Project Milestone
Rubberhose
John Craig
Professor Aaron Kippins
Security Algorithms
April 11, 2022

Rubberhose, also known as Marutukku, is a cryptographic filesystem defined to defend against so-called “rubberhose” cryptanalytic attacks; that is, rather than being in possession of plaintext or ciphertext and attempting to break the encryption itself, an attacker in possession of the individual who knows the keys, and attempts to compel them to surrender them through various means-- namely, torture via rubberhose.

Marutukku provides a solution to this form attack through deniable encryption. An encrypted storage device can be used to store multiple different plaintexts, each of which is split apart and stored sporadically throughout the device with a mapping of its positions. Both the fragments of the plaintext and the mappings are then encrypted; additionally, the remaining space on the drive is filled with cryptographically random data.

When executed successfully this means that any segment of the drive is just as likely to contain meaningful ciphertext as it is to contain meaningless junk. This allows a user to create one or more decoy plaintexts and passwords. The user may then disclose a decoy password to an attacker, and the attacker will have no means of determining whether this password revealed all of the possible plaintext in the device, or only part of it.

At the time of writing I have successfully updated the existing Marutukku codebase so that it will compile and run on a modern Linux kernel. The next steps are to implement the more modern AES cipher into the codebase so that it can be run natively by the program, and also to add support for OpenSSL ciphers in general so that they may be used as a dependency.