Project Ideas

This page lists some final project ideas and resources. We are just collecting ideas tossed out in class. Your specific project still requires approval from the course staff. Also, we prefer that groups work on somewhat distinct topics.

New Topic Ideas

Implement a program to measure the amount of randomness available in a system

> Many systems assume a source of randomness to generate cryptographic keys. Without a source of good randomness, keys are extremely easy to guess. The default Linux random number generator gathers randomness from IDE disk events and mouse/keyboard I/O. On headless server machines with SCSI disks locked in hosting centers, there may be little or no randomness. Can you measure the effectiveness of random number generation? Develop a suite of tests to determine how fast randomness is exhausted?

Peer-to-Peer Security

Anti-spam techniques

Sample Topics

- SEC: SSH like client
- A Secure Media Distribution Framework
- How to Make the User Authentication Process in MS Passport More Secure
- Blinded Distributed Computing
- Security of Wireless Networks and Mobile Devices
- Cracking Digital Satellite TV
- User Authentication in Cryptographic File Systems
- Steganography in Spam
- Proactive Cryptography Applications in Smart Cards
- Execution-Based Software Protection
- Steganography in TCP timestamps
- Rethinking Software Piracy: Active Software Rights Verification for Effective Control of Piracy
- Reputation-Based Certificate Authorities
- Cookie authentication
- Analyzing the Security of 802.11 Wireless Networks
- Threshold Signatures and Open Source
- Honeypots
- Security and Privacy Issues of Microsoft Passport
- Security Aspects of Unicode
- Digital Signatures for Physical Mail
- Differential Fault Analysis of RC5
- Secure Instant Messengers
- A Review of AES Candidates
- A Payword Implementation
- An Analysis of TIMEBOMB
- Purple: Japanese ciphers in WWII
- Identity Theft
- Approaches to MIXNets
- SmartCards: Back from the Dead
- Payment via GSM Mobile phones
- Digital Multimedia Copyright Protection
- Security Analysis of Electronic Postage Systems
- Security of Network Attached Storage

- Software Bugging
- Design of a secure Pilot-based Authentication System
- Intrusion Detection Systems
- Cellular Telephone Security
- A Computer Testing System
- Copyright Protection Mechanisms in DVD + DIVx
- CGI Security Issues
- Network Access Controls
- Digital Money-- Fault Tolerant Multibank System
- Security Policy Models
- An Overview of Biometric Technologies and their Real World Applications
- Netbook
- Secure Sockets Layer 3.0: Overiew and Analysis
- Secure Perfectly Forward Secure Email Wizard
- Cryp: An All-or-Nothing Encryption Scheme for Secure Multi-user Information Distribution
- Frosty the Random Number Generator
- Impact of Quantum Theory on Cryptography
- Cartemis:Secure Electronic Wallet Technology
- Preventing Media Piracy
- Netscape's "What's Related" Service and Privacy/Security Issues
- Secure Electronic Poker
- PGP vs S/MIME
- A Study of SSH
- ATM A trusted machine?
- Secure Mobile Code Framework
- Pseudonyms and Credential Transfer
- Electronic Payment Schemes
- eCheck:A Safety-Oriented Electronic Check Scheme
- Computing with Encrypted Data
- Receipt-Free Secure Elections
- A well-hidden module for remote control of Linux machines
- The feasibility of quantum computation
- Network Security for Chat Programs
- Electronic Voting
