Research Directions in Trustworthy {Trusted, Dependable} Computing

Dr. Carl E. Landwehr,
Program Director
National Science Foundation
clandweh@nsf.gov
+1 703-292-8910

IFIP WG 10.4 41st Meeting

January 6, 2002

Some past efforts to develop research challenge lists in related areas

- 1998 NSF CIP workshop
- 1998 NSF/ONR Workshops:
  Computer Security, Dependability, and Assurance
  see: www.isse.gmu.edu/~csis/conf/fns98
- 1999: Infosec Research Council: INFOSEC Hard Problems
  see www.infosec-research.org/docs_public/IRC-HPL-as-released-990921.doc
- 1999: NRC (DARPA/NSA) - Trust in Cyberspace
  see: http://www.nap.edu/books/0309065585/html/index.html
- 2001: NSF Workshop on Information Technologies for Security

Vision

Society in which

- People can justifiably rely on computer-based systems to perform critical functions
  - national scale infrastructures: water, power, communication, transportation, ...
  - localized systems: cars, homes, ...
- People can justifiably rely on systems processing sensitive information about them to conform to public policy
  - health, banking, libraries, e-commerce, government records

Present State - 1

- Flaws and weaknesses in existing computer-dependent infrastructures
  - latent flaws in widely distributed software
  - decreasing diversity of software components
  - poor technical means for managing security
  - inadequate technical controls for needed collaboration policies
  - lack of convenient, scalable, strong authentication
  - inadequate security mechanisms for new technologies

Present State - 2

- Lack of effective means for detecting the exploitation of these flaws and weaknesses, both tactically and strategically
- Lack of controllable, graduated responses to such exploitations

Present State - 3

- Inadequate methods and tools for design, development, analysis, and evaluation of systems that can satisfy stated security requirements, including
  - Design methods for system security
  - Design methods for effective human interfaces to security mechanisms
  - Commercially viable methods for developing and implementing security mechanisms
  - System engineering and evaluation tools that support explicit evaluation of tradeoffs among security design alternatives and permit prediction of security behavior of large-scale systems

Trusted Computing Program Goal

- Create and sustain the science and technology needed to
  - discover
  - develop
  - deploy

  strong security and privacy methods and tools
- Educate a new generation of researchers and specialists to meet demands for skilled workforce

TC Program Identified Research Areas - 1

- Component technologies:
  - what specification, design, development, test, verification methods can provide quantifiable assurance that specified properties are met?
- Composition (and decomposition) methods:
  - how can components be assembled into subsystems and systems with known and quantifiable trustworthiness?
- Methods for maintaining trustworthiness as systems adapt and evolve.

TC Program Identified Research Areas - 2

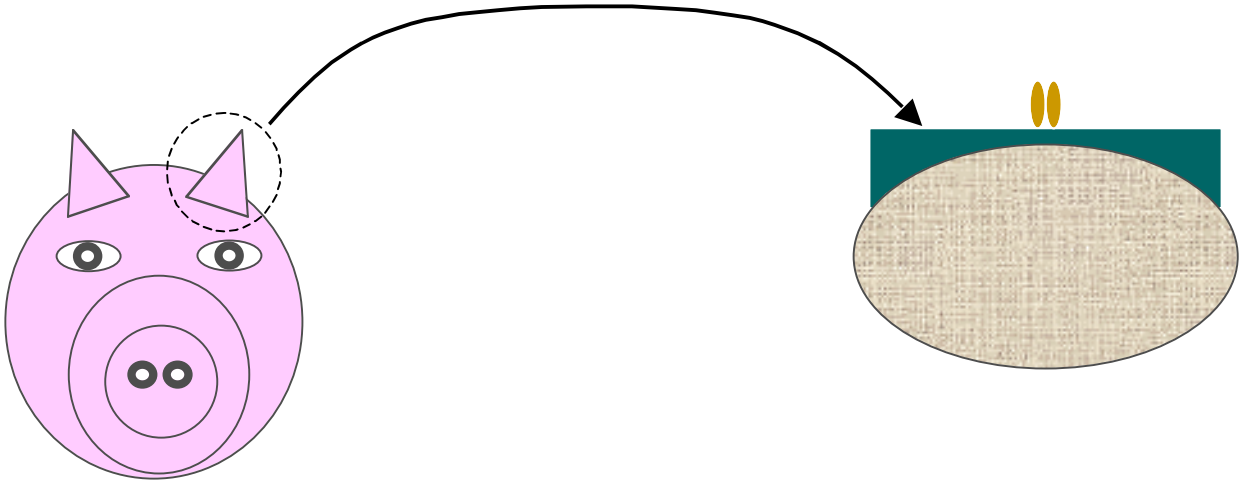
- Methods for improving human understanding of critical system behavior and control:
  - How can system trustworthiness be visualized, particularly for operators of critical systems, including those that are geographically distributed?
- Methods for assessing tradeoffs in trustworthy system design, for example between security and performance.
- Techniques for modeling, analyzing, and predicting trust properties of systems and components.

TC Program Method

- Fund innovative research in all aspects of secure, reliable information systems, including methods for assessing the trustworthiness of systems
- Continuing program with annual announcement
- Initial funding $4-$6M / year
- Initial proposal deadline: 5 December 2001
- Received more than 130 proposals (!)

In this way, develop, support, sustain university faculties and facilities to train the needed workforce

The ultimate challenge?



- Make a silk purse from a sow's ear, or:
- Make dependable systems from COTS