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. At this point the plaintext is encrypted, 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.

There is only a minor weakness to this approach: the mappings of each encrypted plaintext (called an “aspect” in Marutukku’s terminology) must be kept as separate files. This means that a user must have a safe place to store them, as both the quantity of these mappings and their content would give an attacker important clues about the ciphertext present on a device. Ideally these mappings would themselves would be among the encrypted contents to eliminate this issue.

Potentially, the password for each aspect could be used to derive an offset into the device at which the encrypted mapping for its aspect would be stored. When a user wishes to unlock the aspect

this offset would be re-calculated from the password, used to decrypt the mapping, and from there the mapping would be used to decrypt the remaining segments of ciphertext.

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, and have begun the process of implementing the AES algorithm. When this is complete the remaining goal will be to add support for OpenSSL ciphers. Past that I may chose to pursue a major modification of the existing remapping system, as detailed above.

Citations

Assange, Julian, Ralf P. Weinmann, and Suelette Dreyfus. "Rubberhose filesystem." *Archive available at: http://web. archive. org/web/20120716034441/http://marutukku. org* (2001).