CYBER502x
Computer Forensics

Week 8: Steganography and Steganalysis

Concepts

- **Steganography** is the art and science of hiding communications.
  - From Greek
    - “Steganos” means‘hidden’ or ‘covered’
    - “-graphy” means‘writing’

Cryptography vs steganography

- Cryptography
  - Provides *confidentiality* but doesn‘t conceal that data is embedded
  - Uses mathematical algorithms to renders the information message unreadable without a specific key
- Steganography
  - Hides the existence of a message or hidden data

Concepts

- Steganalysis is the process of
  - Detecting steganography
  - Recovering hidden evidence

Steganography - stego

- Origins date back to 2500 years ago
- The early Greeks used various forms of covered writing to conceal the communication of secret
- Germans used Null Ciphers during World War I
- Modern day stego hides secret in digital media.

Use of stego today

- Hide information in a digital audio, video, or image
- Corporate espionage
  - Hides electronic messages including nuclear weapons research behind computer images, June, 2010.
- Malware hides configuration files
  - Zeus - http://www.net-security.org/malware_news.php?id=2721
- Watermarking used for copyright protection for intellectual property that is in digital format

Stego terms

- Payload
  - The secret message/information that you want to conceal
- Carrier (or host)
  - The data body that conceals the payload. It can be an existing file or generated “on the fly”
- Covert
  - The combination of the payload and the carrier

Why stego works?

- Exploiting Human Weaknesses
  - Human Sight is poor to identify different colors
  - Human Hearing is weak in detecting slight amplitude and phase shifts
- The cover massage (to human) appears identical to the carrier

General Steganography technologies

- Injection
- Substitution
- Generation of completely new files
- Covert Channels
- …

Injection Stego methods

- Add/modify data to existing file
- Increases file size

Injection Stego methods - Camouflage

- http://camouflage.unfiction.com/Download.html
- Appends payload after the carrier's standard end-of-file marker
- Advantages
  - Simple to use
  - Does not modify the carrier file's appearance or function
- Disadvantages
  - Easily to be detected

Substitution

- Replace existing data with hidden content
- it could degrade original file quality
- Usually replaces “insignificant” data in the carrier
  - MSB to left, LSB to right
  - 10001100

  - File size remains approximately same

Substitution - LSB encoding

- Change LSB, SMALL difference in value
- Change 1 or 2 bits of LSB’s creates minimal impact
  - Human ears can not detect the sound changes
  - Human eyes can not detect the color changes

Generation of a completely new file

- Spam Mimic
    - Web-based steganography tool
    - http://www.spammimic.com
    - Enter your secret, spam mimic will automatically create “spam” like messages that actually contain the hidden data
    - To decode, turn the spam back to the hidden data
    - Usually use publicly available computer to do that

Covert Channels

- Use TCP packets as carrier files
- Covert-TCP (freeware)
- Create the initial Sequence Number by a constant value
  - The ASCII of the hidden character
- The receiver will reveal the hidden character by the ISN divides the-constant

Digital Audio/Video

- CD Audio, wave files
  - Uncompressed samples (16-bit/per-sample)
  - Each sample is collected at a frequency of 44.1 Khz or 44.1K times per second based on Nyquist-Shannon sampling theorem
- MP3 Files
  - Use lossy data compression to reduce file sizes without noticeably affecting the sound quality
  - Superfluous data is removed
  - Modified Discrete Cosine Transform (MDCT) coefficients

Audio/Video Steganography Techniques

- Least Significant Bits (LSB) embedding into wav raw sample values
  - Changes the LSB of the samples
  - hide information in wav files
  - example: S-tools

- LSB embedding into MP3/MP4 coefficients
  - hide information in MP3 files or MP4 video
  - By modifying the MP3 / MP4 encoding algorithm to insert data
  - Examples: MP3stego / MP4stego

Why Audio/Video Stego is dangerous

- Has the potential to conceal more information
- YouTube and personal audio players, MP3 and MP4 player, iPod, smart phone, are common
- Our hearing is not sensitive to the amplitude changes

Digital Images

- Digital images are made up of pixels
- Three popular methods exist today
  - True color images
  - Compressed images
  - Palette images

True Color Images

- Each pixel holds color triplet (Red-Green-Blue) that represents the color intensities
- 8 bits for each color
- There are total 28 x 28 x 28 possible colors
- Often called 24-bit true color
- Pro: Color is more accurate
- Con: File size is much larger
- Example
  - BMP
  - PNG

Compressed Images

- Lossless
  - Maintains complete digital image
  - Compressed data is fully recoverable
  - For example, GIF and PNG
- Lossy
  - Some information is discarded
  - Original image is NOT fully recoverable
  - For example, JPEG

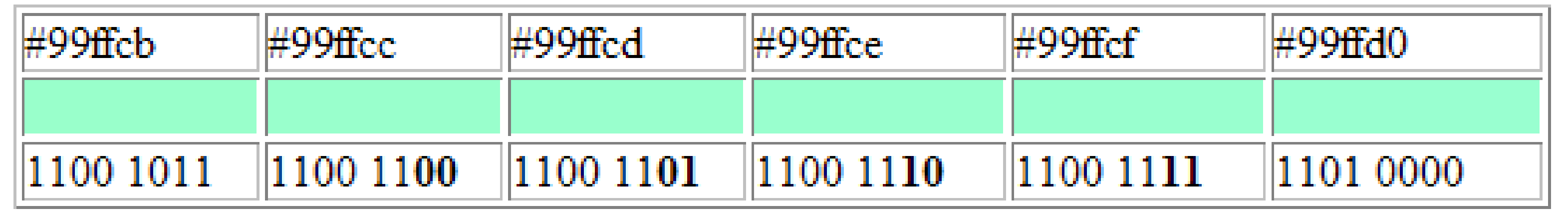
Palette Images

- Each screen pixel is represented by 8-bit binary data
- This 8-bit is mapped to one predefined color on a table
- Typically 28=256 colors in the table
- Pro: Small files
- Con: Reduced resolution
- Example
    - GIF

Using LSB Encoding to true color images

- Make subtle changes to each pixel of the image
- It is undetectable through visual inspection
- S-Tools Version 4.0
  - Does not change the file size
- Typically applied to BMP images

Data in the pixels…



#99ffcb	#99ffcc	#99ffcd	#99ffce	#99ffcf	#99ffd0
🟩	🟩	🟩	🟩	🟩	🟩
1100 1011	1100 1100	1100 1101	1100 1110	1100 1111	1101 0000

- A table created in DreamWeaver (24-bit color)
  - Background colors (hex) in top row
  - Color in center row
  - Bit value in bottom row
  - Can you see the difference in the colors?

Using LSB Encoding to the lossy compressed images - JPEG

- LSB modification are made to the coefficients of the Discrete Cosine Transform prior to the stage of compression
- Typically applied to JPEG files
- Tools
  - JP Hide and Seek – JPHS
    - The size of the covert message usually is smaller
    - The header information is usually stripped

Hide data in palette images

- Sort the colors in the palette to have the closest colors fall next to each other
- Similar colors are paired up, one color represents 1 while the other represents 0
- Use the paired colors to hide data

- Software examples
  - EzStego, Gif-it-Up

Gif-it-Up

- Advantages
  - Fast and simple
  - Palette based images are usually lower in quality, so the minor changes may not be detected
- Disadvantages
  - Low capacity for data hiding

Tools vs carrier files

Tools	Apply to:
S-tools	gif, bmp and wav
Gif-it-up	gif
JPHS	jpg
Camouflage	any carrier

Steganography for smart phones

- Stego programs have emerged targeting to Android, iOS, and Windows mobile platform.
  - SPYPIX - iphone stago using LSB

Steganalysis – stego detection

- Two types of methods for detecting
  - Visual analysis
    - Compares a suspected covert file with the original to reveal the presence of secret
  - Statistical analysis
    - Detects changes in pixels or amplitudes or frequency coefficients to see if its statistical properties deviate from a norm

Steganalysis – stego content recovery

- Identify known steganography tools (live or unallocated)
- Identify artifacts of these steganography programs
- If possible, break the password and recover the hidden message

Tools to detect and recover hidden content

- If you have original image, it’s easier
    - If md5 or sha available, check for match
    - Look for Diff between the orig and unknown
- Otherwise, it’s not easy
    - Outguess’ stegdetect and stegbreak by Niels Provos
        - may detect Jsteg, Jphide, Invisible secrets, outguess, F5 and camouflage

Detecting stego from WetStone Tech

- Stego Hunter from Wetstone
  - Check hashes to match known stego tools
- Gargoyle Investigator Forensics Pro Edition
  - Advanced malware detection software package for in-depth forensic investigations
- Stego Suite
  - StegoWatch – steganography detection
  - StegoAnalyst – image and audio analysis
  - StegoBreak – steganography password breaking

Stego Watch

- The detection algorithm
  - compares the mathematical and statistical models of “normal” with the suspected files
  - produces outputs with flags of different levels of alerts

Stego Analyst

- Examine the details and artifacts about each image
  - Meta data – file size, number of color used, header info, closed color, DCT
  - HSB – Hue-Saturation-Brightness

Stego Break

- Once you have
  - Suspicious images that may hides information
  - what stego tools may be used to hide secrets.

- You crack password

Steps to utilize stego suite

1. **StegoHunter** to detect known stego tools
2. **StegoWatch** to detect suspicious files
3. **StegoAnalyst** to examine the suspicious files
4. **StegoBreak** to try to break passwords
5. Reveal the hidden message using the passwords
6. Passwords may be added into StegoBreak library to assist further breaking