

Summary of Accomplishments

Kevin W. Hamlen

December 16, 2011

1 Introduction

My research approaches software security challenges from the perspective of programming language design and analysis. Such *language-based approaches to security* constitute an increasingly important area of converging research because they provide provable, mathematical guarantees about the security of large, real-world software systems, rather than relying upon error-prone, manual inspection of programs or incomprehensive random testing. My work at UTD since 2006 has resulted in

- **\$4.0 million** in federal research awards (\$1.9 million as PI + \$2.1 million as Co-PI) including **2 Career awards** (from AFOSR and NSF, respectively),
- approximately **30 scholarly research publications** in peer-reviewed conferences and journals,
- a history of **intellectually challenging, high-quality classroom teaching** (median student evaluation: 9/10 intellectual challenge, 4.54/5 overall quality = “Excellent” over 12 courses), and
- supervision of **7 Ph.D. students** (first 2 graduations expected Fall 2011 [**1**, **2**]) and **3 Masters students** (2 graduations [**3**], 1 pending).

2 Original Investigation

This section describes my three main research directions: **machine-certified, binary, in-lined reference monitors** (§2.1), **next-generation malware attacks and defenses** (§2.2), and **cloud and peer-to-peer computing security** (§2.3). Successes are briefly highlighted in terms of noteworthy publications and grants awarded.

2.1 Language-based binary analysis

The birth of computer science as a discipline can be traced to a pair of famous proofs by Gödel and Turing, who discovered that certain mathematical problems are inherently *undecidable*—that is, no machine or algorithm can ever solve them

reliably. This imposes fundamental limitations on the ability of security systems to reliably distinguish safe software from unsafe software.

My 2006 publication in **ACM Transactions On Programming Languages And Systems (TOPLAS)** [4] showed that protection systems based on automated binary *transformation* (instead of merely inspection) can potentially circumvent this historic computability barrier. For example, a compiler or binary rewriter can automatically remove all safety-violating behaviors (without corrupting any safe behaviors) for many large classes of programs and safety policies that are undecidable by static inspection alone. This established an important connection between computational complexity theory and software security research that has been **cited over 120 times** since its publication (according to Google Scholar).

My subsequent research has leveraged this insight to build powerful, high-assurance software protection systems based on formally certified, *in-lined reference monitors* (IRMs). IRM systems automatically augment untrusted binary software with runtime security checks to produce safe, self-monitoring code. The transformed code can subsequently be formally machine-verified to prove that it respects the original policy. This removes the potentially complex binary rewriter from the trusted computing base (TCB) in favor of a smaller verifier. Soundness proofs for the verifier further reduce the TCB to the foundations of mathematics. This novel strategy thus marries the strong formal guarantees of provably sound, static program analysis with the power of dynamic protection systems.

My research has developed practical IRM systems for .NET bytecode [5], Java bytecode [6, 7, 8, 9, 3, 10, 11, 1, 12], and ActionScript Flash bytecode [13, 14, 15], and my most recent work has extended the approach to x86 native code architectures [16, 17]. I have published algorithms for realizing automated, formal IRM certification as **type-checking** [5, 18] and as **model-checking** [14, 19]. My work has received a

- 2008–2011 Young Investigator (Career) award from the U.S. Air Force Office of Scientific Research (AFOSR).

Such awards are highly competitive; mine was the only one awarded for cybersecurity that year to my knowledge.

My recent 2010 publication in the **9th International Conference on Aspect-Oriented Software Development (AOSD)** [8] draws from these experiences to propose a *purely declarative, aspect-oriented* approach to IRM policy specification. Policy specifications for IRMs must be extraordinarily detailed in order to facilitate fully automated, binary-level enforcement and verification. This can make them extraordinarily difficult for humans to write, leading to dangerous policy specification errors. We show that when policies are expressed in a purely declarative, aspect-oriented style, many errors become detectable as *inconsistencies* that can be automatically uncovered by exposing non-determinism in the policy's underlying security automaton. The work has significant applications for *advice conflict detection* in traditional aspect-oriented programming as well. AOSD is a Tier-1 software engineering conference (a 22% acceptance rate in 2010).

As part of our work on applying IRMs to CISC native code, I this year published a paper in the **European Conference on Machine Learning and Principles**

and Practice of Knowledge Discovery in Databases (ECML PKDD) [17] that proposes the first machine learning-based approach to *static x86 disassembly*. The x86 disassembly problem is notoriously difficult, yet a necessary first step for many secure software analyses, such as reverse engineering and binary instrumentation. Our approach inferred substantially better disassemblies of large, real-world (non-open source) software applications than the best commercial disassemblers used for reverse engineering today. ECML PKDD is a Tier-1 conference (acceptance rate 20% for 2011).

My future plans [21] include extending IRM-based security to *mobile web advertisements* in collaboration with the University of Illinois at Chicago (UIC). The proposed project has been awarded a

- National Science Foundation (NSF) Trustworthy Computing grant for collaborative research that was funded for over \$1.2 million for 2011–2014 (\$560K for UTD).

I am the sole UTD PI for the proposal.

2.2 Malware attacks and defenses

Cyber-security research is not just about defending against existing attacks; it must also anticipate next-generation attacks and even develop counter-attack strategies for cyber-warfare. This is exemplified by the ongoing virus-antivirus arms race, in which defenders relentlessly develop new malware detection strategies to anticipate and counter new malware developed by attackers. My work applies recent advances in *automated stream mining* to the problem of malware detection [22, 23, 24, 25, 26, 27] and malware obfuscation and propagation [28]. The work has been awarded an

- Active Defense grant from the U.S. Air Force Office of Scientific Research (AFOSR) (\$450K for 2011–2014), and a
- 2011 grant from the U.S. Army (\$350K for 2011–2012).

I am the PI for the first proposal and a Co-PI for the second.

This ongoing work addresses challenges faced by a malware defense community that must currently rely upon time-consuming, semi-manual approaches to virus signature inference and generation. This places defenders at a significant disadvantage relative to attackers, who can introduce new binary obfuscations with far less time and effort. As a result, defenders struggle to keep pace with the ever growing pool of malicious software, and remain particularly vulnerable to zero-day attacks.

Our research shows that highly accurate malware classifications can be obtained fully automatically through the use of data mining algorithms for *unbounded-length, concept-drifting streams*. Supporting concept-drift allows such algorithms to adapt as attackers introduce new obfuscations, and identify zero-day attacks far more quickly than is possible with approaches that require human intervention.

For example, our publication in the **ACM Transactions on Management Information Systems (TMIS)** [26] demonstrates that stream mining-based malware detection can be elegantly expressed as parallelized Hadoop MapReduce computations. This makes it exceptionally well suited to cloud computing architectures.

Stream mining-based defenses can also become powerful attacks if directed against conventional antivirus protections. Our 2009 publication in the **Computer Standards & Interfaces Journal** [28] demonstrates that any antivirus product that divulges its classification decisions leaks enough information for a stream mining algorithm to infer and usually defeat its classification model. Such *reactively adaptive malware* learns and adapts to signature-based antivirus protections fully automatically in the wild, rendering such defenses ineffective. Attackers already exploit this information manually when crafting new attacks, and we believe it will not be long before the technique begins appearing in automated form within self-propagating malware.

My ongoing research in this area is studying possible defenses for next-generation malware attacks, as well as language-based approaches that leverage stream mining for polymorphic, zero-day malware defense. The proposed work has garnered a

- 2011 National Science Foundation (NSF) Career award for language-based polymorphic malware security (\$504K for 2011–2016).

NSF Career awards are widely regarded as some of the most prestigious grants available to untenured researchers, and are highly competitive—only 22% of proposals were funded in 2010.

2.3 Cloud computing security

Cloud computing is significant area of current data security research that extends decentralized, distributed computing technologies, such as peer-to-peer networking, to massively distributed clouds of low-cost, heterogeneous machines. My research has developed new security-aware protocols and security applications for cloud computers [29, 30, 31, 32, 33, 26, 34].

As an example of this work, my 2007 publication in the **23rd Annual Computer Security Applications Conference (ACSAC)** [29] introduced a flexible, efficient data ownership privacy enforcement strategy for structured, decentralized, peer-to-peer networks. ACSAC is one of the top five national security conferences (with a 20.9% acceptance rate for 2007). My more recent work has applied these technologies for data security in the semantic web [33], and using economic theory (e.g., [35, 36]) to incentivize non-malicious behavior in networks of mutually distrusting cloud nodes.

The work has been awarded an

- NSF EArly-concept Grant for Exploratory Research (EAGER) for 2009–2011 (\$80K).

EAGER grants are increasingly difficult to obtain; they are awarded only to highly novel research proposals that are deemed to have a potential for exceptionally high reward.

3 Classroom teaching

One significant root of the software security crisis is a dearth of adequate security training in most computer science programs today. Computer science undergraduates are typically trained to program quickly to meet tight product deadlines, and to meet quality standards that are measured purely in terms of code correctness and efficiency under standard conditions and with standard program inputs. They are not typically trained to think systematically about adversarial conditions or security vulnerabilities as they write code. The result is an industrial culture that often incorrectly presumes that security is a finishing touch that can be added to software near the end of its development.

Software engineering experts increasingly agree that this approach to security does not scale adequately to large systems, and has been a major contributor to the deeply flawed critical cyber-infrastructure we see today. Code that is robust against attacks requires careful planning during all stages of the software development lifecycle, including an implementation phase manned by programmers who have been trained to think like attackers as they write code. This means that effective computer security education cannot be limited to isolated courses outside the main curriculum (though such courses are still valuable). Security awareness and best practices must be integrated into all aspects of the curriculum as a fundamental quality criterion for all programming tasks.

I have put this philosophy into practice at UTD through the introduction and integration of significant security components to numerous traditionally non-security courses in the computer science program. My efforts along those of my colleagues have received a

- \$1.7 million award from the National Science Foundation (NSF) for a **Federal Cyber Service: Scholarship for Service** program at UTD for 2010–2014.

(I am one of four Co-PIs for the proposal.)

In 2008 a Masters student under my supervision was awarded a prestigious

- Information Assurance Scholarship from the U.S. Department of Defense (\$42K for 2008–2009).

(I was the sole PI for the proposal.) This was the first such award ever granted to a UTD student. The student was employed by the DoD upon graduation, and has subsequently entered the Ph.D. program of Harvard University. Two undergraduates under my supervision have been admitted to the Computer Science graduate programs of Carnegie Mellon and Oxford, respectively, demonstrating that students graduating under my supervision are competitive with top candidates in the field.

In Fall and Spring 2009 I taught two instances of the computer science **Senior Design Course (CS4485)** in which undergraduates worked in teams of 4 or 5 to design and implement secure peer-to-peer file-sharing systems. This aggressive curriculum introduced students to a vast array of security considerations to which most had never before been exposed. These included data integrity and privacy

considerations, network protocol analysis, the advantages and limitations of cryptographic I/O, security implications of race conditions, and man-in-the-middle attacks. Rather than presenting students upfront with the security ramifications of their design choices, students were permitted to discover vulnerabilities in a natural way as they became apparent, whereupon I introduced the advanced concepts necessary to address them. For many students this resulted in a first-time understanding of why a systematic, methodological approach to programming is so important in a large project, and how hard it is to “add security” later when security has not been properly considered from the ground up.

As a result of their efforts, two teams submitted their final projects to the **Dallas ComputingFest** competition, one of which earned **second place** in the senior-level division for their innovative approach to securing Chord peer-to-peer networks against message-dropping attacks. Student evaluations rated the course an average of 4.7 out of 5.0 in overall satisfaction—an extremely high rating for a non-elective. (For comparison, the average evaluation over the previous years was 2.5 out of 5.0, and evaluations for my offerings are both higher than any other offering of the course currently on record.)

At the graduate level, I have significantly redesigned the **Advanced Programming Languages (CS6371)** core course to emphasize the security applications of advanced program analyses such as polymorphic type theory, automated verification condition generation and checking, axiomatic semantics, and advanced programming paradigms such as functional and logic programming. This material is extended and elaborated in my **Language-based Security (CS7301)** graduate elective, which builds upon this foundation to train students in software verification through automated theorem-proving, model-checking, binary analysis and modification, malware detection, and information flow tracking. Student evaluations of both courses are consistently high (4.2 for CS6371 and 4.8 for CS7301, on average) despite difficulty rankings that are consistently in the 9th decile relative to other UTD courses. This shows that students are learning extremely challenging material, but in a way that is accessible and interesting.

My teaching has also subsequently led to the **National Science Foundation (NSF) Career Award** that I received in 2011 (\$504K for 2011–2016). Career proposals require a very significant educational component that integrates cutting-edge research with learning opportunities for graduates and undergraduates. My history of creative, high-quality classroom teaching was therefore essential for receiving this award.

4 Service

Over the past five years I have served on the program committees of 3 conferences related to programming languages, software engineering, and/or computer security, as well as serving as the **General Chair of the 11th ACM International Symposium on Practical Aspects of Declarative Languages (PADL)** in 2009, and the **Registration Chair of the 10th IEEE High Assurance Systems Engineering Symposium (HASE)** in 2007. In addition to these titled

appointments, I regularly review scientific articles for such high-profile venues as the **IEEE Transactions on Dependable and Secure Computing (TDSC)** and the **ACM Transactions on Information and System Security (TISSEC)**. Personally writing rigorous, constructive reviews for these journals (rather than delegating the task to students) is time-consuming, but I feel that doing so is important for maintaining the high quality standards of these journals, and is therefore an important contribution to the field.

I also hold memberships with the two most important professional societies in my discipline—the **Association of Computing Machinery (ACM)** and the **Institute of Electrical and Electronics Engineers (IEEE)**.

Within the computer science department, I have served on the 3-person **Teaching Assistant committee** for the past 3 years, and on the **Computer Systems Group Committee** since joining the department in 2006.

In Fall 2009 I voluntarily extended my required course load to teach **CS4485: Computer Science Project** for a second straight semester when a substitute instructor became needed at the last minute. This was a significant time sacrifice because at that time CS4485 essentially required the instructor to individually advise every student in the class in a medium-to-large software development project. Enrollment in 2009 was higher than in any prior year because CS4485 had just become a required course, with the result that I individually advised **over 80 undergraduate students** during 2009. Although the effort was exhausting, it was also rewarding; several of the positive outcomes are discussed earlier in this narrative (see §3).

5 Future Plans

In 2011 I brought in over \$1 million in funding for UTD dedicated to two new NSF research projects that I will lead over the next 3–5 years. The projects will combine my work described in §2.1 and §2.2 to develop advanced malware protection technologies for commercial operating systems and web browsers. I am therefore well positioned to continue and expand my research program at UTD over the next 5 years. I have an active pipeline of submitted and in-progress research manuscripts toward these projects (about 4 submitted and 6 in-progress at the time of this writing).

The NSF Career portion of the funding includes a significant educational component that supports the integration of my research into educational opportunities for graduate and undergraduate students. This is important for supporting our department’s new federally funded Scholarship for Service program with courses and material that teach advanced computer security skills demanded by federal employers and Dallas-area defense contractors such as Raytheon and Rockwell-Collins that constitute significant sources of enrollment in UTD’s CS program.

References

- [1] Micah Jones. *Declarative Aspect-oriented Security Policies for In-lined Reference Monitors*. PhD thesis, The University of Texas at Dallas, Richardson, Texas, December 2011. (Advisor: Kevin Hamlen).
- [2] Sunitha Ramanujam. *Towards an Integrated Semantic Web: Interoperability Between Data Models*. PhD thesis, The University of Texas at Dallas, Richardson, Texas, December 2011. (Advisors: Latifur Khan and Kevin Hamlen).
- [3] Aditi A. Patwardhan. Security-aware program visualization for analyzing in-lined reference monitors. Master's thesis, The University of Texas at Dallas, Richardson, Texas, June 2010. (Advisors: Kevin Hamlen and Kendra Cooper).
- [4] Kevin W. Hamlen, Greg Morrisett, and Fred B. Schneider. Computability classes for enforcement mechanisms. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 28(1):175–205, January 2006.
- [5] Kevin W. Hamlen, Greg Morrisett, and Fred B. Schneider. Certified in-lined reference monitoring on .NET. In Vugranam C. Sreedhar and Steve Zdancewic, editors, *Proceedings of the 1st ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS)*, pages 7–16, Ottawa, Ontario, June 2006.
- [6] Kevin W. Hamlen and Micah Jones. Aspect-oriented in-lined reference monitors. In Úlfar Erlingsson and Marco Pistoiia, editors, *Proceedings of the ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS)*, pages 11–20, Tucson, Arizona, June 2008.
- [7] Micah Jones and Kevin W. Hamlen. Enforcing IRM security policies: Two case studies. In *Proceedings of the IEEE Intelligence and Security Informatics Conference (ISI)*, pages 214–216, Dallas, Texas, June 2009.
- [8] Micah Jons and Kevin W. Hamlen. Disambiguating aspect-oriented security policies. In Jean-Marc Jézéquel and Mario Südholt, editors, *Proceedings of the 9th International Conference on Aspect-Oriented Software Development (AOSD)*, pages 193–204, Rennes, France, March 2010.
- [9] Aditi Patwardhan, Kevin W. Hamlen, and Kendra Cooper. Towards security-aware program visualization for analyzing in-lined reference monitors. In *Proceedings of the International Workshop on Visual Languages and Computing (VLC)*, pages 257–260, Oak Brook, Illinois, October 2010.
- [10] Micah Jones and Kevin W. Hamlen. A service-oriented approach to mobile code security. In Elhadi Shakshuka and Muhammad Younas, editors, *Proceedings of the 8th International Conference on Mobile Web Information Systems (MobiWIS)*, pages 531–538, Niagara Falls, Ontario, September 2011.

- [11] Kevin W. Hamlen and Bhavani Thuraisingham. Secure semantic computing. *International Journal of Semantic Computing*, 5(2):121–131, June 2011.
- [12] Kevin W. Hamlen, Micah M. Jones, and Meera Sridhar. Aspect-oriented runtime monitor certification. In *Proceedings of the 18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, Tallinn, Estonia, March–April 2012. forthcoming.
- [13] Brian W. DeVries, Gopal Gupta, Kevin W. Hamlen, Scott Moore, and Meera Sridhar. ActionScript bytecode verification with co-logic programming. In Stephen Chong and David A. Naumann, editors, *Proceedings of the ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS)*, pages 9–15, Dublin, Ireland, June 2009.
- [14] Meera Sridhar and Kevin W. Hamlen. Model-checking in-lined reference monitors. In Gilles Barthe and Manuel V. Hermenegildo, editors, *In Proceedings of the 11th International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI)*, pages 312–327, Madrid, Spain, January 2010.
- [15] Meera Sridhar and Kevin W. Hamlen. ActionScript in-lined reference monitoring in Prolog. In Manuel Carro and Ricardo Peña, editors, *Proceedings of the 12th International Symposium on Practical Aspects of Declarative Languages (PADL)*, pages 149–151, Madrid, Spain, January 2010.
- [16] Kevin W. Hamlen, Vishwath Mohan, and Richard Wartell. Reining in Windows API abuses with in-lined reference monitors. Technical Report UTDCS-18-10, Computer Science Department, The University of Texas at Dallas, Richardson, Texas, June 2010.
- [17] Richard Wartell, Yan Zhou, Kevin W. Hamlen, Murat Kantarcioglu, and Bhavani Thuraisingham. Differentiating code from data in x86 binaries. In Dimitrios Gunopulos, Thomas Hofmann, Donato Malerba, and Michalis Vazirgianis, editors, *Proceedings of the European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD)*, volume 3, pages 522–536, 2011.
- [18] Kevin W. Hamlen. *Security Policy Enforcement by Automated Program-rewriting*. PhD thesis, Cornell University, Ithaca, New York, August 2006.
- [19] Kevin W. Hamlen, Micah M. Jones, and Meera Sridhar. Chekov: Aspect-oriented runtime monitor certification via model-checking. Technical Report UTDCS-16-11, Computer Science Department, The University of Texas at Dallas, Richardson, Texas, May 2011.
- [20] Bhavani Thuraisingham and Kevin W. Hamlen. Challenges and future directions of software technology: Secure software development, invited paper. In Seikh Iqbal Ahamed, Doo-Hwan Bae, Sung Deok Cha, Carl K. Chang, Rajesh Subramanyan, Eric Wong, and Hen-I Yang, editors, *Proceedings of the 34th*

IEEE Annual International Computer Security and Applications Conference (COMPSAC), pages 17–20, Seoul, Korea, July 2010.

- [21] Meera Sridhar and Kevin W. Hamlen. Flexible in-lined reference monitor certification: Challenges and future directions. In Ranjit Jhala and Wouter Swierstra, editors, *Proceedings of the 5th ACM SIGPLAN Workshop on Programming Languages meets Program Verification (PLPV)*, pages 55–60, Austin, Texas, January 2011.
- [22] Mohammed M. Masud, Tahseen Al-khateeb, Latifur Khan, Bhavani Thuraisingham, and Kevin W. Hamlen. Flow-based identification of botnet traffic by mining multiple log files. In *Proceedings of the International Conference on Distributed Framework & Applications (DFMA)*, pages 200–206, Penang, Malaysia, October 2008.
- [23] Bhavani Thuraisingham, Latifur Khan, Mohammed M. Masud, and Kevin W. Hamlen. Data mining for security applications. In Cheng-Zhong Xu and Minyi Guo, editors, *Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC)*, pages 585–589, Shanghai, China, December 2008.
- [24] Pallabi Parveen, Jonathan Evans, Bhavani Thuraisingham, Kevin W. Hamlen, and Latifur Khan. Insider threat detection using stream mining and graph mining. In *Proceedings of the 3rd IEEE Conference on Privacy, Security, Risk and Trust (PASSAT)*, Boston, Massachusetts, October 2011.
- [25] Pallabi Parveen, Zackary R. Weger, Bhavani Thuraisingham, Kevin W. Hamlen, and Latifur Khan. Supervised learning for insider threat detection using stream mining. In *Proceedings of the 23rd IEEE International Conference on Tools with Artificial Intelligence (ICTAI)*, Boca Raton, Florida, November 2011. (Best Paper Award).
- [26] Mohammad M. Masud, Tahseen M. Al-Khateeb, Kevin W. Hamlen, Jing Gao, Latifur Khan, Jiawei Han, and Bhavani Thuraisingham. Cloud-based malware detection for evolving data streams. *ACM Transactions on Management Information Systems (TMIS)*, 2(3), October 2011.
- [27] Mohammad Mehedy Masud, Clay Woolam, Jing Gao, Latifur Khan, Jiawei Han, Kevin W. Hamlen, and Nikunj C. Oza. Facing the reality of data stream classification: Coping with scarcity of labeled data. *Knowledge and Information Systems (KAIS)*, 2011. forthcoming.
- [28] Kevin W. Hamlen, Vishwath Mohan, Mohammad M. Masud, Latifur Khan, and Bhavani Thuraisingham. Exploiting an antivirus interface. *Computer Standards & Interfaces Journal*, 31(6):1182–1189, April 2009.
- [29] Nathalie Tsybulnik, Kevin W. Hamlen, and Bhavani Thuraisingham. Centralized security labels in decentralized p2p networks. In *Proceedings of the 23rd*

- Annual Computer Security Applications Conference (ACSAC)*, pages 315–324, Miami Beach, Florida, December 2007.
- [30] Kevin W. Hamlen and Bhavani Thuraisingham. Secure peer-to-peer networks for trusted collaboration, invited paper. In *Proceedings of the 2nd IEEE International Workshop on Trusted Collaboration (TrustCol)*, pages 58–63, White Plains, New York, November 2007.
- [31] Bhavani Thuraisingham and Kevin W. Hamlen. Secure semantic sensor web and pervasive computing. In *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC)*, pages 5–10, Newport Beach, California, June 2010.
- [32] Kevin W. Hamlen, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. Security issues for cloud computing. *International Journal of Information Security and Privacy (IJISP)*, 4(2):36–48, April–June 2010.
- [33] Arindam Khaled, Mohammad Farhan Husain, Latifur Khan, Kevin W. Hamlen, and Bhavani Thuraisingham. A token-based access control system for RDF data in the clouds. In *Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, pages 104–111, Indianapolis, Indiana, November/December 2010.
- [34] Bhavani Thuraisingham, Vaibhav Khadilkar, Jyothsna Rachapalli, Tyrone Cadenhead, Murat Kantarcioglu, Kevin Hamlen, Latifur Khan, and Farhan Husain. Towards the design and implementation of a cloud-centric assured information sharing system. Technical Report UTDCS-27-11, Computer Science Department, The University of Texas at Dallas, Richardson, Texas, September 2011.
- [35] William Hamlen and Kevin W. Hamlen. A closed system of production possibility and social welfare. *Computers in Higher Education Economics Review (CHEER)*, 18, December 2006.
- [36] Bill Hamlen and Kevin W. Hamlen. An interactive computer model of two-country trade. *Computers in Higher Education Economics Review (CHEER)*, 2011. forthcoming.
- [37] Ramiah Natarajan, Bhavani Thuraisingham, Balakrishnan Prabhakaran, Latifur Khan, and Kevin W. Hamlen. A database inference controller for 3D motion capture databases. *International Journal of Information Security and Privacy (IJISP)*, 2011. forthcoming.