A Legal Framework for Cybersecurity

Deirdre K. Mulligan
School of Information
UC Berkeley

Fred B. Schneider
Computer Science
Cornell University

Outline of Talk

- Brief background
- Why shift in legal framework is appropriate
  - Advances in science entering market place
  - Insufficiency of current law
- Why public health-inspired model is appropriate
  - Similarities of problem space
  - Similarity of goals
- Features of new model
  - Example interventions
- Political environment open to new solutions
- Benefits of Public Law
- Role of Computer Security community

Background

If you build it they will come…

or maybe not…

Security in the market place is **“remarkably below what “known best Practices”** could provide.”

The existence of technology solutions **on their own** does not improve security or privacy.

Advances in Science

- Diversity
- Type-safe programming languages
- Virus checkers
- Automatic updates
- PKI
- Virtualization
- Automated diagnostics
- firewalls

Insufficiency of current law

- Limits of deterrence
  - theory of crime
    - Rational actors? Situational?
  - Identification
  - Jurisdiction
- Limits of security standards
  - substantive, procedural
- Misalignment of resources
  - Prevention 1st priority b/c no full recover

problem space

- Problems of the commons
- Constantly evolving threats
  - Perfection of artifact impossible
- Information gaps
  - Vulnerabilities, threats, investments, losses
- Openness, exchange, interaction
  - necessary for social, economic and political
- Complex value trade-offs
- Value of prevention
  - Need to motivate good guys
  - pits immediate, individual, tangible interests against collective, long-term, statistical probabilities of harm

goals of public health

- The mission of public health
  - "fulfilling society's interest in assuring conditions in which people can be healthy" *The Future of Public Health IOM, 1988*
  - "to generate organized community effort to address the public interest in health by applying scientific and technical knowledge to prevent disease and promote health" *The Future of Public Health IOM, 1988*

Goals of cybersecurity

- President Obama
  - "treated as…a strategic national asset."
  - "ensure that these networks are secure, trustworthy and resilient."
  - "deter, prevent, detect, and defend against attacks"
  - "recover quickly from any disruptions or damage."

CS perspective on security

- *Trust in Cyberspace (2007)*:
  - revisit “the paradigm of ‘absolute security’”
  - use technology and sound practices to reduce vulnerabilities (introduced insecurity)
  - wrt inherent insecurity, move toward a model built on three axioms:
    - insecurity exists; insecurity cannot be destroyed; and, insecurity can be moved around”
- *A Clean-Slate Design for the Next-Generation Secure Internet (2005):*
  - move away from a fixation on building secure systems
  - to a more nuanced understanding of the security design space that allows trade-offs among a range of dimensions including
    - prevention, detection and recovery, resilience and deterrence

policy reorientation

Parallel arguments to Public Health:

- generate organized community effort
  - revisit dominant legal focus on the bad guy
  - address individual actions that create collective insecurity
  - move from atomized view of security to collective approach to managing insecurity
- Apply scientific and technical knowledge to limit vulnerabilities, promote security, and manage insecurity
  - research on causes of insecurity
  - fruits of research that makes new forms of intervention possible
- Build on insights from CS
  - build upon CS three axioms of inherent insecurity
  - relocating insecurity to improve its manageability reduce risk

Prevention

Public health strategies
- targeted regulations
- conditioning
- subsidies
- safe harbors
- public insurance

Reducing vulnerabilities

Producers

- Development
  - Standards
    - Process, substantive, performance
- Post-market
  - Monitoring
  - Notification
  - Issuing patches and patch management
    - defaults

Reducing vulnerabilities

Deployers

- Security?
  - How defined?
  - Protects what?
  - At what cost to other(‘s) security?

Insufficiency of prevention

- Bug free software is an elusive goal
  - Vulnerabilities $\neq 0$
  - Interaction between components of networks generate new vulnerabilities
- Motivated adversaries
  - Defense in depth
  - but reality of defend everywhere attack anywhere

Reducing and mitigating vulnerabilities

Users

- Patch management and Herd Immunity
- Intermediaries
  - Incentives for ISPs?
    - Liability
    - Resources
      - Education
      - Direct assistance
      - containment
- Configuration management
  - Ease of updating

inherent insecurity

Raising cost of exploitation

- Diversity
  - Natural and artificial
  - Where?
  - How?

Inherent insecurity

- Detection
  - Anomaly?
  - Reporting v. surveillance
  - testers
  - Trees and forest

Inherent insecurity

- Containment
  - Accountability
    - Time scale
    - binding

Inherent insecurity

- research

Inherent insecuriry

- Public education
  - Hygiene
  - Self-monitoring
    - Vital signs?
    - Check-ups?
  - Monitoring partners
    - Reporting breaches? Exposures?
    - Facilitate shielding

Responsive to today's problems

- Reducing vulnerabilities
  - better development, deployment, after-market maintenance
- Dealing with inherent insecurity
  - need to maintain herd immunity
    - incentivize, coerce actions that yield collective benefit
    - deal with "unacceptable" harm to individuals who act to advance collective interest
- Conceptualizing value trade-offs, mitigating conflict
  - interventions to address insecurity present threats to individual interests
  - Models presented for mitigating tensions

Political will

- “From now on, our digital infrastructure -- the networks and computers we depend on every day -- will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority.” President Obama

Change in Political Climate

- PCCIP
- CNCI
- 60 Day review
- Cybersecurity Act of 2009

Complex Balancing

- Value conflicts
  - Intrusions on core individual liberty and property interests
    - Communication
    - Social networking (transactional surveillance)
    - Privacy
    - Private property
  - Access to increasingly essential services
    - Phone, banking, government etc.

Benefits of Public Law

- Political System
  - Transparent
  - Participatory
  - Accountable
  - Contestable

Moving forward

Key time for researchers

- Open research questions
  - Litany of interventions need more info to choose well
- Research agenda
  - Silos v. interdisciplinary
- *Knowledge transfer* not just tech transfer
  - Demise of OTA; fragmentation of funding
  - Lack of agency responsible for cybersecurity
    - ongoing gap in leadership
    - Lack of clear positive agenda on *policy*
  - Importance of participation