

Project Ideas for ECE 458

Vijay Ganesh
Winter 2013

Project Guidelines

- Give us the names of your team-members by end of week
- No more than 2 members per team
- A proposal is a must to get a grade (10 % of the project grade)
- Proposals due via the Learn system before Jan 29th, 2013
- Implementation and demo is a must to get a grade (70% of the project grade)
- 5-10 page final report is a must to get a grade (20% of the project grade)

Project Ideas

- **Bio-metric based login mechanism**
 - Phones/Tablets have many more sensors in them than laptops/desktops. Can you build a bio-metric based login mechanisms that leverage this aspect of phones.
- **Create an electronic voting system**
 - Electronic voting is increasingly being used in many countries. Build a “secure” electronic voting system, and discuss the security measures you have added.
- **An arithmetic server**
 - Build a server that accepts request and performs arithmetic computation (basic arithmetic operations such as +, -, *, /, %, and !(factorial). Counter-measures must be implemented to protect against DoS attacks

Project Ideas

- Work with tools like Klee, Blast, C-Cured (bug-finders and model-checkers) to find exploitable bugs
 - Software bugs are often the first step in an exploit. Tools such as Klee help find such bugs. Your goal is to apply these tools to non-trivial software and find some interesting bugs, and propose an exploitation strategy. (Refer papers on Klee, Blast, etc. These tools are open-source)
- Build a SAT solver based system to cryptanalyze hash functions
 - SAT solvers have become so efficient that they can be used to partially automate cryptanalysis. Download a SAT solver and morph it to automate aspects of hash function analysis (refer 2006 paper by Ilya Miranov)

TALK EARLY AND OFTEN ABOUT PROJECT WITH ME AND TAs