Cybersecurity – Compliance Borne Insecurities

Avi Kak

kak@purdue.edu

Robot Vision Lab,
Purdue University

CIKR Cybersecurity
Today's Reality vs. What's Needed

- **Today's Reality: All Federal Agencies are required by law to follow the "NIST 800 Series of publications" for their cybersecurity needs.**
  (This is a prescriptive approach based on known security vulnerabilities.)

- **What's Needed: Each CIKR entity must contain well-funded code and protocol analysis units capable of launching mock cyber attacks on the entity in the same manner as our adversaries.**

CIKR: Critical Infrastructure and Key Resources

Problem 1 with Cybersecurity Based on 800-Series Publications

- **It provides a convenient escape hatch for those who are charged with ensuring cybersecurity for a CKIR entity.**

> **"If an attack were to be successful despite compliance with the 800-series, then the attack simply could not have been avoided."**

Problem 2 with Cybersecurity Based on 800-Series Publications

- **RMF as presented in the 800-Series is more appropriate for entities that can create statistical models of risk --- which is something that cannot be done for cyber attacks.**

- **The worst cybersecurity attacks are based on newly discovered vulnerabilities in protocols and code. Therefore, it is not possible to create models of risk mitigation in advance for such attacks.**

RMF: Risk Management Framework

It is Good to Remember that…

- **Nothing in the 800-series could have anticipated the massive 600 Gbs DDoS attack on KrebsOnSecurity.com in September 2016 or the 1 Tbs DDoS attack on the OVH web hosting service in France around the same time.**

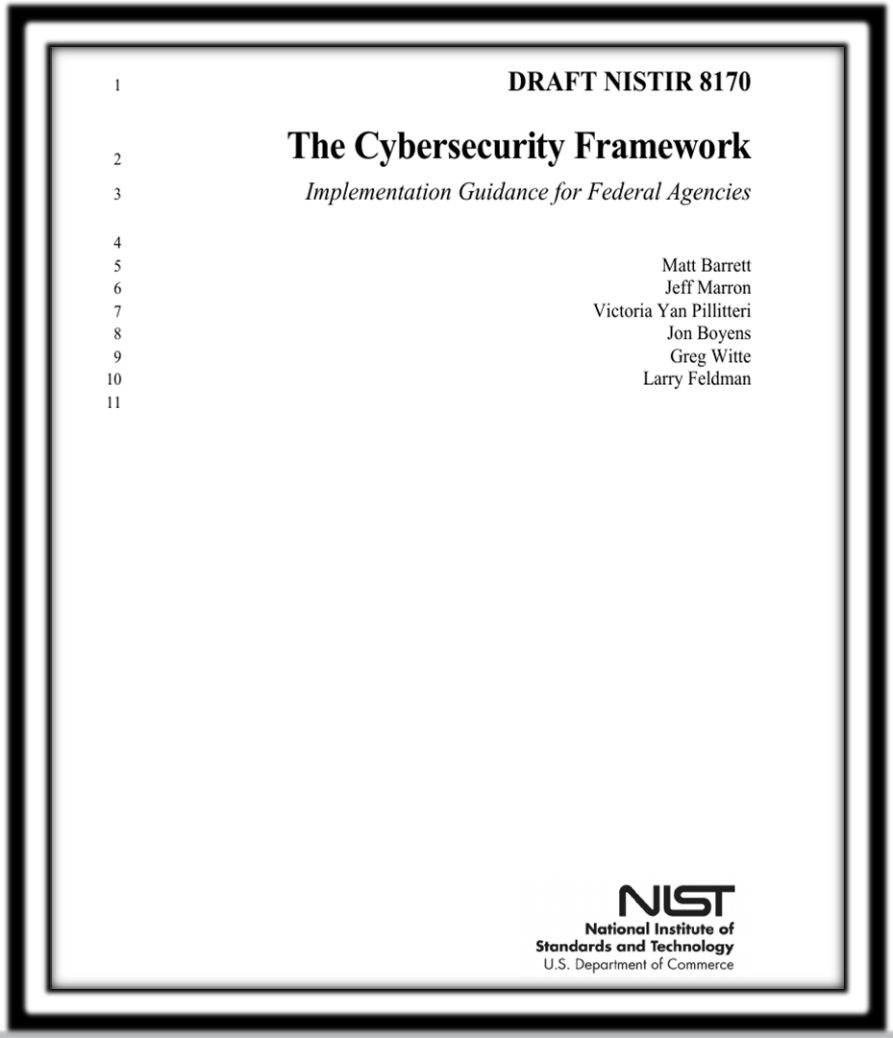
- **If the most dangerous of the cybersecurity attacks cannot be anticipated (because they are zero-day attacks), any risk mitigation strategies laid out by a committee (as is the case with the 800 series of docs) are going to be useless.**

A Disclaimer for the Slides to Come

- **In the rest of my talk, I'll comment on the contents of**
  - **The NIST Cybersecurity Framework**
  - **800-37, 800-39, 800-53, 800-61, etc.**
- **I will critique the recommendations in these docs from the standpoint of their applicability to the security of CIKR entities like TSA. However, I shall do so without intending any disrespect for NIST, which is one of the most venerable organizations in the US.**

The Cybersecurity Framework -- A Key Document in the 800 Series

- **Presents guidelines for cybersecurity risk management**
- **Presents six steps of a Security Life Cycle Approach: Categorize, Select, Implement, Assess, Authorize, and Monitor**
- **Focuses on the five functions of cybersecurity: Identify, Protect, Detect, Respond, and Recover**



DRAFT NISTIR 8170

The Cybersecurity Framework

Implementation Guidance for Federal Agencies

Matt Barrett
Jeff Marron
Victoria Yan Pillitteri
Jon Boyens
Greg Witte
Larry Feldman

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Replacing "cybersecurity" with "alien attack security"

alien attack = alien attack security

800-53 Security and Privacy Controls

(This is the main "access control" doc in the NIST 800 series)

- **Much of 800-53 sounds like a tech manifesto**

  "To understand how to achieve trustworthy systems and the role assurance plays, it is important to first define the term trustworthiness. **Trustworthiness, in this context, means simply worthy of being trusted to fulfill whatever critical requirements may be needed for a particular component, subsystem, system, network, application, mission, business function, enterprise, or other entity"**

800-61: Computer Security Incident Handling Guide

Here is one of the recommendations in 800-61 for how to prevent DDoS attacks:

"… disable all unneeded services and restrict the use of services that may be used in DDoS attacks"

Two possible meanings for "used in DDoS attacks": (1) A computer that is being used to amplify a DDoS attack whose real target is some other computer. Or, (2) The computer is itself a target of a DDoS attack.

In Summary

- **The more elaborate a bureaucratic structure for dealing with cybersecurity, the less likely that it will possess the agility to cope with ever-new and constantly evolving nature of attacks.**

- **The sort of risk management that is practiced by, say, insurance companies cannot be extended to dealing with cybersecurity. The insurance companies construct statistical models of how long people live, how frequently natural disasters strike, etc. Such models cannot be built for cyber vulnerabilities.**

In Summary (contd.)

- **It makes no sense to assume that the cybersecurity needs of, say, TSA would be anywhere close to those for, say, the National Park Service. This common denominator approach that permeates the NIST 800 series publications puts our country in great danger.**

- **Organizations like TSA need to devise their own strategies for coping with cybersecurity problems.**

THANK YOU