Information Assurance and Computer Security at UB

Shambhu Upadhyaya (CSE) and Raghav Rao (MIS)

Advisory Board Meeting

May 8, 2008
Outline

- History
- Advisory Board
- IA Related Courses
- IA Certificate Program
- IASP Program Accomplishments
- SFS Program Accomplishments
- Research Accomplishments
- Publication Activities and Student Placement
- Other Creative and Collaborative Activities
- Path Forward
1. History

• CEISARE is a Multidisciplinary Center, certified by NSA in 2002 and re-designated in 2005 and 2008 by NSA and DHS
  – Computing, mathematical, legal and managerial
• Curriculum mapped to CNSS No. 4011 and CNSS No. 4013 (Committee on National Security Systems)
    • minimum course content for the training of INFOSEC professionals in telecommunications security and automated information systems (AIS) security (awareness level and performance level)
    • minimum standards for administrators of national security systems for administrators of unclassified systems
Prior NSA Site Visits

- **Site Visit 1 (March 6, 2003)**
  - Tim Mucklow and Cathey Fillare
  - CSE, CCR and SOM Lab tours
  - Lunch meeting at M&T Bank (hosted by John Walp)
  - Meeting with IASP scholars, faculty, Deans

- **Site Visit 2 (May 8, 2003)**
  - Robert McGraw and Tim Mucklow
  - Meeting with the PIs, visitor from AFRL (Kevin Kwiat)
  - Meeting with deans of SEAS, SOM and VP for Research
  - Research posters, CEDAR tour

- **Site Visit 3 (March 30, 2006)**
  - Robert McGraw and Lynn Hathaway
  - Half-Day meeting, research posters, meeting with Chairs
2. Center Advisory Board

• Board members
  – Mr. Kevin Comerford, Commissioner, Central Police Services, Erie County
  – Dr. Kevin Kwiat, Principal Computer Engineer, AFRL, Cyber Defense
  – Ms. Margaret Grayson, President, Coalescent Technologies
  – Mr. Charles Dunn, CIO, UB
  – Ms. Helene Kershner, Assistant Chair, CSE Dept., UB
  – Mr. John Reel, Senior Software Engineer, General Dynamics
  – Mr. Robert Vail, Manager, EDS Corporate Security Network Compliance Organization
  – Mr. John Walp, VP E-commerce security, M&T Bank
3. CEISARE Courses

• Courses with IA Content
  – CSE 565 Computer Security
  – CSE 566 Wireless Networks Security
  – CSE 512 Applied Crypto and Computer Security
  – LAW 629 Computers, Law, Technology and Society
  – LAW 645 Copyright
  – Law 956 E-Commerce Law
  – MGA 615 Fraud Examination
  – MGS 650 Information Assurance
  – MGS 651 Network Management
  – MGS 659 E-Commerce Security
  – MGT 681 Intellectual Property
  – MTH 529/530 Introduction to the Theory of Numbers I/II
  – MTH 535 Introduction to Cryptography
  – MTH 567 Stream Ciphers

• Other Courses Planned
  – Computer Forensics
4. Graduate Certificate in IA

- **Effort started with funds from DoD in fall 2003**
  - Funding was to create a new integrative course in IA
- **Two tracks – technical and managerial**
- **Requirements**
  - 6 credits of core courses in the track
  - 5-6 credits of elective in the dept.
  - 3 credits of required integrative course
- **Technical track**
  - Core – Intro. to Crypto, Computer security, Wireless networks security (choose two courses)
- **Managerial track**
  - Core – Network management, E-Commerce security
5. IASP Program Accomplishments

- **5 IASP scholarships from DoD since 2002**
  - Alex Eisen (Joined DISA, Sept. 2004)
    - MS Project: Development of a basic framework for emergency first responder systems
  - Melissa Thomas (Joined NAVAIR, Dec. 2004)
    - MS Project: Study of Copyright law and personal computer security
  - Daniel Britt (Joined NSA, Jan. 2006)
    - MS Project: Enhancing situational awareness through the classification of IDS alerts and the defragmentation of attack tracks using a host based sensor
  - Daniel Krawczyk (Joined SPAWAR, Jan. 2007)
    - MS Project: Study of IPSec
  - Richard Giomundo (Joined NSA, June 2006)
    - MS Project: A comprehensive fusion system for real-time awareness of multistage cyber-attacks
  - Chris Crawford (Will join DISA in June 2009)
Capacity Building Initiatives from DoD

• Capacity building grant 1 from DoD (2002)
  – Develop information security lab, develop an IA course
• Capacity building grant 2 from DoD (2004)
  – Develop Wireless security course, support research on intrusion detection and response
• Capacity building grant 3 from DoD (2007)
  – Vulnerability Aggregation and analysis
• Equipment grant from Cisco (2005)
  – Improve security labs
• A poster on security labs being displayed at today’s workshop
6. SFS Program Accomplishments

• Capacity building grant 1 from NSF (2004)
  – Develop wireless security lab, develop e-commerce security course
  – Jointly with GCC to promote faculty development at GCC
  – Both the lab and the courses have been completed and are being taught
  – Joint Cyber Security workshop on March 31, 2006
    • Co-hosted by ECC, FBI Cyber Task Force

• Capacity building grant 2 from NSF (2007)
  – To develop faculty development and technical expertise for faculty in computer forensics
  – Jointly with Hilbert College
  – Several faculty at UB, ECC, GCC, Hilbert College will undergo training
  – Joint Cyber Security workshop 2008 (today) is a direct outcome of this grant

• We believe that our program is now mature enough to receive the SFS Scholarship grant
7. Research Accomplishments

• **Research Areas**

• **Funding**
  – Over 3M from NSF, DARPA, NSA/ARDA, AFRL, DoD
  – Research, education, infrastructure
  – Couple of internal grants
    • HIPAA Compliant Medical Data Repository for Teaching
    • Analyzing Emergency Response Management Systems in the Context of Katrina and Rita Disasters – A first responder focus
Sample Research Projects (Sponsored)

• Protecting documents from malicious insiders (ARDA)
• Event correlation for cyber attack recognition (ARDA)
• Insider threat modeling and analysis in a corporate intranet or military environment (DARPA)
• Security and Incentives in emerging applications (NSF)
• A Framework for Trusted and Reliable Cyber Interactions (AFRL)
• Women and Cyber Security: Gendered Tasks and (In)equitable Outcomes (NSF)
• Citizen Centric Analysis of Anti/Counter-Terrorism e-Government Services (NSF)
Security-related Faculty

- **Shambhu Upadhyaya (CSE)**
  - Intrusion detection, insider threat modeling, alert correlation, wireless networks security, sensor networks security
- **Hung Ngo (CSE)**
  - Network security, insider threat analysis
- **Chunming Qiao (CSE)**
  - Network survivability
- **Sheng Zhong (CSE)**
  - Security and Incentive based protocols
- **Bharat Jayaraman (CSE)**
  - Language based security issues
- **Ramalingam Sridhar (CSE)**
  - Embedded systems security
- **Venu Govindaraju (CSE)**
  - Biometrics
- **H.R. Rao (MSS, also adjunct faculty in CSE)**
  - Secure e-commerce, web assurance
- **Raj Sharman (MSS)**
  - Database security, emergency response systems, sensor networks security
- **Tom Cusick (Math)**
  - Cryptography
- **Mark Bartholomew (Law)**
  - Intellectual property regime, copyright
8. Publications and Student Placement

• More than 60+ publications in key journals, conferences and workshops

• Some Key papers and Books
  – Towards a Theory of Insider Threat Assessment, IEEE DSN, June 2005
  – Secure Knowledge Management, Encyclopedia Article, IDEA Group, 2005
  – A Book on Managing Information Assurance in Financial Services

• Several Ph.D. Dissertations

• Students Placed at OSU, Cisco, Symantec, Microsoft, Qualcomm, M&T Bank
9. Collaborative Activities & Dissemination

- **Collaboration with ECC (2004 - 07)**
  - Developing an undergrad. Certificate program in IA at ECC
- **Collaboration with GCC (2004 - 07)**
  - Curriculum and faculty improvement at GCC
  - Add security content in their courses, faculty training in security
- **Collaboration with Town of Amherst**
  - Digital government project (2003-04)
- **Collaboration with M&T Bank**
  - Several MBA students working in the security area
- **Collaboration with local FBI branch**
  - Joint workshops, possible internships, computer forensics initiative
- **Collaboration with AFRL, CMIF**
- **High School Cyber Security Workshops**
Collaborative Activities with other CAEs

• Participation and conducting surveys at Cyber Corps 2005 (Syracuse University)
• Participation in Security Week, 2005, 2006 (Polytechnic University) – students won prizes
• Secure Knowledge Management Workshop 2004 at Buffalo, NY
  – 10 technical sessions
  – 3 keynote talks
  – 2 plenary sessions
  – 1 dinner banquet talk
  – 1 luncheon keynote
  – 1 high power panel on women and cyber security
  – 1 technical poster session
• Secure Knowledge Management Workshop 2006 at Brooklyn Polytechnic, NY
• Secure Knowledge Management Workshop 2008 at Dallas, TX
SKM 2008 Workshop

November 3 - 4, 2008
University of Texas at Dallas, Dallas, TX

Important Dates:
- Abstract submission: June 13, 2008
  Paper submission: July 11, 2008
  Author Notification: August 22, 2008
  Camera Ready Copy: Sep 22, 2008
  Workshop: November 3-4, 2008

http://cs.utdallas.edu/skm2008/index.htm
SKM 2008 Topics

- Secure Languages (Secure Knowledge Query Manipulation Language, Security Assertion Markup Language, B2B Circles of Trust)
- Return of Investment on Secure Knowledge Systems
- Digital Rights Management (Digital Policy Management)
- Secure Content Management (Secure Content Management in Authorized Domains, Secure Content Delivery, Content Trust Index)
- Security and Privacy in Knowledge Management
- Wireless security in the context of Knowledge Management
SKM 2008 Organizing Committee

• **Steering Committee**
  – Bhavani Thuraisingham - *University of Texas, Dallas*
  – Kevin Kwiat - *Air Force Research Lab*
  – Raghav Rao - *SUNY at Buffalo*
  – Shambhu Upadhyaya - *SUNY at Buffalo*

• **General Chair**
  – Bhavani Thuraisingham, The University of Texas at Dallas

• **Program Chair**
  – Murat Kantarcioglu, The University of Texas at Dallas

• **Publicity Chair**
  – Jaideep Vaidya, Rutgers University

• **Local Arrangements Chair**
  – Wei T. Yue, The University of Texas at Dallas
  – Jingguo Wang, The University of Texas at Arlington
Path Forward (Discussion Points)

- Alignment with UB 2020 Strategic Strength – ICT
- Forensics Initiative – collaboration with RCFL
- NSF Federal Cyber Service scholarships
- Teach security policies, business integrity
- Research on emergency management, first responder systems
List of Posters

- Activity Theory Guided Role Engineering, Manish Gupta, School of Management, University at Buffalo
- Adaptive Workflow Framework for Effective Emergency Response in Hospitals, Sumant Dutta, Ashwin Kumar Narayanan, School of Management, University at Buffalo
- An Investigation of Factors Affecting Effective Emergency Management during the 2006 October Snow Storm in Buffalo, Minkyun Alex Kim, School of Management, University at Buffalo
- Cyber Security Laboratory Development at UB, Vishal Padhye, School of Management, University at Buffalo
- Detecting Privilege Abuse by Malicious Insiders, Sunu Mathew, Department of Computer Science and Engineering, University at Buffalo
- Digital Forensics Initiative at UB, Rajarshi Chakraborty, Venkatasairam Yanamandram, Department of Computer Science and Engineering, University at Buffalo
- Managing Private Information Safety in Blogs, Sangmi Chai, School of Management, University at Buffalo
- Perceived Risk, Resilience, and Hospital Information Infrastructure Effectiveness in the Context of Disasters, Insu Park, School of Management, University at Buffalo
- Phoney: Mimicking User Response to Detect Phishing Attacks, Madhusudhan Chandrasekaran, Dept. of Computer Science and Engineering, University at Buffalo
- Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations, Tejaswini Herath, School of Management, University at Buffalo
- Secure and Robust Localization in Sensor Networks, Murtuza Jadliwala, Dept. of Computer Science and Engineering, University at Buffalo
- SpyCon: Emulating User Activities to Detect Evasive Spyware, M. Chandrasekaran and S. Vidyaraman, Department of Computer Science and Engineering, University at Buffalo
- Trust Utilization for Routing Robustness in Wireless Mesh Networks, Aniket Patankar, Shrey Ajmera and Mohit Virendra, Department of Computer Science and Engineering, University at Buffalo