

Submission Policy: Group of two-three students could work together and make only one submission/demonstration. You need to give a demonstration of your code during PSO hours (1:30-3:20PM) October 9, 2009. Compilation errors would receive 0 points. A demonstration would include explaining the code first, then compilation, then showing execution on inputs as required by the TA.

Secure Audit Log

Description: In many real-world applications, sensitive information must be kept in log files on an untrusted machine. In the event that an attacker captures this machine, we would like to guarantee that he will gain little or no information from the log files and to limit his ability to corrupt the log files. The project requires you to implement a secure audit log. As part of the project you will use basic cryptographic algorithms such as public-key encryption (RSA), symmetric encryption AES, message authentication code (HMAC with SHA1). The protocol you are required to implement is described in the Section 3 of paper Secure Audit Logs to Support Computer Forensics, by Bruce Schneier and John Kelsey and available at <http://www.schneier.com/paper-auditlogs.html>. You are required to use the openssl cryptographic library: openssl (www.openssl.org).

Your program should take "audit filenames" as inputs.