ELEN689: Topics in Network Security
Guest Lecture: Steganography

Deepa Kundur
Department of Electrical Engineering, Texas A&M University
Outline of Presentation

- Covert Channels
- Introduction to Steganography
- Historical Stego
- Modern Media Stego and Steganalysis
- Internet Steganography
Covert Channels

Objective:

- To transmit hidden information from a source to a destination using “unconventional” means such that the presence of the communication is
  1. not easily detectable, and
  2. not interfered with
What is a covert channel?
- An unintended and/or unauthorized communications path that can be used to transfer data in a manner that violates one or more security policies.
Classes of Covert Communications

- **Computer-Oriented**
  - Due to vulnerabilities in software or operating system

- **Network-Enabled**
  - Exploits format and structure of protocols and algorithms for networked communications

- **Media-Based**
  - Hides information by taking advantage of limited range of human perception
Characteristics of Covert Channels

- Associated communication links are not designed for data exchange
- Employs entities not intended to be data-carrying objects to transfer information
- Established using system resources shared by source and destination parties
Examples of Covert Channels

- **Timing Channels**: start-time or duration of a process is used to communicate information to recipient parties who can observe such resources.

- **Storage Channels**: modulation of storage resources such as disk space and media files to embed information later retrieved by recipient parties.
Covert Communications vs. Encrypted Communications

- Encryption
  - Scrambles transmitted content so it is unintelligible
  - Communicating parties are known

EAVESDROPPING
TAMPERING
IMPERSONATION
Covert Communications vs. Encrypted Communications

- Covert Communications
  - Existence of communications is unknown
What can Covert Channels Accomplish?

- Allow information transfer over an unintentionally created communication channel
Virtual Spectrum™

- Chinook Communications
- Adds digital BW to existing NTSC analog channels
- Up to 6Mbps per channel
- Can embed MPEG-2 data stream into analog TV channels
What can Covert Channels Accomplish? (cont’d)

- Data transfer that violates the system security policy
  - Malicious programs can exploit covert channels to pass sensitive information from highly protected to less secure areas
Covert Channels and Steganography

Covert Channels:
- Unintended and/or unauthorized communication paths used to transfer data

Steganography:
- Process of hiding secret information in innocuous messages
Covert Channels and Steganography

OVERT CHANNEL + STEGANOGRAPHY = COVERT CHANNEL
Prisoner’s Problem (Simmons, 1983)

Escape Plan ...

Alice

Warden

Bob
Options for Private Communications

- Encryption:
  - Warden will suspect something is wrong and frustrate their plan by placing them in solitary confinement

- Steganography:
  - Warden cannot detect nor prove that there is secure communications
Prisoner’s Problem (Simmons, 1983)

Alice: Hello, How are you today? ...

Bob: Hi Alice.

Warden: Have fun!
Steganography

- Steganography: “Stegos” (covered) + “graphy” (writing)
- The process of hiding a secret message $m$ inside another message that masks $m$'s presence
- Facilitates covert communications
Steganalysis

- The process of detecting the use of steganography in a given message or medium
- Characteristics of the hidden message, if any, may be derived
Applications

- Steganography:
  - Covert communications
  - Signal tagging
  - Copy protection
  - Fingerprinting

- Steganalysis:
  - Cyberforensics
  - Cybercrime
Potential “Damage”

Covert data flow possible in media and network packets

Video/Images
- 500 KB per 1 MB raw image
- Substantial bit rate for video

Networks
- 8 bytes per packet
- Large site, 500 million packets/day
- Over 4 GB/day
Implicit and Explicit Steganography

Two strategies for stego:

- Implicit: the cover-object is constructed for the purpose of masking the message

- Explicit: a given object is modified in some way to fundamentally tie the message to the object
Terminology
Terminology

Implicit Steganography

Characteristics to mimic

Secret message

Stego-object

Stego-key

Stego-text
Stego-image
Stego-audio

Secret message

Stego-key

Stego-key
Terminology

Explicit Steganography

Cover-object

Cover-text
Cover-image
Cover-audio

Stego-object

Stego-text
Stego-image
Stego-audio

Secret message

E

Stego-key

D

Stego-key
Historical Example

- WWI Cablegram

PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY

Pershing sails from N.Y. June 1
APPARENTLY NEUTRAL'S PROTEST IS THOROUGHLY DISCOUNTED AND IGNORED. ISMAN HARD HIT. BLOCKADE ISSUE AFFECTS PRETEXT FOR EMBARGO ON BYPRODUCTS, EJECTING SUETS AND VEGETABLE OILS.

Pershing sails from N.Y. June 1
Bob Smith, my assistant programmer, can always be found hard at work in his cubicle. Bob works independently, without wasting company time talking to colleagues. Bob never thinks twice about assisting fellow employees, and he always finishes given assignments on time. Often Bob takes extended measures to complete his work, sometimes skipping coffee breaks. Bob is a dedicated individual who has absolutely no vanity in spite of his high accomplishments and profound knowledge in his field. I firmly believe that Bob can be classed as a high-calibre employee, the type which cannot be dispensed with. Consequently, I duly recommend that Bob be promoted to executive management, and a proposal will be sent away as soon as possible. -- Project Leader
History Lesson #1

- If effort to construct the stego-object is high, it results in a weak construction that makes steganalysis easier.
- Explicit stego more convenient than implicit stego.
Historical Example

- WWI Cablegram
  - FATHER IS DECEASED

- Changed by censors to:
  - FATHER IS DEAD

- Response to changed cablegram:
  - IS FATHER DEAD OR DECEASED?
History Lesson #2

- Robustness of the hidden message is important
Historical Example

- In 1857, D. Brewster suggested hiding messages in areas no larger than a dot of ink.
- Microscopic images of drawings and photographs were also hidden in people’s ears, nostrils and finger nails during the Franco-Prussian war (1870-1871).
History Lesson #3

- Making the hidden message expensive to look for can be beneficial
- A large amount of potential stego-traffic makes steganalysis tedious
Requirements for Successful Stego

- Element of uncertainty
- Possibility to adjust system elements within limits and still maintain overall flavor
- Volume of information readily available to mask/hide covert data
Digital Steganography

Cover-image

Stego-image
Perceptual Coding Paradigm

Steganography vs. Compression
1. SELECTION OF STEGO DOMAIN

2. MERGING STRATEGY
   A. HVS MODELS
   B. THEORY
Stego Domain

- O’Ruanaidh et al. (1996), Kundur and Hatzinakos (1997)

Spatial Domain
Merging Strategy


\[ f(i) \]

Range of coefficient values

MIN \[ \Delta \] MAX

TO EMBED “0”

TO EMBED “1”
Communication Theory Paradigm
Spread Spectrum Embedding

- \( U(i) = \) original media signal
  \( W(i) = \) key sequence
  \( X(i) = \) composite media signal

- \( X(i) = U(i) + k \cdot W(i), \ k = 1, -1 \)

- Can statistically detect \( W(i) \) from \( X(i) \)

- \( \text{SIM}_W[X(i)] = \text{SIM}_W[U(i) + k \cdot W(i)] \)
  
  \[ = \text{SIM}_W[U(i)] + \text{SIM}_W[k \cdot W(i)] \approx 0 + k \]
Steganography and Steganalysis

- Eavesdropping or monitoring point
- Cover-message
- Secret message
- Secret Key $K$
- Steganographic Embedding Algorithm
- Stego-message
- Decoded secret message
- PUBLIC CHANNEL
- Steganographic Extraction Algorithm
- Secret Key $K$
- STEGANOGRAPHY
- STEGANALYSIS
- Is something Hidden? Y or N
- SENDER
- RECEIVER

© Deepa Kundur, 2004 Electrical Engineering, Texas A&M University
Image Steganalysis: Previous Work

- Fridrich, Du and Meng (2000)
- Fridrich, Goljan and Du (2001)
- Avcibas, Sankur and Memon (2001)
- Farid (2002)
Problem: Video Steganalysis

- Video provides high capacity cover-message for covert communications
- Direct frame by frame application of image steganalysis is suboptimal
- Leverage concepts from the field of digital video watermarking
Objectives:

1. Make more general assumptions about the steganography technique
2. Take into account inherent characteristics of the video for greater accuracy
3. Employ previous research in digital watermarking attacks

Hidden Info? Y or N

Video under consideration

Steganalysis
Decision Box

Partial information and assumptions about embedding algorithm
Proposed Framework

Kundur and Budhia (2004)

Video under consideration

Pattern Classifier

Hidden Info?

Y or N

Attack

Estimate of cover-video

“Junk” value
Independent of secret message characteristics

FIGURE OF MERIT:
Probabilities of false positive and false negative.
Steganographic Model

\[ X_k(m,n) = U_k(m,n) + a_k(m,n) W_k(m,n) \]

- \( X_k(m,n) \): stego-video
- \( U_k(m,n) \): cover-video
- \( a_k(m,n) W_k(m,n) \): scaled secret message
Linear Collusion Attack

1. Feature Extraction
2. Discriminator
Classifier

- Features:
  - Kurtosis
  - Entropy
  - 25th percentile

- Discriminator:
  - kNN classifier

With secret message

Without secret message

Y or N
Scatter Plots

“Backyard” video sequence

“Hotel” video sequence

No secret message

Secret message present
Internet Steganography

- “Open” specifications of the Internet
  - Communications
  - Connectedness
  - Collaboration

- Security in the Internet an afterthought
Potential Advantage?

- Can we identify practical covert channels in TCP/IP?
- How can these channels be used to enhance network processing and security?

Stego

Network Protocols

Network Security
Internet Stego Framework

- Covert channel piggy-backed on legitimate overt channel
  - Stego does not affect overt channel
  - Stego undetectable by network filters

Sender

Cover-Packet stream
Steganographic Embedding Algorithm
Secret message
Secret Key $K$

Stego-Packet stream

PUBLIC CHANNEL

Steganographic Extraction Algorithm
Secret Key $K$

Decoded secret message

Receiver
Previous Work

Covert Channel Based

2. Wolf (1989): LAN protocols
4. Rowland (1997): TCP/IP; proof of the concept
5. Ackermann et al. (2000):
   - Weakening of layered concept
   - Additional info. in network packets

Networks Based
Proposed Algorithms

Ahsan and Kundur (2002)

- Illustrative Examples
  - Packet header manipulation
  - Packet “sorting”
Packet Header Manipulation

<table>
<thead>
<tr>
<th>4-bit Ver.</th>
<th>4-bit IHL</th>
<th>8-bit TOS</th>
<th>16-bit Tot. Len.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0100</td>
<td>0101</td>
<td>XXXXXXXUU</td>
<td>XXXXXXXXXXXXXXXX</td>
</tr>
<tr>
<td>0000 0100 RRRRRRRR</td>
<td>XXX</td>
<td>XXXXXXXXXXXXXXXX</td>
<td></td>
</tr>
<tr>
<td>8-bit TTL</td>
<td>8-bit Protocol</td>
<td>16-bit Checksum</td>
<td></td>
</tr>
<tr>
<td>XXXXXXXX</td>
<td>XXXXXXXX</td>
<td>XXXXXXXXXXXXXXXX</td>
<td></td>
</tr>
<tr>
<td>32-bit Source Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32-bit Destination Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Stego Scenario 1

- Multiple interpretation of fragmentation strategy
- Utilize flags field; DF (Do not Fragment) bit

<table>
<thead>
<tr>
<th>Datagram</th>
<th>16-bit Ident. field</th>
<th>3-bit flag field</th>
<th>13-bit frag. offset</th>
<th>16-bit total length</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>XX...XX</td>
<td>010</td>
<td>00...00</td>
<td>472</td>
</tr>
</tbody>
</table>

Covertly Communicating ‘1’

<table>
<thead>
<tr>
<th>Datagram</th>
<th>16-bit Ident. field</th>
<th>3-bit flag field</th>
<th>13-bit frag. offset</th>
<th>16-bit total length</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>XX...XX</td>
<td>000</td>
<td>00...00</td>
<td>472</td>
</tr>
</tbody>
</table>

Covertly Communicating ‘0’
Potential Applications

- Enhanced filtering criteria in firewalls
- Security tied to the content – client-server architecture
- Content delivery networks
Steganography by Packet Sorting

- Sorting: ‘n’ objects can store $\log_2(n!)$ bits

$n = 3$

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & 3 & 2 \\
2 & 1 & 3 \\
2 & 3 & 1 \\
3 & 1 & 2 \\
3 & 2 & 1 \\
\end{array}
\]

$3! = 6$ Possibilities
$\Rightarrow \log_2(6)$ bits
Stego Scenario 2

- Packet “sorting” / “resorting” at network layer
  - Reference = Sequence number field of IPSec
  - No major modification in header fields
  - Sorting: chaotic mixing
  - Resorting: best sequence estimation
Final Remarks

- Health of covert channel often proportional to health of overt channel
- Robustness and capacity trade-offs must be carefully considered for each application