Hard Problems in Information Security

IRC Hard Problems Group

David B. Nelson, Ph.D., CISSP
Director
National Coordination Office for
Information Technology Research and Development

March 17, 2004

What is the Federal Networking and Information Technology Research and Development Program (NITRD)?

- Coordinates and focuses interagency IT R&D:
  - Identify common research needs
  - Plan interagency research programs
  - Coordinate research announcements and funding
  - Review research results and adjust accordingly
- Evolved from the Federal High Performance Computing and Communications Initiative (HPCC), Computing Information and Communications Program (CIC), and Next Generation Internet Program (NGI)
- Includes 14 Federal agencies, about $2B budget
- Cybersecurity will be cross-cutting special topic this year
- www.nitrd.gov

NITRD Program Coordination

WHITE HOUSE

Executive Office of the President
Office of Science and Technology Policy

National Science and Technology Council

President's Information Technology Advisory Committee (PITAC)

U.S. Congress

NITRD Authorization and Appropriations Legislation

National Coordination Office (NCO) for Information Technology Research and Development

Interagency Working Group (IWG) on Information Technology R&D

Participating Agencies: AHRQ, DARPA, DOE/NNSA, DOE/SC, EPA, NASA, NIH, NIST, NOAA, NSA, NSF, ODDR&E

- **High End Computing Coordinating Group (HEC)**
- **Large Scale Networking Coordinating Group (LSN)**
- **High Confidence Software and Systems Coordinating Group (HCSS)**
- **Human Computer Interaction & Information Management Coordinating Group (HCI & IM)**
- **Software Design and Productivity Coordinating Group (SDP)**
- **Social, Economic and Workforce Implications of IT and IT Workforce Development Coordinating Group (SEW)**

Participating Agencies and Departments

- Department of Defense (DoD)
  - Defense Advanced Research Projects Agency (DARPA)
  - Defense Information Systems Agency (DISA)
  - National Security Agency (NSA)
  - Office of the Director of Defense Research and Engineering (ODDR&E)
- Department of Energy
  - Office of Science (DOE/SC)
  - National Nuclear Security Administration (NOE/NNSA)
- Department of Health and Human Services
  - National Institutes of Health
  - Agency for Health Research and Quality (AHRQ)
- Department of Commerce
  - National Institute of Standards and Technology (NIST)
  - National Oceanic and Atmospheric Administration (NASA)
- National Science Foundation
- National Aeronautics and Space Aministration
- Environmental Protection Agency (EPA)
- Observer: Federal Aviation Administration (FAA)

Role of President's Information Technology Advisory Committee (PITAC)

- PITAC reports to President through OSTP
- PITAC has begun study of Federal cybersecurity research
  - First public meeting on this topic scheduled for April 13 in Washington, DC
  - Likely will recommend changes in both incremental and fundamental research
  - Further information available at http://www.nitrd.gov/pitac/ over next few weeks
  - Public comments will be welcome at pitac-comments@nitrd.gov

Security Concerns Are Evolving

- Classic security concerns dealt more with data
  - Confidentiality (Data only available to those authorized)
  - Availability (Data is available when you want it)
  - Integrity (Data hasn't been changed)
- Newer concerns deal more with people, transactions and functions
  - Trust (Who you are and what you are authorized to do; either as person or system)
  - Non-repudiation (You can't deny doing something you did)
  - Auditability (I can check what you or the system did)
  - Reliability and predictability (The system does what what it should do)
  - Privacy (Within certain limits no one should know who I am or what I do)
- Some solutions in stand-alone mainframe environment are less effective in networked environment

Security Challenges of Future Computing Environment

- How to accommodate vision of distributed large-scale collaborations, access to resources, eCommerce, without compromising security?
- How to accommodate dynamic computing environment within current framework of security risk management?
- How to evolve security practices and technologies to keep up with future computing environment?
- How to build security into architecture of future environment, including ability to withstand, identify, and respond to attacks while carrying on critical functions?
- How to say “yes” rather than “no” to users and developers without compromising security?

What's the Problem?

- Current computing environment was not designed to be secure, e.g.
  - C language lacks intrinsic bounds checking
  - IP lacks source address verification
  - Border Gateway Protocol highly vulnerable to attacks
  - Operating systems shipped with wide-open services
- The result is "coping" behavior to deal with intrinsically insecure environment
  - Constant discovery of new vulnerabilities (mostly network exploitable)
  - Scramble to release and install patches and updates
  - Crackers reverse engineer patches to develop viruses, worms, trojans, etc.
  - Economic loss, embarrassment, denial of service, waste of resources
  - Time window between discovery of vulnerability and launch of attack is shrinking
  - Companies shift risk to customers, e.g. recent Verizon news

How can InfoSec research help?

- Research can identify incremental improvements
  - Coping with intrinsically insecure environment
- Research can identify fundamental improvements
  - Creating intrinsically secure environment
  - Modifying current networked computing environment to improve security and reliability
- Researchers must pay attention to issues associated with implementation
  - Impact on existing systems and services
  - Incentives to deploy – ROI
  - Backwards compatibility

We are not idea limited: Examples

- Concepts of controlled composability
  - Build up trustworthy systems from secure atoms
  - Both data and function tightly controlled, e.g. using analogy with objects
  - Provable security may not be possible, but probable security may be adequate
- Concepts for improved network protocols
- New classes of SCADA systems with goal of intrinsic security
- Languages and tools to assure “probable” security
- Basic theories for dealing with security, reliability, and trust
  - Old example: reliable system from unreliable components (Von Neumann, Moore-Shannon, others)

NITRD National Priorities, Grand Challenges and IT Hard Problems

http://www.itrd.gov/pubs/200311_grand_challenges.pdf

- National priorities reflect our country's broad-based values and goals:

  Leadership in Science and Technology
  National and Homeland Security
  Health and Environment
  Economic Prosperity
  A Well-Educated Populace
  A Vibrant Civil Society

- Grand Challenges are long-term science, engineering, or societal advances, whose realization requires innovative breakthroughs in IT R&D, and which will help address our country's priorities. Partial list includes

  High Confidence Infrastructure Control Systems
  Improved Patient Safety and Health Quality
  Predicting Pathways and Health Effects of Pollutants
  Real-Time Detection, Assessment, and Response to Natural or Man-Made Threats
  Safer, More Secure, More Efficient, Higher-Capacity Multi-Modal Transportation System
  Anticipate Consequences of Universal Participation in a Digital Society
  Collaborative Intelligence: Integrating Humans with Intelligent Technologies
  Generating Insights From Information at Your Fingertips
  Managing Knowledge-Intensive Organizations in Dynamic Environments

The 14 IT Hard Problem Areas

- ITHP Areas are broad categories of topics of interest to the IT R&D community and reflect the breadth of the NITRD Program
- Advances in the ITHP Areas must be achieved in order to solve these GCs:

♦Algorithms and Applications*

♦Complex Heterogeneous Systems*

♦Hardware Technologies

♦High Confidence IT*

♦High-End Computing Systems

♦Human Augmentation IT*

♦Information Management*

♦Intelligent Systems*

♦IT Systems Design*

♦IT Usability

♦IT Workforce

♦Management of IT*

♦Networks*

♦Software Technologies*

*Considered relevant to InfoSec hard problems

Similarities Between the NITRD IT Hard Problem Areas and the IRC IT Hard Problems

	NITRD IT HARD PROBLEM AREAS														
IRC IT Hard Problems	Algorithms and Applications	Complex Heterogeneous Systems	Hardware Technologies	High Confidence IT	High-End Computing Systems	Human Augmentation IT	Information Management	Intelligent Systems	IT System Design	IT Usability	IT Workforce	Management of IT	Networks	Software Technologies	
1) Truly Trustworthy Computer Base		■							■						
2) Understandable Models and Interfaces for Security		■		■					■						
3) Global Scale Identification, Authentication, Authorization, and Identity Management							■		■						
4) Methods for Detecting Covert Information Flows				■			■		■						
5) Security **with** Privacy		■							■						
6) Understanding Economics of IT Security							■					■			
7) Crypto for the Post-Quantum World	■			■					■						
8) Survivability		■							■						
8.1) Availability							■		■						
9) Zero Day Attacks				■					■						
10) Embed Strong Security Into Mobile, Embedded, and Distributed Computing				■					■						
11) Techniques and Tools for Building Large Scale Secure Systems				■					■					■	
12) Develop Automated Techniques and Tools for Verifying and Validating Security of Life Critical Systems Against Intelligent Malicious Threats									■			■		■	
13) Attribution							■		■						
14) Forensics				■				■	■						
15) Data Pedigree							■		■						

A Closer Look at the NITRD Security-Related IT Hard Problem Areas

- Algorithms and Applications
  - Modeling and simulation for threat assessment, location, and response
  - Model digital societies and transformations
  - Model interactions between humans and intelligent technologies
- Complex Heterogeneous Systems
  - Understand and balance simultaneous conflicting interacting requirements:
    - Tolerate failures (known as fault-tolerance)
    - Recover within time constraints
    - Maintain security while recovering from failures
  - ***Understand and control emergent (hard-to-predict) behavior in SCADA systems. (Local interactions can lead to global-scale instability)***
- Complex Heterogeneous Systems, cont.
  - Heterogeneous sensors, networks, and computing systems
  - Distributed control of networks of autonomous and semi-autonomous robotic responders
- High Confidence IT
  - Security and reliability
  - Trust tools embedded in applications
  - Policy-enabled infrastructures (for example, protocols, policies, and the embedding of scheduling in knowledge environments)
  - Integrate security (authentication, access control, intrusion detection) into networked embedded systems where it has never existed
  - Establish a new paradigm of operating at acceptable levels through attacks. Shutting down to thwart attacks is not an option.

A Closer Look at the NITRD Security-Related IT Hard Problem Areas Continued

- High Confidence IT Continued
  - ***Security and privacy for health information including authorization, authentication, biometrics, certification, encryption, and interfaces***
  - Models that run for long periods of time on computers that do not crash
  - Privacy and trust
  - Scalability
  - Confidentiality of proprietary information
  - Intelligence agencies need data and information to be stored in a secure fashion, retrieved in a timely manner, and transported safely and correctly.
- Human Augmentation IT
  - Presence and awareness tools embedded in applications used in remote collaboration such as tele-operation
  - Collaboration and visualization technologies for responders
  - Augment human cognition and augment reality with input from agents, robots, and sensors
- Information Management
  - Data mining of transportation system information for increased safety and security
  - ***Access to and data warehousing, data mining, and knowledge management of multi-decade multi-disciplinary data sets***
  - Asynchronous collecting and processing of large numbers of independent data streams
  - Knowledge management for distributed intelligence

A Closer Look at the NITRD Security-Related IT Hard Problem Areas Continued

- Intelligent Systems
  - Knowledge discovery in massive databases of archived knowledge
  - Automated ways of diagnosing and organizing data
  - Assess data across multiple disciplines
  - Generate and represent new knowledge to be shared and integrated across disciplines
  - Reasoning, cooperating robotic responders
  - Cognitive systems aware of context and human affects
- IT System Design
  - Interoperability across diverse communities and diverse platforms
  - Interoperability of health information systems within hospitals, across providers, and among other stakeholders such as insurance companies, accreditation committees, and governments
  - Maintain system stability and predictability when everything is in flux
  - Self-organizing architectures
  - Maintain system stability and predictability when everything is in flux

A Closer Look at the NITRD Security-Related IT Hard Problem Areas Continued

- Management of IT
  - Sequester data in the general models from proprietary data that belong to different companies
  - Available, reliable, safe, secure air traffic, highway, railway, and shipping systems
  - Smart cards to authorize and authenticate transportations system personnel
  - Certification of systems and procedures
  - Preservation of metadata
- Networks
  - ***Reliable, secure networks with differentiated services***
  - Survivable networks
  - Sensor networks and faster, smaller, light-weight sensor networks
  - Deploy, manage, and monitor large-scale dynamically reconfigurable networks of heterogeneous detectors
  - Fault-tolerant sensors and robots, enabling systems to survive and recover

A Closer Look at the NITRD Security-Related IT Hard Problem Areas Continued

- Software Technologies
  - ***Software reliability, performance, and quality assurance***
  - Health information software requirements, engineering, and development
  - Software for developing and operating integrated transportation systems
  - ***New programming methods that let programmers design for properties such as privacy***

For Further Information

Please contact us at:

nco@nitrd.gov

Or visit us on the Web:

www.nitrd.gov