A Scientific Research and Development Approach to Transform Cyber Security

A Report Prepared for the Department of Energy

Charlie Catlett, CIO, Argonne National Laboratory

On behalf of the Cyber Security Community

(DOE Laboratories, Universities, Industry participants)

Charlie Catlett, Argonne National Laboratory, Editor
Mine Altunay, Fermi National Accelerator Laboratory
Robert Armstrong, Sandia National Laboratories (CA)
Kirk Bailey, University of Washington
David Brown, Lawrence Livermore National Laboratory
Robert R. Burleson, Oak Ridge National Laboratory
Matt Crawford, Fermi National Accelerator Laboratory
John Daly, Los Alamos National Laboratory
Don Dixon, Texas A&M University
Barbara Endicott-Popovsky, University of Washington
Ian Foster, Argonne National Laboratory
Deborah Frincke, Pacific Northwest National Laboratory
Irwin Gaines, Fermi National Accelerator Laboratory
Josh Goldfarb, BBN Technologies
Christopher Griffin, Oak Ridge National Laboratory
Yu Jiao, Oak Ridge National Laboratory
Tammy Kolda, Sandia National Laboratories
Ron Minnich, Sandia National Laboratories (CA)
Carmen Pancerella, Sandia National Laboratory
Don Petavick, Fermi National Accelerator Laboratory
J. Christopher Ramming, DARPA
Chad Scherrer, Pacific Northwest National Laboratory
Anne Schur, Pacific Northwest National Laboratory
Frank Siebenlist, Argonne National Laboratory
Dane Skow, Argonne National Laboratory
Adam Stone, Lawrence Berkeley National Laboratory
Chris Strasburg, Ames Laboratory
Richard Strelitz, Los Alamos National Laboratory
Denise Sumikawa, Lawrence Berkeley National Laboratory
Craig Swietlik, Argonne National Laboratory
Edward Talbot, Sandia National Laboratories (CA)
Troy Thompson, Pacific Northwest National Laboratory
Keith Vanderven, Sandia National Laboratories (CA)
Von Welch, NCSA, University of Illinois at Urbana-Champaign
Joanne R. Wendelberger, Los Alamos National Laboratory
Paul Whitney, Pacific Northwest Laboratory
Louis Wilder, Oak Ridge National Laboratory
Brian Worley, Oak Ridge National Laboratory

A Scientific Research and Development Approach
To Cyber Security

December 2008
Submitted to The Department of Energy

Wednesday, March 4, 2009
Background

- Summits
- Working Groups
- Open Workshops
- Report Vetted w/ Industry, Multiple Agencies

AFCYBER, CIA, CND, DHS, DISA, DOD, DOE-IN, DOE-OS, DOE-JIACTF, FDIC, G2, IARPA, JIACTF, KCP, NIARL, NIST, NSA, ODNI, OSD/DoD, OSTP, State, and Treasury.

Source: C. Catlett, c@anl.gov

Wednesday, March 4, 2009
A National *Priority*

2005

“broad failure to invest” in “fundamental research in civilian cyber security.”

2007

“The ability to design and develop secure… systems is a national priority.”

2008

“special focus and prioritization are needed to respond to current national networking security concerns.”

Source: C. Catlett, c@anl.gov

Wednesday, March 4, 2009
The Department of Energy

- **Unique Requirements**
  - National-scale civilian and classified infrastructure, assets, programs
  - International science communities

- **Unique Strengths**
  - National Laboratories with strong multi-disciplinary programs and rich academic and industry collaborations
  - Mathematics and Computational Science programs coupled with Leadership Class facilities.
Cyber Defense Today

• Mathematics & Computational Science Untapped
  • Mathematics-based Intrusion Detection
  • Limited use of modeling and simulation
• Architecture is Anachronistic
  • Inherent trust among components
  • Passive data
• Policy is Reactive and Tactical
  • Defense against specific, previous tactics
  • Underlying model (layered defense) awkward
Incremental vs. revolutionary improvements...

Where you are now

Where you can get with incremental improvements

Where you NEED to be

Big Frickin’ Wall

Source: Kathy Sierra

Wednesday, March 4, 2009
Three Focus Areas

Mathematics
Predictive Awareness for Secure Systems

Information
Self-Protective Data and Software

Platforms
Trustworthy Systems from Untrusted Components

Aiming over the horizon but not into science fiction...

Source: C. Catlett, c@anl.gov
Focus Areas in Context

**PITAC (2005)**
- Authentication Technologies
- Secure Fundamental Protocols
- Secure Software Engineering & Software Assurance
- Holistic System Security
- Monitoring & Detection
- Mitigation & Recovery Methodologies
- Cyber Forensics: Catching & Deterring Criminal Activities
- Modeling & Testbeds for New Technologies
- Metrics, Benchmarks, & Best Practices
- Non-Technology Issues that Compromise Cyber Security

**Mathematics**
Predictive Awareness for Secure Systems

**Information**
Self-Protective Data and Software

**Platforms**
Trustworthy Systems from Untrusted Components

**PCAST (2007)**
- Comprehensive analysis of potential system-level vulnerabilities to inform the design of inherently secure NIT systems
- Generation of the fundamental building blocks for the development of secure NIT systems
- Usability and related social sciences, because progress in improving the security of NIT systems also involves altering user behavior.”

Source: C. Catlett, c@anl.gov

Wednesday, March 4, 2009
Mathematics: Predictive Awareness for Secure Systems

- **Create** capabilities to examine system or network behavior to anticipate failure or attack, including real-time detection of anomalous activity and adaptive “immune system” response.

- **Requires** a deeper understanding of complex applications and systems, appropriate architectures, techniques, and processes – using data-driven modeling, analysis, and simulation.

- **Leverages** DOE programs in mathematics and computational science, and leadership computing expertise and facilities.

“…meteorology provides proof that complex, evolving, large-scale systems are amenable to mathematical analysis and that the network-security community need not necessarily restrict itself to the (probably oversimplified) models now in the literature.” *Workshop on Scalable Cyber-Security Challenges in Large-Scale Networks: Deployment Obstacles, Interagency Working Group for IT R&D, March 2003.*

Source: C. Catlett, c@anl.gov
Information: Self-Protective Data and Software

- **Create** “active” data systems and protocols to enable self-protective, self-advocating, and self-healing digital objects.
- **Requires** data provenance and related research to provide information integrity, awareness of attributes such as source, modification, trace back, and actors; and mechanisms to enforce policy concerning data confidentiality and access.
- **Leverages** DOE leadership in, and mission requirements for, protection of classified and/or controlled information (data, software) and analysis and stewardship of large-scale scientific data sets for international experiments.
Platforms: Trustworthy Systems from Untrusted Components

- **Create** mechanisms for specifying and maintaining overall trust properties for operating environments and platforms.
- **Requires** techniques for quantifying and bounding security and protection, integrity, confidentiality, and access in the context of a “system” comprised of individual components for which there are varying degrees of trust.
- **Leverages** DOE expertise in hardware and software systems architecture, operating systems, and secure build and test facilities.

Google “ebetween…”

Source: C. Catlett, c@anl.gov

Wednesday, March 4, 2009
# DOE: Uniquely Positioned

<table>
<thead>
<tr>
<th></th>
<th>DOE</th>
<th>DARPA</th>
<th>NSF</th>
<th>DOD Labs</th>
<th>NSA, IARPA</th>
<th>NIH</th>
<th>DHS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Programmatic Orientation</strong></td>
<td>Vision &amp; Project</td>
<td>Project</td>
<td>Project</td>
<td>Vision</td>
<td>Project</td>
<td>Vision &amp; Project</td>
<td>Project</td>
</tr>
<tr>
<td><strong>“Customer”</strong></td>
<td>Society; Energy</td>
<td>DARPA</td>
<td>Society</td>
<td>DARPA</td>
<td>Intelligence Community</td>
<td>Society; Medical Community</td>
<td>National Infra.</td>
</tr>
<tr>
<td><strong>National Laboratory Assets</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Research Horizon</strong></td>
<td>Near Mid Long</td>
<td>Mid -</td>
<td>Long</td>
<td>Mid Long</td>
<td>Near Mid Long</td>
<td>Near Mid Long</td>
<td>Near Mid Long</td>
</tr>
<tr>
<td><strong>Cyber Security Expertise</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>some</td>
<td>some</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Primary Results Applicability</strong></td>
<td><strong>Flexible</strong></td>
<td><strong>Classified</strong></td>
<td>Open</td>
<td><strong>Classified</strong></td>
<td><strong>Classified</strong></td>
<td>Open</td>
<td><strong>Classified</strong></td>
</tr>
</tbody>
</table>

Source: C. Catlett, c@anl.gov

Wednesday, March 4, 2009
Example of Industry Work

Source: Ashar Aziz, FireEye Inc.
Recommendations (1 of 2)

- **Focus Areas to Harness DOE Strengths**
  - Mathematics: Predictive Awareness for Secure Systems
    - Leadership computing, mathematics, and computational science programs – cyber security as a computational science and engineering challenge leveraging INCITE.
  - Information: Self-Protective Data and Software
    - Computer science, computer architecture programs to explore novel approaches to *active* data.
  - Platforms: Trustworthy Systems from Untrusted Components
    - System software and architecture programs to pursue new operating system, distributed application, and platform architectures harnessing state-of-the-art such as multicore.

Source: C. Catlett, c@anl.gov

Wednesday, March 4, 2009
Recommendations (2 of 2)

• Programmatic Considerations
  • SciDAC-scale multidisciplinary teams
  • “X-Prize” style – clear targets, broad competition
    • Engage Industry
    • Facilitate many “failures” to find diamonds in the rough (aggressive program leadership/management)
  • Proactive research collaboration with industry, other agencies (NSF, DHS) and DOE programs.
  • Harness Leadership Computing, data analysis, and related infrastructure.
    • Support computational science (modeling and simulation) as well as nearer term needs such as sensor data analysis and intensive software vulnerability testing (e.g. “a software wind tunnel”)

Source: C. Catlett, c@anl.gov

Wednesday, March 4, 2009