February 12, 2018

Comment Template for Draft NIST Interagency Report (NISTIR) 8200 -- Status of International Cybersecurity Standardization for the Internet of Things (IoT)

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
1	Comment preparation: ProjectSafety.org MerlinCryption See white papers: *A Newly Clarified Fourth state of Data* *Embedded Encryption Platform Benefit Analysis* IoT Is Changing the Cybersecurity Industry Is Cybersecurity Encryption Ready to Break?		901 6.4 Identity and Access Management	In, general current authentication uses something known, physically and possessed using a static digital signature algorithm for access. The use of authentication signatures normally allow access to an individual who in turn accesses digital processes. IoT many times is an extension of human to machine, machine to machine, machine to app and even app to app processes. IoT can also be connected to its own local ecosystem and not a network. This requires IoT to have new levels of authentication. Criminals can crack security when they can anticipate and predict the actions, behaviors, and outputs of their target's processes. Current authentication algorithms are static which present a beginning and end crackable capability with Super and Quantum Computers. To a address this, a technology based on Nondeterministic Algorithms must be designed to exhibit different behaviors on every 'run'. Current identity and access management techniques are not effective in the interoperable crossing of all hardware, network, software and IoT protocols. There must be standard criteria for IoT identity and access management techniques that connect and interoperate across all process platforms Authentication must be from human to machine, machine to machine, machine to app and app to app across many IoT protocols and cloud connections. To both properly offer access and privacy there must be continuous and separate approaches to multi-level authentication techniques offering proper levels of access, security and privacy. Reinforced Control and Access Security factors need to be controlled only by designated top, trusted and authorized security individuals, Independent control. These security factors must be invisible to users and provide multi-dimensional security.	Most authentication is one or two factors in which developers can algorithmically use temporary and environmental factors. IoT often extends the authentication requirements with data that could be data in change that may require temporary access to machine only authentication outside of human parameters. The proposed change in authentication offers the required additional factors of reinforced control and access security needed in IoT. The proposed change offers nondeterministic authentication algorithms that hackers cannot anticipate and predict the actions, behaviors, and outputs of their target's processes. This millisecond randomization change offers available technologies that are also Quantum Computer ready. To accomplish reinforced control and access to one or multiple points, an 'Independent Control' is propose that can provide security checks and balances within a system. Also offered in proposed change is one trusted/authorized person/team designated to control certain mechanisms/factors, while another point of control determines other mechanisms/factors. In addition, the propose change offers a proactive security design or immediate situational response that may be required in even blind machine to machine actions. These differences require changes in human to machine identity and access management which is separate from machine to machine identity and access management. The proposed change offers an operational identity and access management solution that addresses these changes The proposed change offers types of security that need to be unknown and invisible to everyone else in the organization if they are to be effective. This is especially true when initiated by an un seen machine authenticated actions like IoT. In addition, we propose security factors that cannot be accessed or changed, by either error or malicious intent. Independent control, invisible to users, provides multi-dimensional security. This circumvents outside access to security control by users or inside attacker. This unknown category reinforces stealth while increasing authentication factor availability.
