2nd Annual New England Faculty Summit on Cyber Security

Boston University, June 18, 2012

Breakout Groups: Facilitators and Provocative Propositions

Cybersecurity Education

Facilitator: Craig Wills, WPI

Proposition: The problem with cyber security education is that it is treated as an add-on, or specialization in computer science and engineering, when in fact it is inherently interdisciplinary: education and training in cyber security at the undergraduate and master levels must be liberated from the tyranny of CS and CE requirements. Cyber security is worthy of its own undergraduate degree program.

Proposition: Building secure systems requires broad-based understanding of security principles for all programmers and software engineers, not cyber security specialists.

Proposition: The best defense is a good offense. Consequently, the best cyber security experts are those trained as hackers and spies, which is not compatible with traditional academic ethics.

Socio-Economic Aspects of Cybersecurity

Facilitator: Susan Landau, Harvard

Proposition: Cyber security can only be assured by viewing it from an economic perspective. As such, effective approaches to enhancing cyber security include eliminating the economic incentives for mounting cyber-attacks, quantifying the financial liability resulting from security and privacy breaches, and making it inexpensive to incorporate security into systems, among others.

Proposition: The marketplace is showing that demand for information privacy is nearly non-existent, especially for the iPad generation. Moreover, the well-being of society suggests that it is worth giving up anonymity for accountability in cyber space. Thus, in a connected world, privacy should not be an expectation, but a privilege to acquire and maintain.

Proposition: Cyber security is no longer an essentially technical problem. And, as long as we think about it from a purely technical perspective -- both in education and research -- we are bound to fail. In particular, "security" is impossible to achieve without a general consensus on what are appropriate behaviors in cyber space, and enforced punishments for those behave inappropriately.

Technological Drivers of Cybersecurity

Facilitator: TBD

Proposition: The consolidation of data assets in support of an economy driven by "big data" without the development of the proper security and privacy infrastructure -- both technical and legal -- is a disaster waiting to happen. Investments in "big data" initiatives must go hand in hand with investments in developing the necessary support for "big data" security and privacy.

Proposition: The movement of computing to the cloud without the development of the proper security and privacy infrastructure -- both technical and legal -- is a disaster waiting to happen. Investments in outsourced computing must go hand in hand with investments in developing the necessary support for cloud computing security and privacy.

Proposition: Cyber security will only advance when issues of liability and accountability are well understood -- both technically and legally. For this to happen, software systems must be built with the equivalent of a "black box" that could be used to identify and collect evidence for post-mortem incident analysis and remediation.

Basic versus Applied Research in Cybersecurity

Facilitator: Nickolai Zeldovich, MIT

Proposition: Cyber security research often requires access to data that academic researchers don't have (e.g., network traffic, social networks). Research results published by industry that have the data cannot be scientifically validated without public access, so they do not benefit science either. Without ways to break this logjam, many branches of effective cyber security research are effectively cut off.

Proposition: Academic research in cyber security should stop pretending to solve real problems. Rather, it should be thought of as basic research for its intrinsic intellectual value.

Proposition: Safety, security, and privacy guarantees do not compose. This implies that approaches such as formal verification, safe programming languages, and certifiable software cannot scale successfully in practical applications.

Proposition: We should accept the fact that building secure systems is a fantasy. Rather than focusing on research that seeks to build secure systems, we ought to focus on research that is able to cope with cyber insecurities, including research areas such as situational awareness, containment, risk assessment, among others.