CS 444/544 Spring 2017 Lab 2

Lab 2 is due by 11:59pm on Monday, 20 March 2017.

Submit your lab as an email to crandall@cs.unm.edu. You must include two things in the email, or your lab will not be graded:

- The plaintext message that corresponds to the ciphertext for the keyID assigned to you specifically. Send this in the body of the email, with characters that do not display readily in email bodies escaped, *e.g.*, "\t" for tab, "\n" for newline, *etc*.
- A gzipped tar ball of your source code for carrying out the attack. The extension should be *.tgz and the `file` command in Linux should report the format of the file as "`gzip compressed data`". Your tar ball should be no more than 1MB.

Lab 2 is worth 100 points, all or nothing. If you fail to include your source code as a tar ball, or your plaintext does not match the plaintext that was encrypted using the keyID specifically assigned to you as a student, then you will get 0 points. I won't grade your source code for style, *etc*., and I won't attempt to run it. The source code is a fallback if I suspect any students of cheating.

You are expected to do your own work. From writing the source code to carrying out the attack, it should be an individual effort carried out only by you. Any instance of not doing your own work will be considered cheating. You are encouraged to discuss the assignment with your classmates at a high level. Exchanging publicly available source code that existed before the assignment was assigned, and thoughts about approaches to specific problems is okay. It is also okay to go through attack examples together at a high level (*e.g.*, pencil and paper), but do not share any concrete info (such as a network capture) about any specific attack. As a reminder of the course policy, if you cheat on any assignment in this class including this assignment (cheating includes, but is not limited to, representing somebody else's work as your own or fabricating files or text to make it look like you completed the assignment) you will receive an F in the class. Every student's keyID, key, and plaintext are unique, and you should not extract the ciphertext or attempt to recover the plaintext of any other student. You may use the Python code (written by Brandon Lites and Nidia Yadira Vaquera Chavez) provided as part of the tar ball for the assignment however you like without restriction (*e.g.*, you can run your own server locally for testing, you can write your own script that calls client.py, you can borrow from the provided code or turn it into a library, use at as a starting point for your own code, or whatever).

Your mission, should you choose to accept it (the drop date with Dean's permission is April 14th) is to extract the ciphertext corresponding to the keyID that will be assigned to you, and then use a CBC padding oracle attack to recover the plaintext that corresponds to your ciphertext. The server is listening on ports 10000-10060 on shasta.cs.unm.edu, but you must only use the port that was assigned to you. You are not limited in the number of queries you can submit to the server, but please be respectful of the resources. If you need more than on the order of tens of thousands of queries to complete the attack, then you're doing it wrong. Any kind of denial-of-service attack or other attack on shasta.cs.unm.edu itself is not authorized.

A unique student number, that corresponds to your keyID, will be assigned to you. Do not extract ciphertexts that weren't assigned to you or connect to ports that weren't assigned to you. The TA used port 10000 for all keyIDs to make the provided ciphertext, and the README.txt refers to port 10000,

but since none of you are student 0 nobody should actually connect to port 10000 on shasta. You should always connect to port 10000 plus your student number. For example, if you are student number 55, you will always only connect to port 10055 on shasta. Connecting to ports not assigned to you will be considered cheating (because you're interfering with other students' ability to complete the assignment). Extracting ciphertexts, or asking any oracle for information about the corresponding plaintext , for any ciphertext not assigned to you will also be considered cheating (because there is no reason to do this unless you are doing someone else's assignment). Honest mistakes will be forgiven, but still be very careful to only work with your own ciphertext and your own port. Do not share your assigned ciphertext, plaintext, or keyID with anyone else.

To be clear:

- The ciphertext assigned to you is the one where the keyID is exactly equal to the student number assigned to you for this lab.
- The port assigned to you on shasta is 10000 plus your student number.
- Your student number should be kept secret and only shared with the instructor and the TA, do not tell other students what your student number is or let them see your port number or ciphertext.