



*A partnership between industry, academia, and government  
Working today to solve tomorrow's security problems*

### Overview of Stony Brook Site

<http://cip.cs.stonybrook.edu/>

R. Sekar

### Overview of Presentation

- ◆ Overview of I/UCRC program
- ◆ CIP Goals and Benefits
- ◆ Center organization and operation
- ◆ Institutional and Faculty strengths
- ◆ Goals for today

### I/UCRC Model

- ◆ **A long track-record (over 25 years) of highly successful industry-university partnerships**
  - About 80 centers established in diverse areas of engineering
  - 100 university and 700 industry members, including many of the country's biggest corporations.
  - Average industry investment per center is \$1M to \$2M per year
- ◆ **Established blueprint for successful management**
  - Organizational structures
  - Procedures, policies and practices well-accepted by participants
    - ▼ Funding
    - ▼ Project selection
    - ▼ Progress monitoring,
    - ▼ Intellectual property rights

### CIP Goals and Benefits

### Center for Information Protection

- ◆ **Goals**
  - pursue scientifically important and industry-relevant research in all aspects of cyber security and privacy
  - accelerate and promote the transfer of knowledge and technology to industry
- ◆ **Vision**

*To become a world-leader in cyber security, and the preeminent forum to address scientific and technological challenges faced by the industry in their quest to support an increasingly network- and information-centric society*
- ◆ **The only NSF I/U CRC with cyber security focus**

### The Benefits

- ◆ **Leverage**
  - Typical membership buys access to research program 20x larger
    - ▼ Pooling funds from multiple companies
    - ▼ Additional funds from NSF IUCRC, University and other sources
  - Additional leveraging: CIP faculty's research funded outside CIP
    - ▼ Currently about \$2M per year in federal grants
  - Can invest in larger/longer-term research that can't be pursued by any single member
- ◆ **Access**
  - Early access to **all** research results of the Center and its faculty
    - ▼ Includes most results of CIP faculty's sponsored research outside CIP
  - Access to world-class faculty, and highly skilled graduate students
- ◆ **Input**
  - Set the research agenda of the center
  - Share ideas and get feedback from faculty and students

### ***CIP: An Upcoming Multi-University I/UCRC***

- ◆ **The Center at Iowa State is already operational**
  - First IAB meeting to select projects took place last fall
  - Current members:
 

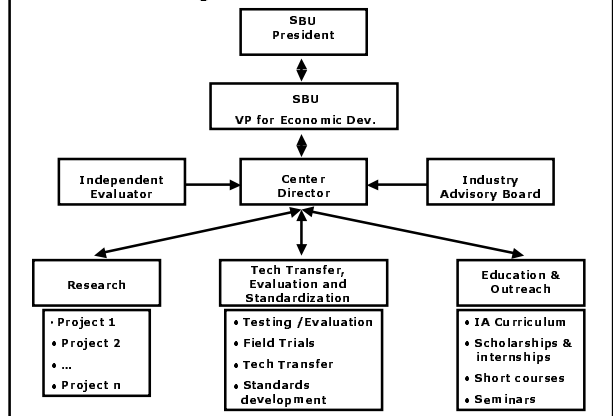
➢ Boeing	➢ Network Security Solutions
➢ Principal Financial	➢ Xandros
➢ Rockwell Collins	➢ Tech Logistics
➢ Cargill	➢ XPRT Solutions Inc
➢ John Deere	➢ StarBank
➢ Palisade Systems	
  - Currently 7 projects funded at ISU
    - ▼ New projects decided in 2005 October meeting, started in January
    - ▼ Progress reports in 2006 May meeting
- ◆ **Other sites to be added**
  - Stony Brook, NJIT, NCSU, ...

### ***Ongoing CIP Projects***

- ◆ **Began in Jan 2006 at Iowa State**
- ◆ **7 projects funded by the IAB**
  - Hybrid approaches for Intrusion Detection
  - Learning-based techniques for Egress Filtering
  - DDoS Detection and Avoidance
  - Detecting Stealth/Reconnaissance network attacks
  - Alert Correlation for Snort IDS
  - Malware detection
  - Secure and dependable communication in MANETs
- ◆ **Results from one Center site are available to members that join through an other site**

### ***Center Organization and Operation***

### ***Organization of SBU Site***



### ***Fee Structure***

- ◆ **Regular Member: \$30K**
- ◆ **Small Business: \$10K**
- ◆ **One vote per \$1K**
- ◆ **Government agencies can join CIP**

### ***Membership Agreement***

- ◆ **Membership is typically for 2 years**
  - But companies can cancel any time with 90 day notice
- ◆ **Publication delay on request by a member**
- ◆ **IP (Patents/software) owned by university, but *all members have royalty-free, non-exclusive access***
- ◆ **Other by-laws decided by the IAB**
- ◆ **Membership and Letter of Intent templates are in your folders**

### ***Project Selection and Evaluation***

- ◆ **Projects selected during annual IAB meetings**
  - Faculty develop new projects in consultation with members and present them at the IAB meeting
  - IAB votes on which projects to fund
- ◆ **Typical projects are 1 year, 1 grad student**
  - Multi-year projects divided into 1 year chunks
- ◆ **Projects are evaluated semi-annually at the IAB meetings, based on faculty presentations**
- ◆ **An independent evaluator complements IAB evaluation on a project-by-project basis**
  - Evaluates usefulness of faculty-industry interactions
  - Assessment of research quality is up to the members

### ***Institutional and Faculty Strengths***

### ***Stony Brook University***

- ◆ **Established in 1957**
- ◆ **22K students, including 6K grad students**
- ◆ **Over 1600 faculty**
- ◆ **Rated by some measures as one of top three public schools in U.S. (JHU Press)**
- ◆ **Type I research university**
- ◆ **Recent annual research expenditure over \$160M**

### ***CS @ Stony Brook***

- ◆ **People**
  - 40+ faculty, 100+PhD and 175+ M.S. students
- ◆ **Ranking**
  - 15<sup>th</sup> in US in undergrad CS education [Gourman Report]
    - ▼ 2<sup>nd</sup> in New York state
  - 17<sup>th</sup> in US in Research [Graham-Diamond Report, 2004]
- ◆ **NSA-designated Center of Excellence in Information Assurance Education**
- ◆ **CEWIT (Center for Wireless and Information Technology)**
  - Funded by \$50M NY funds, plus significant industry support
  - A state-of-the-art 100K sqft building being constructed
- ◆ **Sensor CAT (funded by NYSTAR)**

### ***CIP People***

- ◆ **7 core faculty**
  - Tzi-cker Chiueh, Rob Johnson, C.R. Ramakrishnan, R. Sekar, Radu Sion, Scott Stoller, Erez Zadok
- ◆ **Additional faculty with relevant skills**
  - Wireless and networking (5)
    - ▼ Samir Das, Jie Gao, Himanshu Gupta, Alex Mohr, Jennifer Wong
  - Software and system assurance (3)
    - ▼ Radu Grosu, Annie Liu, Scott Smolka
  - Intelligent information systems (3)
    - ▼ Michael Kifer, I.V. Ramakrishnan, David Warren
  - Most of these faculty will participate in CIP when in matures
- ◆ **Graduate Students**
  - 20+ Ph.D. students
  - 20+ M.S. students

### ***CIP Facilities and Equipment***

- ◆ **Large research testbed (CEWIT)**
  - \$1.6M equipment acquired for security, storage, networking, wireless and visualization research
  - Clusters together have
    - ▼ ~600 CPUs over ~300 nodes
    - ▼ ~1TB main memory
    - ▼ ~150TB disk storage
- ◆ **Currently, over 6000 sqft of lab space**
  - Experimental Computer Systems
  - File systems and Storage Laboratory
  - Secure Systems Laboratory
  - Applied Logic Laboratory
  - Design and Analysis Research Laboratory
  - ...
- ◆ **A lot more room for growth in CEWIT building**

### Current Funding for CIP Faculty

- ◆ **Over \$10M current federal research grants**
  - 5 NSF CAREER, 1 ONR Young Investigator, 1 IBM faculty award
  - DoD Critical Infrastructure Protection and IA Fellowship award (1 of 12 in US, 1 of 2 in NY)
  - DoD Critical Infrastructure Protection/High Confidence Software award (1 of 20 in US, 1 of 2 in NY)
  - Several NSF ITR and many Cyber Trust awards
  - \$2.5M NSF award to support Scholarships for students specializing in IA (only new award in 2004)
- Significant experience in working with industry
  - Industry-funded projects
  - Collaborative projects with industry (federally funded)

19

### Recent Security Publications

- ◆ **One of the most visible groups in the nation in top systems/security conferences**
- ◆ **20+ pubs/year in highly competitive forums**
  - Representative publications:
    - ▼2006: IEEE S&P, USENIX Security, OSDI (2), FC, CSFW, ICDCS, DSN, ...
    - ▼2005: NDSS (2), USENIX Security (2), USENIX Technical, ACM CCS, ACSAC (2, incl. best paper), FAST, RAID, DSN, IKDE, ...
    - ▼2004: USENIX Security (2), VLDB, ICDE, TKDE, PLDI, FSE, TOPLAS, ACSAC (3), FAST, RAID, DSN, ...
    - ▼2003: SOSP, ACSAC (best paper), USENIX Technical (2), USENIX Security, ICDCS (3), DSN(2), RAID, ...
  - ▼Acceptance rates between 12% and 25%, avg ~16%
- ◆ **Total refereed publications typically exceed 30/yr**

20

### Technical Areas of Expertise

- Software security
  - Compilers
  - Operating systems
  - Verification/assurance
- Hardware security
  - Hardware support for security
  - Trustworthy hardware
- Data security
  - Storage/file security
  - Database security
  - IP Protection
- Network security
  - Wireless security
  - Applied Cryptography
- Distributed systems security
  - Trust management
  - Vulnerability analysis
  - Privacy preservation
- Security policies
  - Frameworks
  - Monitoring and compliance
  - Intrusion detection

### Cyber Security Problems Targeted

- Attacks/Intrusions
  - Detection/prevention
    - Policy based
    - Anomaly based
  - Recovery
  - Automated signature generation
- Malware/mobile code
  - Containment
  - Analysis
- Watermarking
- Vulnerability detection
  - Source-code analysis
  - Model-based analysis
- Design for security
  - Operating system
  - File system
  - Applications
- Privacy preservation
- Policy analysis and validation

### Leveraging membership fees at SBU...

- ◆ **Your membership dollars go farther**

Industry contribution	\$1000
NSF IUCRC	\$250
University match	\$250 -- \$330
NYSTAR match	\$200 -- \$330
Total CIP funds	\$1700 -- 1910

- \$1000 contribution controls investment of almost \$2000 in Center research

▼ Higher end of estimates based on obtaining matching support from NY State sources, and total memberships of about \$250 to 300K

- ◆ **Additional 5x to 10x leveraging through pooling of resources from multiple members**

### Interested Companies (SBU Site)

- Admit Computer Svcs
- AFCO Systems
- AppliedE Inc.
- ATC-NY
- BBN
- Cablevision
- Computer Associates
- Citigroup
- Goldman-Sachs
- Google
- Global Infotek
- Intel
- IBM
- HP
- LISTNet
- Northrup Grumman
- Oracle
- Renaissance Technologies
- Rether Networks
- Secure Software
- Softeon
- SVAM International
- Symantec
- Telcordia Technologies
- Verizon
- XSB Inc.

### **Goals for Today**

- ◆ **Provide overview of faculty research**
  - Poster session provides a broad sampling
  - Faculty presentations focus on a specific project, similar to those that would be offered when the CIP is in operation
- ◆ **Each project proposed by faculty will be discussed in the afternoon session**
  - Industry provides feedback using LIFE (level-of interest evaluation) forms
  - Goal: understand the specific needs and concerns of potential members, so that appropriate projects could be proposed in the future
- ◆ **Please don't forget to turn in your LIFE forms before you leave!**

### **Faculty Contact Information**

- ◆ **Tzi-cker Chiueh** ([chiueh@cs.stonybrook.edu](mailto:chiueh@cs.stonybrook.edu))
  - Compiler transformations, attack recovery
- ◆ **Rob Johnson** ([rtjohnso@cs.stonybrook.edu](mailto:rtjohnso@cs.stonybrook.edu))
  - Program analysis, cryptography
- ◆ **C.R. Ramakrishnan** ([cram@cs.stonybrook.edu](mailto:cram@cs.stonybrook.edu))
  - Formal methods, vulnerability analysis
- ◆ **R. Sekar** ([sekar@cs.stonybrook.edu](mailto:sekar@cs.stonybrook.edu))
  - Program analysis/transformation, policy enforcement, attack detection and recovery
- ◆ **Radu Sion** ([sion@cs.stonybrook.edu](mailto:sion@cs.stonybrook.edu))
  - Database security, Privacy, Watermarking, Cryptography
- ◆ **Scott Stoller** ([stoller@cs.stonybrook.edu](mailto:stoller@cs.stonybrook.edu))
  - Trust management, vulnerability analysis, program analysis
- ◆ **Erez Zadok** ([ezk@cs.stonybrook.edu](mailto:ezk@cs.stonybrook.edu))
  - File system and storage security

26