IT R&D Program

PITAC Briefing

Feb. 25, 2000

R.J. (Jerry) Linn

Jerry.Linn@nist.gov

FY 2001 New Thrusts

HCSS/CIP

Computer Security & Information Infrastructure Protection

+ Advanced Encryption Standard
+ Security Management
+ Best Practices

LSN/SII

Modeling, Simulation, Analysis, Test Methods & Standards for Broadband Wireless Protocols & Access Technologies

+ Bluetooth (picocell) and
+ Local, Multipoint Distribution Services (LMDS)
+ CDMA-2000, W-CDMA.

FY 2001 Budget
New Thrusts

PCA	FY1999 Actual	FY2000 Enacted	FY2001 Request	Change +/-
HCI & IM	1.8	6.2	6.2	
LSN	5.2	5.2	4.2	-1.0
HECC R&D				
HECC Apps & Infrastructure	3.5	3.5	3.5	
SDP			2.0	2.0
HCSS/CIP	2.5	3.5	8.5	5.0
SEW & Workforce Dev.				
Total	13.0	18.4	24.4	6.0

Notes:

+1.0M	LSN/SSI/ Wireless
-2.0M	LSN/NGI/Manufacturing Applications
+2.0M	SDP/Manufacturing
+5.0M	HCSS/Critical Infrastructure Protection

Broadband Wireless Protocols and Access Technologies
LSN/SSI

Goal

Foster the development of industry consensus standards for broadband wireless communications systems by providing reliable measurements and data through Testbeds

Technical Areas

Modeling, simulation, and design analysis before standards; develop standards & test methodologies:

- 3rd Generation mobile wireless, coding and modulation: CDMA 2000, W-CDMA
- Pico-cellular Wireless Access Systems: Bluetooth
- Two-way point-to-multipoint digital wireless systems: Local Multi-point Distribution Services (LMDS)

Impacts

- Improve quality of standards and drive down costs
- Enhance competition in telecommunications market
- Open the market to smaller companies
- Strengthen U.S. in international standards competition
- Provide Industry with access to test methods and testbeds

Collaborators

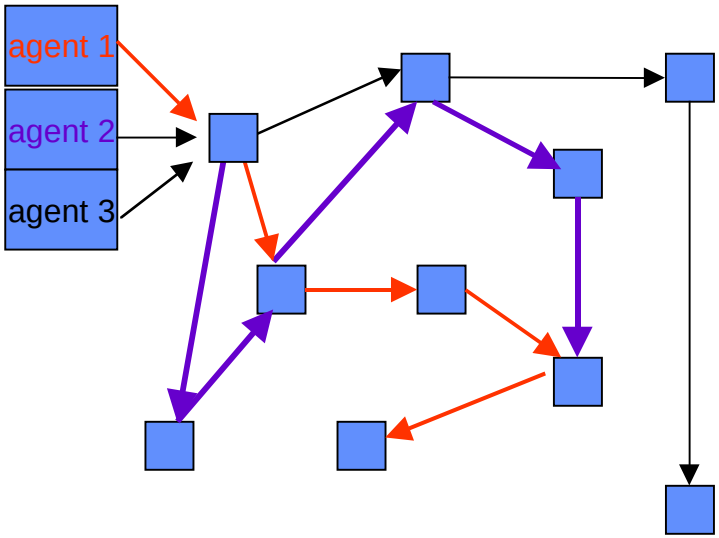
Federal: DARPA, NTIA / Institute for Telecomm Sciences

Industry: Institute of Electrical and Electronics Engineers (IEEE),
Bluetooth Consortium, Telcom Industry Association, Intl. Standards Bodies (e.g., T1, 3GPP, and ITU)

Milestones

- Develop Physical layer model under in C/C++
- Modeling and analysis of link layer protocol w/ Promela/SPIND
- Develop new algorithms & protocols for 3G and 4G systems
- Develop interference models; conduct analysis and empirical studies; analysis reported to standards bodies and industry.
- Build testbeds, initiate data collection;
- Test methods, and access to testbeds opened to industry w/ test suites and tools placed in public domain.
- Evaluate IETF and DARPA GloMo MANET Routing Protocols
- Evaluate MANETs for national security / emergency preparedness applications
- Industry consensus standards adopted internationally

Active Network Security
HCSS/CIP



Goal

Develop security services applicable to active and "intelligent" networks, and security architecture for active networks

Technical Areas of Focus

- Define significant security impediments to the utilization of active networks in commercial applications
- Protect mobile code from the host as well as protect the host from the mobile code.

Expected Impacts

- Improved E-commerce capabilities
- Improved Intelligent Network capabilities for the telecommunications industry

Potential Customers and Collaborators

Industry: Telcordia, NTA, Bell Atlantic, US West Intelligent Network Forum, Boeing, IBM, ATIS

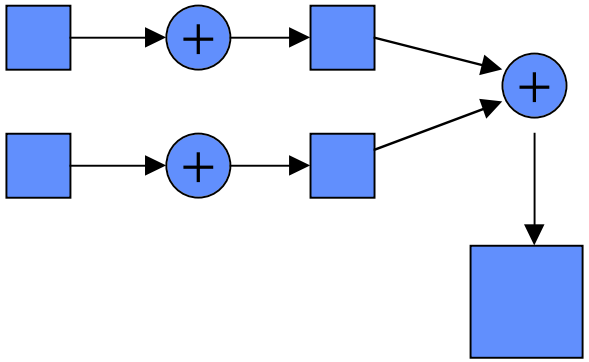
Academic: UMBC, UMich, Purdue University

Federal: National Communications System, NSA, DARPA, InfoSec Research Council,

Milestones

- Proof-of-concept implementation of new security mechanisms for active networks
- Improved mobile agent technology for implementing active network security features
- Development of agent-based virtual private network
- Proof-of-concept implementation of secure architecture for maintaining active networks
- Acceptance of solutions in the e-commerce and telecommunications industries.

Advanced Security Modeling and Simulation
HCSS/CIP



Security of any object is determined by composing more primitive objects.

Goals

Define the primitive security measurement characteristics that will enable security modeling and simulation

Technical Areas of Focus

- Develop methods to measure the security features of fundamental, or primitive, objects.
- Develop methods to compose these measurements into a viable model

Expected Impacts

- Measurement of security features
- Ability to analyze the security features of composed systems
- Ability to compose models of security relevant systems and subsequently simulate their behavior

Potential Customers and Collaborators

Industry: CISCO, Lucent, ATT, Worldcom, Telcordia, Sprint

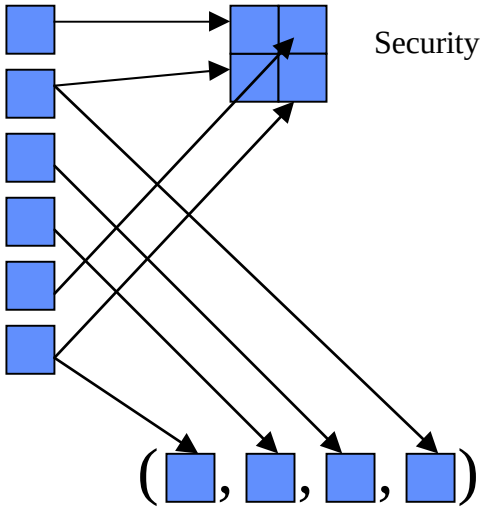
Academic: University of Tulsa, Georgia Tech, University of Illinois

Federal: OSTP, NSA, DARPA, FBI, National Simulation Center, Defense Modeling and Simulation Office

Milestones

- Definition of security features required in a primitive object.
- Development of a specification language to describe these primitive security features
- Development of a modeling architecture that allows these primitive objects to be combined
- Development of a simulation architecture that predicts the behavior of these composed objects.

Security Engineering and Best Practice Guidelines
HCSS/CIP



Goals

Develop guidelines for the security engineering community that enable secure system solutions, and guidelines for industry and government defining security best practices and implementation

Technical Areas of Focus

- Identify security engineering problems and develop applicable solutions
- Define specifications, APIs, and middleware, that facilitate the security engineering function
- Identify and document best security practices for specific architectures and functions.

Expected Impacts

- Improved security engineering capability
- Improved security posture by industry and government

Potential Customers and Collaborators

Industry: Oracle, CISCO, HP, Lucent, Microsoft, SAIC, CSC, Cygnacom, Arca, IBM, EDS, VISA

Federal: NSA, DoS, FISSEA, Federal Computer Security Manager's Forum, HHS, DoJ, CIO Council.

Milestones

- Development of "best practice" guidance documents for systems administrators, users, gateway administrators, and other appropriate functions
- Acceptance of best practice guidance as the standard practice for government systems
- Development of security engineering practices, APIs, and specifications.
- Adaptation of security engineering practices, APIs and specifications by industry partners.
- Acceptance of security engineering practices, APIs, and specifications as standards