OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Research Priorities: Tailored Spaces, Moving Target, Cyber Economics

ODNI/AT&F

LEADING INTELLIGENCE INTEGRATION

Pat Muoio, patricia.a.muoio@dni.gov

Briefing to NIST ISPAB

November 3, 2010

Coordinated Effort on Game-Changers

- It's about trustworthiness of digital infrastructure
  - Security, reliability, resiliency, privacy, usability
  - How can we:
    - Enable risk-aware safe operations in compromised environments
    - Minimize critical system risk while increasing adversaries' costs and exposure
    - Support informed trust decisions, necessitating flexible security strategies, and allowing for effective risk/benefit analyses and implementations
- Strong commitment to focus on game-changing technologies for coordinated cybersecurity R&D agenda

Three Themes

- Tailored trustworthy spaces
  - Supporting context specific trust decisions
- Moving target
  - Providing resilience through agility
- Cyber economics
  - Providing incentives to good security

Remember: These are just starting points.

Tailored Trustworthy Spaces

In the physical world, we operate in many spaces with many characteristics

- Home, school, workplace, shopping mall, doctor’s office, bank, theatre
- Different behaviors and controls are appropriate in different spaces

Yet we tend to treat the cyber world as a homogenous, undifferentiated space.

New Paradigm

- Users can select different environments for different activities (e.g., online banking, commerce, healthcare, personal communications) providing operating capabilities across many dimensions, including confidentiality, anonymity, data and system integrity, provenance, availability, performance

- Users can negotiate with others to create new environments with mutually agreed characteristics and lifetimes

Challenge: Identifying requirements of a particular tailored trustworthy space

- Degree of identification / authentication
- Information flow rules
- Strength of separation mechanisms
- Degree of monitoring / violation detection

Challenge: Policy Specification and Management

- Convenient specification of a tailored space
- Convenient mechanisms to know it
- Convenient mechanisms to change it

- Challenge: Validation of platform integrity
- Challenge: Violation detection
- Challenge: Verifiable separation of spaces
- . . . and many more

What’s New?

Nothing. Few of these individual problems or component technologies are novel

Everything. A structure that puts the pieces together to provide integrated, usable support for diverse trust environments would change the game.

Which technology areas matter?

- Identity management
- Component assurance
- Composition methods and logics
- Trust negotiation and management
- ...

Moving Target

- Controlled change across multiple system dimensions to:
  - Increase uncertainty and apparent complexity for attackers, reduce their windows of opportunity, and increase their costs in time and effort
  - Increase resiliency and fault tolerance within a system

New Paradigm

- All systems are compromised; perfect security is unattainable
- Objective is to continue safe operation in a compromised environment, to have systems that are defensible, rather than perfectly secure
- Cybersecurity is an adversarial science

Challenge: Managing Moving Target Systems

- Moving target systems should confound the adversary, not the user
  - Need system management and configuration capabilities that can support correct use of highly complex systems
  - Need cognitive interfaces to moving target systems
- Deployment of moving target mechanisms requires complex cost/benefit analysis
  - Need metrics and analytic methods to enable such analysis
- Each moving target mechanism addresses only a subset of the attack vectors
  - Need decision support mechanism for deployment of moving target systems

Challenge: Smart Movement

- Moving targets need to be agile
  - We need to consider autonomic behavior and concepts learned from analysis of immune systems, species evolution, and other natural responses to threat
- Moving target mechanisms need to adapt quickly
  - We need to get within the adversaries re-design loop
- Moving target mechanisms have performance costs
  - We need system control mechanisms that enable real-time threat-appropriate selection of moving target protections

Challenge: Developing a Cyber Ecosystem to Support Agility

- Keyed random moving target systems present key management challenges
  - Need systems that accommodate ad hoc key distribution, rapid re-keying
- Moving target mechanisms require complex decisions
  - Need enhanced capabilities to provide situational awareness of system state and current threats
  - Need metrics to support both human and machine decision making
- Moving target at scale may result in highly complex systems
  - Need new methods to model, test and evaluate such systems

Cyber Economics

- An examination to determine what impacts cyber economics and what incentives can be provided to enable ubiquitous security:
  - New theories and models of investments, markets, and the social dimensions of cyber economics
  - Data, data, and more data with measurement and analysis based on that data
  - Improved SW development models and support for “personal data ownership”

New Paradigm

- Promotion of science-based understanding of markets, decision-making and investment motivation
  - Develop new theories and models
  - Promote the role of economics as part of that understanding
- Creation of environments where deployment of security technology is balanced
  - Incentives to engage in socially responsible behavior
  - Deterrence for those who participate in criminal and malicious behavior

Challenge: Cyberspace Data

- Legal and ethical collection, protection and distribution
  - Ensure *all* data types/categories are available to the R&D community, including international sharing
  - Provide protections to data providers, e.g., anonymization
- Lack of appropriate data to support effective economic analysis
  - Why isn't there cyber "insurance actuarial information"?
  - Current incident trending information inadequate for decision-makers (e.g., no "ground truth" for malware, incidents, etc.)

Challenge: Personal Info/Behavior

- Educating users about the benefits of secure practices and acceptable cyber behavior
  - Currently, the "user" is the weakest link
  - Will improved usability impact the security deployment picture?
- "Personal Data"
  - Lack of understanding and agreement of what it is
  - Who's ultimately responsible for *my* personal data? Can I hold them accountable? Do I actually *own* it? What economic issues are associated with "personal data"?

Challenge: Empowerment of critical infrastructure providers

- Assess economic benefits and costs of protecting critical infrastructure against disruption
  - Educate vendors about their role w.r.t. “secure” software
- Provide legal frameworks allowing service providers to be more active in defense of their systems/services
  - What is allowable scope of action in “active response”, within the context of global legal capacities and partnerships?
  - How do we empower providers to reduce abusive or criminal behavior and provide appropriate law enforcement support?

What is the end result?

- Data for everyone, anytime, anywhere
- Security deployment decisions based on knowledge, metrics, and proper motivations
- Properly incentivized vendors
- Individual users taking ownership of their personal data
- Critical infrastructure providers able to better defend their networks and systems

New Emphasis Area: Science of Cyber Security

- A major research initiative on the *science of security* that
  - is aggressive in nature
  - Supports interdisciplinary efforts
  - willing to support high-risk explorations is needed to establish such a scientific basis
  - ultimate goal of protecting deployed systems
  - public-private partnership of government agencies, universities and industry
  - must be integrated in a cohesive whole to produce results that impact large-scale systems.

Some Key Science of Security Research Thrusts

- Methods to model adversaries
- Techniques for component, policy and system composition
- A control theory for maintaining security in the presence of partially successful attacks
- Sound methods for integrating the human in the system: usability and security
- Quantifiable, forward-looking, security metrics (using formal and stochastic modeling methods)
- Measurement methodologies and testbeds for security properties
- Development of comprehensive, open, and anonymized data repositories.