Cybersecurity at the Nexus of a Hyper-Connected World

Azer Bestavros, Wayne Burleson, Frans Kaashoek, Greg Morrisett, and Engin Kirda

Draft of April 4, 2012

This document identifies a number of major research thrusts that faculty members at MGHPCG institutions believe to be of major importance, and which could form the basis of a research manifesto for the envisioned MGHPCG/ACSC Cybersecurity Initiative. Many of the ideas in this document reflect discussions that took place during and since the New England Cybersecurity Faculty Summit organized at BU in June 2011. The document identifies four themes that unify most of the current cybersecurity research efforts at the MGHPCG universities.

Note: at this stage, this document is centered on a computer science view of cybersecurity research, and the presentation tends towards technical topics. Future work will include broadening the discussion to include other disciplines and interdisciplinary aspects of relevant research, as well as to framing the research agenda in the context of making real progress in solving cybersecurity challenges.

A Unifying Theme

It is increasingly evident that cybersecurity challenges cannot be addressed unless we are able to take cyber-security beyond point solutions, by recognizing the necessity for models and solutions to interact, compose, and federate along a number of dimensions, spanning not only technological but also social, economic, and legal considerations.

Supporting Federal Priorities

Pursuing basic and applied research in support of integrative solutions to cybersecurity (i.e., those that go beyond point solutions) is evident in all recently spelled-out priorities of federal agencies and recently announced funding initiatives.

With respect to the cybersecurity thrusts recently-announced by the White House National Science and Technology Council (NSTC), it is clearly the case that they are all about the need to go beyond “point solutions” – they are all focusing on capabilities and technologies at the nexus of multiple security research areas or at the intersection of a subset of these areas with practice. Specifically,

• The Designed-In Security thrust focuses on integrating security and software engineering practices (or at least the software development process), including the need for metrics, models, and analytics to effectively manage “risk, cost, schedule, quality, and complexity.”

• The Tailored Trustworthy Spaces thrust focuses on synthesizing security for specific scenarios/contexts, which requires the alignment of the levers we design in our systems (or the assumptions we make in our models) with the “functional and policy requirements arising from a wide spectrum of activities.”
• The Moving Target Defense thrust projects security in a dynamic/control-theoretic framework, requiring us to develop the basic building blocks that can be composed into an evolving system with “security mechanisms and strategies that continually shift and change over time to increase complexity and cost for attackers.”

• The Cyber Economic Incentives thrust is concerned with the intersection between security and economics at multiple levels, requiring the development of not only “sound metrics” that allow for “cost risk analysis”, but also it requires “understanding (and modeling) the motivations and vulnerabilities of markets and humans and how [they] interact with technical systems.”

One should note that the above four NSTC thrusts – in addition to being highly interdisciplinary – share some common characteristics, most notably, the need for security models and metrics that could provide the “glue” for composition, interaction, and integration of various point solutions.

The importance of the cybersecurity nexus is also evident in the critical challenges identified by other federal agencies and national organizations. For instance, many if not all of the “hard problems” spelled out by the Department of Homeland Security (DHS) as well as the “grand challenges” spelled out by the Computing Research Association (CRA) can be related to the 4 NSTC thrusts above. While some are generic (e.g., focusing on scalability, or on the interplay between security and privacy), others are more focused (e.g., combatting malware and botnets, or attack attribution). But, in both cases, there is no question that the emphasis is on issues of “composition” and “integration” with the associated concerns of “metrics” and “usability”.

Leveraging New England Assets

Within the “Cybersecurity at the Nexus” theme, it is important to focus on challenges that New England (NE) is uniquely poised to tackle. Namely, these challenges should be (a) drivers for basic research problems that NE academic institutions are well-positioned to address, and (b) catalysts for applied R&D projects that NE industries, both cybersecurity providers and consumers from various sectors, are well-positioned to pursue.

Drivers for basic research are concrete yet broad applications for which point solutions do not work, and in which various NE academic constituents can sink their teeth in a multi/cross/inter-disciplinary manner. Catalysts for applied R&D are projects that address immediate and pressing practical needs, and which leverage unique NE assets.

Four “Cybersecurity at the Nexus” challenges that are both good drivers for basic research and good catalysts for applied R&D are:

• Challenges at the nexus of security and society. These challenges leverage New England’s unique strengths in social sciences, law, business, and government studies, including nationally unique research centers (e.g., Harvard’s Berkman and CRCS centers, and UMass Center for Forensics). Also, these challenges involve applications to important sectors of the local economy, including healthcare and e-commerce.
• **Challenges at the nexus of security and high-assurance systems.** These challenges leverage significant strength in academic research on formal methods, software verification, trusted platforms and clean-slate architectures, medical devices, and embedded and CPS/SCADA systems. Also, it is aligned with the significant presence in NE of major R&D players (e.g., Lincoln Labs, MITRE, Raytheon, and BBN).

• **Challenges at the nexus of security and cloud computing.** These challenges leverage significant strength in basic research in a number of areas, ranging from purely theoretical ones (e.g., homomorphic encryption and obfuscation) to highly applied ones (e.g., operating systems and distributed systems). Also, it connects well with the MGHPC effort and with the interests of local/MGHPC industries (e.g., VMware, Microsoft, and Cisco).

• **Challenges at the nexus of security and IS&T.** These challenges leverage significant strength in academic research in NE on network measurement, characterization, and anomaly detection. Also, it is aligned with the current ACSC focus, reflecting the critical need of local companies, especially in the financial sector.

**Research Thrusts**

Consistent with the above, we identify the following four research thrusts, each with a list of bullets/keywords that are meant to exemplify (and certainly not exhaust) the various issues underlying that thrust.

*TBD: specifically identify the individual topics with current researchers and research projects. To a first approximation, all of these topics represent actual work at the universities.*

1. **Trusted Interactions in Cyberspace (the Society Nexus)**
   - Technologies for Trusted Identities in Cyberspace
   - Censorship and Freedom of Speech in Cyberspace
   - Digital Rights Management and Enforcement
   - Cyber Law Enforcement, Governance, and Jurisdiction
   - Privacy-enhancing Regulations and Technologies
   - Tracking, profiling, and personalization
   - Cybercrime and cyber forensics
   - Non-repudiation and plausible deniability
   - Implications of “Code is Law”
   - e-Voting
   - e-Cash
   - Legal and ethical implications for safe use of embedded devices

2. **Certifiable Software and Systems (the High-Assurance Nexus)**
   - Safe Programming Languages
   - Formal Verification
   - Automated Theorem proving
• Composable Formal Security Analysis
• Zero-knowledge Proofs
• Model checking
• Secure Embedded Software and Systems
• Trusted Platforms and Architectures
• Secure BGP/DNS/... protocol deployment
• Clean-slate Architectures
• Role of regulatory requirements
• Secure architecture and implementation for mobile devices
• Providing improved security for existing and legacy systems

3. Cyber Situational Awareness (the IS&T Nexus)
• Economics models for risk assessment and management
• Game-theoretic adversarial/threat modeling
• Federated, cross-organizational monitoring
• Network traffic characterization and anomaly detection
• Intrusion Detection/Prevention Systems
• Recovery and remediation capabilities
• Auditing and regulatory compliance
• Real-time big data analytics
• Information/disinformation propagation in social networks
• Cyber forensics
• Detection and analysis of malware
• Detection of online malicious activity
• Detecting social engineering and privacy attacks

4. Secure Outsourcing of Data and Computation (the Cloud Nexus)
• Expressive security SLAs
• Computing over Encrypted Data
• Homomorphic Encryption
• Differential Privacy
• Software Obfuscation
• Data Integrity in the Cloud
• Access control and policy deconfliction
• Trusted platforms
• Virtualization in systems and networks

Thrust-Aligned Projects and Activities at NE Institutions
[TBD by grouping representative projects from NE institutions under the various thrusts. For each project, provide a title, PIs, and a list of keywords from the lists above.]
Thrust-Aligned Opportunities for Impact on NE Economy

[TBD – Note: we need to make sure to present a balanced view of the sectors in the NE economy, which goes beyond the focus on the financial sector evident in the current ACSC membership.]

Needed Resources

The following resources are believed to be essential for the pursuit of the multi-pronged research vision spelled out in this document:

a. Anchor facility to collocate PIs and serve as community hub
b. Faculty/postdoc/visiting fellows programs
c. Research engineers and professional staff support

[TBD by adding narrative and by emphasizing relationship to the bigger picture – e.g., shared course development/offerings, workforce training/development, consulting arm, ...]

References

[TBD]