What makes a challenge grand?

Our grand challenges:

- Address a major socio-technical issue in cybersecurity
  - Program size issue
  - Clear intellectual merit and broader impacts
  - Multidisciplinary
  - Need not be solvable, but should be able to determine progress towards a goal

CRA: Four Grand Challenges in Trustworthy Computing (11/16-19, 2003)

Presented four research challenges

1. Eliminate Epidemic Attacks by 2014
2. Enable Trusted Systems for Important Societal Applications
3. Develop Accurate Risk Analysis for Cybersecurity
4. Secure the Ubiquitous Computing Environments of the Future

CRA: Four Grand Challenges in Trustworthy Computing (11/16-19, 2003)

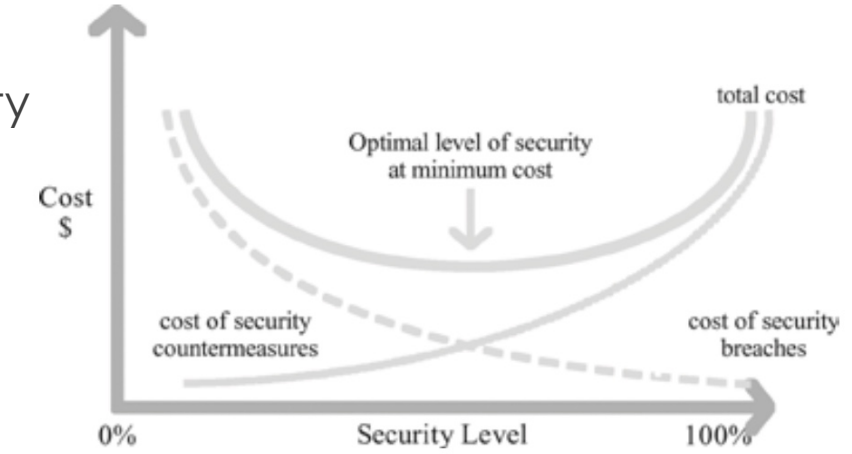
General structure

1. What is the problem and why is it important?
2. Why is this difficult to do?
3. Why is progress possible?
4. What are the barriers for success?

CRA: Four Grand Challenges in Trustworthy Computing (11/16-19, 2003)

Challenge 3: Develop Accurate Risk Analysis for Cybersecurity

- Proven ineffective in spurring effective investments in ICT.
  - In part due to lack of effective models of risk.
  - Need some assurance that increasing spending on security measures actually increases security.
- Develop, within ten years, quantitative IT risk management that is at least as effective as quantitative financial risk management.



Why is this difficult?

- We don't yet understand the full nature of IT risk.
  - As systems become more complex and interconnected, emergent behavior of global systems exposes emergent vulnerabilities
  - For example, failure dependency in networked systems
- Ultimate goal is to be able to accurately model and predict such failures
- Two aspects of measurement that need the most attention are:
  - Measuring the wrong thing is worse than not measuring anything at all.
  - Because choices and decisions need to be made by many organizations over long periods of time, the measures need to be consistent, unbiased and unambiguous

Why is progress possible?

- Related fields mathematics of investment risk, epidemiology, public health, accelerated failure time testing, software assurance and other endeavors is undergoing a resurgence of development
- Researchers are collecting data in sometimes prodigious amounts
- In an attempt to protect against terrorist attacks, policy- and decision-makers, as well as the citizenry in general, have become accustomed to rough models of risk that can be used to adjust resources and behavior.

Barriers to success

Many significant social and cultural barriers have to be overcome

- Data-gathering challenges.
  - In many organizations, these kinds of data are either proprietary or closely held. There is no "first mover" advantage in disclosing the data, so finding willing partners for research collaborations will be difficult.
  - In many organizations, there are perceived risks involved in releasing data that expose vulnerabilities. Executives cannot hide behind "plausible deniability" when the data are open to inspection. Some organizations would regard the release of such data as an admission of negligence or wrongdoing.
- Data-sharing challenges.
  - Standards and common terminology do not exist in any useful form, so cooperation among sometimes competing organizations will be required

National Privacy Research Strategy June 2016

- Privacy R&D is multidisciplinary
- Eg, Develop system design methods to incorporate privacy desires requirements, and controls
- Research questions include:
  - How can privacy risk be modeled to support privacy risk identification and management?
  - What kinds of system properties can be associated with privacy to support the implementation of privacy principles and policies?
  - How should privacy properties be characterized, and how can they be assessed or quantified?
  - What privacy design patterns and use cases describe common solutions that would assist system designers, particularly in emerging areas such as smart cyber-physical systems and the Internet of Things?

National Privacy Research Strategy June 2016

- How can privacy-enhancing cryptographic technologies be developed to scale, as well as be integrated into the functional requirements and standards that are already widely adopted in systems?
- What metrics can be used to assess the effectiveness of privacy controls?
- How can privacy risk be considered and controlled in concert with system and data utility needs?
- What metrics and measurements can measure both privacy and system utility, to understand the tradeoffs between the two, and to support the development of systems that can maximize both?

Discussion: How do we wish to structure our grand challenges?