Report of the

New England Faculty Summit on Cyber Security

Held at Boston University on June 28, 2011

Azer Bestavros
(best@bu.edu)

July 2011

Executive Summary

The Hariri Institute for Computing and Computational Science and Engineering at Boston University organized and hosted a one-day summit for leading faculty members in New England institutions to discuss the possibility (and next steps) for setting up a regional academic consortium on Cyber Security research and education. The meeting, which was held on June 28, 2011, attracted around 50 participants – primarily faculty members from MGHPCC institutions (BU, Harvard, MIT, U Mass, and NEU) as well as a few researchers and administrators from industrial and local research labs and organizations.

The summit confirmed the significant opportunity and potential from setting up a multi-institutional hub for cyber security research and education in New England – a hub that will be in position to leverage the expected significant R&D investments in Cyber Security by industry as well as local and federal government. Towards that goal, the summit identified desirable attributes and characteristics of the envisioned multi-institutional consortium, as well as short-term and medium-term next steps that could be pursued to get the academic community ready for such a consortium.

Desirable attributes and characteristics include: the necessity of physical colocation among collaborators; the value of targeting integrative grand challenge problems that cut across traditional social and technical disciplines; and the importance of coordination across institutions by adopting a best-of-breed, whole-bigger-than-the-sum-of-its-parts approach to integrating the existing strengths in cyber-security among participating institutions.

Next steps to be pursued include: organizing follow-up meetings that help coalesce the academic community along specific activities and interests; identifying potential sources of support from industry, local government, and federal government; coordinating with related regional and national efforts; and covening a small working group of faculty and administrators to discuss and propose possible governance structures.

This report summarizes the presentations, discussions, and recommendations of the summit.

Overview

As suggested by the escalation and sophistication of recent cyber-attacks targeting US government agencies (such as the DoD, the State Department, and the CIA) as well as corporate giants (such as Google, Citibank, Sony, and Lockheed Martin), cyber security promises to be the battlefield of the twenty-first century. Cyber warfare uses computer technologies as defensive as well as offensive weaponry involving corporate, government, mercenary, and criminal players that do not recognize traditional International boundaries or norms.

As society develops an understanding of this new cyber world order, and proceeds with new legal national and international frameworks for rules of engagement, it is critically important for various stakeholders to examine the potential from emerging advances in cyber security and cyber forensics, and the implications of these capabilities on future legislations and standards, including impact on personal freedoms and privacy. Timely questions that need to be considered range from the utility (or futility) of network monitoring, to the possibility (or impossibility) of universal trustworthy cyber authentication, to the potential from emerging defensive, offensive, and preemptive cyber operations, to proposed clean-slate designs of future Internet architectures, to the role of the military and intelligence agencies in securing public and private networks, to the role and rules of international law concerning cyber warfare, to the role of cyber security education, among others.

Recognizing the timely and critical nature of these challenges, the **BU Hariri Institute for Computing and Computational Science & Engineering** (http://www.bu.edu/hicse) convened a one-day summit at Boston University on June 28th, 2011, in which leading cyber security faculty members from New England's top institutions (including BU, MIT, Harvard, Brown, Dartmouth, Northeastern and U Mass), as well as select cyber security experts from leading research labs (including Cisco Systems, EMC RSA Labs, Lincoln Labs, and Microsoft Research) explored opportunities for collaboration on cutting-edge research initiatives targeting grand Cyber Security challenges.

The summit's explicit aims was to develop an ambitious roadmap for setting up a multi-institutional hub for cyber security research and education in New England by considering the best ways in which participating institutions might line up their existing strengths in order to be in position to tap into the expected significant investments in Cyber Security R&D in the foreseeable future – in other words *"how do we make New England the silicon valley of cyber security research and education?"*

In preparation for the summit, a list of over 120 academics and 20 industry researchers pursuing basic cyber-security-related research in New England was compiled through consultation with leading research officers at each university, as well as through recommendations received from cyber security research group leaders. Given the nature of the meeting, it was desirable to cap participation to ensure substantive discussions. Thus, invitations to the summit were sent to a total of 60 researchers, of whom 42 indicated that they are able to attend, with 41 actually attending the summit. A small group of administrative leaders from local universities and from industrial labs were also invited, bringing the overall number of attendees to 47.

Without exception, all invitees, including those who could not make the summit due to prior conflicting commitments, indicated an interest in the event and a strong belief in the timeliness and importance of this initiative. A complete list of all participants is included at the end of this report.

The summit opened with a welcome by **Mel Bernstein** (NEU) who emphasized the timely nature of the meeting and the significant opportunity at hand as it relates to other multi-institutional collaborations, especially with respect to the MGHPCC consortium as well as the industry-led Advanced Cyber Security Center (ACSC) in Massachusetts. This was followed by the summit's main plenary session in which the Director of the Hariri Institute **Azer Bestavros** (as the summit organizer) framed the opportunity and laid out the charge to participants, and in which luminaries **Shafi Goldwasser** (MIT) and **Susan Landau** (Harvard) presented their views on cyber security challenges from the computer science and social science perspectives, respectively. This was followed by a presentation by **Robert Brammer** (Northrop Grumman) on his experience with university cyber security research consortia. A panel discussion featuring faculty members who led unique cyber security initiatives followed, with each of **Ran Canetti** (BU), **Salil Vadhan** (Harvard), and **Brian Levine** (U Mass) making short presentations about their experiences with translational research, interdisciplinary computing and society research, and digital forensics and society research, respectively.

During a working lunch session and throughout the afternoon session, participants were divided into four breakout groups:

(1) Cryptographic Models and Protocols,
(2) System and Network Security,
(3) Trust-Enhancing Architectures and Processes, and
(4) Society, Public Policy, and Jurisprudence.

Each breakout group was tasked with the identification of regional strengths and weaknesses, needed resources, and steps towards the envisioned multi-institutional hub for Cyber Security Research and Education in New England. To facilitate the breakout group discussions, a set of questions and ideas (included at the end of this report) were shared with all participants, and two facilitators from each breakout group were asked to summarize the discussion to the entire group at the last session of the summit.

The summit concluded with brief announcements on next steps – including the setting up of channels of communication among faculty regarding this initiative, and a call for ideas (and proposals) for follow-up events and activities to be sponsored by the Hariri Institute at Boston University over the next few semesters.

The Opportunity

In his opening remarks, **Azer Bestavros** provided some context to summit attendees. This included an overview of the Strategic Plan for Federal Cyber Security Research and Development Programs, which was recently developed by the US Networking and IT Research and Development (NITRD), as well as background regarding the on-going multi-institutional collaboration underlying the Massachusetts Green HPC Consortium (MGHPCC).

The recently-publicized NITRD Strategic Plan for Federal Cyber Security Research and Development (http://www.nitrd.gov/fileupload/files/NITRD_IEEE_SSP_2011.pptx) suggests significant additional investments by all government agencies (ranging from 30% to 50% across agencies) in existing as well as new *"game-changing themes"* related to cyber-security, including the new *"Designed-In Security"* theme and increased emphasis on *"The Science of Cyber Security."* Designed-in security requires *"verifiable assurance"* that resilience to attacks be natively part of software design, development, and evolution lifecycle, and that it enables reasoning about a diversity of quality attributes (security, safety, reliability, etc.) and the required assurance evidence and metrics. The emphasis on *"the science"* of cyber security reflects a desire to base cyber security practices on "expressive and realistic models of adversaries" and allow for security assurance to be *"quantifiable"* (emphasizing metrics) and *"composable"* (emphasizing the use of formal and stochastic modeling methods).

The MGHPCC (http://www.mghpcc.org) is a non-profit collaborative, involving a group of five New England Universities (Boston U, Harvard U, MIT, U of Massachusetts, and Northeastern U) in partnership with the Commonwealth of Massachusetts, Cisco, and EMC. The MGHPCC provides state-of-the-art computational infrastructure, indispensible in the increasingly data-rich environment of the post-genomic revolution. One important goal of the MGHPCC is to act as a catalyst for new endeavors that involve the five MGHPCC universities as well as other regional stakeholders. Of particular interest are initiatives that target timely research and education in areas that (1) are of critical national importance and need, and (2) represent significant and complementary presence and strengths in all participating institutions.

Cyber security is one such area that is prime for MGHPCC institutions to pursue collaboratively, with the goal of establishing a national academic center of excellence that acts as a magnet not only for research funding but also for "*brain power*" at a level that is possible to secure collectively through a consortium as opposed to individually through existing centers at participating institutions.

The opportunity is not for the envisioned multi-institutional consortium to supplant existing, strong cyber-security centers and groups at participating institutions – such as MIT's Cryptography and Information Security (CIS) group, BU's Reliable Information Systems and Cyber Security (RISCS) center, U Mass' Commonwealth Center for Forensics and Society, NEU's Institute for Information Assurance, and Harvard's Berkman Center for Internet and Society – but rather to combine and coordinate efforts and allow for a best-of-breed, whole-bigger-than-the-sum-of-its-parts approach.

Summary of Keynote Presentations and Panel Discussion

In her remarks to the summit, **Shafi Goldwasser** underscored the unrivaled strengths in basic and applied cyber-security research in New England. She described recent breakthroughs by local cryptographers that promise a complete paradigm shift in how we address issues related to the security of cloud computing, among others. She also pointed out to the significance of applied research conducted by local system security groups on the security of trusted platforms and cyber-physical systems in general, and medical devices in particular. Her remarks left little doubt as to the quality (and supremacy) of academic research in New England, and the fallacy of portraying academic research as impractical or of drawing distinctions between theoretical and applied cyber-security research.

In her remarks to the summit, **Susan Landau** underscored the importance for academic initiatives to involve a significant social science perspective, and the importance of identifying grand challenges around which to build inter-disciplinary, multi-institutional collaborations. She singled out a few areas of potentially-significant funding opportunities from national agencies, focusing on cloud computing as well as the NSTIC initiative (National Strategy for Trusted Identities in Cyberspace) as a challenge that transcends both computing and social sciences. She suggested that New England may be in a unique position to target grand challenges along these lines with an eye for supporting services for local medical and/or financial institutions, where issues of security and privacy are paramount.

In his remarks to the summit, **Robert Brammer** explained the importance of arbitrage when it comes to supporting academic research through a consortium funded by industry or by the public sector. Specifically, he attributed the success of the Northrop Grumman research consortium that he led (involving MIT, CMU, and Purdue) to the fact that the consortium did not try to dictate the research agenda, but rather that the consortium acted as match maker – connecting the capabilities offered by the highest-ranked research groups to the overall mission of the enterprise. He made it abundantly clear that the presence of New England in cyber security is not only due to the concentration of exceptionally talented academics in area institutions, but also it is due to the concentrations of beneficiaries from advances in cyber security – namely the IT, financial, and medical services sectors.

During the panel discussion, a number of points were emphasized by faculty members regarding their experiences and best practices in initiatives they led in their respective institutions. **Ran Canetti**, who led the Check Point Institute for Information Security at Tel Aviv University in Israel, noted the importance of the availability of flexible funding – *"a little funding could go a long way as long as it is flexible"* – and the importance of viewing research projects in a university setting as indispensable training for future industry hires. He also stressed the importance of *"good communication"* and *"clear, realistic expectations"* in any industry-academia collaboration. **Brian Levine**, who founded and leads the Commonwealth Center for Forensics and Society at UMass Amherst, noted the huge need for (and potential from) translational research, emphasizing the importance to practitioners of understanding new capabilities, and the fact that such practitioners end up being the best advocates for continued research support – a case in point was his experience leveraging the law enforcement agencies of the Commonwealth of Massachusetts with respect to digital forensics. **Salil Vadhan**, who leads the Center

for Research on Computation and Society at Harvard University, emphasized the interesting similarities between lawyers and theoreticians regarding security definitions, and the potential from rewarding interdisciplinary research along these lines. He noted that extended contact time and co-location of principals are crucial elements of success.

The panel discussion also delved into the question of whether it is best for a consortium to first identify grand challenges and then create the best possible teams/collaborations around such challenges (a top-down approach), or whether it is best to identify the best promising academic research projects and use the consortium for funding such projects (a bottom up approach). The discussion revealed that there is room for both approaches and that the two approaches are not necessarily exclusive of one another.

Another observation that resonated with many participants is that *"the region's undeniable presence and strength in cyber-security is under-rated due to the lack of good communication, public relations and outreach support*." Such support is essential to convey to practitioners and to the general public the range of expertise available among academics and the potential from newly developed technologies and capabilities.

Summary of Breakout Group Reports

Anna Lysyanskaya (Brown) and **Leo Reyzin** (BU) presented the main conclusions of the *"Cryptographic Models and Protocols"* breakout group, which encompasses the more theoretical dimensions of cyber-security including foundations of cryptography, cryptographic constructs, applied cryptography, zero-knowledge computation, differential privacy, compositional security, quantum computing, obfuscation, among others. The group reiterated the status of New England as the bedrock of cryptography and cryptography-related research, with trailblazing young academics of the highest caliber following in the footsteps of the giants who made cryptography the enabling technology it is today for Internet e-commerce. They reiterated their belief in the incredible opportunities for cryptographic solutions to many highly practical and timely challenges facing industry and government, including *"crypto-informed cloud and mobile computing, private information retrieval, multiparty computation, and e-voting".* They noted that problems such as the development of trusted cyberspace identities can only be solved through interdisciplinary means that consider social and legal issues of identity, and that problems such as analysis of private data can only be solved through collaborations involving field experts who are able to appreciate information utility – e.g., as they relate to medical and public health records. The group emphasized that *"there are currently few good mechanisms for funding prototyping and/or implementation efforts of projects that do not have immediate industry support but may be of significant public benefit once their potential is demonstrated (e.g., e-voting)"* – using Ph.D. students for such efforts is often detrimental to their careers, and undergraduate students are often under-qualified. The group underscored the *"importance and scarcity of time for advanced research"*, noting that time can be obtained (saved), for example, through *"course buyouts, co-taught offerings, and increased administrative support."* In addition to time pressure, the group attributed the tendency of researchers to favor specialization over interdisciplinary collaborations to the fact that research groups are seldom co-located (noting the *"absolutely essential role of colocation and social interactions for organic,*

meaningful collaborations"). The group noted that a multi-institutional consortium could help address some of these issues by supporting a common postdoc program that allows for a pool of postdocs to work with multiple mentors, a prestigious visiting fellows program that attracts world renowned experts and organizes events around them, a well-funded and well-advertised rotating colloquium, and internship placement programs for graduate and undergraduate students. In terms of training of graduate students, the group noted that the artificial separation between theory and systems and the lack of exposure of graduate students to the social and legal issues related to cyber security contribute to the lack of appreciation for cryptographic-based solutions. The group noted that a multi-institutional consortium could help address some of these issues by coordinating curricular offerings to allow for team-taught, best of breed courses as well as additional specialized courses taught by visitors – "*it is unfortunate to have four or five faculty teach a basic cryptography or network security course within a 5-mile radius of one another."* It was noted that *"having joint credit for both students and instructors would allow offering of advanced courses that wouldn't get enough enrollments at any one institution,"* and that *"such courses often lead to increased research productivity."* The group identified many possible topics for such courses. In terms of a short-term 2011/12 activity to coalesce the academic community in New England, the group proposed that a *"regional technical workshop to learn who is doing what"* would be most useful. The group concluded its remarks by underscoring the importance of figuring out governance issues, including allocation of shared resources and administrative burdens.

Srini Devadas (MIT) and **Ibrahim Matta** (BU) presented the main conclusions of the *"Trust-Enhancing Architectures and Processes"* breakout group, which encompasses the architectures and platforms supporting cyber-security including software certification, formal verification, safe programming languages, virtualization architectures, trusted-hardware platforms, secure CPS and SCADA architectures, clean-slate design, security analysis tools, among others. The group started by emphasizing that the use of trust-enhancing platforms (both hardware and software) and processes (including software engineering practices) are of critical importance to cyber-security. Yet, in terms of academic presence (especially in the US as compared to Europe), research along these dimensions is not reflective of the needs and challenges associated with these areas – not the least of which is education and training. This presents an investment/growth opportunity for New England to raise the bar by recruiting academics focusing on the technologies that provide "security by design" – e.g., through the use of formal models and automated verification as well as the design and implementation of safe programming languages (both of which are areas where additional talents is needed). The group noted that a multi-institutional consortium could help address some of the challenges facing researchers focusing on the development of trusted platforms, especially as it relates to supporting *"research engineers"* since success of research on trusted platforms depends on the ability of academics to produce *"production-quality"* environments and tools. With respect to the most pressing grand challenge, the group noted that rather than following the piecemeal approach to security (which is prevailing in existing architectures and platforms), there is a need for *"a coherent approach that relies on a clean-slate design, including design for security against side-channel attacks and for access-controlled computing."* In terms of important research that requires wider collaboration, the group singled out the challenge of *"minimizing the trusted computing base"* which requires collaboration between software platform security, hardware platform security, and cryptography. In terms of

contributions from other areas that will be crucial for the development of trustworthy platforms, the group identified the need for understanding *"the influence of policies on security architectures."* In terms of hurdles that limit inter- and intra-disciplinary work involving trusted platforms, the group singled out the *"learning curve associated with learning each other's language"* and the *"lack of awareness about new approaches."* Along these lines, the group indicated that a *"summer school for training faculty and graduate students on emerging formalisms, platforms, and methodologies"* would be the most useful short-term 2011/12 activity to coalesce the academic community.

Mark Crovella (BU) and **Dave Kaeli** (NEU) presented the main conclusions of the *"System and Network Security"* breakout group, which encompasses the operational and empirical aspects of cyber-security, including anomaly detection, intrusion detection, access control, secure routing, social network analysis, data mining, wireless and mobile network security, secure cloud computing, network anonymity, among others. The group emphasized that New England has a number of resources that are rather unique, including the forthcoming MGHPCC facility as well as the unparalleled number of major organizations – namely hospitals, banks, and universities – that involve huge IS&T infrastructures and operations with significant cyber security needs. The group noted that the current "cyber arms race" nature of cyber security in an operational environment makes aspects of *"detection"* and *"containment"* particularly important, noting that research along these lines requires access to data from real operating environment, and could benefit significantly from shared infrastructures and test-beds. As an example of how the MGHPCC facility (itself a multi-institutional shared resource) could be used in support of a multi-institutional collaboration in cyber security, the group postulated that novel detection technologies (which requires instrumentation and measurement) and containment technologies (which requires sandboxing, firewalling, and access control management) "*could be deployed as part of an EC2-like service hosted in Holyoke."* Another possible use of the MGHPCC facility may well be an experimental evaluation of the potential from *"testing homomorphic encryption in the cloud at scale."* Both of these are examples of grand challenges that require significant collaborations among multi-institutional and multi-disciplinary teams, and require significant HPC infrastructure. The group noted that the availability of a large shared infrastructure with technical/admin staff able to deal with regulatory and compliance issues is exemplary of the type of support that is not possible for a single research group or even a single institution to provide – hence the need for a regional facility and major industrial and government investments. The group noted the importance of having regular venues (annual symposia or rotating seminars) that allow academics in collaborating institutions to *"know what each other are doing."* The group also identified a number of much-needed activities that a multi-institutional consortium could carry out, including *"seed funding as a catalyst for collaboration"*, *"collection, sanitization, and anonymization of proprietary data (e.g., incident reports) from partnering organizations for sharing with consortium research groups"*, and *"crowd-sourcing of defense/offense cyber security capabilities by organizing high-school level hackathons and competitions"*. Finally, the group underscored that while attribution and motivation are complex, cyber-attacks are often simple – but increasingly leveraging social engineering – indicating the need for human-computer interaction (HCI) and psychology dimensions in order to *"design for transparency to defeating social engineering."*

Jim Waldo (Harvard) and **Judith Perrolle** (NEU) presented the main conclusions of the *"Society, Public Policy, and Jurisprudence"* breakout group, which encompasses the more societal dimensions of cyber-security including digital identity management, censorship, law enforcement, cyber forensics, industrial espionage, economics of cyber-security, privacy standards and practices, e-voting, international relations, among others. The group noted that while the strength and status of New England as a hub for excellence in computing research is indisputable, what sets it apart from any other national or international academic hub with respect to cyber-security is the fact that the region is also home to some of the best academics in the social sciences and in professional disciplines, including world-renown schools of medicine, education, business management, law, and government, as well as related industrial labs, non-profit organizations, and second-to-none financial and medical institutions. *"In short, it is the strength of the broad set of inter-acting academic and business concerns that makes New England unique. If we are to put together a center, we should leverage this unique set of strengths and not try to narrowly focus on an area where there is credible competition elsewhere."* The group noted that cyber security problems that are not necessarily technical need to be addressed. Problems of foundational nature that define cyber security include *"What governance can or should be established that has the proper scope? How can attack/defense data be shared? What laws support/could support efforts in the area? What incentives (computational, economic, and legal) play into cyber-security? How do privacy and security interact?"* Additionally, the group recognized the importance of tackling problems that are of a practical nature, including *"How do computer forensics track legal requirements? How can large-scale data research interact with privacy? What protections can be developed and deployed to aid in attack resistance?"* The consensus of the group was that this is a *"target-rich area"* and that any multi-institutional initiative would be better off focusing on some set of (practical) problems that can be addressed and then "setting up the research and development to address those problems" rather than *"trying to fit problems to a pre-set research agenda."* The group also noted that following this problem-oriented approach would also act as *"a guide for where to obtain funding."* In terms of initial steps towards any envisioned multi-institutional initiative, the group felt strongly that *"initial actions should be simple, administratively straightforward, and designed to break down intra- and inter-school barriers."* One example of such steps is the development of tools (e.g., through a wiki) to coordinate guest lectures in courses which would allow for *"spreading of expertise (teach the teachers) and encourage interaction and collaboration."* Another example of small initial steps proposed by the group is a regular half-day cross-institutional colloquia featuring a set of co-located talks at each participating institutions – *"which would be a better draw for those not at the hosting institution."* The group also reiterated the value of supporting a multi-institutional internship program, noting that *"establishing an internship program that is by nature cross-institutional would begin to break down barriers at the most important level, that of the students"* and that *"such internships should be at all levels including undergraduates, graduates, and postdocs."* The group also pointed out that the international dimension of cyber security offers some of the most complex problems to tackle and that *"it is important that views from non-US participants be part of the DNA of such a collaborative venture."* Specifically, the group noted that establishing a visiting scholars program or coordinating placement of international exchanges are important goals – *"identifying and encouraging non-US participants from each of the collaborating institutions would be an immediate first step."*

Speakers

Mel Bernstein is Vice Provost for Research at Northeastern University. Prior joining NEU, he was acting director of research and development for the US Department of Homeland Security, where he had primary responsibility for a significant portion of the extramural research programs within the Science and Technology Directorate, including homeland security-related research at all the U.S. Department of Energy's (DOE) National Laboratories, universities (particularly DHS Centers of Excellence) and DHS-related laboratory facilities. He was also responsible for developing joint programs with other key science-based federal agencies, such as the NSF, DOE, DoD, and NIH.

Azer Bestavros is Professor of Computer Science and the Founding Director of the BU Hariri Institute for Computing and Computational Science & Engineering at Boston University. His research is on scalable and trustworthy Internet systems. He is the chair of the IEEE Computer Society TC on the Internet, and the recipient of distinguished service awards from both the ACM and the IEEE. He is the recipient of the United Methodist Scholar Teacher Award for outstanding dedication and contributions to the learning arts at BU, and co-winner of the ACM Sigmetrics Inaugural Test of Time Award for seminal work on Internet and web characterization whose impact is still felt 10-15 years after its initial publication.

Robert Brammer is VP for advanced technology at Northrop Grumman's IS sector, where he is responsible for overall technology strategy as well as R&D programs and partnerships. He holds a PhD degree in mathematics from the University of Maryland. He is a Woodrow Wilson Fellow, received achievement awards for work on the Apollo program and for research on NASA and NOAA satellite remote-sensing programs. He has served on advisory boards for the DoD Defense Science Board, the National Academy of Sciences, the Naval Studies Board, and the NSF, among others. He is a member of the External Relations Council for the Internet2 Consortium and the Virginia governor's Broadband Roundtable. He was recently named by Security Magazine as one of the 25 most influential people in the security industry and by ExecutiveBiz as one of the top ten CTOs in the Greater Washington area to watch in 2009.

Ran Canetti is Professor of Computer Science and Director of Research at the Reliable Information Systems and Cyber Security (RISCS) Center at Boston University. Prior to joining BU, Canetti spent 12 years as a researcher at the Cryptography group, IBM T.J. Watson Research Center, and also headed the Check Point Institute for Information Security in Israel. His research interests lie in cryptography and system security, with emphasis on the design and analysis of cryptographic protocols and algorithms. His major contributions include foundational results on composable formal security analysis, and on software obfuscation.

Shafi Goldwasser is the RSA Professor of EECS at MIT. Goldwasser is the co-inventor of zero-knowledge proofs, which probabilistically and interactively demonstrate the validity of an assertion without conveying any additional knowledge, and are a key tool in the design of cryptographic protocols. She has twice won the Gödel Prize in theoretical computer science. Other awards include the ACM Grace Murray Hopper Award, the RSA Award for outstanding contributions to cryptography, the IACR Fellow, the Athena Lecturer Award of the ACM's Committee on Women in Computing, and the Benjamin Franklin Medal in Computer and Cognitive Science.

Susan Landau is the Elizabeth S. and Richard M. Cashin Fellow at Sun Microsystems, and Radcliffe Institute Fellow at Harvard University, where she studies the interplay between privacy, cyber security, and public policy. She has briefed Congress on a variety of issues, including digital rights management and security and privacy of digital identity systems. She is the recipient of a 2008 Women of Vision Award, a fellow of the American Association for the Advancement of Science, and an ACM Distinguished Engineer. She is a member of the Computer Science and Telecommunications Board of the National Academies and of the advisory committee for the CISE Directorate of the NSF. She is coauthor of "Privacy on the Line: the Politics of Wiretapping and Encryption" and of "Surveillance or Security? The Risks Posed by New Wiretapping Technologies".

Brian Levine is Professor of Computer Science at UMass, Amherst. Levine's research focuses on mobile networks, privacy and forensics, and the Internet. His active funding includes awards from the NSF on CyberTrust and on clean-slate Internet designs, and from the DoD's capacity building program for security education, and from the National Institute of Justice's Electronic Crime program. His awards include the UMass Lilly Teaching Award, the UMass College Outstanding Teacher Award, and the U of Albany Alumni Award for Excellence in Science and Technology. He heads the Commonwealth Center for Forensics and Society at UMass Amherst.

Salil Vadhan is the Vicky Joseph Professor of Computer Science and Applied Mathematics and Director of the Center for Research on Computation and Society at Harvard University. He held appointments as an NSF Mathematical Sciences postdoctoral fellow at MIT and at the Institute for Advanced Study, a Fellow at the Radcliffe Institute for Advanced Study, and a Miller Visiting Professor at UC Berkeley. His Ph.D. thesis on statistical zero-knowledge proofs received the ACM Doctoral Dissertation Award in 2000, and his paper on the zig-zag product for expander graphs was a co-recipient of the Gödel Prize in 2009. His other awards include the Guggenheim Fellowship, the ONR Young Investigator Award, the Sloan Fellowship, the NSF CAREER Award, and a Phi Beta Kappa Award for Excellence in Teaching.

Participants

1	Melvin Bernstein	Northeastern U	http://www.northeastern.edu/provost/about/staff/research.html
2	Azer Bestavros	Boston U	http://www.cs.bu.edu/~best
3	Robert Brammer	Northrop Grumman	http://www.is.northropgrumman.com/about/leadership/assets/BrammerRobert.pdf
4	Jeff Brancato	U Mass	
5	Ran Canetti	Boston U	http://www.cs.tau.ac.il/~canetti
6	Agnes Chan	Northeastern U	http://www.ccs.neu.edu/home/ahchan
7	Mark Crovella	Boston U	http://www.cs.bu.edu/~crovella
8	Bruce Davie	MIT & Cisco	http://nms.lcs.mit.edu/~bdavie/
9	Srini Devadas	MIT	http://people.csail.mit.edu/devadas
10	Shafi Goldwasser	MIT	http://people.csail.mit.edu/shafi
11	John Goodhue	MGHPCC	http://www.mghpcc.org
12	Bill Guenther	Mass Insight	http://www.massinsight.com/about/staff/
13	Steve Homer	Boston U	http://www.cs.bu.edu/~homer
14	Arthur Hulnick	Boston U	http://www.bu.edu/ir/faculty/alphabetical/hulnick
15	David Kaeli	Northeastern U	http://www.ece.neu.edu/faculty/kaeli.html
16	Mark Karpovsky	Boston U	http://reliable.bu.edu/People/karp.aspx
17	Assaf Kfoury	Boston U	http://www.cs.bu.edu/~kfoury
18	Engin Kirda	Northeastern U	http://www.ccs.neu.edu/people/faculty/kirda.html
19	Susan Landau	Harvard	http://radcliffe.harvard.edu/fellowships/fellows_2011slandau.aspx
20	Leonid Levin	Boston U	http://www.cs.bu.edu/~lnd
21	Brian Levine	U Mass Amherst	http://www.cs.umass.edu/~brian
22	Andrew Lo	MIT	http://web.mit.edu/alo/www/
23	Anna Lysyanskaya	Brown	http://www.cs.brown.edu/people/faculty/anna.html
24	Anne Margulies	Harvard	http://news.harvard.edu/gazette/story/2010/07/cio/
25	Ibrahim Matta	Boston U	http://www.cs.bu.edu/~matta
26	Alan Mislov	Northeastern U	http://www.ccs.neu.edu/home/amislove/
27	Tyler Moore	Harvard	http://cyber.law.harvard.edu/people/tmoore
28	Caroline Nolan	Harvard	http://cyber.law.harvard.edu/people/cnolan
29	Guevara Noubir	Northeastern U	http://www.ccs.neu.edu/home/noubir
30	Judith Perrolle	Northeastern U	http://www.northeastern.edu/socant/?page_id=316
31	Leo Reyzin	Boston U	http://www.cs.bu.edu/~reyzin
32	Ron Rivest	MIT	http://people.csail.mit.edu/rivest
33	Vipin Swarup	MITRE	http://www.ziplink.net/~swarup/vipin/
34	Evimaria Terzi	Boston U	http://www.cs.bu.edu/~evimaria
35	Ari Trachtenberg	Boston U	http://www.bu.edu/ece/people/faculty/o-z/ari-trachtenberg
36	Nikos Triandopoulos	EMC RSA Labs	http://www.cs.bu.edu/~nikos
37	Salil Vadhan	Harvard	http://people.seas.harvard.edu/~salil
38	Marshall Van Alstyne	Boston U	http://smgapps.bu.edu/mgmt_new/profiles/VanAlstyneMarshall.html
39	Marten van Dijk	EMC RSA Labs	http://www.rsa.com/rsalabs/node.asp?id=3774
40	Mayank Varia	Lincoln Labs	http://www.variabilities.com/
41	Jim Waldo	Harvard	http://www.eecs.harvard.edu/~waldo/
42	Dan Walsh	Mass Gov	
43	Jie Wang	U Mass Lowell	http://www.cs.uml.edu/~wang
44	John Williams	MIT	http://cee.mit.edu/williams
45	Joseph Wippl	Boston U	http://www.bu.edu/ir/faculty/alphabetical/wippl
46	Nickolai Zeldovich	MIT	http://www.csail.mit.edu/user/1705
47	Tanya Zlateva	Boston U	http://people.bu.edu/zlateva/

Questions to Breakout Groups

- What strengths do we have along the "prevention", "detection", "containment", and "deterrence" *cyber security capabilities*? Examples? Others?
- What strengths do we have along the "health informatics", "smart grid and CPS", "financial services", "cloud computing", and "freedom and democracy" *cyber security application domains*? Examples? Others?
- What are the significant problems of *academic interest* to your breakout group?
- What are the problems that should be of *industrial interest* from your breakout group?
- How could other research areas *collaborate* on significant problems you identified?
- Are there problems that can *only* be tackled in collaboration with areas not represented in your breakout group?
- What are the *hurdles for collaboration* with researchers not in your breakout group?
- What *education and training* is missing for graduate students in your breakout group?
- Are there unique cyber security grand challenges that you believe to be particularly suited for *New England*? Why?
- What could a multi-institutional consortium offer that would help increase your *research productivity*?
- What of the following *resources and services* are useful to have on a multi-institutional scale? How do they rank? What else?
    - Multi-institutional postdoc program
    - Multi-institutional visiting fellows program
    - International exchange program
    - Course cross registration among participating institutions
    - Rotating colloquium series
    - Internship programs for graduate and undergraduate students
    - Joint REU programs
    - Cyber war game competitions/camps
    - Support for research engineers
    - Thematic workshops *a la* IACR and DIMACS
    - Access to industrial platforms and data
- What would be a good *community-building, integrative activity* to shoot for in 2011/12, possibly funded through the ACSC, the MGHPCC, and/or the Hariri Institute? Other sources?