Federal standards. However, the DDS Security Standard [10] allows for different mechanism to be used to implement IA. This allows the IA methodology to evolve. For example, the current trend is towards the use of biometrics, the DDS implementations only needs to be modified to accept these new IA policies. If an IA policy such as PINs become invalid in the future, a DDS Secure implementation that relies on PIN methodology can no longer gain access to the DDS implementation that strictly requires biometrics.

7. International Markets

DDS is already widely available within the international community and is standardized through the Object Management Group (OMG) [16]. OMG has an effort underway to have the OMG standards made available as International Standards Organization (ISO) standards also[12]. DDS is an open standard it has an advantage over products which are only Open Source Software (OSS) since the standardization process is openly developed using stringent transparent rules and is not subject to obstacles which protect OSS products or individuals that support the product. Often, the OSS software community derive their incomes from consulting services which is not conducive in building the best products. See Where Can I Get DDS [26].

8. Internet of Things

The Internet of Things (IOT) is divided into the Industrial Industry of Things (IIoT) and the Consumer Internet of Things (CIoT) [14]. Although it is easy to consider only the CIoT when thinking about a digital economy, the concepts of a digital economy can easily be applied to IIoT especially when it is applied to optimization and budgeting. For example, should an IIoT device wait to work after 7:00 pm to get the cheapest price for energy, or can it tap into the excess solar energy during the day. If the IIoT device is “billed” for its energy use, the decisions it makes may be different. Additionally, is the CIoT only for devices that a human consumer uses or can it be for robotic or automated devices?

There are numerous standard protocols that are used to connect the CIoT devices together such as such as WiFi, Bluetooth, ZigBee and 2G/3G/4G cellular [1]. However, the cybersecurity of many of these protocols is questionable, especially the implementation of these protocols (i.e., Is https used? Is data sent encrypted? Is proximity of the CIoT devices used as security?).

The IIoT seems to have aggregated around the use of the OMG DDS protocol, especially “at the edge”, and its family of standards. It is also extensively used in Supervisory Control And Data Acquisition (SCADA) environment [9] which substantiates its use in large scale, mission critical systems. DDS has security “baked in” when the DDS Security [10] protocol is used. This would be analogous to HTTPS, but extremely lightweight and offering speeds that can exceed 1,000 times the speed of HTTPS and Web Sockets.

9. Public Awareness and Education

After years of trying to inform the public of the need to use secure and strong passwords, the two most common computer passwords in 2015 were “123456” and “password,” according to SplashData, a supplier of security applications. [24]. Consequently, the best way forward seems to be the adoption of easy to use and more secure techniques for data that are required to secure digital economy data and transactions. At the heart of these techniques is the use of biometrics [4]. The rapid and relatively painless adoption of the use of Apple's fingerprint scanner called Touch Id for securing iPhones is well known [5] indicates a willingness to adopt stronger cybersecurity. The IA methodology can not be arcane or cumbersome requiring the user to remember dozens of passwords.

Android has already made progress towards facial recognition for IA[21]. Apple is also working on iris scanners for release in 2018 [17].

The biggest stumbling block is the assurance that biometric information is protected and is not shared internally or externally from the application. For example, sending biometric data to centralized servers does not sit well with many people. There is still skepticism about the use of private and personal data by corporation referred to as Pervasive Monitoring Is an Attack. [11]

10. State and Local Government Cybersecurity

A major advantaged of using standards based technologies with quite a few vendor implementations [26], is the ability for different parts of the government to select and use the products that best meet their functional and non-functional requirements at the time the systems are built. Because the DDS family of standards also include a wire protocol which has been successfully demonstrated by 13 companies vendor interoperability is ensured. The wire protocol allows a hybrid mix of DDS vendors to work together. In other words, each government entity (Federal branches, agencies, etc, State and Local government bodies) can choose the DDS product meets their needs and that works best for them. When the time for interaction or integration occurs, there is no need to break existing systems to adopt the “new solution”.

Since the used of DDS Security [10] requires Identification and Authentication (IA) which meets NSA standards, State and Local governments can leverage the “out of the box” cybersecurity with minimum preparation. If a governing body for some reason does not choose to implement DDS Security, they can not interact with the secure DDS implementation directly. This in essence can crate a firewall of sorts between secure installation and non-secure installations.

DDS Security relies on the highest levels of encryption for data over the wire. This means that certain types of network attacks, like Man In The Middle (MITM) [13], are near impossible since network and systems administrators can not read the information with “snoopy” software such as Wireshark [23].

References

1. “11 Internet of Things (IoT) Protocols You Need to Know About» DesignSpark.” Accessed September 9, 2016. http://www.rs-online.com/designspark/electronics/knowledge-item/eleven-internet-of-things-iot-protocols-you-need-to-know-about.

2. “12.5 - An Extension of Effect Modification - Additive vs Multiplicative Effect Modification | STAT 507.” Accessed September 9, 2016. https://onlinecourses.science.psu.edu/stat507/node/86.

3. “2016 Cybercrime Reloaded: Our Predictions for the Year Ahead.” Accessed September 9, 2016. https://securityintelligence.com/2016-cybercrime-reloaded-our-predictions-for-the-year-ahead/.

4. “A Survey of Biometrics Security Systems.” Accessed September 9, 2016. http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/.

5. “About Touch ID Security on iPhone and iPad.” Apple Support. Accessed September 9, 2016. https://support.apple.com/en-us/HT204587.

6. “Classroom - Udacity.” Accessed September 9, 2016. https://www.udacity.com/course/viewer#!/c-ud805/l-1777008537/m-657128555.

7. “Coupling And Cohesion.” Accessed September 9, 2016. http://c2.com/cgi/wiki?CouplingAndCohesion.

8. “DDS.” Accessed September 9, 2016. http://www.omg.org/spec/DDS/.

9. “DDS in SCADA, Utilities, Smart Grid and Smart Cities.” 10:40:42 UTC. http://www.slideshare.net/Angelo.Corsaro/dds-in-scada-utilities-smart-grid-and-smart-cities.

10. “DDS-Security.” Accessed September 9, 2016. http://www.omg.org/spec/DDS-SECURITY/.

11. Farrell, Stephen, and Hannes Tschofenig. “Pervasive Monitoring Is an Attack.” Accessed September 9, 2016. https://tools.ietf.org/html/rfc7258.

12. “ISO - International Organization for Standardization.” ISO. Accessed September 9, 2016. http://www.iso.org/iso/home.html.

13. “Man-in-the-Middle Attack.” Wikipedia, the Free Encyclopedia, September 8, 2016. https://en.wikipedia.org/w/index.php?title=Man-in-the-middle_attack&oldid=738326400.

13a. “Mobile Wallet Guide - Pros, Cons and Who Accepts Them.” Tom’s Guide, October 19, 2015. http://www.tomsguide.com/us/mobile-wallet-guide,news-20666.html.

14. Nagaraj, Varun. “The Industrial IoT Isn’t the Same as the Consumer IoT - O’Reilly Radar.” Accessed September 9, 2016. http://radar.oreilly.com/2014/02/the-industrial-iot-isnt-the-same-as-the-consumer-iot.html.

15. “NESI.” Wikipedia, the Free Encyclopedia, November 26, 2014. https://en.wikipedia.org/w/index.php?title=NESI&oldid=635570346.

16. “Object Management Group.” Accessed September 9, 2016. http://www.omg.org/.

17. “Report: Eye Scanning Capabilities Coming to the iPhone in 2018 | 9to5Mac.” Accessed September 9, 2016. https://9to5mac.com/2016/07/25/eye-recognition-support-for-iphone/.

17a. Ross, Sean. “How Does a Block Chain Prevent Double-Spending of Bitcoins?” Investopedia, June

19, 2015. http://www.investopedia.com/ask/answers/061915/how-does-block-chain-prevent-doublespending-bitcoins.asp.

18. Sanger, David E., and Eric Schmitt. “Snowden Used Low-Cost Tool to Best N.S.A.” The New York Times, February 8, 2014. http://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.html.

19. ———. “Spy Agency Consensus Grows That Russia Hacked D.N.C.” The New York Times, July 26, 2016. http://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html.

20. “Security - Creating a Fake Transaction - Bitcoin Stack Exchange.” Accessed September 9, 2016. http://bitcoin.stackexchange.com/questions/21445/creating-a-fake-transaction.

21. “Snapdragon SDK for Android: Facial Recognition.” Qualcomm Developer Network. Accessed September 9, 2016. https://developer.qualcomm.com/software/snapdragon-sdk-android/facial-recognition.

22. “The Future of Cybersecurity Jobs | Monster.com.” Monster Career Advice. Accessed September 9, 2016. http://www.monster.com/career-advice/article/future-of-cybersecurity-jobs.

23. “Tools - The Wireshark Wiki.” Accessed September 9, 2016. https://wiki.wireshark.org/Tools.

24. “Weak Passwords Only Part of the Cyber-Security Problem - CGMA Magazine.” Accessed September 9, 2016. http://www.cgma.org/Magazine/News/Pages/weak-passwords-top-cyber-security-problems-201613887.aspx?TestCookiesEnabled=redirect.

25. “What Is Loose Coupling? Webopedia Definition.” Accessed September 9, 2016. http://www.webopedia.com/TERM/L/loose_coupling.html.

26. “Where Can I Get DDS?” Accessed September 9, 2016. http://portals.omg.org/dds/where-can-i-get-dds/.

27. zachmider, Miles Weiss Zachary Mider. “Legendary Hedge Fund Wants to Use Atomic Clocks to Beat High-Speed Traders.” Bloomberg.com, July 7, 2016. http://www.bloomberg.com/news/articles/2016-07-07/jim-simons-has-a-killer-flash-boy-app-and-you-can-t-have-it.