Word of Thanks

- Black Hat
 - http://www.blackhat.com
- Wetstone Technologies
 - http://www.wetstonetech.com

The Keys to the Kingdom

Understanding Covert Channels of Communication



Russ Rogers CEO Security Horizon, Inc. Co-Founder securitytribe.com

Agenda

- What are Covert Channels?
- Why do they work?
- What are the consequences?
- The history of Covert Channels
- Covert Channels Today
- The Future of Information Hiding



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 current security tools & products

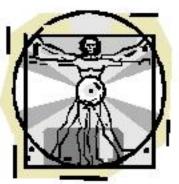


What are Covert Channels?

- 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

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
- System Design Discrepancies
 - Components utilized in unintended manner



Why Do They Work?

- Many covert channels will elude detection simply because most individuals have never considered the possibility
- Perception over rides reality

Measuring the Threat

- Availability of software tools and applications allow for easy creation of covert channels
 - Graphics editors
 - Audio editors
 - Packet insertion or manipulation libraries
 - Text generators
 - Operating systems (Windows)
- Plethora of web sites that list known applications for creating covert channels and steganography
- 250+ tools available on the Internet



A Needle in a Haystack

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



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
- Technology has created a large enough haystack within the Internet to hide terabytes of data without detection

Potential Damage

- Corporate Espionage
 - Loss of competitive advantage
- Government or Military Activities
 - Increased threat to National Security
- Criminal Activities
 - Transfer of pornography or commercial software
- Financial Impact
 - Transfer of confidential financial data

News Worthy?

- Terrorism articles
 - http://msnbc.msn.com/id/3067670/
- Criminal Intent
 - http://www.theregister.co.uk/content/55/36 485.html
- Speculation
 - http://www.nbr.co.nz/home/column_article. asp?id=8962&cid=3&cname=Technology

Fighting Covert Channels

- To defend against these channels, you must understand how they work
- Once we know what we're up against, we can take decisive action
- Let's look at some common forms of covert channels

Types of Covert Channels

- Steganography
 - Images / Audio / Executables
- Network Based
 - TCP / IP Channels
- Text Manipulation
 - Word Manipulation/Substitution
- Operating Systems
 - Data Hiding/Alternate Data Streams
- Data Appending
 - EOF / Headers / Footers



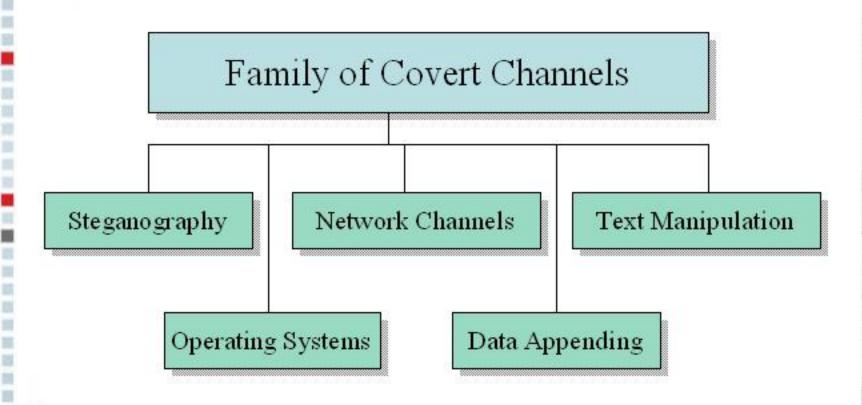








Hierarchy of Covert Channels





The History of Covert Channels

- Covert channels have existed throughout history
- 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

- Invisible Ink
- Wax Tablets
- Microdots
- Shaved heads of Slaves
- Messages hidden in hunted animals

Modern Covert Channels

- Take into account the technology
 - Widespread computer use
 - Powerful hardware technology
 - Advanced software technology
 - The Internet
 - Network access in public places
 - Free access to many network applications
 - Anonymity of Internet services
 - www, newsgroups, email



Steganography

- Steganography has two parts:
 - Carrier: The file we hide information IN
 - Payload: The information we hide in the Carrier
- Modern steganographic techniques utilize binary files as the medium for transportation
- The most popular and easily used formats are digital image and audio files
- Most current stego tools also encrypt the payload to increase security

Steganography - Images

- Too much data = Easier detection
- In general, the payload should be between 20-25% of the carrier file size
 - e.g., a 1 MB image could carry 200k of info
 - More than 25% can result in noticeable distortion

The Future of Stego

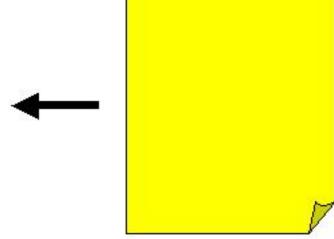
Carrier Groups

- Carrier groups could allow better hiding of information
- They can provide for much larger payload sizes
- Multiple carrier files are used versus the traditional single carrier
- New concept introduced in 2004

Traditional Carriers



Single Carrier File 400k in size



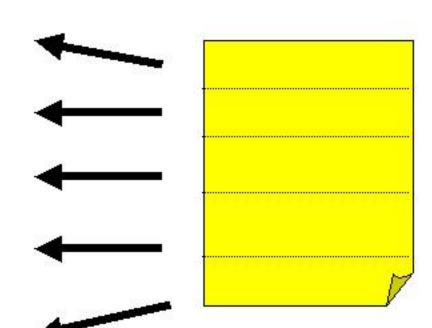
Payload File 100k max



Carrier Group Concept

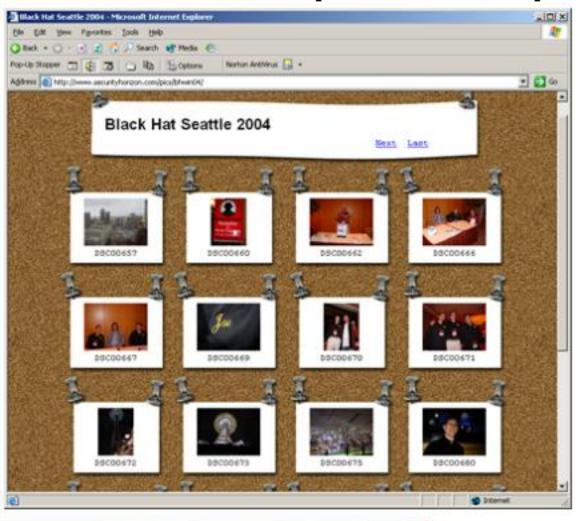






Payload File 100k max

Carrier Group Concept



Carrier Groups - Audio

- Using audio files instead of images:
 - 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
 - Using 5x 5MB audio files gives us the ability to store 5MB as a payload
 - Drastic increase in hidden storage

Stego Noise Concept

- The stego noise concept was introduced 1997 by Fabian Hansmann, author of Steganos
- Creating a benign virus that spreads rapidly across the Net creating benign stego within target files
 - Image Files
 - Audio Files

http://www.woodmann.com/fravia/fabian2.htm

Stego Noise Concept

- File Sharing is huge on the Internet
- Detection algorithms can't differentiate between decoy stego and the real thing
 - Huge waste of resources to examine all files on the Internet
- This concept can be improved upon by inserting random information into each decoy
 - Helps avoid signature based detection

StegoBot Concept

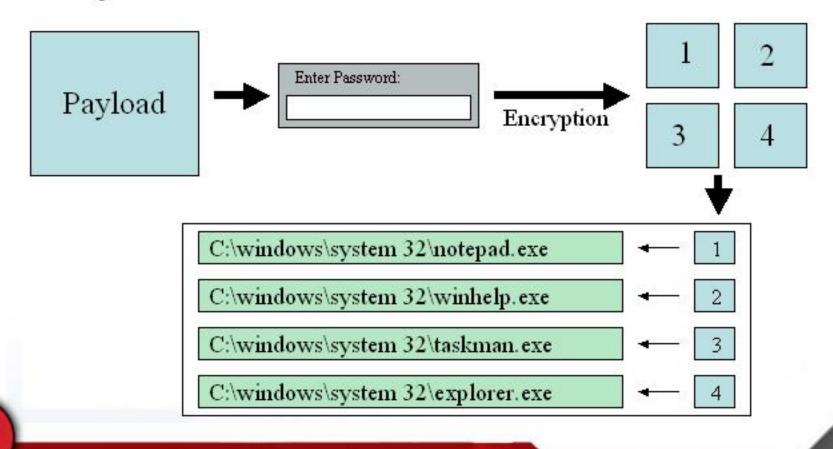
- The idea of the stegobot takes the stego noise concept one step further
- Sites with vulnerabilities can be infected with the stego noise virus
 - Infected files then pass on to the visitors of the site.
- E.g. The slammer worm hit critical mass in just 3 minutes

- Data hiding in common operating systems is quite easy
- Under NTFS, files can be hidden in Alternate Data Streams
 - Originally put in place with NTFS to provide compatibility with Mac OS
- Allows multiple files (streams) to be attached to ANY file
 - Regardless of ownership or permissions

- Files with alternate streams of data could also be encapsulated and moved across normal TCP/IP enabled networks
- Windows does not come with default tools for listing ADS
 - Files stored in an ADS will not show up in listings
 - File size of carrier does not show an increase

- Project Prometheus, at securitytribe.com/~vertigo/ plans to allow for ADS transmission across TCP networks
- We're also working on ways to use ADS for secure storage on host computers
- Critical files could be stored in distributed streams across a file system
 - Files are broken into parts, each part is encrypted, stored in separate ADS across the system

Project Prometheus



- Manipulating text is an easy
- 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

- Mailing lists are a dime a dozen now
 - Easy to buy
 - Easy to Generate
- Contain millions of email addresses
- Using a mailing list with millions of addresses and a few target addresses reduces the likelihood of detection
- Spam provides a perfect means for mass communication of covert messages

"Welcome to Black Hat Europe!"

- 10

111

22 22

-

III III

III III

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, Titlé 2, Section 306. This is a ligitimate 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 ligitimate business proposal . Why work for somebody else when you can become rich as few as 93 days!

"Welcome to Black Hat Europe!"

-

II II

30

III III

= =

10 E

10

- 10

III III

W 100

III IX

.

SE 19

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, Titlé 2, Section 306. This is a ligitimate 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 ligitimate business proposal. Why work for somebody else when you can become rich as few as 93 days!

Word Manipulation



- Perfecting the engine used to create spammimic.com is just a matter of time.
- Remove redundant strings
- Increase coherency within the email
- Having mass emails deleted by spam filters is not an issue
 - Messages can be conveyed to personal accounts not using spam filter technology
 - Intended recipients still get the message

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 nonsense when read in depth
 - But most folks don't get this far
- The sheer amount of spam on the Net would make detection of actual messages very difficult

Covert Network 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

Black Hat Japan 2004

Covert Network Channels

Standard IPv4 Header

Ver	HLEN	Service :	Туре	Total Length
le	dentifica	tion	Flags	Fragment Offset
1	TL	Protoco	1 1	Header Checksum
		So	urce IP Add	ress
		Desti	nation IP Ad	dress
	110000	tions	Î	Padding

Covert Network Channels

- ID field (IPv4 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

Other possibilities:

- IPv4 Sequence Number field
- IPv4 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

Future Network Channels

- IPv6 provides a mechanism for growth on the Internet
- It also provides the possibility for new forms of network covert channels
- Most IPv6 implementations today represent tunneled IPv4 protocols
 - Provides further potential for hidden information in an IPv6 tunnel
 - The Header Extension field could allow for additional mechanisms for covert channels
 - E.g. The Destination Options Header

Future Network Channels

Standard IPv6 Header

Ver	Priorit	у	Flow Label	
Payload Length		Next Header		Hop Limit
	So	ource IF	Address	
	De	estinatio	on IP Addres	s
Next F	Header			
4		3	2 Bits	

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

Defensive Mechanisms

- Know where to look for hidden information
- Recognize the potential for hidden information
- Utilize least privilege to control access to operating systems
- Know what tools exist to create these channels
- Know what tools exist to help detect covert channels

Black Hat Japan 2004

Defensive Mechanisms

- It becomes more difficult to create covert channels when operating systems are locked down
 - Least Privilege
 - No ability to install software
 - No access to critical system files or registry
- Users lose the ability to easily create hidden data on your networks

Detection Products

- Stego detection industry is still very young
- Few detection tools are available
- Few detection tools that work reliability
- Too many false positives
 - Difficult to detect covert channels
 - 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/CsADS
 DetectorArticle.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
- You can only combat covert channels if you understand how it works

Contact Information

- Russ Rogers
- russ@securityhorizon.com
- http://www.securityhorizon.com
- vertigo@securitytribe.com
- http://www.securitytribe.com

