

Security as an Element of Cyberinfrastructure

Guy Almes <gaimes@nsf.gov>

CISE Directorate

Shared Cyberinfrastructure Division



Secure IT 2005 Conference

April 21, 2005

Overview

- Cyberinfrastructure Overview
- Claim: Security is key to Cyberinfrastructure
- Personal thoughts on why it's hard
- NSF activities of interest
- Closing thoughts





Cyberinfrastructure Overview

- Due to the nature of university mission
 - each university wants a few people from each key research specialty
 - therefore, research colleagues are scattered across the nation / world
- Enabling their collaborative work is key to NSF



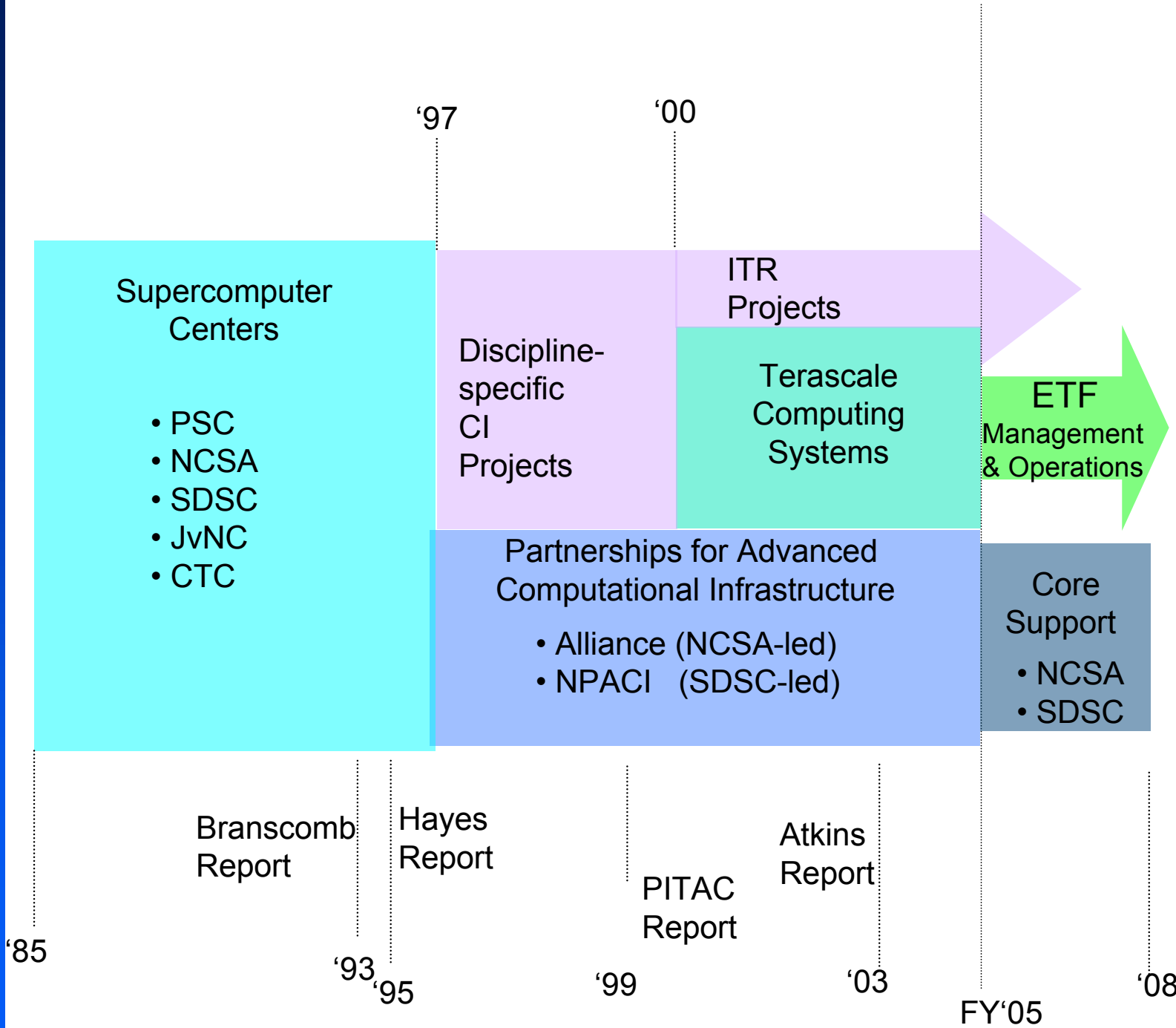
- Traditionally, there were two approaches to doing science:
 - theoretical / analytical
 - experimental / observational
- Now the use of aggressive computational resources has led to third approach
 - *in silico* simulation / modeling



Historical Elements

- Supercomputer Center program from 1980s
 - NCSA, SDSC, and PSC leading centers ever since
- NSFnet program of 1985-95
 - connect users *to (and through)* those centers
 - 56 kb/s to 1.5 Mb/s to 45 Mb/s within ten years
- Sensors: telescopes, radars, environmental
- Middleware: of growing importance

National Science Foundation

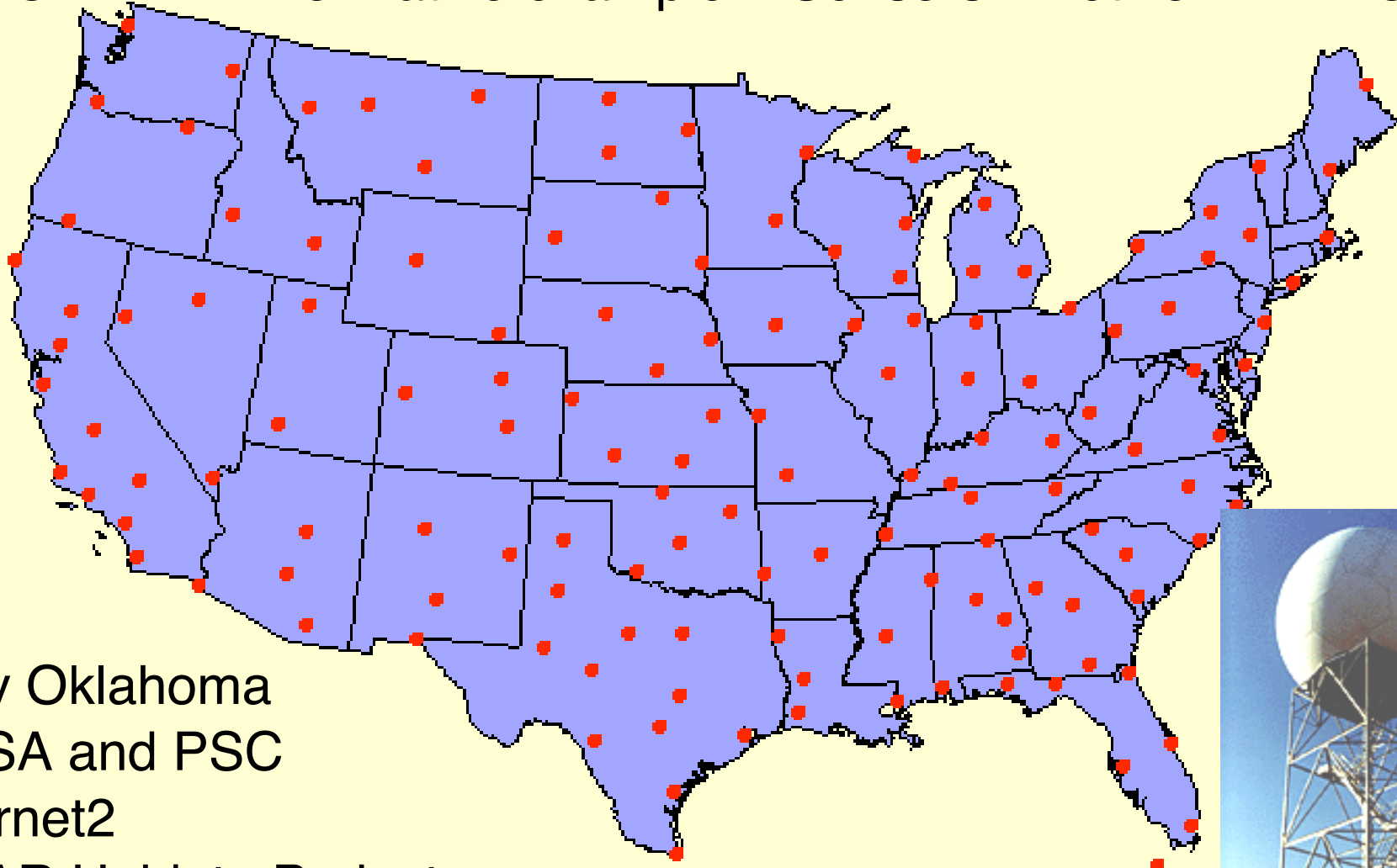




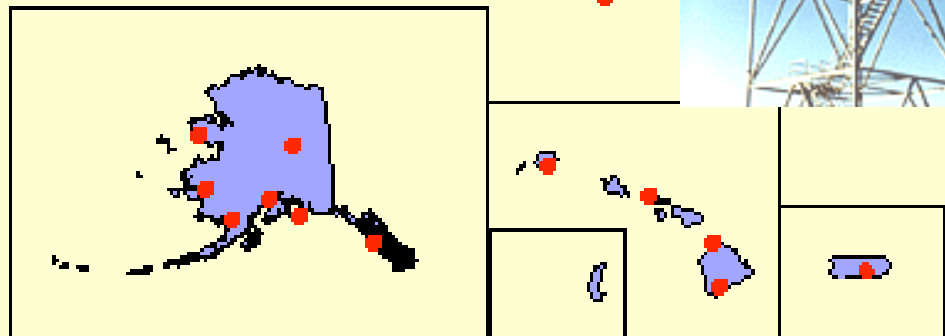
Explicit Elements

- Advanced Computing
 - Variety of strengths, e.g., data-, compute-
- Advanced Instruments
 - Sensor networks, weather radars, telescopes, etc.
- Advanced Networks
 - Connecting researchers, instruments, and computers together in real time
- Advanced Middleware
 - Enable the potential sharing and collaboration
- Note the synergies!

CRAFT: A normative example – Sensors + network + HEC



Univ Oklahoma
NCSA and PSC
Internet2
UCAR Unidata Project
National Weather Service
WSR-88D LOCATIONS



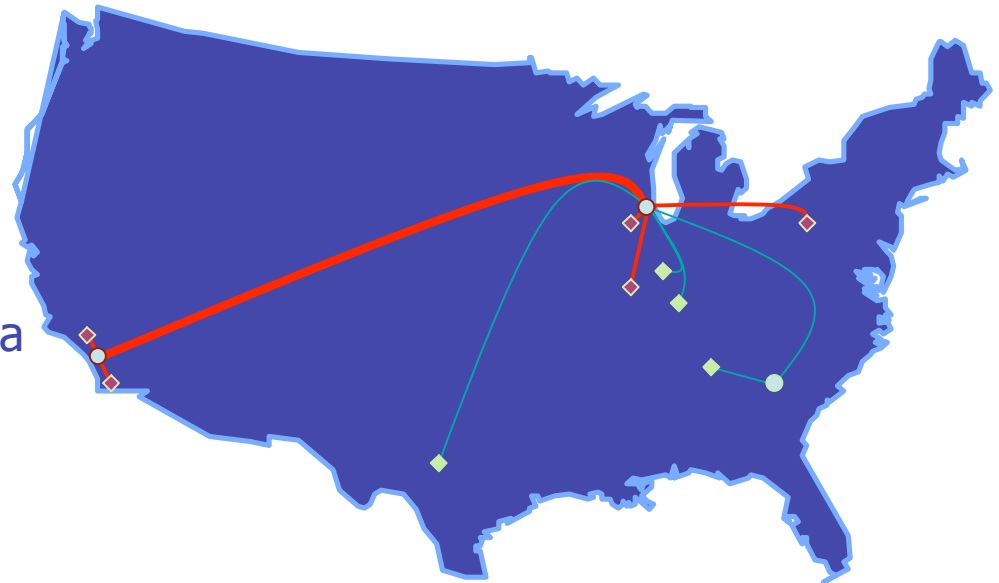


Current Projects within SCI

- Division of Shared Cyberinfrastructure
 - HEC + X
 - Extensible Terascale Facility (ETF)
 - International Research Network Connections
 - Middleware (evolving to Software Cyberinfrastructure)
 - Integrative Activities: Computational Science
 - Integrative Activities: Education, Outreach & Training
 - Social and Economic Frontiers in Cyberinfrastructure

TeraGrid: One Component

- A distributed system of unprecedented scale
 - 30+ TF, 1+ PB, 40Gb/s net
- Unified user environment across resources
 - User software environment
 - User support resources
- Integrated new partners to introduce new capabilities
 - Additional computing, visualization capabilities
 - New types of resources: data collections, instruments
- *Built a strong, extensible Team*
- Created an initial community of over 500 users, 80 PIs
- Created User Portal in collaboration with NMI





Interesting ETF Resources

- Computational
 - very tightly coupled clusters
 - LeMieux and Red Storm systems at PSC
 - tightly coupled clusters
 - Itanium2 and Xeon clusters at several sites
 - data-intensive systems
 - DataStar at SDSC
 - memory-intensive systems
 - Maverick at TACC and Cobalt at NCSA



- Online and Archival Storage
 - e.g., more than a PB online at SDSC
- Data Collections
 - numerous
- Instruments
 - Spallation Neutron Source at Oak Ridge
 - Purdue Terrestrial Observatory



Technology Drivers

- Moore's Law
 - power of electronics doubles every 18 months
- But for online storage
 - gigabytes / dollar doubles every 12 months
- And users, including scientists and engineers, exploit these drivers

Summary Points

- Architectural diversity
- Ideally suited to foster collaboration
- Increasingly data-intensive
- Note two key requirements:
 - *performance*
 - *security*





Primary Claim of the Talk

- Security is Key to successful Cyberinfrastructure



Why is this true?

- Data-intensive science, combined with highly skilled/experienced storage and data collection resources, foster cyberinfrastructure resources as natural place for collaboration data
- Cyberinfrastructure Resources are typically time-shared computer systems
- Corruption or abuse of data a key threat



- Two key sub-claims:
 - Making Cyberinfrastructure secure is important
 - Making Cyberinfrastructure secure is hard



Personal Observations

- 1970s: Operating Systems area was active and prestigious
 - sharing physical and information resources
 - the world in which the ARPAnet and TCP/IP were created
- 1980s: Personal Computer revolution
 - myth that operating systems not needed
 - the world in which the Internet was deployed



We are now paying the price

- We need to (re)elevate the areas of operating systems and security
- This is long overdue
- In the meantime, hats off to those working with the current environment
- But we need deeply improved technologies



Relevant NSF Programs

- Cyber Trust Program
 - Carl Landwehr
 - Cyber Trust Program Coordinator

- *TRUST*: Team for Research in Ubiquitous Secure Technologies
 - Steven Mahaney
 - Oversees this new Science and Technology Center

Cyber Trust Vision

Society in which

- People can justifiably rely on computer-based systems to perform critical functions securely
- People can justifiably rely on systems to process and communicate sensitive information securely
- 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



Award Summary FY04

Cyber Trust FY04	Small	Team	Center- Scale	Total
# projects proposed	230	135	25	390
# projects awarded	18	15	2	35
Success rate	8%	11%	8%	9%
Total funds obligated	\$6.5M	\$17.3M	\$12.6M	\$36.3

Includes Co-funding from DARPA ~\$6M

Excludes related CAREERs (10) and ITR (5)





TRUST: Team for Research in Ubiquitous Secure Technologies

- New NSF Science and Technology Center
- Participants:
 - University of California -- Berkeley (lead)
 - Carnegie Mellon University
 - Cornell University
 - Mills College
 - San Jacinto State University
 - Smith College
 - Stanford University
 - Vanderbilt University



Closing Thoughts

- I invite your interest in contributing to secure shared computer systems



Closing Thoughts

- We, as a community, cannot accept the current endemic of infected and vulnerable systems
- (both a technical and a non-technical point)



Closing Thoughts

- We may need to reduce the (over?)generality of many of our systems



Closing Thoughts

- Practical scalable federated strong authentication is needed
- Reduces hassle for each user
- Increases motivation for enterprises and campuses to invest in strong authentication
- Improves security of shared systems



Thanks to all who contribute
to improved Secure
Information Technology!