Security in knowledge

WAITER, THERE'S A FLY IN MY CODE!
Top Regrettable Government Proposals

Mary Ann Davidson

Oracle Corp.

Joshua Brickman

CA Technologies

RSACONFERENCE2013

Session ID: PNG-F43

Session Classification: General Interest

Overview

- General Keith Alexander, head of the U.S. Military Cyber Command, says computer attacks on critical infrastructure have increased 17-fold since 2009. On a scale of one to 10 on cybersecurity readiness, he says, the U.S. is stuck at three.*
- Three kinds of cyber threats:
  - Cyber crime (e.g., identity theft)
  - Cyber espionage
  - Cyber acts of war (e.g., damage or disruption of critical infrastructure)
- Result: Over the past few years, dozens of draft bills, laws, policies and white papers have attempted to address "US government cybersecurity concerns"

* "General Keith Alexander on Protecting the Homeland from Cyber Attacks," by Elizabeth Nicolas, The Aspen Institute July 26, 2012

Why "Regrettable"?

- Without clearly stated objectives
  - Solving the wrong problem – or solve no problem
- Without specific and unambiguous language
  - Nobody but the author knows what is meant
- Without remedies that consider economic realities
  - Market Distortion
- Without limited scope
  - The problem gets worse – or creates new problems

NISTIR 7622

- 1. (US Government) National Institute for Standards and Technology Interagency Report (NISTIR) 7622 Notional Supply Chain Risk Management Practices for Federal Information Systems - March 2012
- Goal: Supply Chain Risk Advisory
- Problem: Didn't work because it tried to be a be-all/end-all to address "supply chain risk"
- What Might Work: A much narrower and clearer problem statement

NISTIR 7622--Example

- *"Define, design, and implement roles that limit privilege and create redundancy throughout the supply chain and element life cycle so that no single role can, intentionally or unintentionally, create adverse consequences."**
- Intent: ???
- Industry Reality: Businesses are looking for ways to reduce redundancies, not add them.

*Reference: NISTIR 7622 Section 4.1.3

Resilience STAR

- 2. (US Government Department of Homeland Security) Resilience STAR for Software Concept Paper Pre-decisional Working Draft as of July 13, 2012
- Goal: Modeled on “Energy Star,” would evaluate products as to their vulnerability to cyber attacks and score them (bronze, silver, gold)
- Problem: Creates yet another non-standard evaluation scheme that would be US-specific and focused on vulnerabilities
- What Might Work: Leverage existing industry programs, apply risk-based frameworks

Resilience Star--Example

- *" … The Resilience STAR for Software Initiative seeks to pro-actively mitigate risks attributable to exploitable software by incentivizing stakeholders to enhance the resilience of software that enables and controls products and systems upon which citizens and commerce rely."*
- Intent: Provide US civilian agencies with a list of approved products
- Industry Reality: COTS needs one evaluation that is comprehensive and applicable globally

NDAA of 2013

- What: (US Government) Sec. 933 of the National Defense Authorization Act of 2013, S 3254
- Goal: Improve security & quality of software procured by the Department of Defense
- Problem: Imposed government-specific, US-only software assurance practices at odds with COTS technology development realities
- What might work: Leverage international, industry-led standards for software assurance

NDAA of 2013--Example

- Example: Section 933: "(2) require covered systems to identify and prioritize security vulnerabilities and, based on risk, determine appropriate remediation strategies for such security vulnerabilities; (3) ensure such remediation strategies are translated into contract requirements and evaluated during source selection; …"
- Intent: Find and fix bugs before products are deployed
- Industry Reality: Industry uses a risk based approach to eliminating the most significant threats, but no company can guarantee that their software is perfectly secure and/or defect-free.
- Comment: Represents a significant improvement from previous versions (e.g., requirement for non-standard third party testing)

Conclusion

- Cybersecurity issues are not going away and neither are the vulnerabilities that contribute to them
- In some cases, regulations and legislation *may* make sense; however, clear problem definition, clear language and clear (and limited) scope would make them more likely to succeed and increase acceptance
- Industry is working through a number of these issues already:
  - as individual companies
  - via public/private partnerships (e.g., Open Group)

Continue the Discussion

- We would love to hear from you!

Joshua Brickman
CA Technologies
508-628-8917 | joshua.brickman@ca.com

Mary Ann Davidson
Oracle Corp.
650 506 5464 | mary.ann.davidson@oracle.com

Addendum

Security in knowledge

Multi-Level Protection Scheme

- 3. (Chinese Government) Multi-Level Protection Scheme (MLPS)
- Goal: Prioritizes information networks in China based on importance to national security, social order, and economic interests. Systems classified as critical are subject to certain security standards.
- Problem: MLPS is an attempt to boost the domestic IT industry disguised as a security program. MLPS is overly burdensome, the standards are outdated, and domestic Chinese products may not be more secure.
- What Might Work: Adoption of internationally-recognized standards and cyber resilience best practices

MLPS -- Example

- *MLPS requires that all IT security products used in level three and above systems contain indigenous (Chinese) IP. Vendors must submit products used in these systems to Chinese government labs for testing and evaluation.*
- Intent: Enhance the cyber resilience of critical information systems by reducing reliance on foreign technology
- Industry Reality: Significant IP concerns over giving code to any and all governments for "testing"
- Suggested Improvement: Apply the Common Criteria in a risk-based manner to only the most critical systems and assets

Security in knowledge

WAITER, THERE'S A FLY IN MY CODE!

Mary Ann Davidson

Oracle Corp.

Joshua Brickman

CA Technologies

RSACONFERENCE2013

Session ID: PNG-F43

Session Classification: General Interest