Homework Number: 12
Name: Yi Qiao
ECN Login: qiao22
Due Date: 04/23/2019

Critiques on NIST 800-53

NIST 800-53, as its name suggests, is a document of security and privacy controls for federal information systems and organizations. The document showed us security control models, baselines, designations, and also specified the process of achieving a certain security level.

In section 2.1, the document introduced the three-tiered risk management approach and the risk management framework. The three-tiered risk management model addresses risk at the (i) organization level; (ii) mission/business level; (iii) information system level, while the risk management framework splits the process of building a secure system into 6 different steps.

In my perspective, it is good to have a generic framework for building up secure information systems. By doing what the risk management framework suggests, Categorize, Select, Implement, Assess, Authorize, Monitor, step by step with the guidelines provided in the 800-series documents, one can certainly build a secure information system in some sense. However, it seems like such a system may take too long to respond to a real world zero-day vulnerability due to its complicated nature.

In the cyber security world, everything is changing extremely fast. While a system was unbreakable yesterday, with the birth of a zero-day bug, it simply might not be as secure as before at all. In April 2014, when everyone still believe HTTPS with SSL/TLS is extremely secure, the Heartbleed vulnerability is discovered. Since the Heartbleed allows the attacker can easily get data in the memory of the victim machine, it is possible for the attacker to find the key, hijack the entire session and easily get your credit card information or something else interesting. From there, we can see a bit of the unpredictability of the cyber security world. Even though we learn from the past failures, the damage a single new glitch could make can still be numerous in a very short amount of time. No attacker will wait until the framework process the new bug and assessment of the solution is done. Thus, the framework 800-53 suggests will simply fail due to long response time of its 6 steps model.

Moreover, it seems like the way the document suggests lacks redundancy for future-proof. To me, it seems like it is almost impossible to predict what is going to happen at what time in the cyber security world. We will never know if there will be a zero-day bug leaking out tomorrow. So the only thing we can do, on top of built our system securely with the knowledge we already have, is to build at least some redundancy systems that protect us when something actually happens. Not in a particular part of the system (like get redundancy to mitigate DDOS attack),

but in a more generic way. We should require more redundancy systems for critical parts in our society. (like governments, banks, etc.)

All in all, it is good to have regulations for security control, but we have to do it in a more efficient and effective manner.