Encryption and Steganography for OS X and iOS Platforms

Gary C. Kessler
Vermont Internet Crimes Against Children Task Force
Gary Kessler Associates
Norwich University

Ryan R. Kubasiak
AppleExaminer.com

June, 2011

http://www.garykessler.net/presentations/

Overview

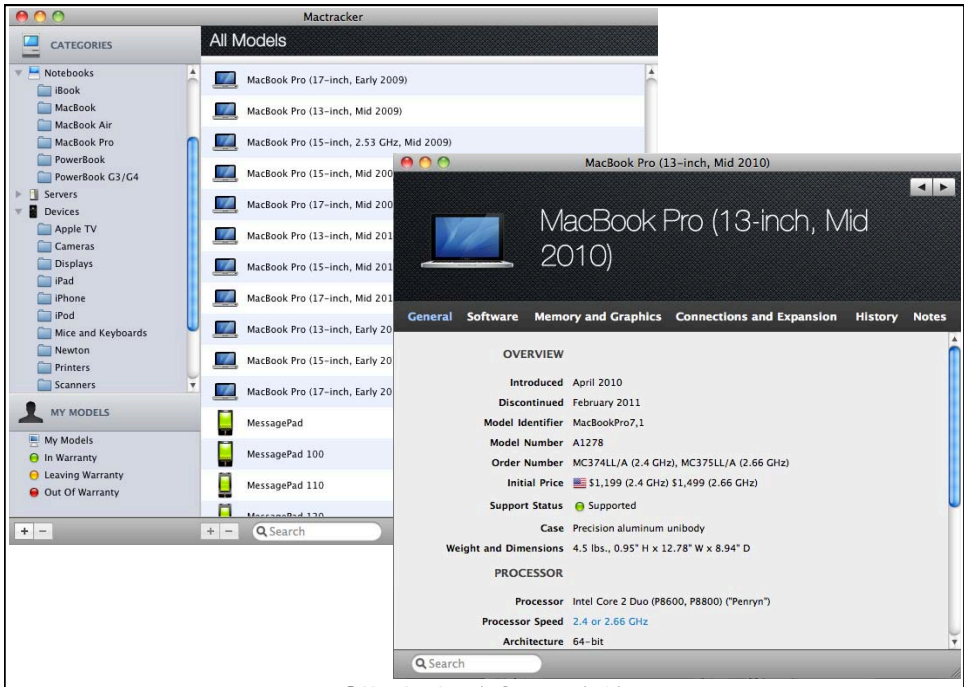
- OS X and iOS overview
- Cryptography review
  - OS X cryptography
  - iOS cryptography
- Steganography review
  - OS X steganography
  - iOS steganography
- Summary

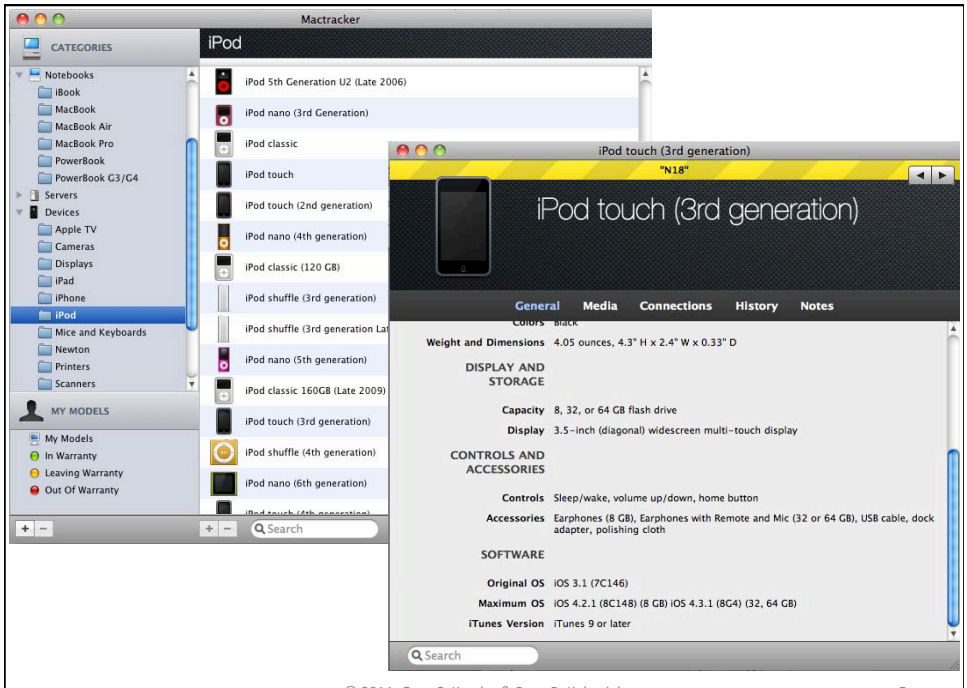
OS X

- Mac OS is a family of GUI operating systems from Apple Corp.
  - Mac OS X (pronounced "oh es ten") is Unix-based
    - "Classic" Mac OS (thru Mac OS 9) was proprietary
  - Code named for cats: Mac OS X v10.0-10.7 called Cheetah, Puma, Jaguar, Panther, Tiger, Leopard, Snow Leopard, and Lion, respectively
- OS X was first Mac OS to allow access to a CLI

iOS

- Mobile operating system based on OS X
- Originally developed for iPhone
  - Formerly known as *iPhone OS*
- Currently also supports iPod touch (iTouch), iPad, and Apple TV (2nd gen.)



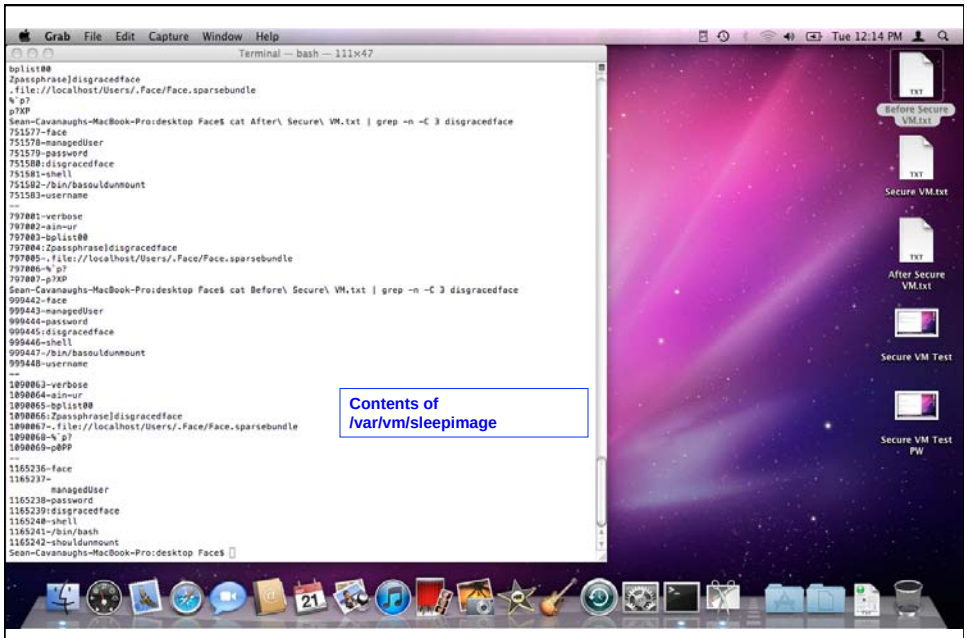


Encryption Basics

- *Cryptography* means "secret writing"
  - Used when communicating over an untrusted medium
  - Protect against unauthorized access to systems and data
- Digital cryptography methods come in three varieties:
  - Hash functions (no key)
  - Secret key cryptography (one key)
  - Public key cryptography (two keys)

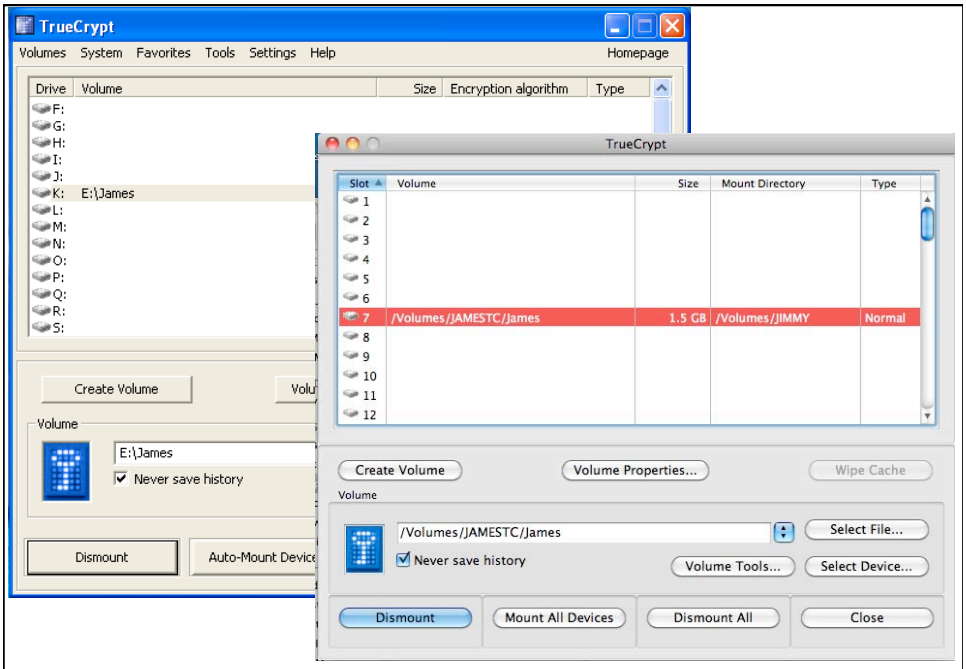
FileVault

- FileVault
  - File encryption function built-in with Mac OS
  - Provides whole-disk encryption (as of OS X 10.7)
    - Prior to 10.7, FileVault only encrypted the user's Home directory
  - Uses AES
  - Password derived from user's login password

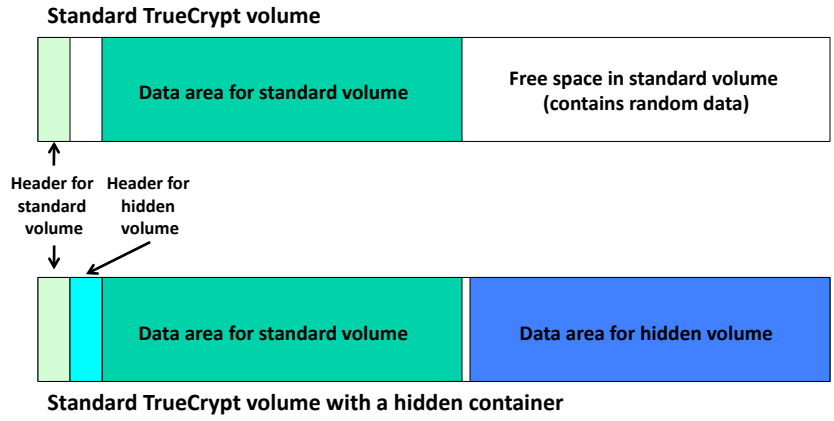


TrueCrypt

- Open source encryption for Windows or Linux
  - Cross-OS compatibility
  - Creates an encrypted volume on fixed or removable media
- Virtual encrypted disk using AES, Serpent, or Twofish
  - Encryption occurs on-the-fly
  - Encrypted TrueCrypt volume appears to be random data
  - Can create hidden encrypted volume (aka *plausible deniability*)

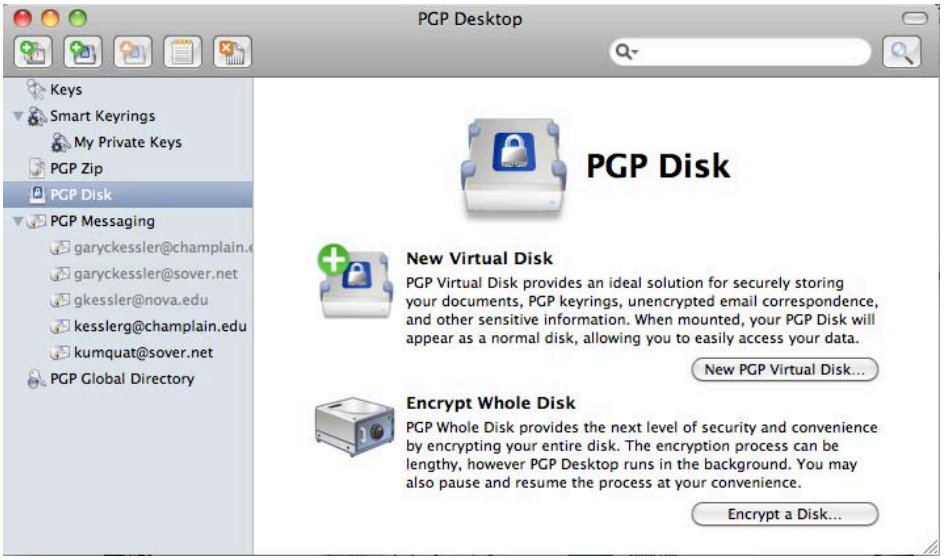


Plausible Deniability



Pretty Good Privacy

- PGP Whole Disk Encryption
  - Version for Mac OS X 10.5 and later, Linux, Windows
  - AES-based
  - Can create virtual encrypted disks or protect entire disk
  - Can sign and/or encrypt e-mail



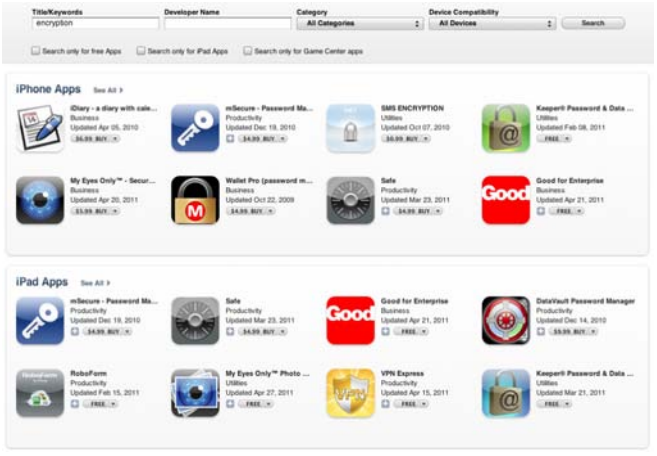
iOS Encryption (Old)

- Early iOS devices (e.g., iPhone thru iPhone 3, iPod Touch) do not encrypt the storage device
- Secure erase on these older models is a true secure wipe taking up to several hours to complete

iOS Encryption (New)

- Later iOS devices (e.g., iPhone 3GS and 4, iPad 1 and 2) have two partitions
  - First partition is read-only, contains only the OS
  - Second partition contains apps, app data, and user files, and is encrypted using a key built into the device's hardware
- Secure erase on these newer devices is a quick process, simply securely wiping the encryption key and rebooting the device

iOS Encryption Apps



Many Apps are available to encrypt data from the App Store

iOS Device Passcodes

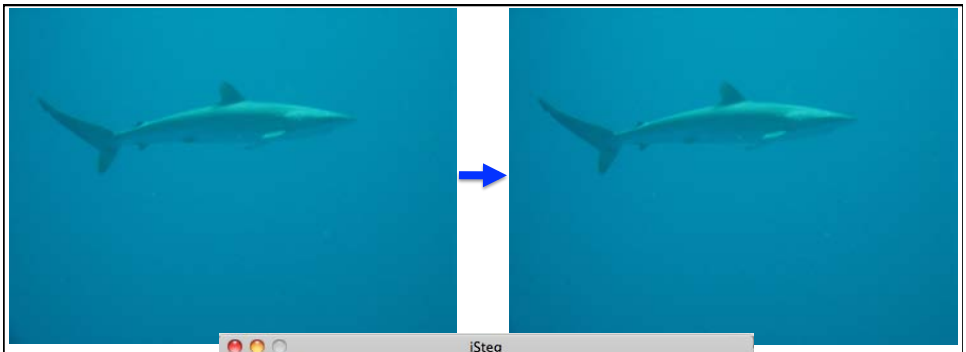
- iOS devices can also be protected with a passcode
- The passcode can be circumvented (or retrieved) from the iTunes device with which the iOS is synched
  - *Lockdown/*.plist* files need to be accessed

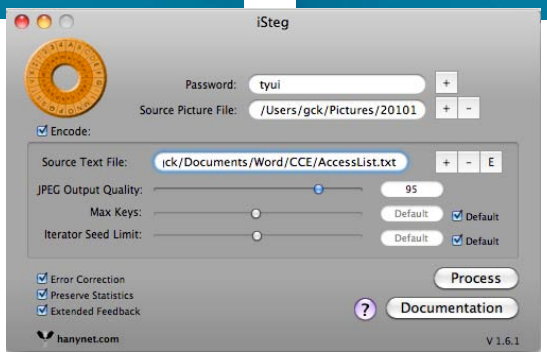
Steganography Overview

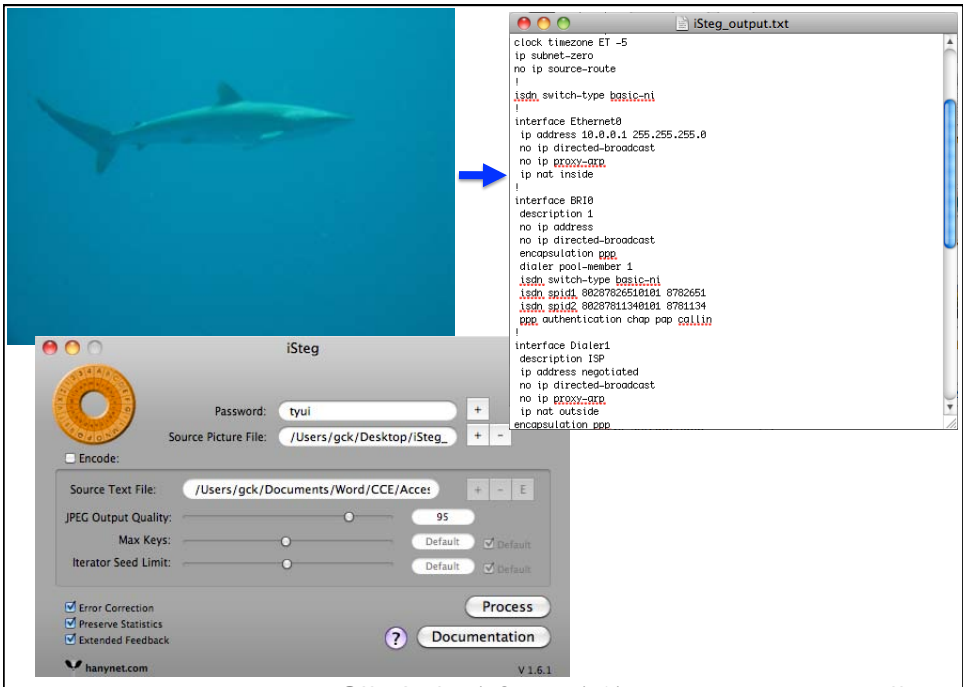
- *Steganography* means "hidden writing"
  - Provides a covert communications channel *in plain sight*
- There are many stego algorithms, including:
  - Least significant bit overwriting (BMP, GIF, PNG, WAV)
  - Encoding algorithm modification (JPEG, MP3)
  - Format modification (Word, text)
  - Covert channels (TCP/IP)

iSteg

- Hides text or ZIP file in JPEG images
  - Also has an encryption function

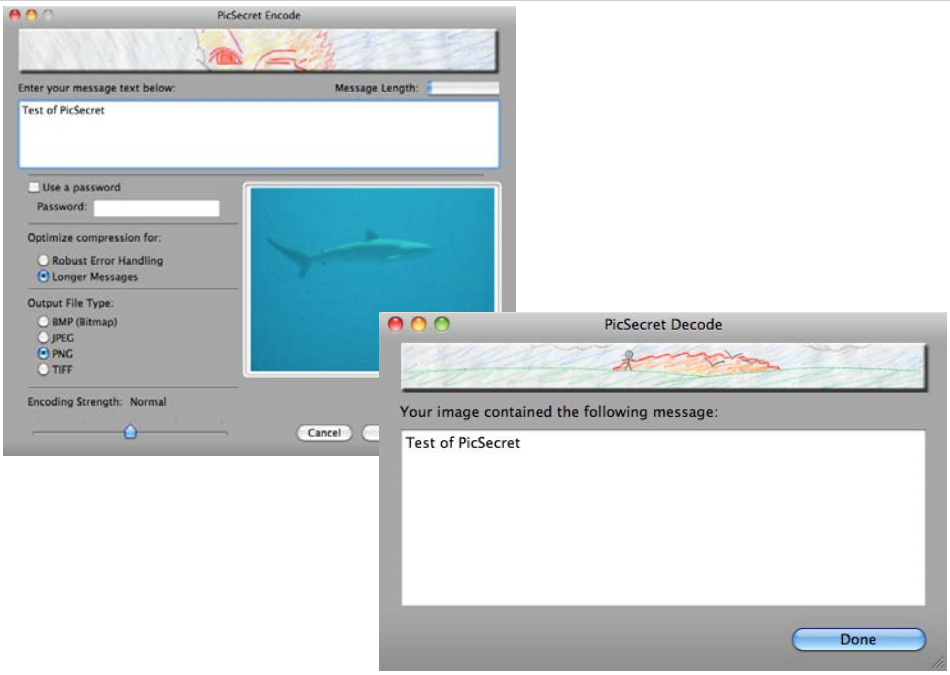






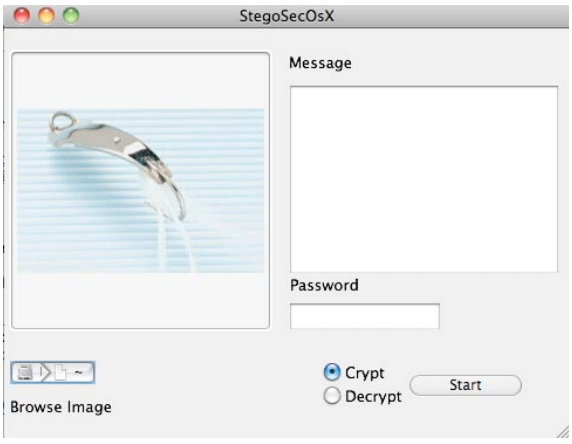
PicSecret

- Hides text in image files
- May or may not encrypt contents



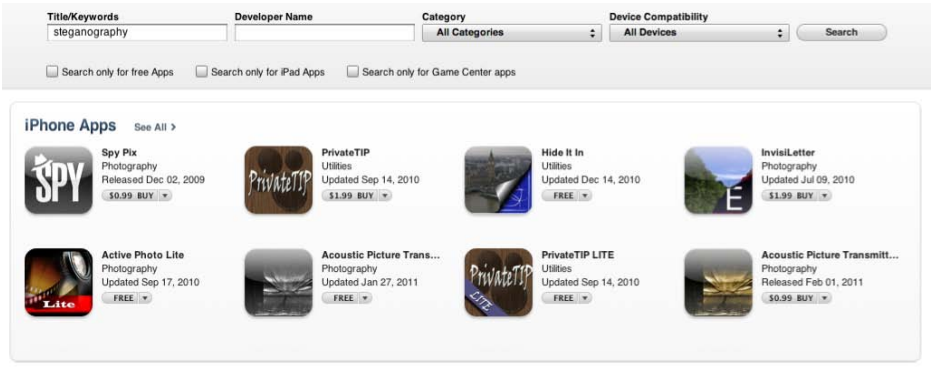
StegoSec (OS X)

- OS X and iOS versions
- Hides text in image files
  - Also has an encryption function



StegoSec (iOS)

iOS Steganography Apps



Simple search of "App Store" for the keyword of 'steganography'

Spy Pix

iOS Steganography

Free App

Category: Utilities
Updated: Dec 14, 2010
Current Version: 1.2
1.2
Size: 1.3 MB
Languages: English, French, Spanish

Hide It In

Description

Hide an image inside another one for free!!!

Hide It In allows you to hide an image inside another in a quick, easy and secure way!!

Hide It In is an app that hides an image taken with your iPhone camera into another seemingly innocuos image from your photo library that can be sent by email. Simply select the cover image and take a picture with your phone. Then introduce a password to encrypt the secret image with AES (Advanced Encryption Standard)

Hide It In includes the following features:
- AES encryption to ensure that only password owners will be able to recover the hidden image.
- QuickMode: Take a photo, Hide it In and send it with just three taps!
- Easy configure mail options such as: subject, body, attachment name and recipients. This allows you to send the image without raising any suspicions.
- Recover the secret image in two taps through your iPhone camera roll.
- And its totally free!!!

Let's go and Hide It It some images!!!

Free "App" that easily hides pictures inside of pictures

Hide It In

Summary

- Cryptography and steganography are neither just for PCs nor desktop/laptop computers
- As smartphones and other mobile devices become portable Internet terminals that can be used anywhere, we will see an increase in use of crypto and will start to see stego, as well.

Overview

- OS X and iOS overview
- Cryptography review
  - OS X cryptography
  - iOS cryptography
- Steganography review
  - OS X steganography
  - iOS steganography
- Summary

URLs

These URLs are provided for reference only and are not an endorsement for any product

Acoustic Picture Transmitter -- *http://appshopper.com/photography/acoustic-picture-transmitter-pro*
Active Photo Lite -- *http://appshopper.com/photography/active-photo-lite*
DataVault -- *http://www.ascendo-inc.com/datavault/iphone/Password-Manager.html*
Good for Enterprise -- *http://itunes.apple.com/us/app/good-for-enterprise/id333202351*
Hide It In -- *http://itunes.apple.com/us/app/hide-it-in/id401162613*
iDiary -- *http://www.macworld.com/appguide/app.html?id=89583*
InvisiLetter -- *http://itunes.apple.com/us/app/invisiletter/id375557298*
-- *http://samurai-apps.com/en/invisiletter/*
iSteg -- *http://www.hanynet.com/isteg/*
Keeper Password & Date Vault -- *http://itunes.apple.com/us/app/keeper-password-data-vault/id287170072*
Mactracker -- *http://www.mactracker.ca/*
mSecure -- *http://msevensoftware.com/msecure_ios*
My Eyes Only -- *http://www.softwareops.com/products/myeyesonly.html*
PGP Whole Disk Encryption -- *http://www.symantec.com/business/whole-disk-encryption*
PicSecret -- *http://www.macupdate.com/app/mac/24255/picsecret*
PrivateTIP -- *http://appshopper.com/utilities/privatetip*
Safe -- *http://itunes.apple.com/us/app/safe/id290169191*
SMS Encryption -- *http://www.4shared.com/file/326Maep4/SMS_Encryption_App.html*
StegoSec -- *http://csocks.altervista.org/Stegosec.html*
Spy Pix -- *http://www.juicybitssoftware.com/spypix/*
TrueCrypt -- *http://www.truecrypt.org/*
Wallet Pro -- *http://itunes.apple.com/us/app/wallet-pro-password-manager/id284950097*

Acronyms and Abbreviations

AES	**Advanced Encryption Standard**
CLI	**Command line interface**
GUI	**Graphical user interface**
JPEG	**Joint Photographic Experts Group**
OS	**Operating system**
PC	**Personal computer**
PGP	**Pretty Good Privacy**

Author Contact Information

Gary C. Kessler, Ph.D., CCE, CISSP
Gary Kessler Associates
2 Southwind Drive
Burlington, VT 05401

mobile: +1 802-238-8913
e-mail: gck@gary*kessler.net*
gkessler@bpdvt.org
Skype: *gary.c.kessler*

http://www.garykessler.net
http://www.vtinternetcrimes.org
http://infoassurance.norwich.edu

Ryan R. Kubasiak, ACTC, ACSP, GCFA,
CCE, ACE, EnCE, CEECS
AppleExaminer.com

e-mail: *rkubasiak@appleexaminer.com*
Twitter: *@appleexaminer*

http://www.appleexaminer.com