The Center for Cyber Defenders
Expanding Computer Security Knowledge

FIREAXE

Forging Impervious and Resilient Entities for Adversarial Execution Environments

Project Mentors: Will Atkins, 5627; Yevgeniy "Eugene" Vorobeychik, 8953

NM Team: Adam Anderson, University of Nebraska at Omaha; Daming Chen, Arizona State University; Michael Lee, The University of Texas at Austin

CA Team: Robert Adair, The University of Texas at Dallas; Alan Berryhill, University of California, Berkeley; W. Owen Redwood, Florida State University

Problem:

Application security is a crucial problem in today's technological society. Currently, there does not exist a place for discovering and testing secure design principles in an isolated environment. There also does not exist a venue where students can put theory into practice and further their education.
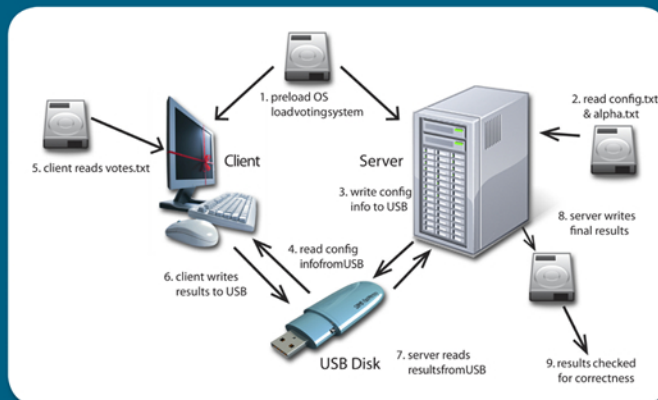
Approach:

Competition provides an environment for participants to think about security and implement secure design principles. Limiting design space and attack surfaces creates a tractable problem for teams to try many different tactics for defense and attack.

Trial Competition:

This scenario asks the design teams to create a mock electronic voting system following a simple specification. Two teams, one in New Mexico and one in California, participated in two rounds of design and attack.

Blue Team:

The design team needs to account for multiple attack scenarios at different privilege levels and access points. Real world attack scenarios also need to consider vectors like hardware access and network attacks.

1. preload OS loadvotingsystem
2. read config.txt & alpha.txt
3. write config info to USB
4. read config infofromUSB
5. client reads votes.txt
6. client writes results to USB
7. server reads resultsfromUSB
8. server writes final results
9. results checked for correctness

Client — Server — USB Disk

The high level representation of the client and server interaction in the trial scenario.

Red Team:

The attacking team gets full access to both the source code and running system of the opposing design team. They are given a small amount of time to create attacks against specific parts of the system.

White Team:

The evaluation team executes the voting systems and attacks. The blue team has time to iterate their design before the next attack phase.

Key Design Takeaways:

– Keep it simple and make it small
– Remove unnecessary functions
– Enforce policies at the lowest level
– Test the final configuration

Contributions:

Testing the initial specification provides early feedback for the competition designers. It also allows the students to apply security principles and discover novel methods and techniques for securing real systems. Going forward, this trial will serve as a model for future competitions.