DESSEC

DEsigning a Secure Systems Engineering Competition

Revolution through Competition?

An experimental approach to a dependable cyberinfrastructure

Flashback
2003: Dancing Pigs and Robot Soccer

- “Every day in every way my job gets easier and easier”
  -- Earl Boebert, commenting on system penetration exercises, ca. 2003

Robocup Soccer 2002: held in baseball stadium, Fukuoka Japan

188 teams, 1004 participants, 117,000 spectators

What is the problem?

- Not that there are attackers
- But that our systems are full of holes
- Underlying problems
  - we don’t use sound building blocks
  - we can’t measure (in)security
  - we don’t know how to build manageable, usable, extensible large scale systems with sound assurance arguments
  - our workforce is not properly prepared to succeed at these tasks

We've been working on this problem for nearly 40 years

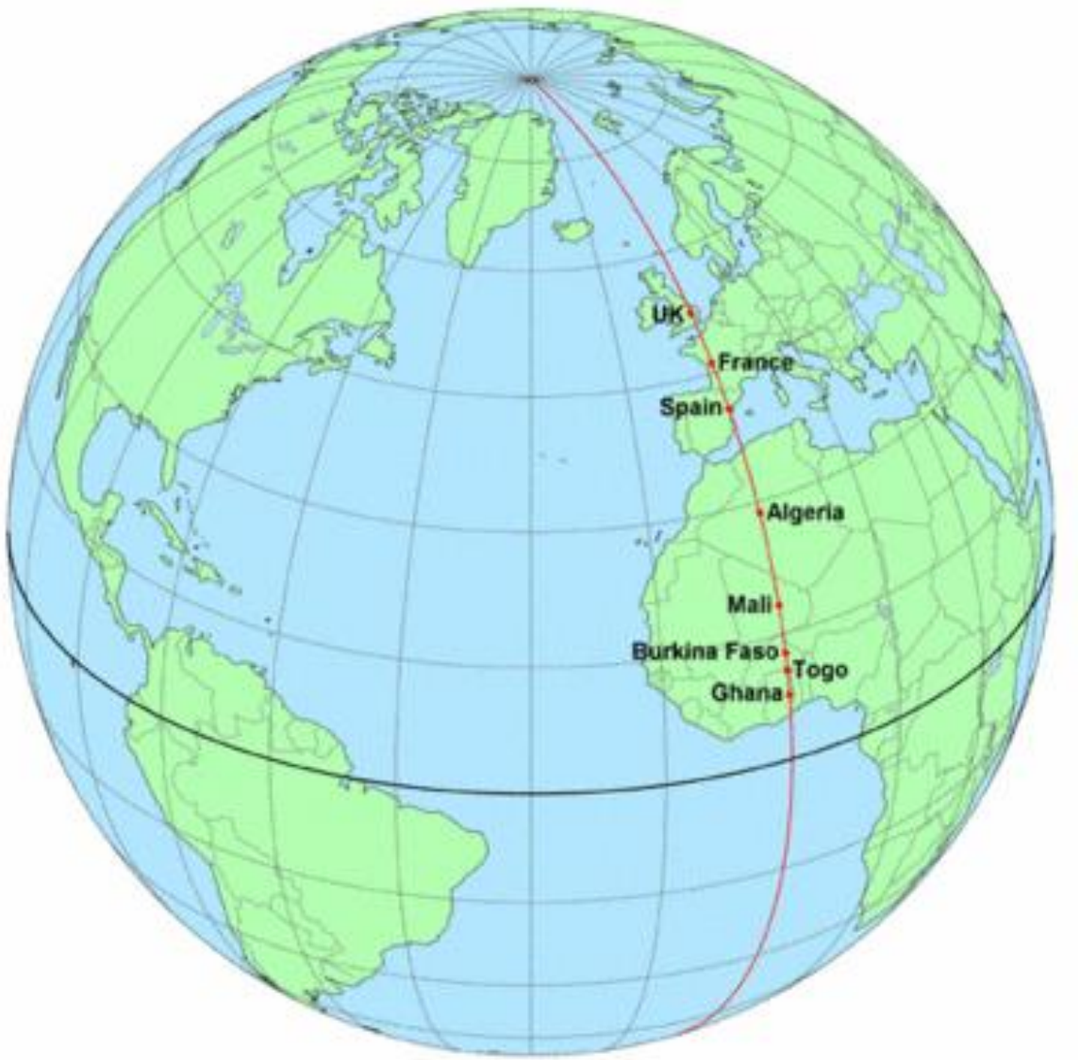
- Security industry focused on band-aids: virus scanners, intrusion detection, recovery, forensics
- Research community often looking at the science of band-aids
- How to
  - reinvigorate research community
  - attract strong students
  - educate students to produce systems with fewer vulnerabilities
  - learn how to build usable, manageable, extensible systems of significant scale with sound assurance arguments

Florence, 1418+

- Vaulting the dome of Santa Maria del Fiore

Finding the Longitude

- 1714: British Parliament offers £20,000 prize to find the longitude




SOLAR DECATHLON
A DESIGN COMPETITION FOR HOMES
POWERED BY THE SUN
AIA
NAHB
diy
Sprint
NREL
HORIZON
Entertainment

ACM International Programming Contest

- Solve 8 to 11 problems in 5 hours in Java, C, C++

- 3 people, 1 computer

- Global, 22,000 students, hundreds of institutions

National Collegiate Cyber Defense Competition

- Up to 8 students per team
- Small business networking scenario, common configuration
- Keep services alive over 3 day contest period
- Regional competitions, national finals

Many other examples ...

(McKinsey “And the Winner is ...” report lists 14 pages of prizes, from the Abel Prize for Mathematics to the Zayed International Prize for the Environment)

Kremer Prize:
Gossamer Condor

DARPA Desert Challenge

2009 McKinsey report on prize competitions:
Core Design Questions

Defining Participants
• What will be the composition of the **candidate pool**?
What qualifications will participants require?
- open
- CV-driven
- Financial
• Does competition admit individuals, teams, both?

Setting the award
• What will be the **incentive structure**?
- Monetary -- cash, further investment, winner-directed grants, etc.
- Non-monetary -- a physical award, networks, publicity, experience, etc.?
• How many winners will there be?
- Will there be multiple categories of award?
• What size will the cash award be?

Determining participant rights
• What are the rules for existing **intellectual property** or that developed during competition?
- e.g., competitor-owned, sponsor-owned, licenses, public domain
•Are there legal issues to address?
- e.g., master team agreements, indemnification, media rights
• Will there be **sponsors** for the award, process, or competitors?

Setting the Rules
• What will be the winning **criteria**?
- Objective vs. subjective balance
- Application: First to complete, best of a group at deadline, all entries above a set bar, hybrid?
•What is the **staging and timing** of competition?
- Single round or multiple rounds (e.g., screening, short-lists, interim prizes)
- What is the duration, cut-off date?
• Will **collaboration** be encouraged and how?
- e.g., in the team formation process, idea-sharing during competition, etc.?

Secure System Engineering Competition: Overarching Goals

DEsigning a Secure Systems Engineering Competition

- Learn how to build usable, manageable, extensible systems of significant scale with sound assurance arguments

- Reinvigorate and refocus the research community:
  - Cathedrals, not band-aids
  - Foster academic - industry - government collaboration,
  - Attract strong students

- Develop the skilled workforce needed to build the trustworthy cyber infrastructure 21st century applications demand

Elements of a competition specification

DEsigning a Secure Systems Engineering Competition

1. A specification of a system to be built, at a reasonable level of detail, including usability and manageability goals

2. A definition of the security to be provided by the system

3. A definition of the threat environment in which the system is expected to operate

4. A method for evaluating what is built against the specification, (the form of an assurance argument might be specified, for example)

5. A description of how an extensibility challenge can be posed

6. A method for evaluating the extended system (may be the same as (4))

7. A list of potential supporting tools and resources that could be made available to competitors

8. An estimate of the level of effort (number of person years) that might be required to produce an entry

DESSEC Workshop Preparations

DEsigning a Secure Systems Engineering Competition

- Workshop announced fall 2009; candidate competitions due December; Charles Palmer (I3P, Dartmouth, IBM) as chair, with support from Martha Austin and Nicole Hall Hewitt
- About 20 competition ideas received and reviewed
- Track leads: Anup Ghosh, GMU; George Cybenko, Dartmouth; Ben Cook, Sandia
- Numerous telecons to organize. Three tracks: Foundational Secure Components (Ghosh), Secure System Implementation (Cybenko), and Workforce Development (Cook)
- Participants invited, wiki set up in advance, registrants selected track preferences
- Workshop held at Washington Duke Inn, Raleigh, NC April 6-8 2010
- Keynotes from:
  - Carl Landwehr: “History and motivation”
  - Eileen Bartholomew, X-Prize Foundation: “The winning team will...”
  - Nick Weaver, ICSI: “‘Build-it’ competitions vs. ‘skills-based’ competitions”
  - Alan Paller, SANS: “U.S. Cyber Challenge can attract people we don’t otherwise reach and get them on our side”

53 DESSEC Participants

DEsigning a Secure Systems Engineering Competition

- Susan Alexander, ODNI
- Lee Badger, NIST
- Eileen Bartholomew, X-PRIZE Foundation
- Jennifer Bayuk, Stevens Institute
- Terry Benzel, USC ISI
- Daniel Bilar,U. New Orleans
- Bob Blakley, Gartner
- Earl Boebert
- Lawrence Carin, Duke University
- Ramaswamy Chandramouli, NIST
- Alessandro Coglio, Kestrel Institute
- Ben Cook,Sandia
- Douglas Creager, RedJack LLC
- Rob Cunningham, MIT Lincoln Lab
- George Cybenko, Dartmouth
- Drew Dean, DARPA
- Anand Ekbote, Emerson Network Power
- Jeremy Epstein, SRI International
- Eduardo Fernandez, Florida Atlantic U.
- Darlene Fisher, NSF
- Anup Ghosh, George Mason U.
- Cordell Green, Kestrel Institute
- Steven J. Greenwald, Consultant
- Tim Hahn, Rational / IBM
- Joseph Lorenzo Hall, UCB /Princeton
- Jeff Hughes, AFRL/WPAFB
- Cynthia Irvine, NPS
- Carl Landwehr, U. Maryland
- Wenke Lee, Georgia Tech
- Doug Maughan, DHS
- Brad Martin, NSA
- John McHugh, RedJack and UNC
- Rick Metzger, AFRL/Rome
- Jelena Mirkovic, USC ISI
- Sanjai Narain, Telcordia
- Charles Palmer, I3P, IBM
- Chuck Pfleeger, Pfleeger Consulting
- Shari Lawrence Pfleeger, RAND
- Declan Rieb, Sandia National Laboratories
- Roger Schell, Aesec Corporation
- Adam Shostack, Microsoft Trustworthy
- Jon A. Solworth, U. of Illinois at Chicago
- Jason Syversen, Siege Technologies
- Andras R. Szakal, IBM Software Group
- Dan Thomsen, Sandia
- Kevin Thompson, DHS
- Jonathan Trostle,Johns Hopkins U.W.
- Konrad Vesey, IARPA
- Giovanni Vigna, UCSB
- Grant Wagner, NSA
- Cliff Wang, ARO
- Nicholas Weaver, ICSI
- Mary Ellen (Mez) Zurko, IBM

DESSEC Results

DESSEC
DEsigning a Secure Systems Engineering Competition

- Each track produced 2 or 3 competition specifications:
- Foundational Security Components
    - Secure Development Tool Chain
    - Private Data / Public Stations
    - Security Tricorder
- Secure System Implementation
    - Voting Systems
    - Security-Enhanced (SE) Facebook
- Workforce Development
    - Cyber Cup
    - Cyber Village
    - The Weakest Link
- Final report currently in preparation; Wiki not yet open to public

LEGACY LINE

Foundational Security Components

Secure Development Tool Chain Competition

DEsigning a Secure Systems Engineering Competition

- The winning team will build a chain of tools that allows non-security-expert developers to rapidly build a significant application (eg. minimal email server or simple on-line database) with zero vulnerabilities as detected by an extensive public test suite

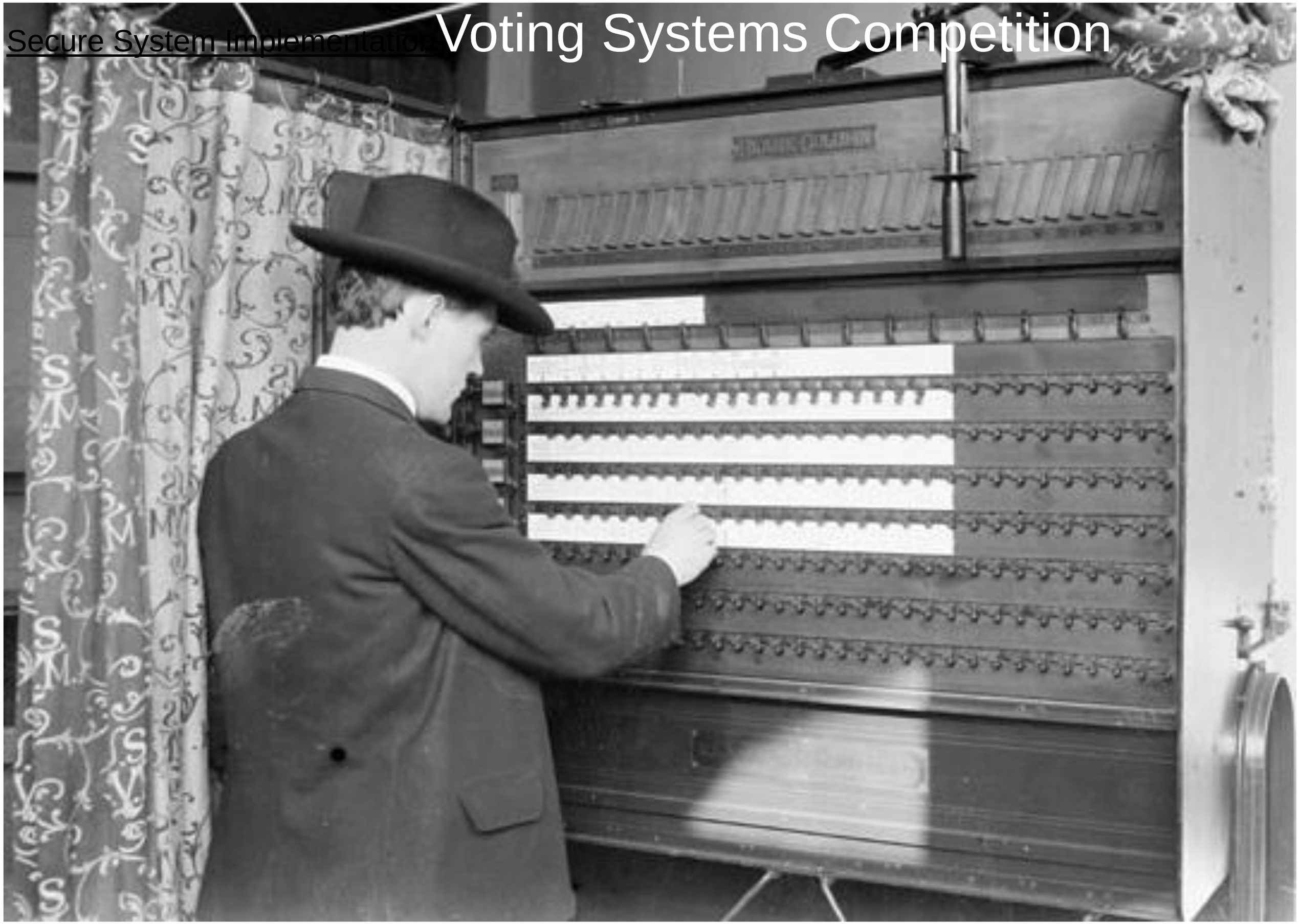
- Two-phase competition planned:
  - Initial phase produces tool chains suited to expert users (e.g., command line interfaces, noisy output). Success = “provisional win”
  - Second phase: produce tools suited for non-experts usable on similar (but not identical) problems. Success = “final win”

- Tool inputs: code libraries, software design diagrams, security models / properties; source code; code annotations

- Tool outputs: source code; design-level structure of the module (submodules, dependencies, call trees); binaries/bytecodes; lists of achieved security properties; lists of flaws that are not ruled out (but may be flagged)

Secure System Implementation

Voting Systems Competition



Secure System Implementation

Voting Systems Competition

DEsigning a Secure Systems Engineering Competition

- The winning team will produce a secure voting system suitable for use in U.S. Federal elections, composed from existing high-assurance components.

- Candidate submits: Design documentation, source code, artifacts, rights for third-party to duplicate, modify andproduce the system in a commercial integration context

- An assurance argument demonstrating the required (see below) security properties are achieved by the system

- Security properties (to be specified in detail) include: ballot confidentiality, integrity of vote data, integrity of software, secure initial state, auditability of vote totals, forensic logging capability, automatic recovery, secure recovery, trustworthy update process, availability, usability, physical security

- Threat environment and other details in report

Workforce Development

Cyber Cup Competition

Workforce Development

Cyber Cup Competition

DEsigning a Secure Systems Engineering Competition

- Think “America’s Cup” sailing competition: this year’s winner must defend next year’s challenger
- Initialization: Referees set up target system providing a real service and create long-term development plan for incremental evolution of services over rounds of the competition
- Competition round has defender and challenger(s).
  - Challengers negotiate an attack objective that will violate key elements of system’s “rules”; plan includes objective metrics for success.
  - Referees approve/require revision to attack plan.
  - Challenger initiates approved attack.
  - Attack fails --> negotiate new attack plan.
  - Attack succeeds: Challenger must implement new referee-selected functions (with expert mentor, provided) and becomes defender in next round.
- The idea is to both train the teams and learn how to design systems in which functions can be added safely
- Overall metrics (vs. attack metrics) will focus on evaluating the educational aspects: number of participants, number of successful attacks, how long average defender stands, value of mentor relationships

What's Next?

DEsigning a Secure Systems Engineering Competition

- Complete the report
- Publicize the results
- Refine and detail the definitions and rules
- Seek sponsors/participants

Thank You

Carl Landwehr
Director, Trustworthy Computing Program
National Science Foundation
clandweh@nsf.gov