Exceptional service in the national interest

Sandia National Laboratories

Piloting a Secure System Design Competition

Ben Cook on behalf of the FIREAXE Team

Adam Anderson, Mitch Adair, William Atkins, Alan Berryhill, Dominic Chen, Ben Cook, Jeremy Erickson, Michael Z. Lee, Steve Hurd, Ron Olsberg, Lyndon Pierson, Owen Redwood, Yevgeniy Vorobeychik

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2012-10175C

Origins of a Secure System Design Competition for Students

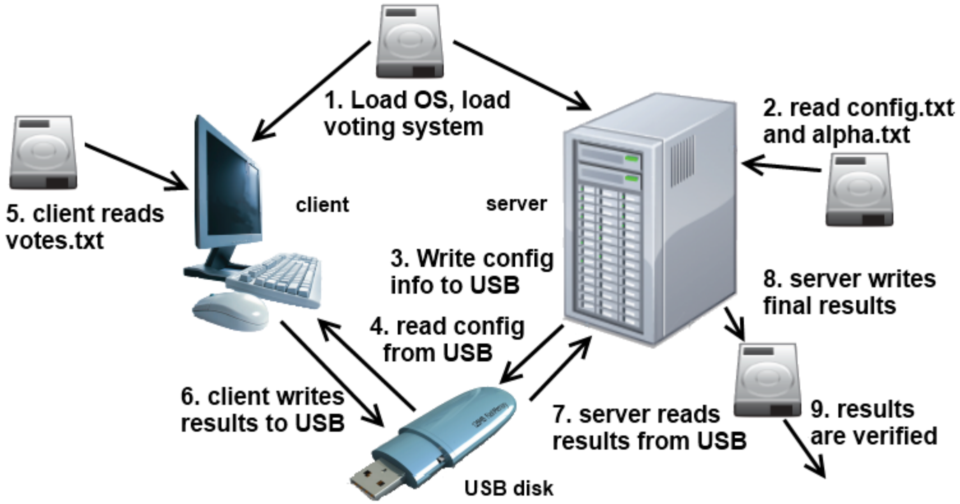
- April 2010 at Carl Landwehr's Designing a Secure Systems Engineering Competition (DESSEC) Workshop
- DESSEC's Workforce Development track identified needs and potential competition "specifications"
  - Considered how to attract, motivate, inform, and educate students in cyber security
  - Acknowledged significant gap in secure design education
  - Highlighted importance of adversarial mindset, understanding of "lore", ability to convert attack knowledge to robust defense, and confidence to take on real-world system engineering problems
  - Produced several loosely developed competition ideas: *Cyber Cup*, *Cyber Village*, *Cyber Scouts*, *Weakest Link*
- In late 2010 Doug Maughan at DHS S&T endorsed CCD pilot

The Competition Setting: Sandia's Center for Cyber Defenders (CCD)

- CCD is a highly selective, applied research internship institute at Sandia's New Mexico and California sites
  - Hosted 30 undergraduate and graduate students in summer 2012 from about 20 universities (selected from over 300 applicants)
  - Offers collaborative, threat-informed, project-based internships in cyber security
  - Contributes enabling solutions to real national security R&D projects in cyber security: examples include control system modeling, network situational awareness, protocol analysis, digital forensics, and red teaming

The Competition Specification: A Stylized Electronic Voting System

- Designed to help students identify and internalize security principles
- Assumed realistic but limited threat model
- Clearly (or so we thought) spelled out specification including requirements, rules, and evaluation and scoring procedure


1. Load OS, load voting system
2. read config.txt and alpha.txt
client
server
5. client reads votes.txt
3. Write config info to USB
4. read config from USB
8. server writes final results
6. client writes results to USB
7. server reads results from USB
9. results are verified
USB disk

EVS consists of a server (election management system) and client (voting station) with sneakernet USB for data transfer

Competition Structure and Results

- Competition structured into multiple rounds each having a distinct *design* and then *red team* phase
  - "Design and red team" iterative structure was chosen to cultivate and integrate adversarial mindset into an evolutionary design process
  - Pilot included two, three-person student teams and white team for oversight
  - Constrained red teaming to predefined attack scenarios with either user- or root-level access
- Students produced two substantially different designs
  - NM team focused on customizing the kernel and produced very small, highly restricted OS, while CA team implemented limited user shell and "red pill"
  - Teams choose different development platforms, tools, and crypto libraries

Observations

- Students improved their understanding of and ability to articulate secure design principles
  - Reduce attack surface
  - Use existing tools
  - Enforce policies at lowest level
  - Defense in depth
  - Prevent easy access
- Specification of an effective competition is nontrivial: despite extensive pre-work, numerous ambiguities surfaced and unanticipated issues arose
- Competitions are great motivator… this was billed as research project but students were quick to forget

What's Ahead?

- Scale and sustain competition
  - Need to automate evaluation and find partners
- Experiment with different formats and themes, e.g.,
  - Could competition be used to familiarize students with new technologies and accelerate adoption?
  - What are realistic expectations with respect to innovation versus education?

Gratefully acknowledge DHS S&T – Doug Maughan and Ed Rhyne – for their funding and encouragement

and

Special thanks to Jeremy Epstein and Carl Landwehr for their technical guidance

More info…

DESSEC Workshop Report produced by I3P

www.thei3p.org/docs/publications/410.pdf

ACSAC Poster Session next week

Upcoming CSIIRW presentation and paper,

FIREAXE: The DHS Secure Design Competition Pilot

Connect with Sandia's technical leads:

Eugene Vorobeychik, yvorobe@sandia.gov

Will Atkins, wdatkin@sandia.gov