

ENCRYPTION WITHIN MAC OS X (Work In Progress)

Michael Graham, Prof. Marcus Thompson
Department of Computer and Information Technology
Purdue University

Abstract

The purpose of this poster is to present the growing practice of data hiding and data encryption on consumer Apple computers. The technique of encryption was once only for government agencies but now is fully integrated into the Macintosh OS X. Hiding data on an Apple computer can be as easy as hiding the file/folder so that an icon no longer appears, or users can enable a 128-bit AES encryption program that is built in.

Background

Hiding personal data on a computer is not a new concept, however the techniques that consumers have available to hide data has vastly increased over the past decade. Encryption is no longer something that only top secret government organizations use to hide sensitive information from foreign spies. Today just about any person can encrypt and hide any information they want. From pictures to text messages to instant messaging and emails, there are ways for people to keep others from seeing what they are doing.

Problem

The growing use of encryption makes it more difficult for analysts and investigators to find evidence on a computer. The ability to recognize encryption and know where to look for latent evidence will be crucial in future investigations.

Encryption Techniques

Full Disk Encryption

- FileVault 2
- Symantec
- McAfee

File Encryption

- Hider 2
- VeraCrypt
- 7-Zip

Methods

- Test three (3) systems with identical images
- Encrypt each system with a different technique/program
- Acquire forensic image of each system
- Analyze to find viable information
- Find evidence that may have been left unencrypted by the file system
- Is this evidence useful in litigation?
- Determine if any encryption technique works better than the rest

