Name: John Craig

Class: MSCS650 Security Algorithms

Date: March 7, 2022

Project Name: Rubberhose

Rubberhose was a deniable-encryption filesystem originally created by Julian Assange, Ralf P. Weinmann and Suelette Dreyfus. It was intended to be used by journalists and political dissidents who might be in a situation where they were being coerced into surrendering the cryptographic keys for their hard drives, known colloquially as rubberhose cryptanalysis, from which the filesystem got its name.

Rubberhose functions by first filling a hard drive with random data which is indistinguishable from ciphertext. Decoy plaintext and sensitive plaintext are then encrypted with different keys and stored sporadically throughout the hard drive. This allows a user to surrender a key to the decoy data if coerced without also revealing the sensitive data stored on the filesystem.

However, Rubberhose is an outdated project. The most recent iteration was build to run on the Linux 2 kernel, and only makes use of the now-defunct DES algorithm. My proposal for a semester project is to update the project so that it can be run on the latest Linux 5 kernel and makes use of modern cryptographic algorithms such as AES.