

# The Keys to the Kingdom



Understanding Covert Channels  
of Communication



Russ Rogers  
CEO & CTO  
Security Horizon, Inc.



# What are Covert Channels?

## Covert Channels

- “...any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy.”
- In short, covert channels transfer information using non-standard methods
- Against the system design
- Communication is obscured; unnoticed
- Easily bypass modern security tools & products

# What are Covert Channels?

➤ Covert Channels allow multiple parties to communicate 'unseen'

- The intent is to hide the fact that communication is even occurring
- Ensures privacy

➤ Unlike encryption, where communication is obvious but obscured

- Encryption is easily identified
- Clear and visible indications of encryption

# The History of Covert Channels

- Covert channels are not a new phenomenon
- The first known publication on covert channels was in 1499
  - Trithemius published his work on Steganography, '*Steganographia*'
- Steganography is one of the best known methods of covert communication

# The History of Covert Channels

## 🌀 Examples of Historical Covert Channels

- Shaven heads of slaves (ancient Greece)
- Stuffed animals carcasses carried by hunters
- Wax tablets
- Invisible inks, such as urine or milk (ancient Rome)
- Microdots
- Art work (drawings and paintings)
- Handmade quilts

# Historical Evidence



- Herodotus tells of a man who sends messages in the belly of a hare
- The Germans used a technology known as a *microdot* during WWII
- A Nazi spy used to hide his messages on his handkerchief using invisible ink
  - copper sulfite (ammonia fumes would reveal)
- American slaves were thought to have used quilt designs as codes and maps

# Why Do They Work?

➤ Covert Channels work because of human deficiencies

- Eye sight
- Hearing
- Analysis skills

➤ Lack of Interest

- It's not really a problem, doesn't happen
- Prove it to me

# Why Do They Work?

## Human Eyesight

- Poor sensitivity to very slight changes in color
  - Small transitions won't be noticed
- Poor recognition of intense color shades
  - Various shades of blue are difficult for the human eyes to distinguish
- Quality of human eyesight degrades with age

# Why Do They Work?

## Human Hearing

- Ears can't detect slight changes in amplitude caused by changes in the LSB
- Ears can't distinguish slight changes in phase shifts
- Susceptible to noise and distortion, but not in discrete quantities
- Human hearing degrades with age
- Human hearing is overwhelmed by noise

# Why Do They Work?

## 🌀 Human Analysis

- Most humans aren't bred for discrete analysis
- Things considered 'normal' are typically overlooked
- Only the most creative people can "think outside the box"

# Why Do They Work?

## ➤ Lack of Interest

- Many covert channels will elude people simply because those people have never considered the possibility
- The truth doesn't matter if there is a perception of truth

# Measuring the Threat

➤ Availability of software tools and applications allow for easy creation of covert channels

- Graphics editors
- Audio editors
- Packet insertion libraries
- Text generators
- Operating systems (Windows)

# The Bottom Line

- Good Covert Channels do what they're supposed to do
  - They hide the fact that communication between two or more individuals is occurring

# Modern Covert Channels

➤ Modern methods of covert communication also take into account our technology

- Widespread computer use
  - Powerful hardware technology
  - Advanced software technology
- The Internet
- Network access in public places
- Anonymity of Internet services
  - www, newsgroups, email

# A Needle in the Haystack

- Public and private web sites
- Email
- Newsgroups
- FTP sites
- Peer-to-peer software
- Instant messaging
- TCP/IP networking
- Shared file systems

# News Worthy?

## 🌀 Terrorism articles

- <http://msnbc.msn.com/id/3067670/>

## 🌀 Criminal Intent

- <http://www.theregister.co.uk/content/55/36485.html>

## 🌀 Speculation

- [http://www.nbr.co.nz/home/column\\_article.asp?id=8962&cid=3&cname=Technology](http://www.nbr.co.nz/home/column_article.asp?id=8962&cid=3&cname=Technology)

# Types of Covert Channels

## ➤ Steganography

- Images
- Audio

## ➤ TCP Covert Channels

## ➤ Word Manipulation/Substitution

## ➤ Data Hiding/Alternate Data Streams

## ➤ Data Appending

- EOF / Headers / Footers

# Steganography

- Steganography has been in use for millennia
- Modern steganographic techniques utilize binary files as the medium for transportation
  - The hidden information is also in binary format
- The most popular and easily used formats are digital image and audio files

# Steganography - Images

- ✧ Bitmapped images are the most suited for hiding information
- ✧ Digital images are “normalized” when created
  - They fall within expected boundaries
- ✧ Not suitable for vector graphics using the same model of steganography
- ✧ JPG, GIF, PNG, TIF, etc

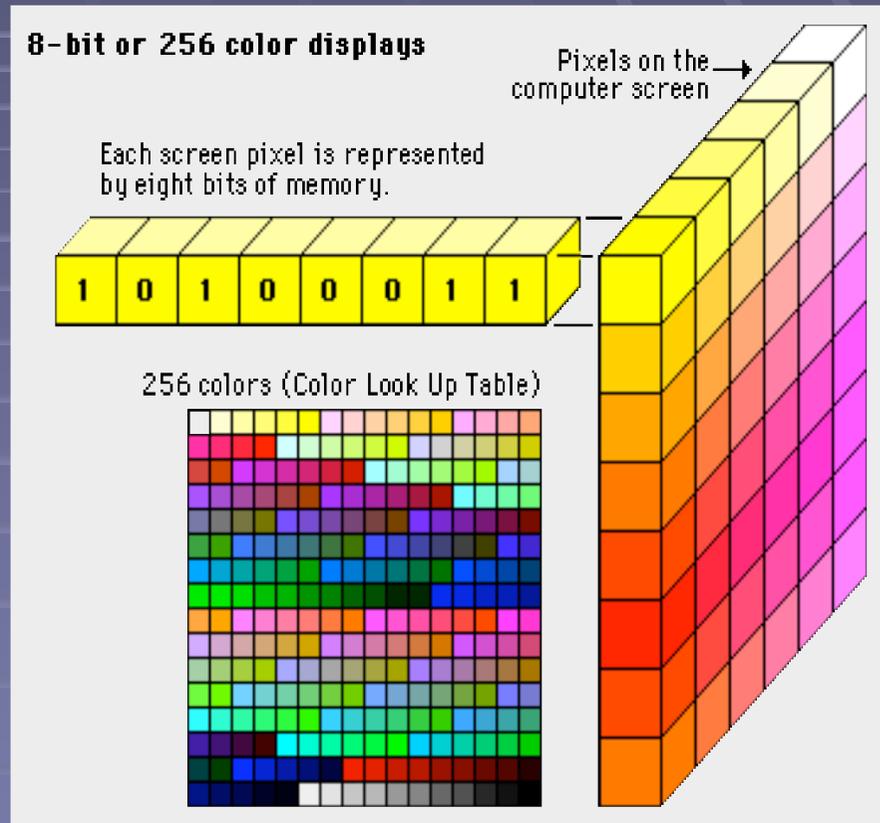
# Steganography - Images

- ✧ Bitmaps are based on colored pixels
- ✧ Each pixel contains a single color
- ✧ Each of 16.7 million possible colors are defined by bits
- ✧ The bit that causes the slightest change in shade when altered is called the Least Significant Bit (LSB)
- ✧ Humans can not detect these slight color changes

# Steganography - Images

## ☞ A simple example:

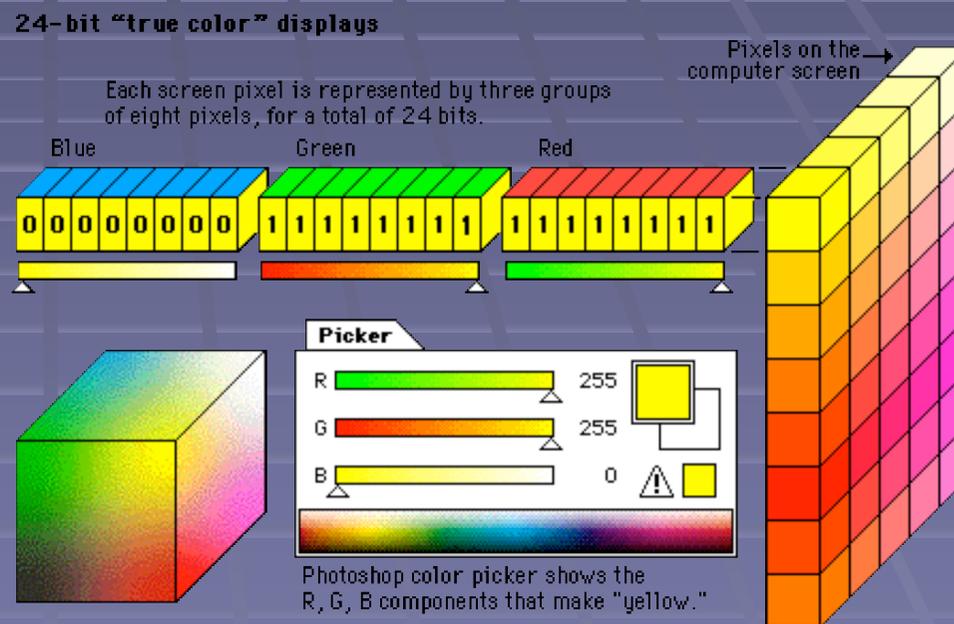
- A palette of 256 colors
- Defined by 8 bits
- Bit on far right is LSB
- Changes to this bit are imperceptible to human eyes



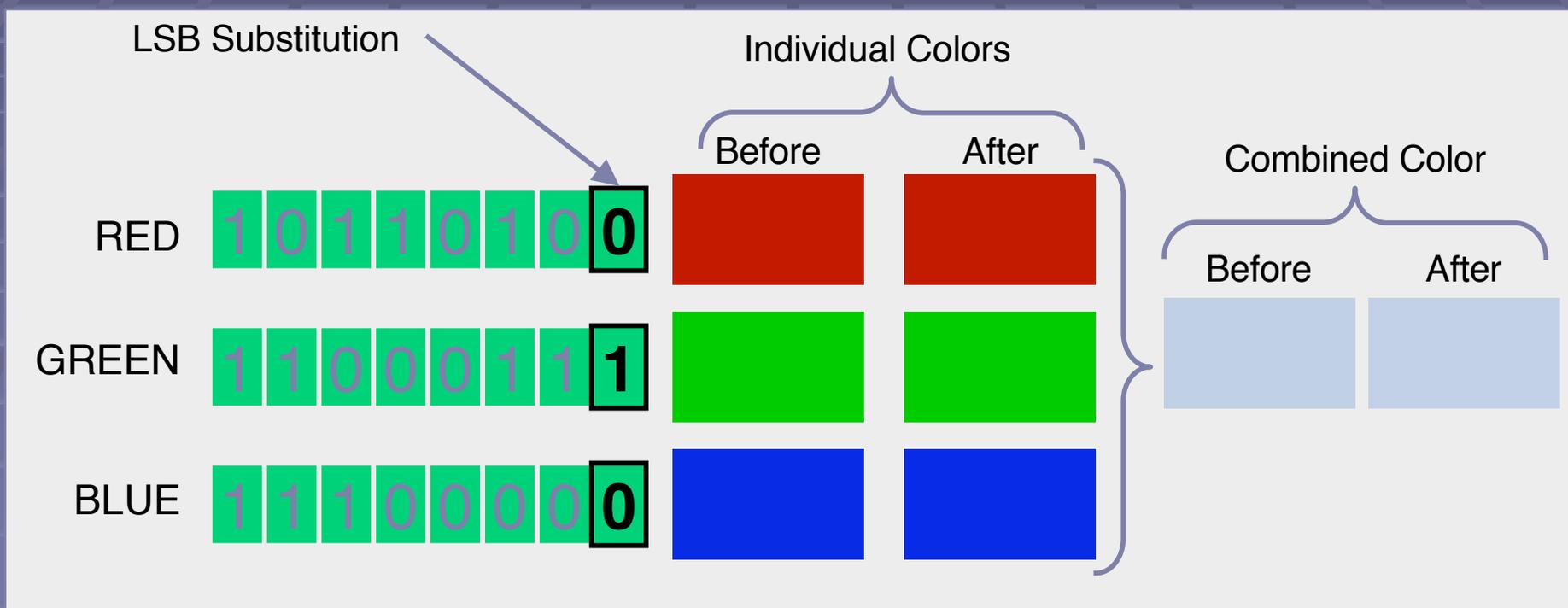
# Steganography - Images

## ☞ A simple example:

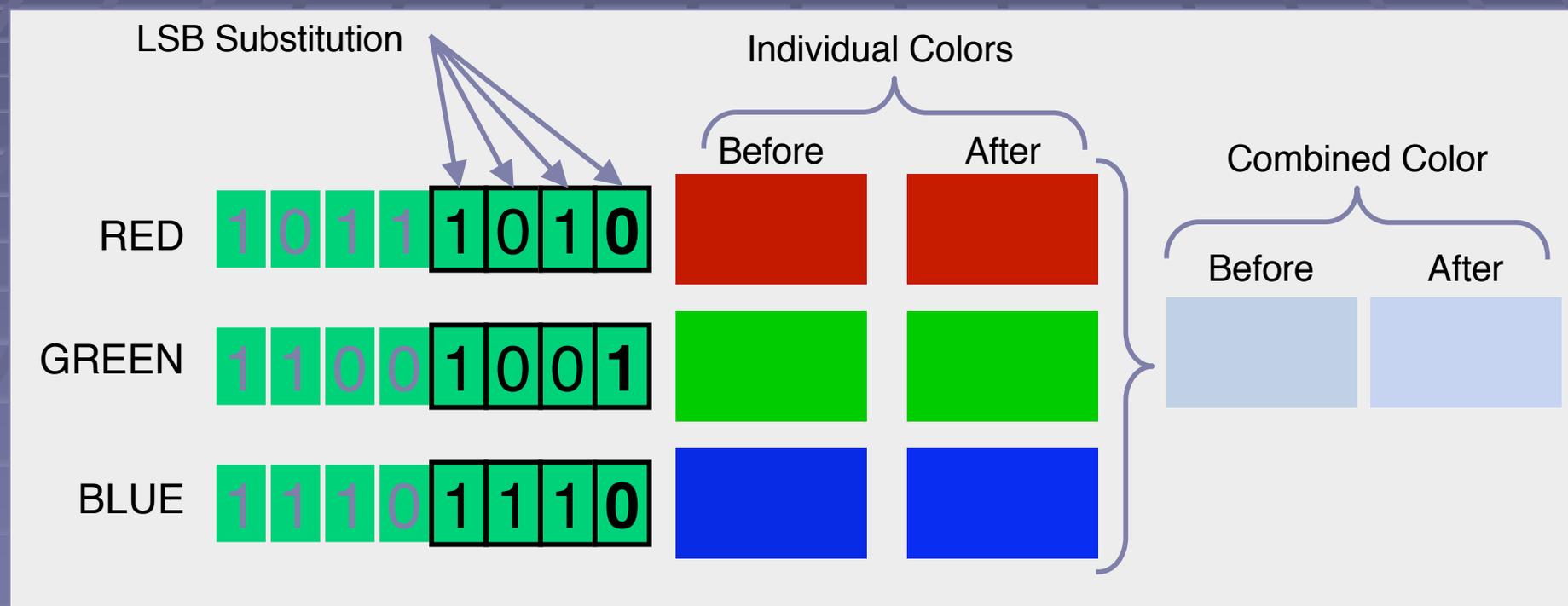
- A true color image with all 16.7 million colors
- Defined by 24 bits – 8 bits for Red / Green / Blue
- Bit on far right of each is LSB
- Changes here are even more imperceptible to human eyes



# Steganography - Images



# Steganography - Images



# Steganography - Images



# Considerations

- ❧ Most LSB data hiding techniques won't survive a lossy compression algorithm
  - Stego must occur AFTER the image has been compressed
- ❧ Too much data stego'd into an image will cause noticeable distortion, compromising the covert channel
- ❧ In general, the hidden file should be between 20-25% of the carrier file size
  - e.g., a 1 MB image could carry 200k of info

# Considerations

## ➤ Problems with detection:

- Small amounts of data hidden in large files are difficult to detect
- Stego-noise
  - The idea that you can create significant stego-trash out on the Net to make detecting legit files more difficult and time consuming
- Watermarks
  - Watermarks are simply standardized stego
  - Look similar to stego at first glance

# Steganography - Audio

- Audio files are perfect for data hiding because of the size of the carrier files
  - e.g., 5 MB is not an unusual file size
  - Using the 20% rule, our data can be 1 MB
- Peer-to-Peer distribution is high
- Can be transports via audio players (e.g. iPod)

# Steganography - Audio

- Digital audio is created through the use of an Analog/Digital Converter
- Samples of the analog signal are taken at known intervals (frequency)
- We end up with a binary representation of the sounds
  - 1's and 0's
- The loudness of the signal is designated by the peaks and valleys (amplitude)

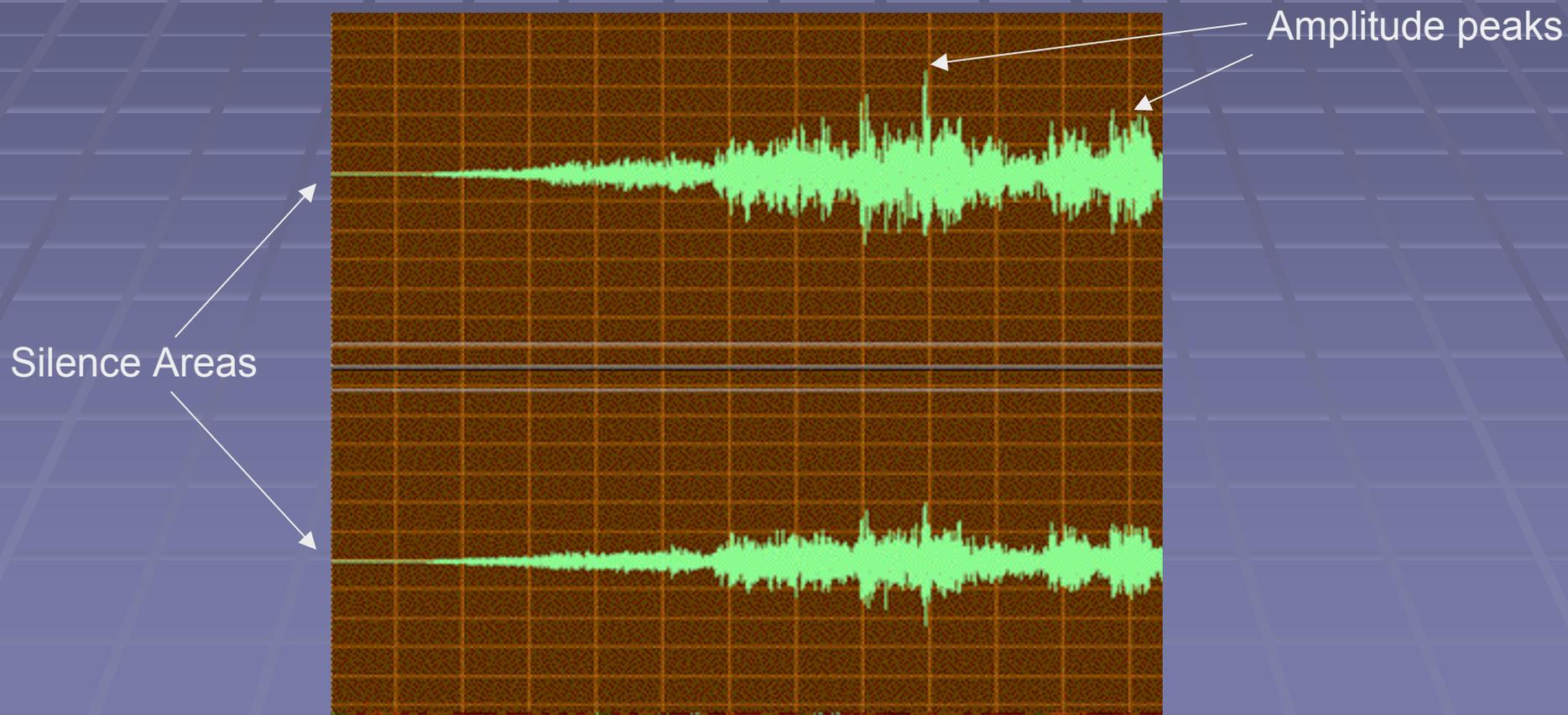
# Steganography - Audio

## Four known methods of Audio Stego

- low-bit encoding (most common)
- phase coding
- spread spectrum
- echo data hiding

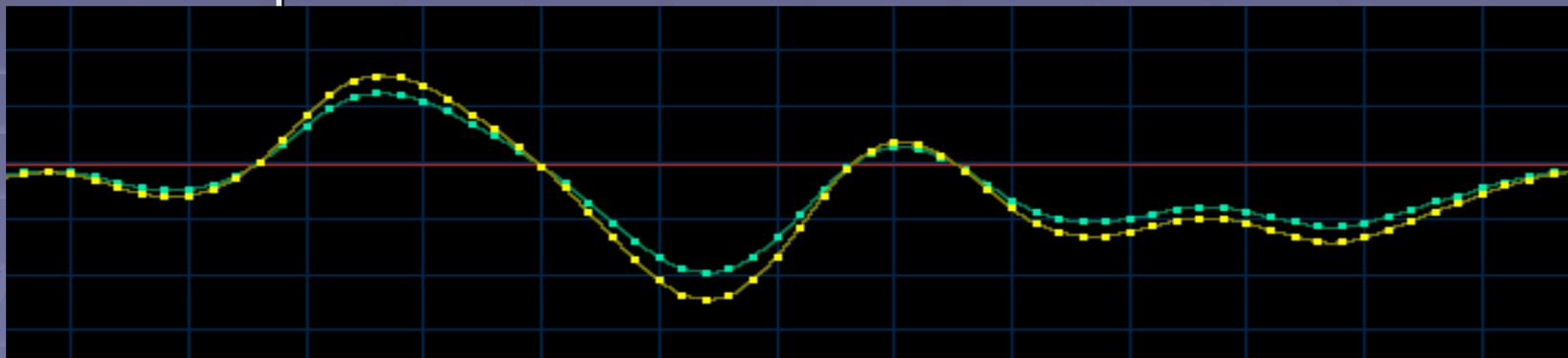
# Steganography - Audio

## Low Bit Encoding



# Steganography - Audio

- Adding data into an audio file maintains the wave form, but adds to the amplitude
  - Almost impossible to hear without the original file to compare



- Stego in audio files begins at the very beginning of the file, leaving 1's and 0's in the silent areas
  - This makes it easier to detect

# Considerations

✎ There are a large number of audio formats

- WAV, MP3
- AU, MWA, AIFF

✎ There are a multitude of methods for delivering the files

- Flash drives
- MP3 players
- File sharing

# Considerations

- ✎ The human ear is poor at hearing slight changes in volume (amplitude) or frequency
- ✎ Steganography software that works on audio files alter the amplitude for each sample by 1 or 0
- ✎ This change is imperceptible to our ears
- ✎ The silence area lead in to audio files can be deleted, making detection more difficult

# File Systems

- Data hiding in common operating systems is quite easy
- Under FAT file systems, files can be hidden in directories with invisible names
  - Directory names using the ASCII character 255
- Under NTFS, files can be hidden in Alternate Data Streams
  - A Windows “feature”

# File Systems

- Under UNIX, files can be hidden in directories named with a period and a space
  - Requires a special escape code
- You can also hide files in directories that have other directories mounted to them

# File Systems

- *Alternate Data Streams* in NTFS allow users to “attach” files to other files
- Does not change the apparent file size
- Will not show up in a directory listing
- Multiple data streams per each carrier file
  - Text, binary, executable, etc
- No default tools or utilities within Windows to detect or list ADS

# Considerations

- ADS can not be emailed
- ADS will not be picked up by third party applications unless *specifically* built in
  - Winzip
  - FTP
- Carrier files CAN be moved across network shares and maintain the ADS
- In 2000, the W2K.Stream virus was carried in ADS

# Word Manipulation

- Manipulating text is another easy form of covert channel
- Been in use for centuries
  - Caesar originally created a rotational cipher that would change text
  - Spammimic.com will take a phrase you type in and create a spam email from the text
    - Can only be retrieved with the appropriate password

# Word Manipulation

## ☞ “Welcome to Black Hat Europe!”

☞ Dear Friend ; Your email address has been submitted to us indicating your interest in our newsletter . We will comply with all removal requests . This mail is being sent in compliance with Senate bill 1623 ; Title 4 ; Section 302 . This is not multi-level marketing ! Why work for somebody else when you can become rich as few as 22 days . Have you ever noticed people will do almost anything to avoid mailing their bills and the baby boomers are more demanding than their parents ! Well, now is your chance to capitalize on this . WE will help YOU deliver goods right to the customer's doorstep plus use credit cards on your website ! The best thing about our system is that it is absolutely risk free for you ! But don't believe us . Prof Ames who resides in Washington tried us and says "I was skeptical but it worked for me" . We are licensed to operate in all states . Do not go to sleep without ordering . Sign up a friend and you'll get a discount of 40% . Thank-you for your serious consideration of our offer ! Dear Business person ; Especially for you - this red-hot information . This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 2516 , Title 2 , Section 306 . This is a legitimate business proposal . Why work for somebody else when you can become rich as few as 96 days ! Have you ever noticed how long the line-ups are at bank machines and people will do almost anything to avoid mailing their bills ! Well, now is your chance to capitalize on this ! WE will help YOU SELL MORE & sell more ! The best thing about our system is that it is absolutely risk free for you ! But don't believe us . Mrs Ames of Alabama tried us and says "I was skeptical but it worked for me" ! We are a BBB member in good standing . You have no reason not to act now . Sign up a friend and you'll get a discount of 80% . Thanks ! Dear Internet user , Especially for you - this breath-taking announcement . If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail . This mail is being sent in compliance with Senate bill 1625 ; Title 4 ; Section 301 . This is a legitimate business proposal . Why work for somebody else when you can become rich as few as 93 days ! Have you ever noticed how many people you know are on the Internet & society seems to be moving faster and faster . Well, now is your chance to capitalize on this . We will help you process your orders within seconds plus process your orders within seconds . You can begin at absolutely no cost to you . But don't believe us ! Mr Ames who resides in Montana tried us and says "I was skeptical but it worked for me" ! We are a BBB member in good standing ! We beseech you - act now ! Sign up a friend and you'll get a discount of 60%. Warmest regards !

# Word Manipulation

## ☞ “Welcome to Black Hat Europe!”

☞ **Dear Friend** ; Your email address has been submitted to us indicating your interest in our newsletter . We will comply with all removal requests . This mail is being sent in compliance with Senate bill 1623 ; Title 4 ; Section 302 . This is not multi-level marketing ! Why work for somebody else when you can become rich as few as 22 days . Have you ever noticed people will do almost anything to avoid mailing their bills and the baby boomers are more demanding than their parents ! Well, now is your chance to capitalize on this . WE will help YOU deliver goods right to the customer's doorstep plus use credit cards on your website ! The best thing about our system is that it is absolutely risk free for you ! But don't believe us . Prof Ames who resides in Washington tried us and says "I was skeptical but it worked for me" . We are licensed to operate in all states . Do not go to sleep without ordering . Sign up a friend and you'll get a discount of 40% . Thank-you for your serious consideration of our offer ! **Dear Business person** ; Especially for you - this red-hot information . This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 2516 , Title 2 , Section 306 . This is a legitimate business proposal . Why work for somebody else when you can become rich as few as 96 days ! Have you ever noticed how long the line-ups are at bank machines and people will do almost anything to avoid mailing their bills ! Well, now is your chance to capitalize on this ! WE will help YOU SELL MORE & sell more ! The best thing about our system is that it is absolutely risk free for you ! But don't believe us . Mrs Ames of Alabama tried us and says "I was skeptical but it worked for me" ! We are a BBB member in good standing . You have no reason not to act now . Sign up a friend and you'll get a discount of 80% . Thanks ! **Dear Internet user** , Especially for you - this breath-taking announcement . If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail . This mail is being sent in compliance with Senate bill 1625 ; Title 4 ; Section 301 . This is a legitimate business proposal . Why work for somebody else when you can become rich as few as 93 days ! Have you ever noticed how many people you know are on the Internet & society seems to be moving faster and faster . Well, now is your chance to capitalize on this . We will help you process your orders within seconds plus process your orders within seconds . You can begin at absolutely no cost to you . But don't believe us ! Mr Ames who resides in Montana tried us and says "I was skeptical but it worked for me" ! We are a BBB member in good standing ! We beseech you - act now ! Sign up a friend and you'll get a discount of 60%. Warmest regards !

# Considerations

- Emails like this normally go completely unnoticed
  - Too much spam out there now
  - The 'noise' generated by REAL spam creates this form of covert channel
  - Spams are normally deleted before being read
- Tend to be repetitive and complete non-sense when read in depth

# Covert TCP Channels

- All network protocols contain headers
- Each header contains areas that could be used to store or transmit data
- Many of these areas are never used for *normal* network transmission
- The most useful fields to store data in are those considered mandatory
  - Less likelihood of being stripped off at a router

# Covert TCP Channels

## 🌀 ID field (IP Header):

- Can transmit one ASCII character per packet
- Represented by unsigned integer
  - E.g. “H” = ASCII 72 = 18432
  - We take the ASCII number for each character and multiply by 256 to give a realistic integer for this field and avoid suspicion

“Hello” = 18432 / 17664 / 19456 / 19456 / 20224

Divide each by 256 to get the ASCII character number

# Covert TCP Channels

## Standard TCP Header

Version	HLEN	Service Type	Total Length	
Identification			Flags	Fragment Offset
TTL	Protocol		Header Checksum	
Source Address				
Destination Address				
Options			Padding	

# Covert TCP Channels

## Other possibilities:

- TCP Sequence Number field
- TCP Ack Number field
- Spoofed packets that “bounce” back to the receiver from a legitimate server
  - Sender encodes the appropriate data, creates a spoofed packet from the “receiver” to the “bounce” server
  - Bounce server responds with RST or ACK to the receiver
  - Data is retrieved from the header by receiver

# Considerations

- Any field can be altered by firewalls or network address translation
  - Could result in lost data

# Data Appending

- ✧ Transfers data by inserting into existing files outside of standard file boundaries
- ✧ Information can be appended beyond the EOF marker
  - Data in an image file that exists beyond the EOF is ignored by the viewing software
  - Not readily seen
- ✧ HTML comments are similar in function
  - Information in comments is ignored

# Considerations

- Data hidden this way is fairly easy to spot
  - File size increases
  - Data is stored beyond the EOF, where there should be no data
  - Embedded text data is easy to view with a text or hex editor

# Known Covert Tools

## 🌀 Images:

- S-tools, Invisible Secrets, Gif-it-up

## 🌀 Audio

- MP3-Stego

## 🌀 Text Manipulation

- Spammimic.com, Invisible Secrets

## 🌀 TCP Covert Channels

- Covert\_TCP

# Detection Products

- Stego detection is very much an infant industry
- Very few detection tools available
- Very few detection tools that work reliability
- Too many false positives
- Can't detect minute amounts of data in large files
- Very few decryption or brute force options

# Detection Products

## ➤ Stego Suite

- <http://www.wetstonetech.com>

## ➤ Encase (very limited)

- <http://www.guidancesoftware.com>

## ➤ StegDetect

- <http://www.outguess.com/detection.php>

# Detection Products

## ↻ LADS

- <http://www.heysoft.de/nt/ep-lads.htm>

## ↻ ADSDetector

- <http://www.codeproject.com/csharp/CsADSDetectorArticle.asp>

# Summary

- Covert Channels provide the means for communicating without being noticed
- They allow you to bypass normal network security mechanisms
- Detection is still in it's infancy
- Creation is a mature science and getting better

# Word of Thanks

## Black Hat

- <http://www.blackhat.com>

## Wetstone Technologies

- <http://www.wetstonetech.com>

# Contact Information

➤ Russ Rogers

➤ Security Horizon, Inc.

➤ [russ@securityhorizon.com](mailto:russ@securityhorizon.com)

➤ <http://www.securityhorizon.com>