Cyber Security Education: My Personal Thoughts

Bharat Doshi
bharat.doshi@jhuapl.edu

APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

Topics

- Personal Background
- Other situations: Similarities and Differences
- Cyber Vulnerabilities
- Student Types and Education/Training Needs
- Dynamics and Continuing Education
- Concluding Thoughts

Driving Safety: Similarities and Differences

- Concept
- Design
- Supply Chain and Manufacturing
- Maintenance and Repair
- Road Building
- Road Operations and Maintenance
- User Driving

- Errors/Failures Vs ‘Attacks’
- Rate of Change
- Early users

Telephony: Similarities and Differences

- Infrastructure and end device architecture
- Designs
- Supply Chain and Manufacturing
- Deployment
- Operations and Maintenance
- User

- Errors/Failures Vs ‘Attacks’
- Rate of Change??

Cyber-security: Users, Attacks, Sources of Vulnerabilities

- Types of Infrastructure and Users
  - DoD and IC (.mil), other Government users (.gov), Critical non-Governmental Infrastructure (.com. .edu, ..), general users (.com., .edu, ..)
- Types of Attacks
  - Hacking for fun or attention, identity theft and other economic motivation, espionage, terrorism, pre-emptive strike
- Other Attacks and/or Damages
  - Actions in social media
  - Privacy issues and persistence in social media
- Cyber-vulnerabilities
  - Architecture, Design, Development
  - Manufacturing and Supply Chain (Globalization)
  - Operations (Configuration, Controls, ….)
  - User Behavior

Student Type and Education/Training: Designer/Developer

- **Core curriculum in Computer Science, Electrical Engineering, or similar Discipline**
- **Supplemented with courses on**
  - **secure programming, applications of crypto, network security, trust establishment, etc.**
  - **Supply chain issues, verification, anti-tamper techniques, etc.**
  - **Policies, ..**
- **Cyber threat analysis**
- **Red teaming and classroom games**
- **Experimental science for Cyber**
- **Secure systems engineering where cyber is a major component of all modern systems (Domain Aware Cyber Architecture and Operation)**
- **4+1 ??**
- **Special Graduate Degrees??**
- **Specialization during education and on the job**

APL

Student Type and Education/Training: IT Operations

- Broad Training (Cisco, Microsoft, ..) including courses on
  - Threat analysis
  - Security equipment (firewalls, IDS, etc)
  - Commercial tools
  - Use existing Open Source software (spam filters, honeypots, etc)
- Some specialization

- **Professional Exams and Certification??**

- Red Teaming
- Games (e.g. CyberCIEGE, NetWars, CyberLink Duo, CyberLink Solo, …)
- **Continuing Education/Training**

Dynamics and Interplay

- How do we keep Designers, Developers, and Operations people to remain current in the face of rapid changes?
- How do we make the above groups interact?

Student Type and Education/Training: General College Students, Adult Population, etc.

- Courses on
  - Cyber: Basic awareness of the presence of cyber, terminology, etc.
  - Online risks (financial, reputation,..) and secure usage practices (passwords, clicking on links, installing software, etc.)
  - Identities in cyberspace - who are we and how do we prove it? Once we know who you are, how do we decide what to let you do (authentication)?
  - Ethical behavior in cyberspace. Use of social media. How to be responsible cyber citizens? How to protect your data and the data entrusted to you? How to maintain desired degree of privacy and propriety?
  - History of computer security - what do we know, who are the "heroes" of early and modern cyber security. How do we keep from repeating the same mistakes over and over again
  - Security issues with cell phones, smart phones, etc.
- Cyber-security Games in courses

K-12

- Simple ‘course’ on computers, cell phones, social media, proper usage and behavior
- Classroom exercises and games
- Career in cyber

Special Needs

- DoD and IC Systems, DHS and Critical Infrastructure
  - Level of sophistication in attack
  - Ease of Use Vs Security Trade-off
  - Restrictions on Cyber Workforce
  - Supply Chain Issues

Concluding Thoughts/Questions

- Education and training for different segments of population and Cyber Workforce
- Awareness training for users
- More interplay among education and training for different population than in other disciplines
- How do we attract bright young students to opt for Cyber-security as a career? How can that be made as attractive as writing cool code for an exciting application?
- How do we provide the continuing education that is needed to remain current in the face of rapid changes?