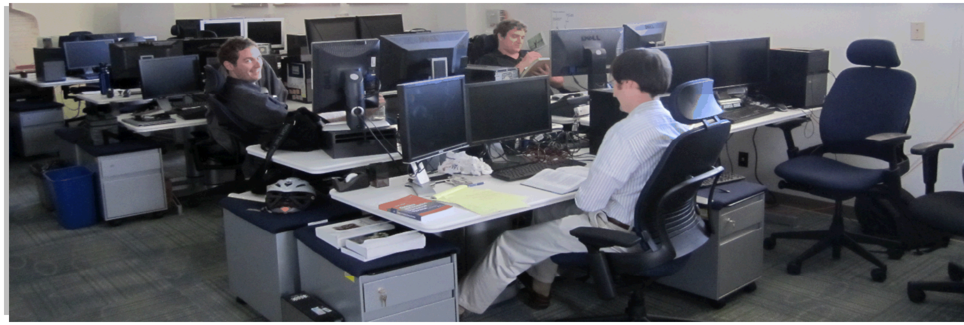
SAND2012-3410P

Cybersecurity: Addressing Hard Problems

Exceptional service in the national interest

Sandia National Laboratories

Steve Hurd,
Sandia National Labs



U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

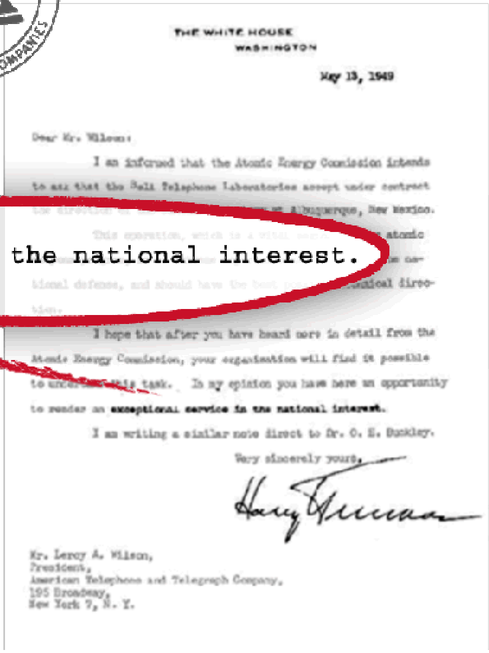
Today's Agenda…

- What is "Sandia"?
- Who am I?
- My Beliefs
- Why Cybersecurity is Hard.
- Enlisting Help From Others.
- Some of My Experience (war stories…)
- Final Thoughts

Sandia’s History

U.S. ATOMIC ENERGY COMM.
SANDIA LABORATORY
ALBUQUERQUE NEW MEXICO

AMERICAN TELEPHONE & TELEGRAPH CO
BELL SYSTEM
AND ASSOCIATED COMPANIES



THE WHITE HOUSE
WASHINGTON

May 13, 1949

Dear Mr. Wilson:

I am informed that the Atomic Energy Commission intends to ask that the Bell Telephone Laboratories accept under contract the direction of [illegible] at Albuquerque, New Mexico.

This operation, which is a vital [illegible] atomic [illegible] na- tional defense, and should have the best [illegible] technical direc- tion.

I hope that after you have heard more in detail from the Atomic Energy Commission, your organization will find it possible to undertake this task. In my opinion you have here an opportunity to render an **exceptional service in the national interest.**

I am writing a similar note direct to Dr. O. E. Buckley.

Very sincerely yours,

Harry Truman

Mr. Leroy A. Wilson,
President,
American Telephone and Telegraph Company,
195 Broadway,
New York 7, N. Y.

exceptional service in the national interest.

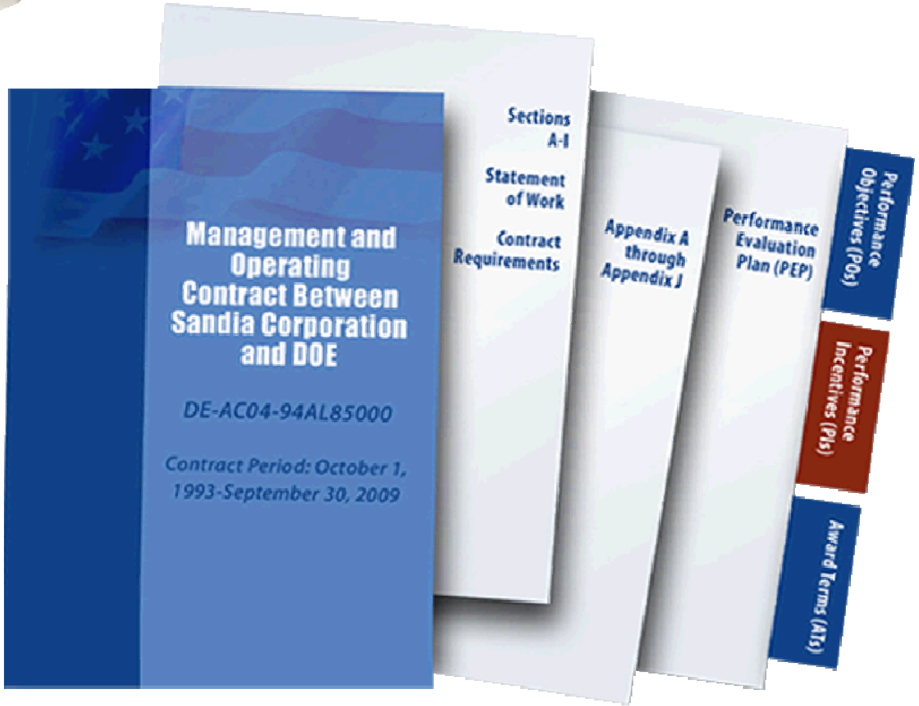
Sandia's Governance Structure

Sandia National Laboratories
MANAGED FOR DOE BY SANDIA CORPORATION
A LOCKHEED MARTIN COMPANY

Sandia Corporation

- **AT&T: 1949–1993**
- **Martin Marietta: 1993–1995**
- **Lockheed Martin: 1995–present**
- **Existing contract expires Sept. 9, 2012**

Government owned, contractor operated



Management and Operating Contract Between Sandia Corporation and DOE

DE-AC04-94AL85000

Contract Period: October 1, 1993-September 30, 2009

Sections A-I

Statement of Work

Contract Requirements

Appendix A through Appendix J

Performance Evaluation Plan (PEP)

Performance Objectives (POs)

Performance Incentives (PIs)

Award Terms (ATs)

Federally funded research and development center

Sandia's Sites

Albuquerque,
New Mexico

Livermore,
California

Tonopah, Nevada

Waste Isolation Pilot Plant,
Carlsbad, New Mexico

United States Department of Energy
Waste Isolation Pilot Plant

Pantex, Texas

But who am I???

- Joined Sandia in 1987…from business school!
- Spent about 12 years in IT Infrastructure
- Started working in security in 1999
  - Vulnerability assessments & red teaming
  - DARPA research (red teaming new technology)
  - Process Control Security
  - Vehicle Security
  - Wide variety of work with DHS
  - Managing the Center for Cyber Defenders internship program
  - Launching Sandia’s Cybersecurity Technology Research Laboratory
- Thus, Steve = “Utility Infielder of Cyber Security”
- I also DJ at Stanford’s campus radio station…

My Beliefs…the bad news

- **MY THESIS: Cybersecurity is going to be a big problem for many decades to come**
  - There will be no “silver bullet” anytime soon
  - It will be made worse by all the “why it is hard” points in the slides that follow
  - We’ll never have enough talented defenders
  - It will get worse…possibly WAY worse before it gets better.

Why is Cybersecurity Hard?

- Complexity of today's "computer"
  - "Guarantees" vulnerabilities
  - Complex system rules apply
  - Designed to be "general purpose"
    - Everyone gets all the capabilities (and associated vulnerabilities)
  - Uses a global supply chain
- "Embedded systems"
  - Even less thought given to security
- A history of sharing truthful information
  - TCP/IP & deterministic responses

Why is Cybersecurity Hard? (cont.)

- Asymmetry between defender & attacker
  - Defender must plug EVERY vulnerability
  - Attacker need only find one vulnerability
  - Most defenders are amateurs
  - Most attackers are professionals
  - There are few rules governing attackers, other than physics & some enforced protocols
  - Defender does not know attacker's goals motivation, values, etc.

Why is Cybersecurity Hard? (cont.)

- What is an attack (or successful attack)?
  - How do you know if you've been attacked?
  - How do you know what has been compromised?
  - How do you know if you've successfully recovered from compromise?
- The law is behind the times & doesn't translate well across international borders
  - Plus, any attribution is hard (multi-step attacks, botnets)

Why is Cyber Security Hard? (cont.)

- Just because a vulnerability isn't publicly known, it does exist (and an attacker may know about it)
- Attacker motivation has changed
  - Before: Mostly "hacker street cred"
  - Now: Organized crime (identity theft, fraud, botnets to send spam, attack, etc.)
  - Thus, keeping discovered vulnerabilities quiet as long as possible is an attacker's goal.
- Infection vectors have changed
  - Before: Attacking servers
  - Now: Attacking clients (via web access)

Why is Cyber Security Hard? (cont.)

- Insider threat (not unique to cyber security, but harder to catch)
- Cyber defense is a thankless job
  - Technically difficult
  - If everything goes well, nothing happens
  - If something goes wrong, not much fun!
  - Far too few good people available
  - False positive burnout

- Threats in hardware & BIOS (supply chain)
- Difficulty truly authenticating anyone

Enlisting the Help of Others

- We need help from our friends…including (but not limited to)
  - Statistical/Math Modelers
  - Economists
  - Psychologists
  - Decision/Risk Analysts
  - Public Policy Experts
  - Attorneys
  - Human/Organizational Factors Experts
  - Communications Professionals
- They can help us navigate an insecure world
  - Prioritizing our efforts, assess trade-offs
  - Turning users from a liability to an asset
  - Yet, they need to understand how things work (at some level)

Enlisting the Help of Others (cont.)

- Example: Assessing the value of deterministic vs. non-deterministic responses around deception
  - Start with the attorneys…
  - Psychologists
  - Behavioral Economists
  - Experimental Design Experts
  - Math/Stat Modelers
- And <u>we still need excellence</u> in Computer Science to make any of this worthwhile.

Some of My Experience

- You must understand the business if you are going to help
  - Auto Manufacturer Example
  - Electric Power Example
- US Government has its "hands full"
  - Everything driven by legal authorities
  - Defining a "national level cybersecurity event?"
  - Securing privately-owned critical infrastructure. Analyzing supply chain risks.
  - Purchasing managed security services.
  - Identifying promising research/tools and helping to rapidly put them into practice

Final Thoughts

- We need to creatively engage, develop, and train the next generation of cyber defenders
- Researchers need to understand “ground truth”
  - Don’t need “expert level” knowledge, just basic fluency
- We need to help our friends to help us
  - Better models, approaches, decisions, incentives to share, etc.
- The big problems will almost certainly require BIG solutions
  - Think “Manhattan Project”, “Bletchley Park”, etc.
  - Need to create incentives for being 1 of many tackling the biggest problems