Covert Channels:
Tunneling for Fun and Profit

Inveniam viam aut faciam

“What are they?”

- Commonly known as: How to hide data
- I suggest: Unexpected ways to transfer data
- The definition change should accompany a mindset change
- Think like a crook to catch a crook
- Use normal resources in unexpected ways

Inveniam viam aut faciam

“What is the fuss about?”

- Loss of sensitive data
- Storage of inappropriate data
- Transmission of inappropriate data
- Industrial espionage, loss of data assets, theft, etc
- Any secret communications, i.e. - Terrorism
- Basically can be used to hide any data wanted
- We’ll be looking a 3 easy and common methods

Inveniam viam aut faciam

“Using an Operating System”

- Windows is commonly used
- Perfect case of a feature causing a security problem
- Even not using the features causing ADS will not help
- No special software is needed to hide the file or to execute it
- Microsoft still does not ship with a default detection utility
- Still works in the latest versions of windows
- Even works via the web
- <Demonstration>

“Using Common Files”

- Two common types looked at: .bmp and .wav
- Uses steganography techniques
- Data which is hidden can be encrypted
- Once a file is used, it can be transferred in any manner
- Not at all difficult to do
- <Demonstration>

Inveniam viam aut faciam

"Using Network Channels"

- We all have firewalls, and we use them to limit traffic
- But do we always know what can be done?
- How do we use firewalls to protect trust relationships and tunneling?
- Network tunneling can use normal tools, and any open channel
- Network tunneling can be used recursively
- Network tunneling can decimate most firewalls
- <Demonstration>

“What Else?”

- Covert channels can use many other ways to transfer data..
- Messages disguised as spam
- Using multiple carrier files to store data
- OS covert channels can even be used for DOS attacks and viruses
- Network covert channels can use packet space or even steganography
- Any new data/protocol/feature can be used for covert channels – Skype
- Physical covert channels
- This is why I say: Think like a crook to catch a crook

Inveniamviamautfaciam

Thank you for your attention

http://www.adeptus-mechanicus.com/codex/cvrtads/cvrtads.html

http://www.adeptus-mechanicus.com/codex/sshfwd/sshfwd.html

http://www.adeptus-mechanicus.com/codex/pttyossh/pttyossh.html

Inveniam viam aut faciam