

Wireless Security Challenges

National Institute of Standards and Technology

Tom Karygiannis
Email: karygiannis@nist.gov

Atlanta, GA
April 10-11, 2008

Presentation Outline

▶ About NIST

▶ Wireless Challenges

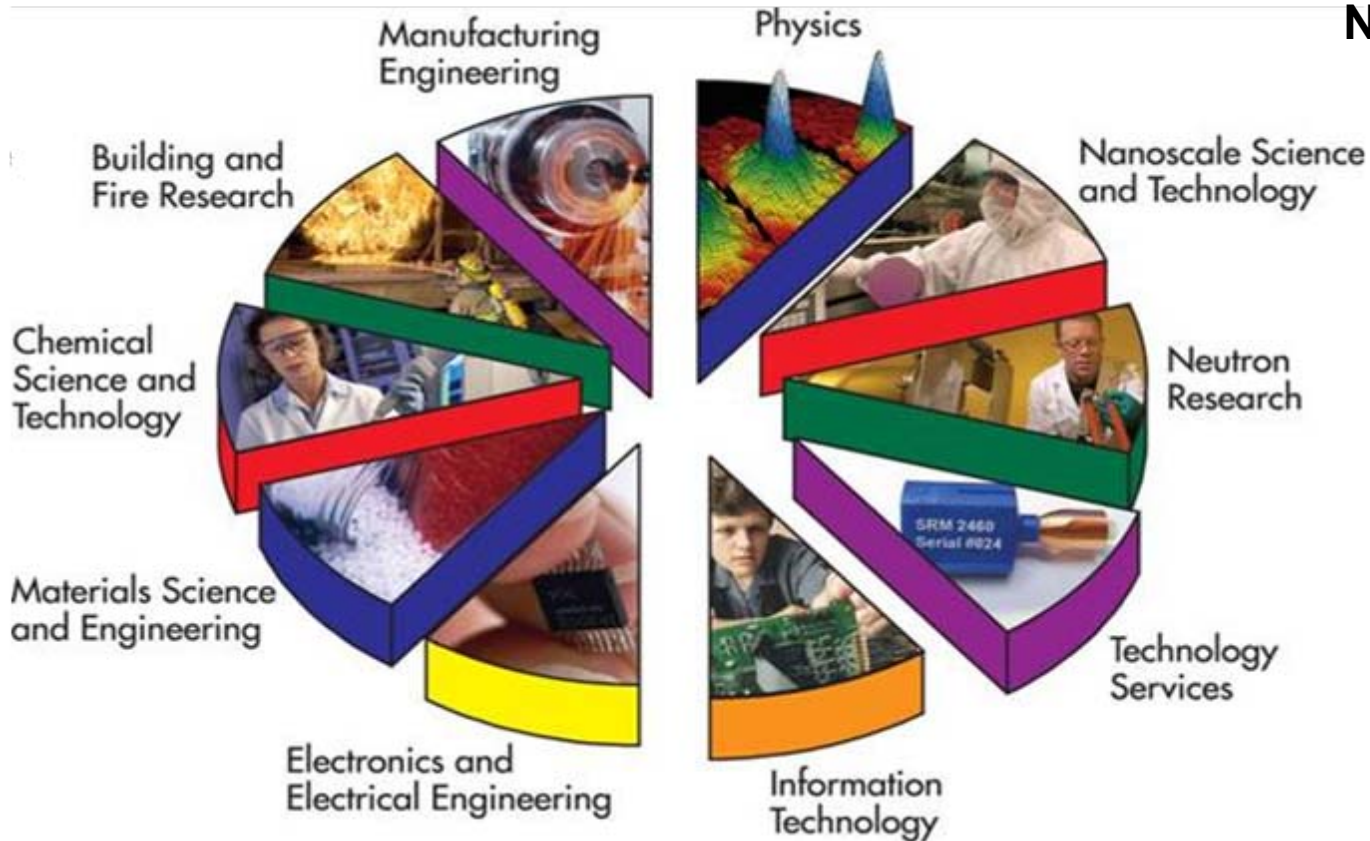
▶ Discussion & Contact Information

NIST Provides Innovation Infrastructure...

- ▶ Non-regulatory agency within U.S. Department of Commerce.
- ▶ Founded in 1901 as National Bureau of Standards
- ▶ ~2900 employees
- ▶ Nobel Prize Winner in Physics in 1997, 2001, 2005
- ▶ NIST Mission: To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
- ▶ **Provide the measurement “tool box” for the nation**
 - Provide solutions to measurement problems
 - Try to assure that the necessary measurements and quality are available to meet the nations most significant needs
- ▶ **Absolute correctness of results is paramount to NIST Labs.**



The NIST Laboratories



NIST's work enables

- Science
- Technology innovation
- Trade
- Public benefit

Research Projects in the Computer Security Division

- ▶ Advanced Cryptography (e.g., hash, public key, quantum, light footprint)
- ▶ Inherently Secure, High Assurance, and Provably Secure Systems and Architectures
- ▶ Composable and Scalable Secure Systems
- ▶ Wireless Security
- ▶ Network Measurement and Visualization Tools
- ▶ Secure Distributed Systems
- ▶ Infrastructure for Information Security R&D
- ▶ Security for Quantum Computing
- ▶ Foundations of Measurement Science for Information Systems
- ▶ Biometrics and Cryptographic Identity Verification
- ▶ URL: <http://csrc.nist.gov>

Presentation Outline

- ▶ About NIST

- ▶ Wireless Challenges

- ▶ Discussion & Contact Information

State of Affairs

- ▶ It is widely recognized that the marketplace **rush to field new networking technologies** of all types often **far out paces** the industry's ability to **adequately address security** and robustness issues in their design.
- ▶ The current state of the art for “trustworthy design” often relies on **human inspection** of early designs by “security experts”.
- ▶ For many distributed IT systems, the **first rigorous test** of their security and robustness properties occurs **after operational deployment**.
- ▶ The state of the art for metrics to characterize the security of such systems is typically focused on testing implementations against **known vulnerabilities** (i.e., yesterday's attacks). There are few, if any, predictive security metrics.
- ▶ In effect, we rely on the bad guys to innovate security and robustness tests, by waiting to detect and **react to their latest successful attacks**.

State of Affairs

- ▶ While there is a tremendous sense of urgency about the state of the problem space, **not enough effort is going into innovative / high risk approaches** to the solution space.
- ▶ **Piecemeal responses** have not yielded significant improvements to the overall state of computer security.
- ▶ “Mess – a difficult situation from which you would like to extricate, but there is no obvious way... **messes are complex and inscrutable**. There is no agreement on whether the mess manifests a single problem or the convergence of many. With a mess, the problem is that we don’t know how to characterize it as a problem.” Peter Denning, April 2007

Some Wireless Security Challenges

- ▶ Data Provenance, Software Provenance and Pedigree
- ▶ Sensors, RFID,
- ▶ Eye-witness images, video, audio
- ▶ Location-based Services and Policies
- ▶ Privacy and Wireless Fingerprinting
- ▶ User Anonymity
- ▶ Attacks on Physical Layer
- ▶ Anti-Tampering Technologies
- ▶ Insider Threat

Same Hard Problems.....

- ▶ Design
- ▶ Testing, Integrity
- ▶ Security Metrics
- ▶ All still hard problems

Presentation Outline

- ▶ About NIST

- ▶ Wireless Challenges

- ▶ Discussion & Contact Information

Contact Information

- ▶ Tom Karygiannis, NIST, 100 Bureau Drive, MS 8930, Gaithersburg, MD 20899, USA. Email: karygiannis@nist.gov, Tel. 301-975-4728
- ▶ Web URLs:
 - NIST <http://www.nist.gov>
 - Computer Security Division <http://csrc.nist.gov/>