NSF Activities in Cyber Trust

For ACM CCS Industry/Govt Track Oct. 26, 2004

Carl Landwehr (clandweh@nsf.gov)
Cyber Trust Coordinator
National Science Foundation
What’s the Problem?

• Today’s software-based systems are far too vulnerable to attack, misuse, and abuse
  – Inadequate attention to security requirements
  – Weak security design
  – Poor user interfaces
  – Flawed implementations
  – Complex configuration and control
  – Poor accountability
  – Inadequately trained operators and users

• Evidence?
  – Worm, virus attacks, misconfigured systems,
  – patch, patch, patch

*We spend too much on patching broken technology!*
System Architecture

- Hardware
- Firmware
- Operating System
- Utilities
- Applications
- H.323
- SNMP
Cyber Security R&D Act (PL 107-305)

- Recognizes
  - interdependencies of cyber and other infrastructures,
  - lack of preparedness for coordinated physical and cyber attacks,
  - lack of needed research capacity;

- Calls for expanded Federal investment in computer and network security research.

- Authorizes NSF to
  - award research grants in cyber security areas
  - establish multidisciplinary research centers
  - build research capacity
  - take a leading role in research and education to improve security of networked information systems

- FY03 – FY07
Cyber Trust Vision

Society in which

- People can justifiably rely on computer-based systems to perform critical functions securely
  - national scale infrastructures: water, power, communication, transportation, ...
  - localized systems: cars, homes, ...
- People can justifiably rely on systems to process and communicate sensitive information securely
  - health, banking, libraries, e-commerce, government records must conform to public policy
- People can rely on a well-trained and diverse workforce to develop, configure, and operate essential computer-based systems
  *Without fear of sudden disruption by cyber attacks*
Homeland Security
Critical Infrastructure Protection
Cyber Security
Cyber Trust
Range of Cyber Trust Solicitation

- Multi-Disciplinary
  - Spanning technical disciplines
  - Exploring relations among technical and social, economic, regulatory, legal domains

- Basic Research
  - Information/Applications
  - Systems Software
  - Communication Networks
  - Fundamentals

- Education and Workforce Development: required component of every proposal
  - For technical specialists and generalists
  - For the general public
# FY04 Cyber Trust Solicitation Summary

<table>
<thead>
<tr>
<th>Cyber Trust FY04 Competition Statistics</th>
<th>Individual/ small group</th>
<th>Team</th>
<th>Center-Scale Activity</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td># Projects received</td>
<td>230</td>
<td>135</td>
<td>25</td>
<td>390</td>
</tr>
<tr>
<td># Projects awarded</td>
<td>18</td>
<td>14</td>
<td>2</td>
<td>34</td>
</tr>
<tr>
<td>Success rate</td>
<td>8%</td>
<td>10%</td>
<td>8%</td>
<td>9%</td>
</tr>
<tr>
<td># Proposals received</td>
<td>255</td>
<td>189</td>
<td>45</td>
<td>489</td>
</tr>
<tr>
<td># Proposals awarded</td>
<td>22</td>
<td>23</td>
<td>3</td>
<td>48</td>
</tr>
<tr>
<td>Success rate</td>
<td>9%</td>
<td>12%</td>
<td>7%</td>
<td>10%</td>
</tr>
<tr>
<td>Total $ awarded (includes co-funding, excludes CAREERs)</td>
<td>$6.5M</td>
<td>$17.3M</td>
<td>$12.6M</td>
<td>$36.4M</td>
</tr>
<tr>
<td>Total $ Cyber Trust only</td>
<td>$6.3M</td>
<td>$12.1M</td>
<td>$12.6M</td>
<td>$31M</td>
</tr>
</tbody>
</table>

**CAREERS ~$2M**

**Co-funding ~ $5M (DARPA ATO, ITO)**
What’s next?

- Revised Cyber Trust solicitation planned for release in October
  - Largely similar to last year’s content
  - Some tweaks to the submission process
    - No LOIs for center-scale
    - Education-only proposals permitted
      - Possible name change
  - Deadline expected to be early Feb., 2005
- Resources available – planned for similar level to this year, pending appropriations, as always
FY04 Award Highlights

- Center-scale awards
  - CMU for Security Through Interaction Modeling
  - UCSD/ICSI for Internet Epidemiology

- Many strong team and individual/small group awards, e.g.
  - Economics of security deployment
  - Studies of user adoption of security mechanisms
  - Software flaw detection/removal
  - Cryptographic foundations
  - Protocols for managing distributed/replicated systems
  - New hardware/software architectures and OS’s
  - New methods for evaluating biometrics

- Further details:
  - See NSF awards search page:
  - select “Program Information” tab
  - Enter in program field: CYBER TRUST
Active Center Scale Awards (prior years)

- Large ITR award ($12.5M total, 5 years):
  - Sensitive Information in a Wired World (Stanford, Yale, Stevens, UNM, NYU): multi-disciplinary investigation of long term issues in automated information handling

- Large scale network testbed established for investigating network attacks, with major support from DHS:
  - Defense Technology Experimental Research (DETER) network, $5.45M total, led by UC-Berkeley, with USC/ISI and others
  - Testing and Benchmarking Methodologies for Future Network Security Mechanisms, to develop attack simulators, traffic generators, datasets for DETER, $5.6M total, (UC-Davis, Penn State, Purdue, ICSI).

- I/UCRCs:
  - Center for Identification Technology Research (Biometrics)(WVU)
  - Cyber Protection Center (Iowa State U, U Kansas, Miss State U)
  - Center for Experimental Research in Computer Systems (Ga Tech)
How to make an uncopyable key?

- Physical Random Functions -> Physical Unclonable Functions = PUFs
- Controllable PUFs: PUF accessible only via algorithm physically bound to PUF in an inseparable way
- Exploit manufacturing variations in silicon wires and gate delays
- Even the manufacturer can’t clone the device
How to compute public statistics without revealing private inputs?

- Suppose you want to collect accurate statistics on salary distributions, but contributors don’t want to (or aren’t allowed to) reveal individual salary information

- Privacy-preserving computation: users jointly compute the statistics
How to limit the damage from password compromise on the web?

• Crypto-Hash the password with the domain name
• Compromise of password on one site does not compromise other sites
• Pwdhash: see http://crypto.stanford.edu/PwdHash/
Cyber Trust in CI SE

Office of the Assistant Director for CI SE

- Computer and Communications Foundations (CCF)
- Computer and Network Systems (CNS)
- Information and Intelligent Systems (IIS)
- Shared Cyber Infrastructure (SCI)

Cyber Trust

CI SE-wide Emphasis Areas

- Science of Design
- Information Integration (SEIII)

NSF Logo
Thank You