Data Forensics

Digital Forensics

Steganography

- Steganography is broadly the process of hiding information in a cover medium
- Digital steganography takes many forms, we will focus on data hiding in file containers
- The 3 common file containers used for this are text files, image files, and audio files
- Video files can be used for steganography, but is less common
- The file we place hidden things into is called a cover file, once the hidden data is inserted, the resulting file is called a stegofile
- The primary goal is keeping an observer from becoming aware there is any hidden data at all

Effectiveness

- When data is hidden in a cover file, it can be very difficult to detect it is there without either:
  - access to the original, unmodified cover file
  - a fingerprint or signature characteristic of the embedding technique
- Hidden data may be the same type as the cover data, or it may be different (i.e. hiding a text file in an image file)
- Hidden data may be compressed to make it harder to recognize
- Hidden data may be encrypted making it harder to recognize, and unusable even when found by anyone other than the intended recipient
- The file may additionally be hidden using system hiding techniques such as alternate data streams or unpartitioned storage space

Uses Of Steganography

- Uses generally considered to be legitimate include embedding artifacts into products
- Artifacts may include:
  - Watermarks
  - IP signatures
  - Copy protection schemes
  - Tracking or phone-home tools
  - Serial numbers for licensing schemes or exfiltration tracing
  - Privacy provision for sensitive data

Steganalysis Software Challenges

- Software can do the hiding, some include encryption functions
- Software can try to detect steganographic techniques
- Software can try to extract payload
- Lawmakers are afraid of it and try to prevent users from getting this kind of software, the state of Michigan outlawed the outguess tools website, taking it down, which is why many stego tools are not hosted in the USA
- Steganography is not new (ref: Steganographica written in the 1600s), the hiding techniques are good enough and math doesn't change, so lots of older methods still work very well
- Identifying stego techniques in files means looking for one or more of the common encoding techniques

Stego Tools

- stegdetect, stegbreak, outguess are examples of CLI tools
- steghide, stegspy, stegsecret are examples of GUI tools
- There are many more, see the course resources links web page
- OpenPuff is interesting and has an excellent list of stego resources and articles on their website

Text Encoding Techniques

- Selecting specific letters from each word to be the content of the hidden message - first letter method, or cardan grille method are common
- Variable spacing for plain text used to indicate bits in the hidden message, spaces at the ends of lines can be used in a similar way, does not survive printing
- Rich text allows for varying font, colour, and line spacing to be used to encode information, HTML can specify hidden elements
- Use of capitals versus lowercase, or even punctuation choices
- Deliberate misspellings or grammatical faux-pas or constructs

Image Encoding Techniques

- LSB encoding, message bits overwrite insignificant portions of actual data in a way that doesn't disturb the graphic presentation, can be exposed visually by masking, or statistically, or by signature - susceptible to chi-square and brute force analysis in some situations, see Steganalysis using chi-square summary and Study of Steganalysis Methods by Wen Chen (2005)
- Color map embedding which either puts data in the map itself, or uses specific colours to represent data - susceptible to file examination
- Multiple methods involve exploiting the encoding mechanisms in formats like JPEG, PNG, and GIF - much harder to detect

Audio Files

- Made famous on Mr. Robot TV show
- Complete file archives are embedded easily in audio files
- Deepsound tool is an example of a Windows GUI tool for audio file stego you can get from jpinsoft.net
- Deepsound demo video