PUBLIC SUBMISSION

As of: 3/23/22 7:59 PM
Received: March 22, 2022
Status: Pending_Post
Tracking No. l11-nn2j-q5eh
Comments Due: April 25, 2022
Submission Type: Web

Docket: NIST-2022-0001
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comment On: NIST-2022-0001-0001
RFI-2022-03642

Document: NIST-2022-0001-DRAFT-0013
Comment on FR Doc # N/A

Submitter Information

Organization: METEORA SYSTEM Co., Ltd.

General Comment

Technology Beyond Security 'Countermeasures'.

Governments and the private sector are battling the threat of cyber terrorism on a daily basis. A series of products and services have been created under the name of 'security' or 'solutions', but 20 years have passed without any solution to the problem. As this history shows, these 'countermeasures' have not achieved cyber defense. This is an important lesson that countermeasure technology cannot fundamentally solve the problem. Shouldn't government and private sector resources be devoted to fundamental cyber defense technologies that can 'solve' the problem, rather than relying on this term and being fooled by it?

We have already perfected two technologies that can 'solve' the problem. As a small business, we did it all on our own, without relying on grants or outside funding. Both proofs of concept were completed before 2015. Unfortunately, Japan does not have a contact point to propose this to policy makers.

One is 'Advanced TCP/IP' and the other is a 'noncommutative algorithm', which corresponds to post-quantum cryptography. These IPs include information-theoretic mathematics, implementation protocols, and patents that have gone through a PoC and will end the era of cyber terrorism.

IP 1: Prior art for Advanced TCP/IP.

The patent specification does not mention the hyperfine time stamp (the third identifier). The patent claimed the basis of the hyperfine time stamp (updating the initial value). NIST (in 2012) saw what this meant and asked me to register 'Figure 4' as a copyrighted work, and we complied. This process helped to give birth to Advanced TCP/IP. If vendors commercialize and promote secondary products, we can realize 'CLEANNET', which guarantees the privacy of the net and does not give freedom to unauthorized attempts to establish connections.

IP 1 has the following features: A 3-way handshake of a backdoor or a virus selectively and forcibly causes a 'TCP/IP connection error', making the TCP/IP communication channel impassable. For example, by stealing the identifier of the communication channel (the third identity), the communication channel can be hijacked under normal circumstances, but this IP causes a 'TCP/IP connection error' against such an attack. This algorithm and protocol paralyze attackers, especially in DDoS attacks. Demonstration and testing of this technology was completed before 2011. At that time, it was implemented at Layer 5. Future implementations are expected to be at Layer 3 and Layer 4. Meeting people who have a desire to leave the world a better place will end the era of cyber terrorism.

IP 2: Consensus algorithm for the post-quantum era.

Usually, ransomware invades a LAN, steals password files, hijacks user's job privileges, and accesses DBs. This behavior is neutralized by this IP. This IP is a technology to realize the key management (knowledge partitioning and dual control) required by PCI DSS v1.2. This can be described as separation of duties and consensus process. The v1.2 did not know how to implement this in the net. In 2013, we discovered a pair of one-way functions. This is the implementation technique. Currently, an online beta version is available for loan. Incidentally, because of the consensus verification algorithm, applying it to the blockchain solves the problems of privacy, finality, scalability, etc. and can even create a digital currency that is perfectly compatible with banknotes.

The "Internetwork Transmission Control Program" of 1974 was a global civilization experiment. This was the first civilizational experiment. I define the trend since 1974 as the 'age of cyber terrorism'. Breaking this conventional wisdom is the mission of my IPs. In other words, it is a 'mission to end the age of cyber terrorism. These IPs have the power to do so logically. If we don't do it, our sense of right and wrong will be paralyzed, and we will not leave a better world for future generations. Therefore, we must work on it from this very moment. To make the second civilization experiment a success, we need a new encounter. 1974 (the first civilization experiment) was led by a U.S. government agency. Who will lead the second civilization experiment? In this light, the estimated $6 trillion in ransomware damage is a concrete measure; in 1974, there was no such clear indicator. This indicator is the significance and rationale for government and private sector investment in 'problem-solving technology'.