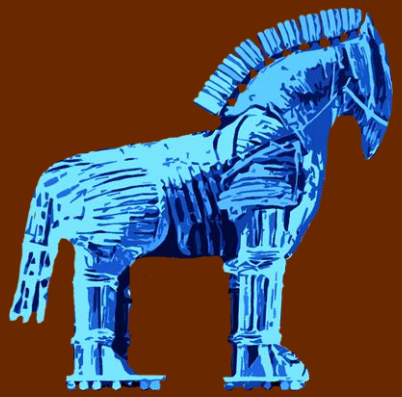
Certifying a Textbook Under NSTISSI 4011



Richard E. Smith

2012 CISSE

Orlando, FL

Outline

- The book's motivation
- Book organization
- Problems with NSTISSI compliance
- Updating the standard
- Addressing fundamental topics
- Sensitive topics

The book's motivation

- Given:
  - Application-oriented undergraduate program
  - Obsolete curriculum

- Goal:
  - Comprehensive cybersecurity course
  - Open to freshmen or sophomores
  - Starting point for an IACE certification
  - No single satisfactory source

Book organization

- A "geographical" topic progression
  - Start with one user, one computer, physical security
  - Add more people, more threats
  - Add networking

- Major Topics
  - Access control: Chapters 1-5
  - Cryptography: Chapters 6-9
  - Networking: Chapters 10-17
    - Chapter 13 focused on enterprise security
    - Chapter 17 focused on US government systems

Problems with NSTISSI compliance

- NSTISSI 4011 is old enough to vote this year!
- Assumes lots of CS fundamentals
- Requires some sensitive topics

Updating the Standard

- Used another standard: ACM/IEEE-CS IT 2008
  - Core Outcomes in Information Assurance and Security
- Topics Added:
  - Public-key cryptography, AES, SSL, IPSec
  - Legal systems, rules of evidence, digital forensics
  - ISO and NIST security standards
  - Modern network threats, TCP/IP vulnerabilities
  - Social engineering, hackers, crackers, black hat, white hat
  - Web service availability

Incorporating Fundamentals

- **Buffer Overflow Attacks**
  - Explain control versus data in RAM
- **Process Separation**
  - Explain kernel/user mode, RAM protection, dispatching
- **Network Vulnerabilities**
  - Protocol fundamentals: ACKs and flow control
  - Packet formats, contents, and firewalling

Sensitive topics

- COMSEC
  - David Boak's NSA lectures: "History of US COMSEC"
    - Recently declassified
  - NISPOM: Security manual for DOD contractors
  - Federation of American Scientists: FOIA documents
- TEMPEST
  - Boak again
  - John Young's Cryptome web site: more FOIA
- OPSEC
  - The legend of the Gulf War spike in Pentagon pizza orders
  - High-level OPSEC policies are unclassified

Contact Information

- Rick Smith
- Cryptosmith
- rick@cryptosmith.com

- Or Google “rick smith crypto” or some such

- I’m also starting an online self-study course based on *Elementary Information Security*