SWINBURNE UNIVERSITY OF TECHNOLOGY

ICT30010 eForensic Fundamentals

Lecture 10

Anti-Forensics

Troy Pretty

Digital Forensic Analyst

Outline and learning goals

- What is anti-forensics
- Computer anti-forensics
- Network anti-forensics

Anti-forensics

- What steps can be taken to hinder a forensic investigation?
  - Avoid detection
  - Hinder information collection
  - Increase time it takes
  - Create doubt in forensic report
  - Divert blame

Anti-forensics

- Information can be
  - Hidden
  - Encrypted
  - Deleted
  - Anonymised

Anti-forensics

- Issues
  - Ease of access to anti-forensic software
  - Vendors secure by default
  - Users are becoming more aware of how to cover their tracks
    - No longer about hiding your browser history from your spouse
    - More interested in hiding from the government/police
  - Mainstream media coverage / awareness
    - Snowden

Covert channels

- Steganography is a variety of covert channel
  - Not just the message is hidden, but the fact a message is being exchanged is also hidden
- Often the existence of communication between parties is as important as the content
  - Covert channels attempt to hide the very existence of there being communication
  - No “metadata” to be collected / examined

Covert channels

- Covert channels can be mapped onto any overt communication channel
- Internet based covert channels can be constructed in the following ways
  - Unused header bits
  - Optional header fields
  - Overloading of header fields such as the Initial Sequence Number in TCP
  - Packet rates (timing channel)
  - Packet reordering in TCP
  - Collisions and retransmissions
  - DNS queries
  - Payload tunneling (usually based on HTTP)
  - Online games

Steganography

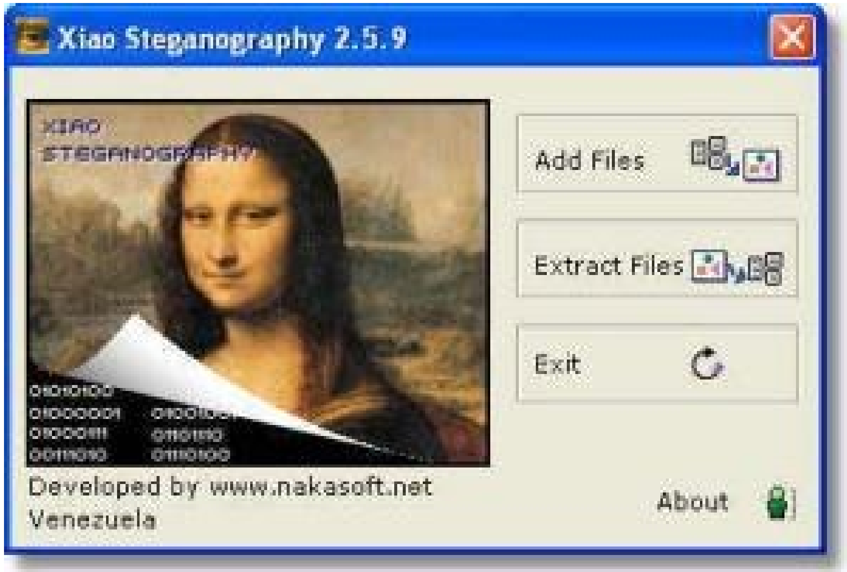
- “Hidden writing”
  - An example of a covert channel
- Hiding one signal inside another
  - Most well-known is hiding of data within images
  - Hiding of signal within audio files
- Typically makes use of the least significant bit in the overt signal

(a)

(b)

Steganography

- Many tools available
- Xiao Steganography
- Uses simple lowest bit to carry the message
  - http://www.garykessler.net/library/fsc_stego.html
  - http://xiao-steganography.en.softonic.com/



Developed by www.nakasoft.net
Venezuela

Overt channels

- Using coded messages over clear text channels
  - NSA communicating with operatives in foreign nations over public twitter feeds
    - Variation of a old cold war technique of using newspaper advertisements
  - Using code words in clear text forums to disguise original meanings

Cryptography

- Cryptography can be used as an anti-forensic technique in a number of ways
  - Encrypting files
  - Encrypting disks
  - Encrypting communications
- Properly encrypted data should be indistinguishable from random noise
  - Random noise is uncommon in practice, and therefore may be an indication of cryptography

Anonymisation

- Anonymisation is the process of hiding information about a particular user that can be used to trace their identity
- The TOR network (The Onion Router) the best known example
  - Provides a layer that hides the original IP address
  - Acts as a relay between the person seeking anonymity and the person or entity they are communicating with.
- Proxying/VPN a similar concept with the difference that it is not necessarily concerned with anonymity
  - Proxy servers sit between two hosts and act as a relay between them

Proxying

- Proxying
  - Configured in the web browser
  - Traditionally only used for web traffic (HTTP/HTTPS)
  - Not traditionally encrypted
  - Will only hide identity but not hide contents of traffic

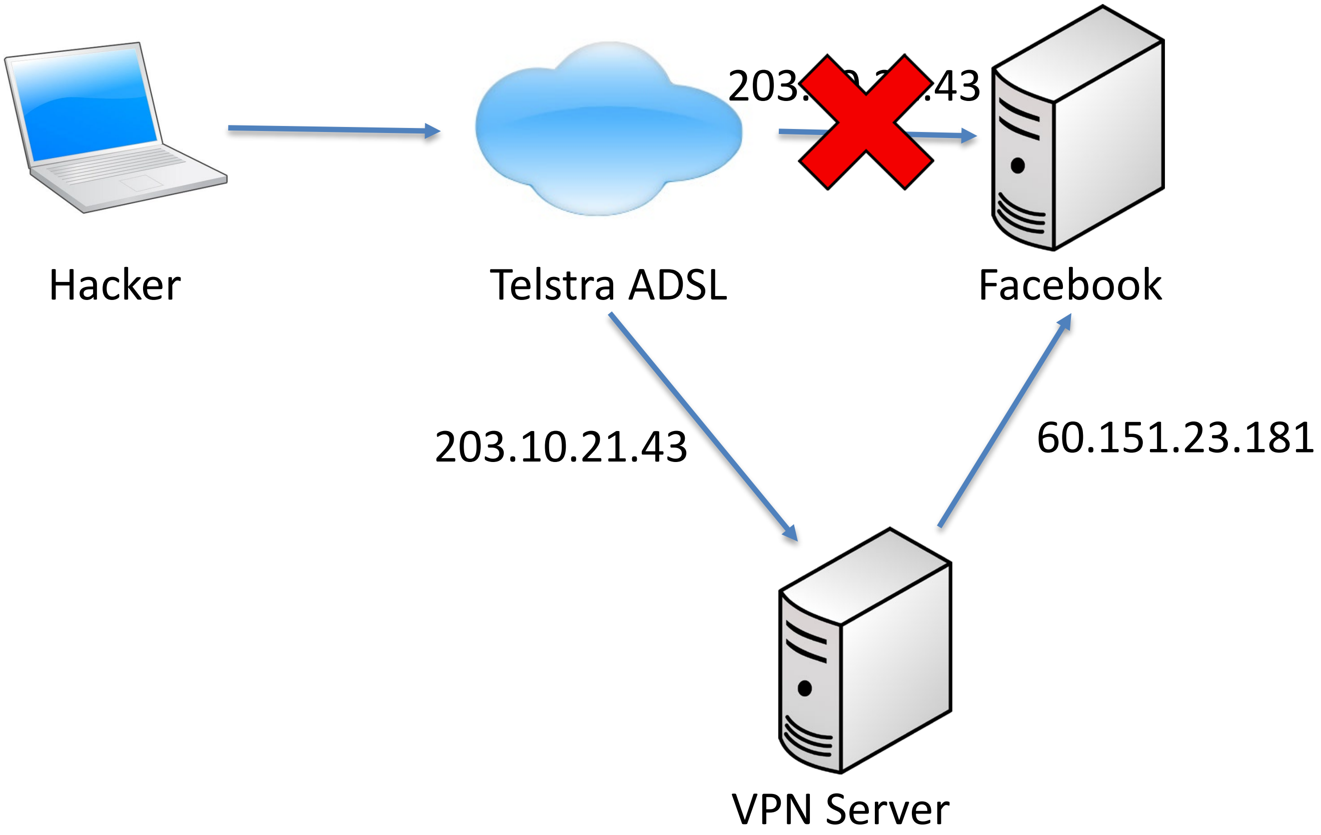
Virtual Private Network (VPN)

- Virtual Private Network (VPN)
  - Configured in network settings or with 3rd party software
  - Sends all traffic to the VPN server
  - Traditionally all traffic is encrypted
  - Originally used to connect securely from home to workplace over the internet
  - Commonly used to hide identity and contents of traffic

Proxying/VPN

- Free or paid services
- Used for the following:
  - Hide identity
  - Hide contents of traffic
  - Bypass geoblocking

Proxying/VPN



Hacker

Telstra ADSL

Facebook

203.10.21.43

203.10.21.43

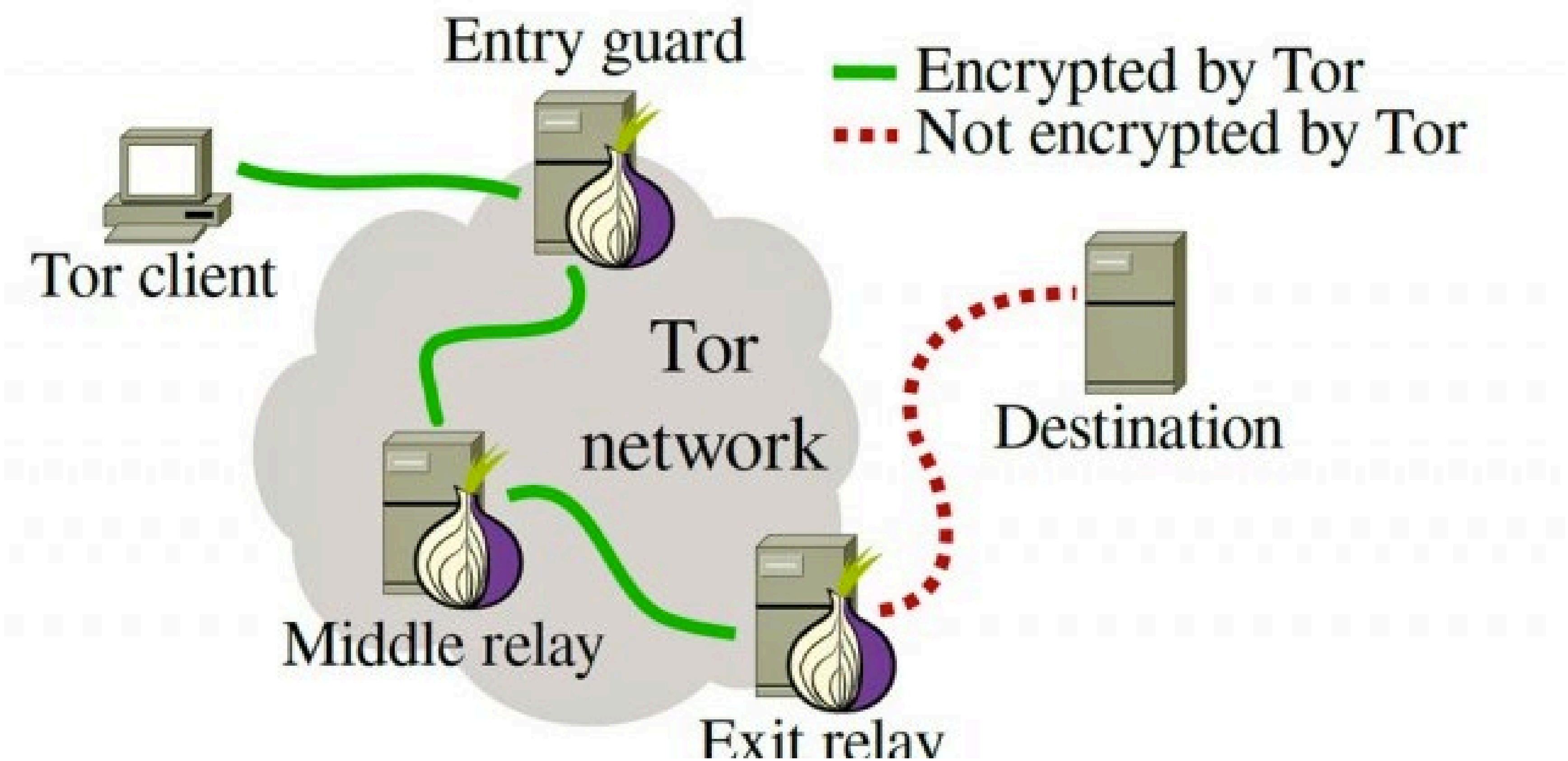
60.151.23.181

VPN Server

Onion Routing (TOR)

- Permits anonymous communication over the Internet
- Consists of an overlay network of “Onion” Routers
  - Each onion router communicates with other onion routers via the Internet
  - Each onion router has its own public / private key pair
- When wishing to communication across the network, a path is chosen via the onion routers
- The message is encrypted with each onion router’s public key
  - Layers of encryption, like an onion
- As each onion router receives a message it decrypts it, obtains the next hop information from the decrypted message and sends it to that next hop

Onion Routing (TOR)



.Source: arstechnica.com

Onion Routing (TOR)

- As each onion router receives the message it decrypts it using its private key
- Tor (The Onion Router) the most well known example
  - Each user runs a ‘Tor proxy’
  - Operates at the Transport layer using SOCKS
- Used primarily for anonymous access to web services
  - Also used for access to hidden services (Silk Road, etc.) on the darkweb
- Some weaknesses – exit node information is in plain text
  - Those hosting exit nodes have sometimes been blamed for actual user’s traffic (e.g. child pornography)

Cloud Computing

- Renting Online Servers
  - Amazon AWS
  - Botnet for hire
- Compromised computers
  - Backdoors/Trojans

Alternate Data Stream

- NTFS supports the concept of Alternate Data Streams
  - Within NTFS parts of the file can be used to store attributes such as author, title, thumbnail and the like
  - These can also be used to hide data from applications
  - Example from Lab 4
    - Encountered a file titled: Just a text file.txt:client.zip.exe
    - File “Just a text file.txt” contains an Alternate Data Stream client.zip.exe

Software

- Timestomp
  - Overwrite (stomp) on MAC times
- CCleaner
  - Secure data deletion
- Bootable OS’s
  - Run in RAM only
  - No evidence after a reboot
- Built-in encoders
  - MS Word
    - Change font size/colour, text boxes, resized images

Secure data deletion

- Deleting a file and erasing a file are usually quite different operations
- Deleting usually means merely marking a particular area of disk that was used by a file as being free
  - The actual content of the file is rarely overwritten by simple deletion
- Secure deletion (sometimes 'erasing') involves removing the actual contents of the file as well as its directory entries
- To erase data need to use a utility such as scrub in Unix systems or Eraser in Windows
  - Writes a random pattern of 0s and 1s to the disk
  - Does it several times

Overwriting Metadata

- Many applications generate metadata that is embedded within the file
- Examples include authors, dates, comments and revisions
- Metadata removal removes metadata or overwrites it
  - The process of converting a Word document to a PDF document removes much of the metadata associated with the Word document

Summary

- Many anti-forensic techniques
- Can be classified into
  - Hiding data
  - Encrypting data
  - Deleting data
  - Anonymising data