Infosec Research Council Hard Problems List

CSIA IWG
Washington, DC
January 26, 2006

Douglas Maughan, Ph.D.
Program Manager, HSARPA
douglas.maughan@dhs.gov
202-254-6145 / 202-360-3170

Homeland Security

Background

- INFOSEC Research Council (IRC)
  - Roundtable of major government investors in Information Security Research
- http://www.infosec-research.org/
- In existence since 1996

Homeland Security

IRC Participating "Agencies"

- ARDA - Advanced Research and Development Activity
- CIA - Central Intelligence Agency
- DOD - Department of Defense (including the Air Force, Army, Defense Advanced Research Projects Agency, National Reconnaissance Office, National Security Agency, Navy, and Office of the Secretary of Defense)
- DOE - Department of Energy
- DHS - Department of Homeland Security
- FAA - Federal Aviation Administration
- NASA - National Aeronautics and Space Administration
- NIH - National Institutes of Health
- NIST - National Institute of Standards and Technology
- NSF - National Science Foundation
- TSWG - Technical Support Working Group.

- In addition, the IRC is regularly attended by partner organizations from Canada and the United Kingdom.

Homeland Security

Hard Problems List (HPL)

- Original Version
  - Composed in 1997-98 based on several government sponsored workshops; Published in 1999
- Topics
  - 1. Intrusion and Misuse Detection
  - 2. Intrusion and Misuse Response
  - 3. Security of Foreign and Mobile Code
  - 4. Controlled Sharing of Sensitive Information
  - 5. Application Security
  - 6. Denial of Service
  - 7. Communications Security
  - 8. Security Management Infrastructure
  - 9. Information Security for Mobile Warfare
  - A. Secure System Composition
  - B. High Assurance Development
  - C. Metrics for Security

Homeland Security

Hard Problems List (HPL)

- 2005 Version
  - In the works since Summer 2003
  - First attempt in over 6 years to identify at Federal level the hardest and most important scientific challenges facing the US in Information Security research
  - External Review Board
    - Steve Bellovin
    - Marc Donner
    - Joan Feigenbaum
    - James R Gosler
    - Steve Kent
    - Peter G. Neumann
    - Fred Schneider
  - Document Structure

Homeland Security

IRC HPL 2005 Topics

1. GLOBAL SCALE IDENTITY MANAGEMENT
2. INSIDER THREAT
3. AVAILABILITY OF TIME-CRITICAL SYSTEMS
4. BUILDING SCALABLE SECURE SYSTEMS
5. ATTACK ATTRIBUTION AND SITUATIONAL UNDERSTANDING
6. INFORMATION PROVENANCE
7. SECURITY WITH PRIVACY
8. ENTERPRISE LEVEL SECURITY METRICS

Homeland Security

1. GLOBAL SCALE IDENTITY MANAGEMENT

- Scope: Identification, authentication, authorization, requisite key infrastructure
- Motivation: Need for seamless IAA across many systems, costs of divergent IAA systems, limits of current PKI, quantum.
- Challenges: Scale, churn, anonymity, federation.
- Metrics: Scale and adversary work factor.

2. INSIDER THREAT

- Motivation: Frequency and severity of incidents historically, increasing potential.
- Challenges: Not unauthorized access, Inside knowledge of defenses, “help” from outsiders with substantial resources.
- Approaches: Connections to HP #1, pervasive auditing, and redundancy.
- Goal: Mitigate the insider threat in cyber space so far as it is in physical space.

3. AVAILABILITY OF TIME-CRITICAL SYSTEMS

- Motivation: SCADA, military, home-land security first responders often
  - Value availability over secrecy.
  - Work in lossy, ad hoc wireless environments.
- Challenges: limited resources
  - Computational processing power.
  - Service quality guarantees given dynamics.
  - Distributed systems compound problem.
- Metric: Range of circumstances over which results can be guaranteed.

4. BUILDING SCALABLE SECURE SYSTEMS

- Motivation: High Consequence Systems
- Challenges: Today's systems are huge.
  - Catastrophic bugs can be tiny.
  - Some developers may be working against us.
  - Components, subsystems, architectures.
- Approaches: Help formal verification scale.
  - Development and formal V&V environments.
  - Means of correctly composing formal models.
- Goal: Fully verified truly trustworthy TCB.

Homeland Security

5. ATTACK ATTRIBUTION AND SITUATIONAL UNDERSTANDING

- Motivation: Respond to the unpreventable.
- Challenges:
  - Some attacks may be acts of war, others the work of teens, others nations posing as teens.
  - Hostile networks, anonymizers, recordless public access such as wi-fi and internet cafes.
  - Big picture and appropriate response
- Metrics:
  - Response selection: Degradation of mission.
  - Attribution: ID of adversaries in exercises.

6. INFORMATION PROVENANCE

- Motivation: Life-critical and releasability decisions both require pedigree of data.
- Challenges: Volume, degree of automated processing and transformation. Connections to HP #7.
- Goal: Track pedigree for every byte of information in exabyte scale systems transforming terabytes of data per day.

Homeland Security

7. SECURITY WITH PRIVACY

- Motivation: More of our interactions and transactions are occurring in cyberspace. Data mining poses risks to privacy and identity theft poses risks to security.
- Challenges: Current strategies for security often involve surveillance at cost of privacy
- Scope: IRC NOT defining privacy policy.
- Approach:
  - Tools to help users keep private info private.
  - Privacy sensitive data mining techniques.

8. ENTERPRISE LEVEL SECURITY METRICS

- Motivation: Without means to measure progress, we're not likely to see much…
- Challenges: Inability to quantify security leaves us with systems that we can't describe
  - Impacts on deployment of security technology
- Goal: IRC supports CRA challenge that within 10 years, quantitative information-systems risk management should be at least as good as quantitative financial risk management.

Summary

- "Stake in the ground" from the front-line
- Topics selected because of their importance to Government missions and the lack of solutions
- Not the only challenges in the IT security space
- Information security is not only about technology
- Several non-technical issues impact the protection of information and systems
  - Policy issues,
  - Legal issues,
  - Technology transition challenges,,
  - Economics and market forces
  - Academic education and training

Homeland Security

Douglas Maughan, Ph.D.

Program Manager, HSARPA

douglas.maughan@dhs.gov

202-254-6145 / 202-360-3170

Homeland Security

Homeland Security