ECE: Intro. to Information and Network Security
The Big Project
Spring 2006

Project Description

In this project, your team (consisting of at most two students) will attempt to *crack* an encrypted document. Often, there are other sources of information available for breaking an encrypted document than just the ciphertext. One key example, is a dump of memory where key information is believed to be stored.

In this project, I will provide for you two different files. One file is an encrypted content file (specifically, it is a .gif file), as well as a dump of memory that contains a region where encryption keys have been stored. You are to *cleverly* search the dumped memory in hopes of finding the key needed to decrypt the content.

One approach you might take to looking for the key is to scan the memory dump and look for regions of higher than normal entropy. Since keys are typically made up of random bits, a region containing the key should yield high entropy.

Project Specifics

Ciphertext : An encrypted gif file encrypted using AES and a 128 bit key.

Memory Dump: An approximately 1 MB file generated using arbitrary chunks of several files of different types. This file has the encryption key hidden in it as part of a block of 480 random bytes. This random block could represent, for example, an area of contiguous memory where a program stores several keys for different applications or services. The entire random block, including the key itself, is a random string of bits obtained from HotBits, which uses the radioactive decay of a Krypton-85 capsule as its source of randomness. (http://www.fourmilab.ch/hotbits/how.html).

Both files are available on the course web page (or soon will be).

Your mission should you choose to accept is to find the key and decrypt the gif file. (Tip: If the first 3 characters in the decrypted file are "GIF", then most likely you have decrypted the file successfully). To decrypt the file you should write your own routine using publicly available AES implementations.

You are allowed to write this program in any language you choose. Java is a natural choice since it provides crypto libraries. However, this is by no means the only choice. One can search to find crypto libraries for C/C++, or even languages like Perl, Python, Ruby, etc.

You should work in teams of 3-4 people. Although it is very easy to break the encryption using a full search of the memory dump, this is not considered a solution to the project, but rather as a starting point. Your task is to refine your solution: make it faster, more clever, etc. In reality, the memory dump could be terrabytes long rather than 1MB, and hence careful engineering of the solution is necessary. A well-done, complete project would involve a thorough treatment of the problem, and a report (10 pages) that details failed strategies, the refinements that were used to improve the strategy, as well as why these strategies were chosen. The report must also contain a printout of the decryption of the GIF file.