University of St Andrews

School of Computer Science
North Haugh
St Andrews KY16 9SX
Scotland, UK

Covert Channels in Internet Protocols

Network Forensics and Covert Channels Analysis in Internet Protocols

David Llamas
PhD Student

Email david@dcs.st-andrews.ac.uk
Web http://www.dcs.st-andrews.ac.uk/~david

BCS Symposium on Intelligence in Security and Forensic Computing
Centre for Mobile Computing and Security
School of Computing at Napier University, Edinburgh 3 Apr 06

Director of Studies:
Dr. Colin Allison

2nd Supervisor:
Dr. Alan Miller

This work is supported by the Defence Science and Technology Laboratory - **DSTL** - a part of the Ministry of Defence of the United Kingdom

Introduction to Network Forensics

- In general, Computer Forensics is the collection, preservation, analysis and presentation of computer-related evidence.
- Although, there does not exist a formal definition of the term **Network Forensics**, it could be said that is a subset of Computer Forensics that mainly deals with the information from networks, at different levels:
  - Topology
  - Hardware devices
  - Configurations
  - Network traffic
  - Etc

Scopes in Network Forensics

Generic

- OS fingerprinting
- Dissection of headers
- Routing analysis
- Tunnelling
- Etc.

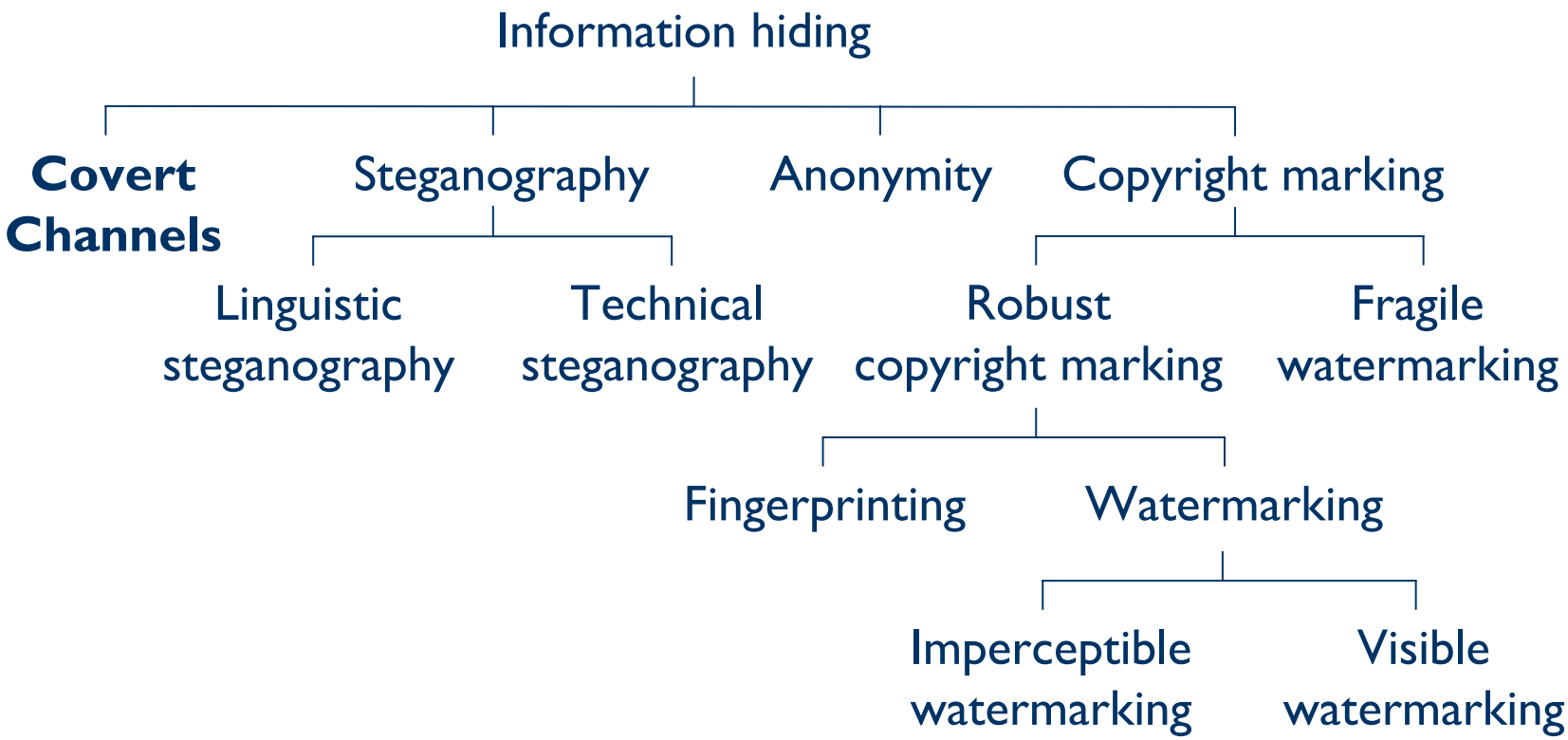
Information Hiding

- Codes
- Steganography
- Covert Channels
- Obfuscation
- Etc.

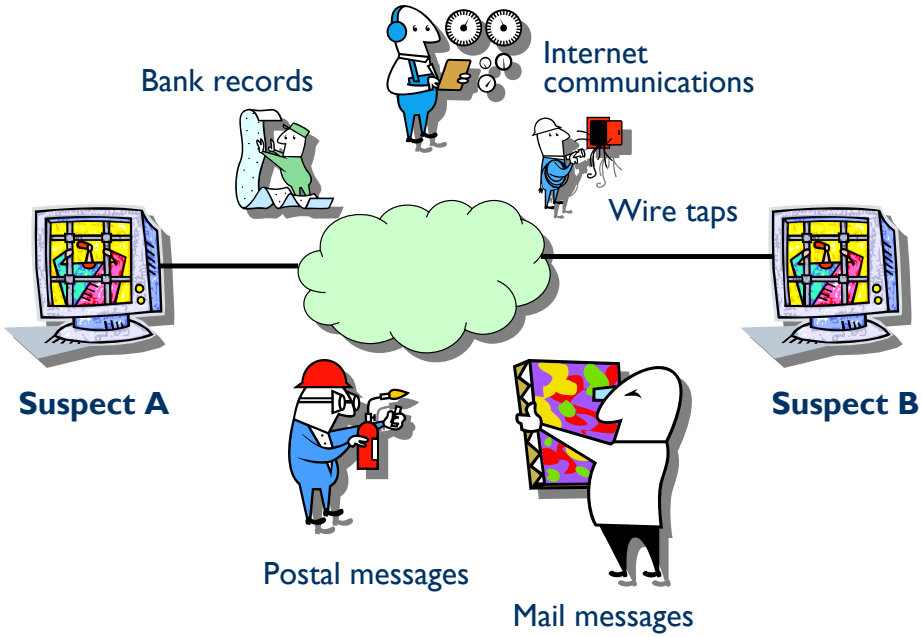
Introduction to Information Hiding

- **Information hiding** is a general term encompassing many disciplines: covert channels, steganography, watermarking, anonymity and so on.
- **Information hiding** is different than cryptography. cryptography is about protecting the content of messages while **Information hiding** is about covering the message within an innocent context or framework.

Information Hiding Classification



Covert Channels Definition

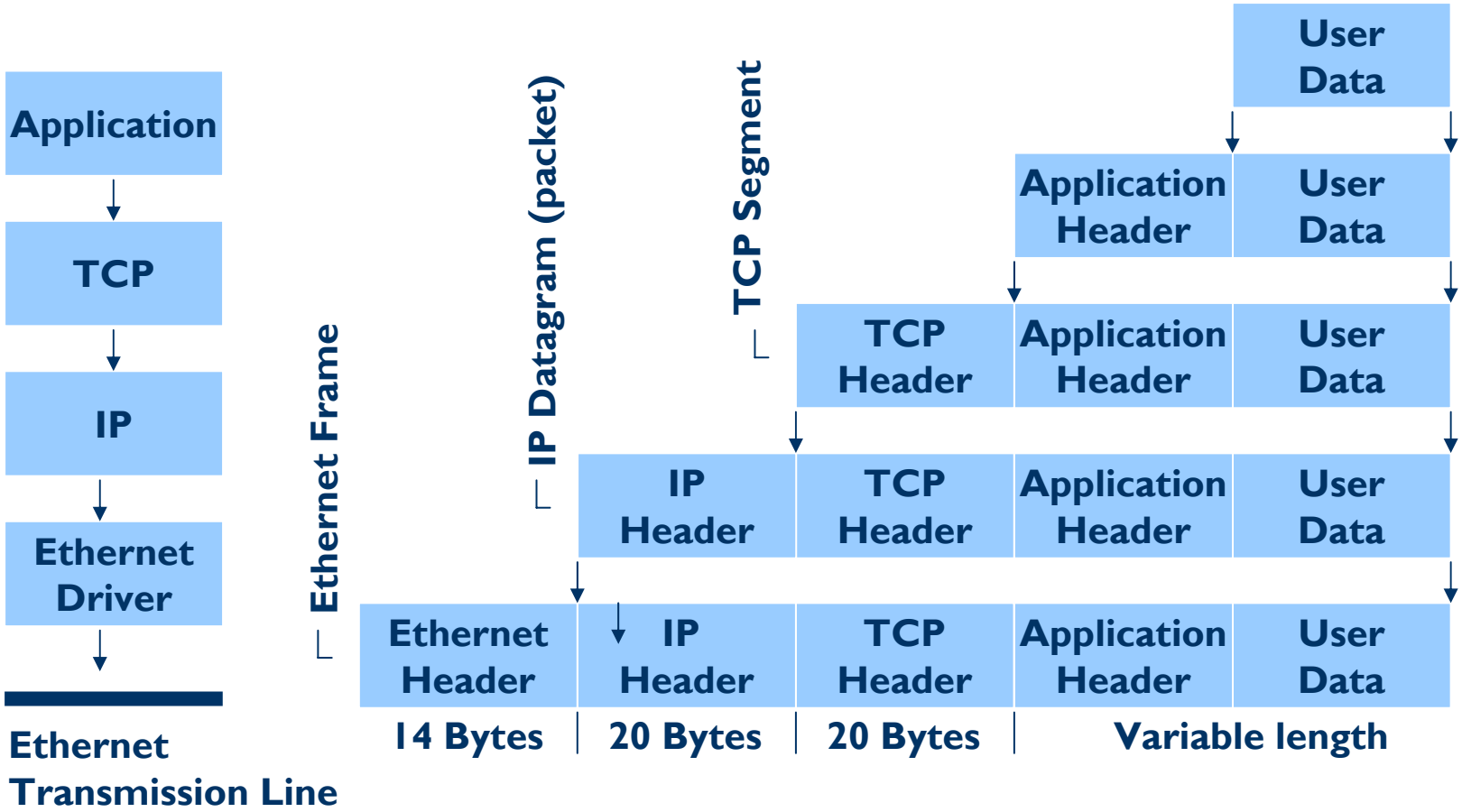


- It is a way of communicating which is not part of the original design of a system, and can be used as a covert way to transfer information between users.

Covert Channels Classification

- **Scenarios**
  1. **Storage**: One process uses direct (or indirect) data writing, whilst another process reads the data.
  2. **Timing**: The modulation of certain resources are used in order to exchange information between processes.
- **Noise**
  1. Based on the probability of receiving exactly what the sender has transmitted
- **Information Flows**
  1. **Aggregated channels**
  2. **Non-aggregated**

Digital Network Based On Layered Model



Covert Channels Analysis in Protocols

WHAT?

Analysis of:

- **Capacity**: The amount of data that can be transmitted through the covert channel
- **Reachability**: If a covert channel is established how far can it reach through the Internet?
- **Suitability**: how appropriate is what is used to be the base of the covert channel for that purpose?
- **Detectability**: the cost that is attached to the detection and other aspects.
- **Disruptability**: Is it possible to disrupt the covert channel transparently, so that the overt data flows and functions associated with the protocol are not adversely affected?
- **Etc**

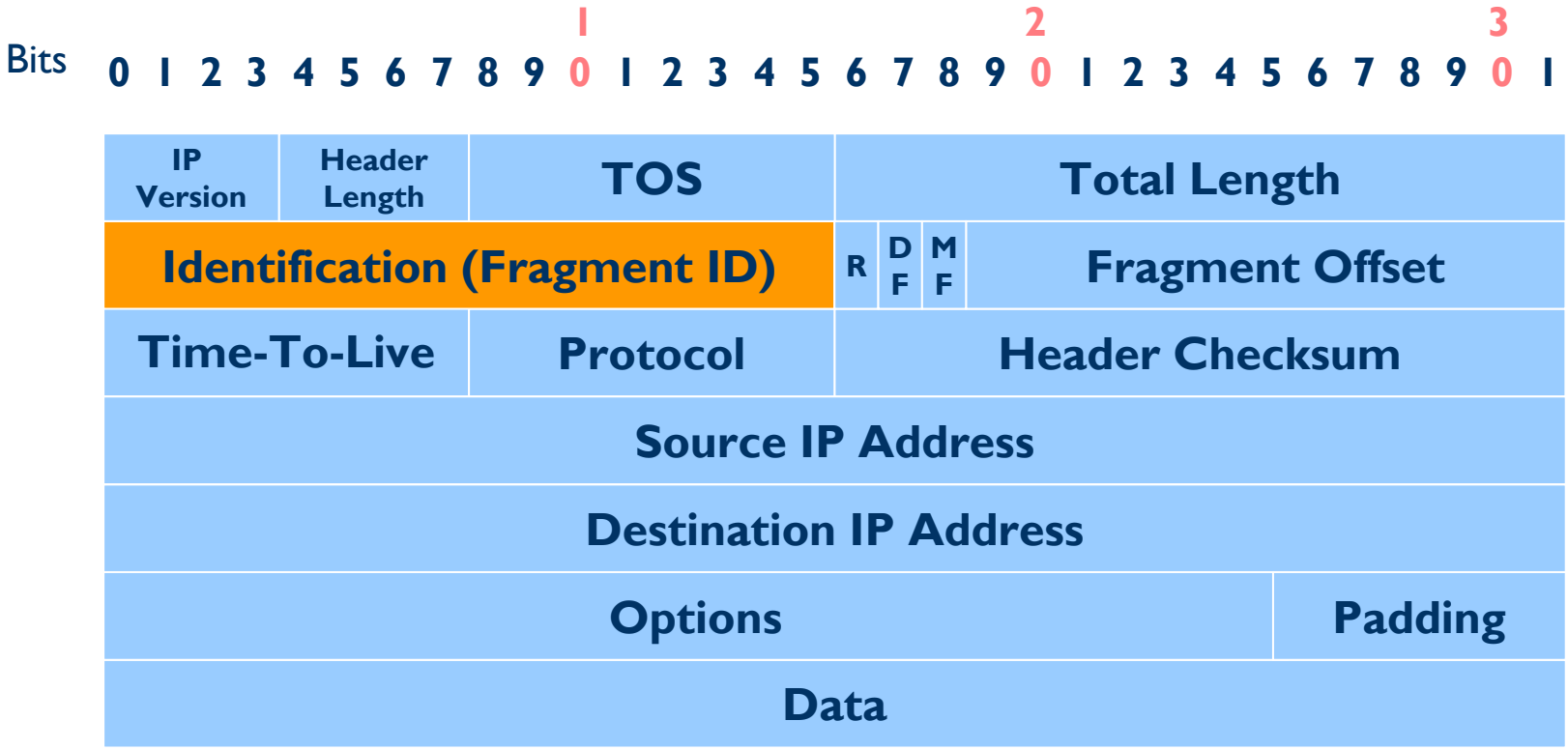
Covert Channels in Protocols Analytical base - I

HOW?

Traditional Analysis based on:

- Authoritative definition

IPv4 Header Format



IPv4 Fragment ID field Authoritative Definition - I

- According to RFC 791 (Internet Protocol):

  "The identification field is used to distinguish the fragments of one datagram from those of another."

  "The originating protocol module of an internet datagram sets the identification field to a value that must be unique for that source-destination pair and protocol for the time the datagram will be active in the internet system."

IPv4 Fragment ID field Authoritative Definition - II

- According to RFC 791 (Internet Protocol):

  "It seems then that a sending protocol module needs to keep a table of Identifiers, one entry for each destination it has communicated with in the last maximum packet lifetime for the internet."

Example of the most consistent implementation of the IP version 4 authoritative definition:

The Mossad, the Israel Secret Intelligence Service website

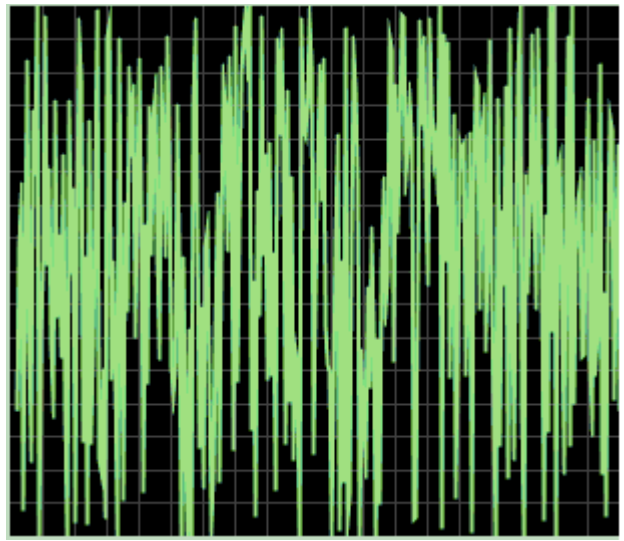
IPv4ID – Authoritative definition - Monitoring traffic

```
Command Prompt - tcpdump -v src host www.mossad.gov.il
16:56:57.546875 IP (tos 0x0, ttl 108, id 24079, o
8:  . 10185:10721(536) ack 580 win 65535
16:56:57.578125 IP (tos 0x0, ttl 108, id 25528, o
9: P 1:267(266) ack 723 win 65535
16:56:57.640625 IP (tos 0x0, ttl 108, id 14189, o
8:  . 11793:12329(536) ack 580 win 65535
16:56:57.640625 IP (tos 0x0, ttl 108, id 16209, o
8:  . 12329:12865(536) ack 580 win 65535
16:56:57.640625 IP (tos 0x0, ttl 108, id 20877, o
8:  . 11257:11793(536) ack 580 win 65535
16:56:57.640625 IP (tos 0x0, ttl 108, id 16515, o
8:  . 12865:13401(536) ack 580 win 65535
16:56:57.640625 IP (tos 0x0, ttl 108, id 44788, o
8:  . 13401:13937(536) ack 580 win 65535
16:56:57.656250 IP (tos 0x0, ttl 108, id 9853, of
:  . 14473:15009(536) ack 580 win 65535
16:56:57.656250 IP (tos 0x0, ttl 108, id 46102, o
8:  . 13937:14473(536) ack 580 win 65535
16:56:57.656250 IP (tos 0x0, ttl 108, id 3939, of
:  . 15009:15545(536) ack 580 win 65535
16:56:57.656250 IP (tos 0x0, ttl 108, id 22789, o
8:  . 15545:16081(536) ack 580 win 65535
16:56:57.656250 IP (tos 0x0, ttl 108, id 6047, of
:  . 16081:16617(536) ack 580 win 65535
16:56:57.656250 IP (tos 0x0, ttl 108, id 38878, o
8:  . 16617:17153(536) ack 580 win 65535
```

המוסד למודיעין ולתפקידים מיוחדים
ISRAEL SECRET INTELLIGENCE SERVICE

http://www.mossad.gov.il

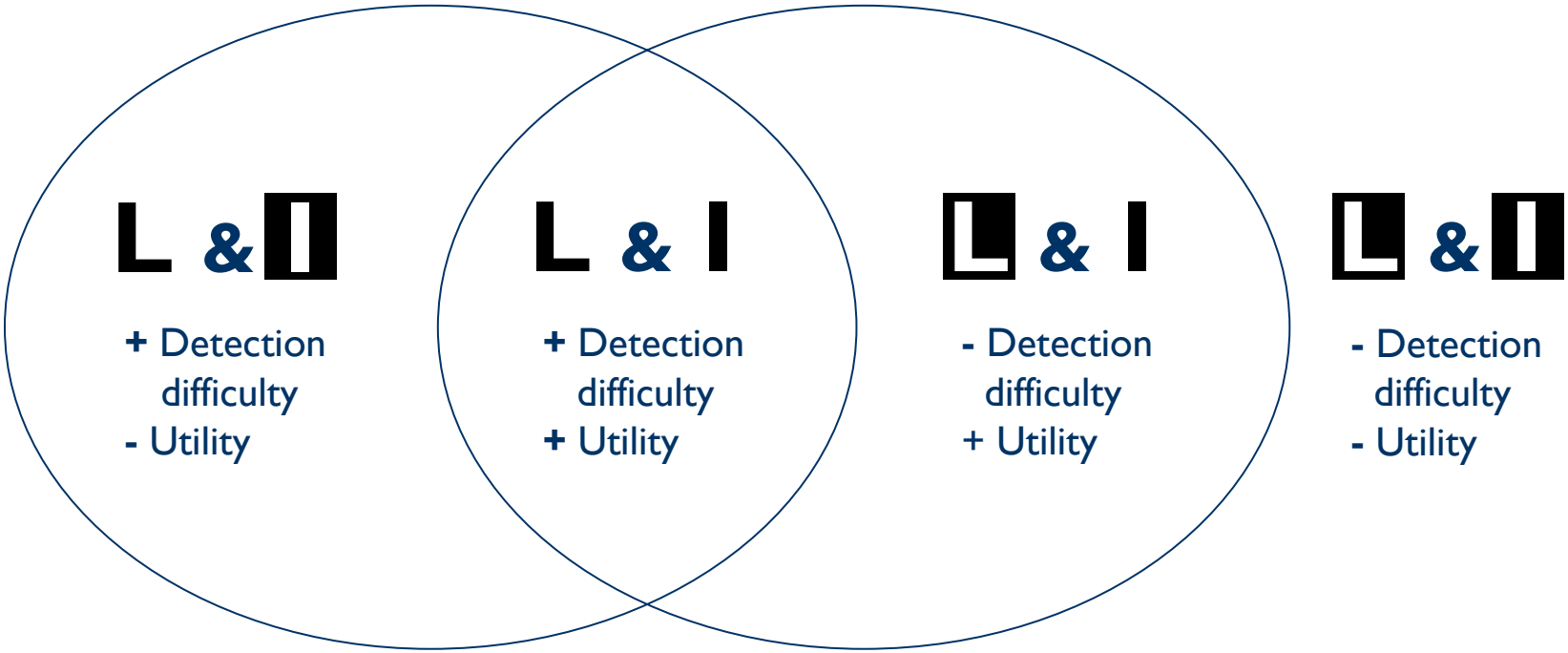
Network Traffic Oscilloscope



Covert Channels Analysis in Protocols

- Legal definitions of protocols are not precise enough to avoid ambiguities what promote the development of different protocol implementations.
- Covert channels could follow the legal definition but might not work at the implementation level, or
- They could not strictly follow the legal definition but work at the implementation level.

Detectability & Utility: Authoritative definition vs. Implementations - II



Covert Channels in Protocols Analytical base - II

HOW

Traditional Analysis based on:

- Authoritative definition

Extension to the Traditional Analysis

- **Implementations**

IPv4ID Implementations in the major operating systems

- In **MS Windows**, the IPv4ID increases monotonically until reaching the maximum value of 65,535 and then starts again from 0.
- From **Linux 2.4.x**, the IPv4ID generation algorithm is initialized associated with the TCP socket, and it's an incrementing sequence from there.
- **SUN Solaris**, the IPv4ID is initialized with a secure random number. IDs are simply incrementing from there or randomized each time is needed.
- The IPv4ID algorithm in **OpenBSD** uses a linear congruential generator, rekeyed every 3 minutes (or after 30,000 IDs have been generated, whichever is sooner).

Covert Channels Analysis in Protocols

- Implementations don't provide solutions for all scenarios that can be produced in the real world.
- Different combinations of implementations working together can show different views from the same traffic.
- External agents to the protocol implementation can interfere as well.

Fragment Identification field in IPv4 – Real world

Different types of interferences have been identified:

- Busy websites or websites based on farms of computers
- Interferences of middleware devices, such as routers, etc.
- Intrusion prevention systems / Firewalls
- Operating system distributions / configurations with specific purposes
- Etc

Covert Channels in Protocols Analytical base - II

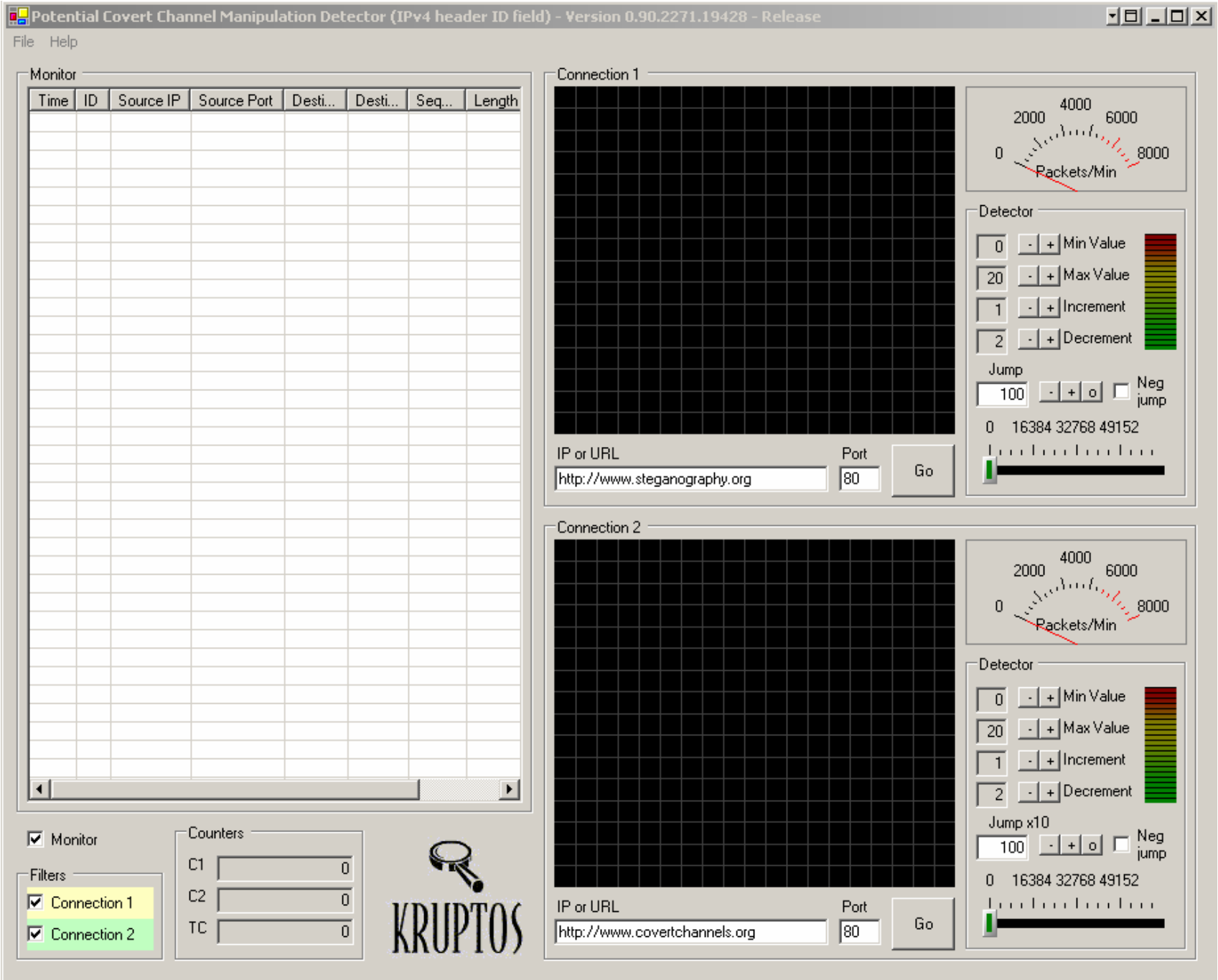
HOW

Traditional Analysis based on:

- Authoritative definition

Extension to the Traditional Analysis

- **Implementations**
- **Interferences produced from the context where the protocol is running**

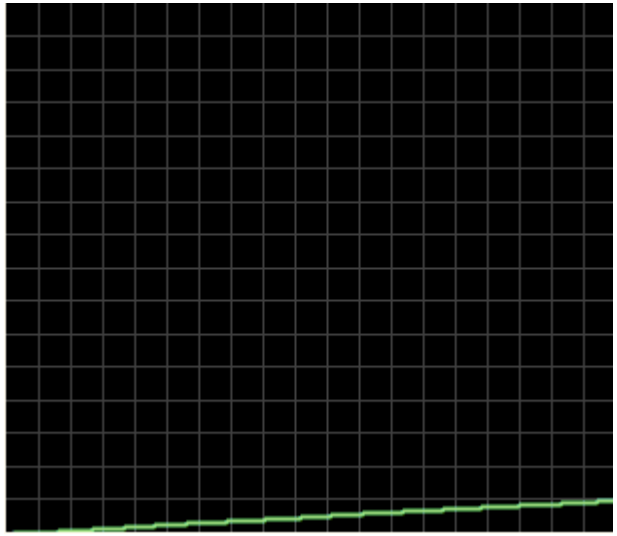

Potential Covert Channel Manipulation Detector (IPv4 header ID field) - Version 0.90.2271.19428 - Release
File
Help
Monitor
Time
ID
Source IP
Source Port
Desti...
Desti...
Seq...
Length
Connection 1
0
2000
4000
6000
8000
Packets/Min
Detector
0
Min Value
20
Max Value
1
Increment
2
Decrement
Jump
100
Neg jump
0 16384 32768 49152
IP or URL
http://www.steganography.org
Port
80
Go
Connection 2
0
2000
4000
6000
8000
Packets/Min
Detector
0
Min Value
20
Max Value
1
Increment
2
Decrement
Jump x10
100
Neg jump
0 16384 32768 49152
IP or URL
http://www.covertchannels.org
Port
80
Go
Monitor
Filters
Connection 1
Connection 2
Counters
C1
0
C2
0
TC
0
KRUPTOS

IPv4ID – Implementations & Real World - Monitoring traffic - I

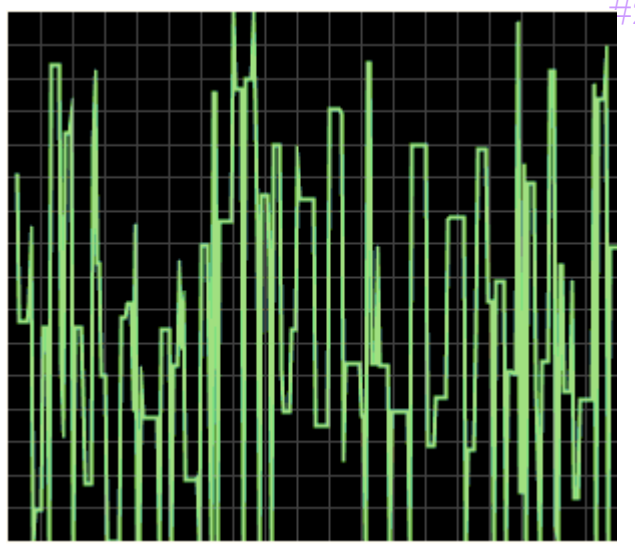
- Example of **MS Windows** implementation:
  http://www.covertchannels.org
  Specialised website about covert channels & steganography
- Example of **Linux 2.4.x** implementation:
  http://www.dcs-st.andrews.ac.uk
  School of Computer Science at the University of St Andrews
- Example of **SUN Solaris** implementation:
  http://www.ebay.co.uk
  Online marketplace
- Example of **OpenBSD** implementation:
  http://www.openbsd.org
  OpenBSD Project

IPv4ID – Implementations & Real World - Monitoring traffic - II

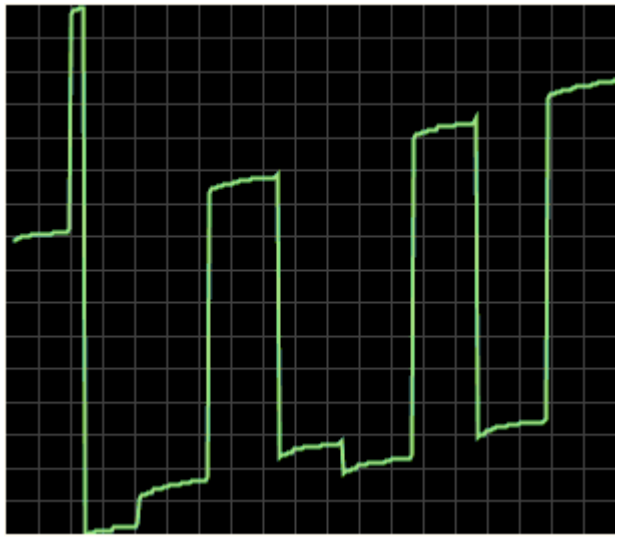
- Example of implementation affected by a Webwall **http://www.dstl.gov.uk**
  Defence Science and Technology Laboratory (MoD)
- Example of implementation manipulated by a Reverse Proxy Server/Disruptor: **http://test.dstl.info**
  Kruptos laboratory
- Example of implementation affected by a real covert channel: **http://213.123.198.144:8003**
  Kruptos laboratory
- Example of an unknown implementation: **http://xxx.xxx.xxx.xxx**
  Kruptos laboratory



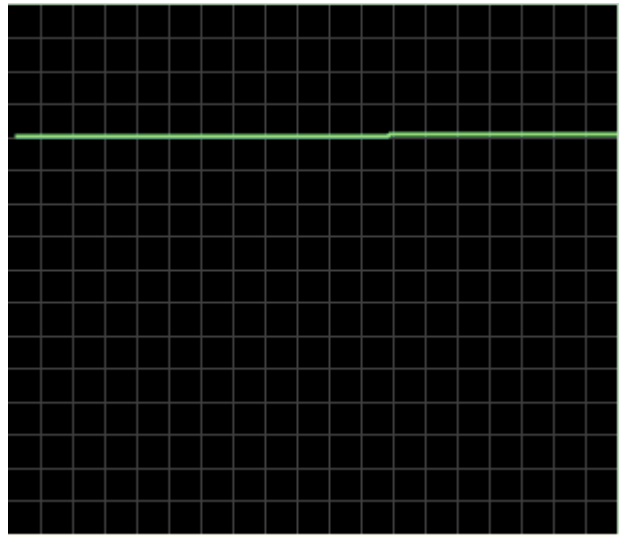
MS Windows – http://www.covertchannels.org



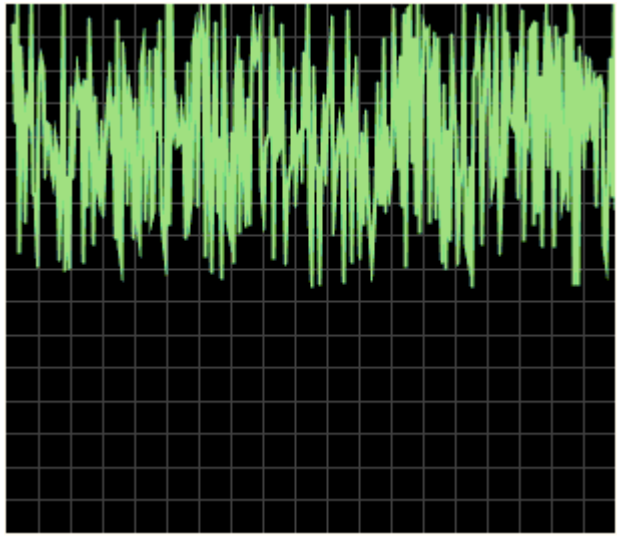
Linux 2.4.x - http://www.dcs-st.andrews.ac.uk



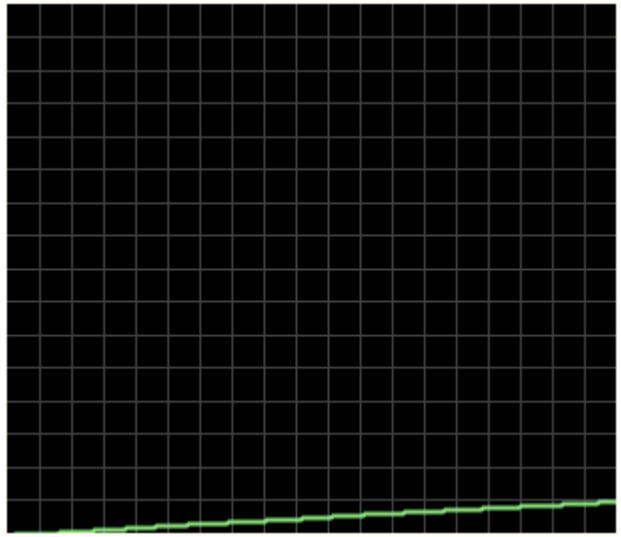
SUN Solaris – http://www.ebay.co.uk



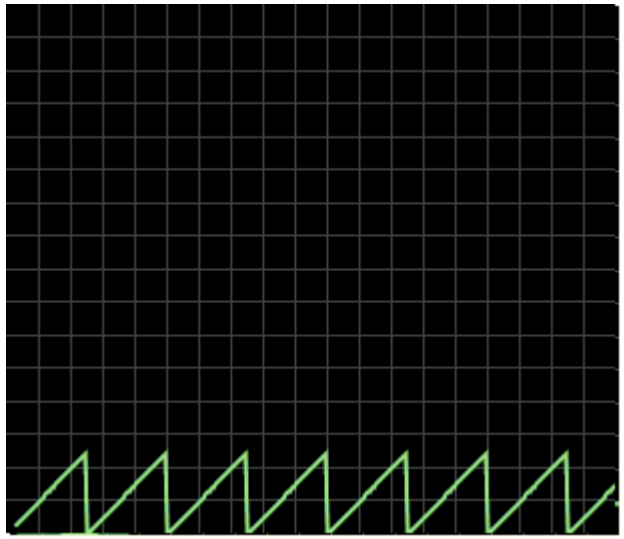
OpenBSD – http://www.openbsd.org



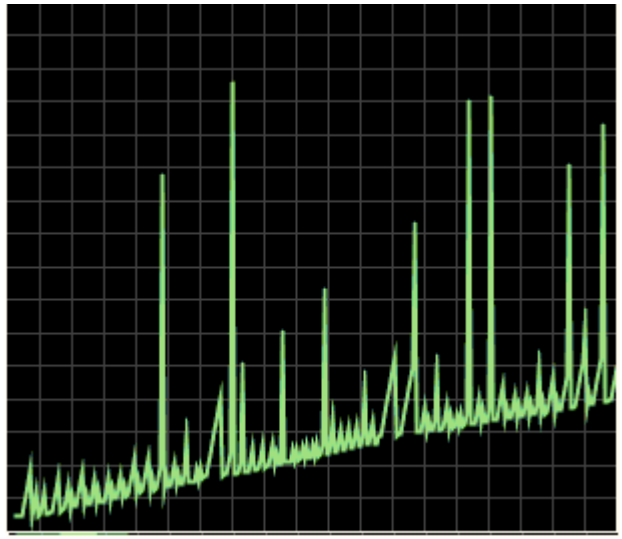
Webwall - http://www.dstl.gov.uk



Reverse Proxy Server –http://test.dstl.info

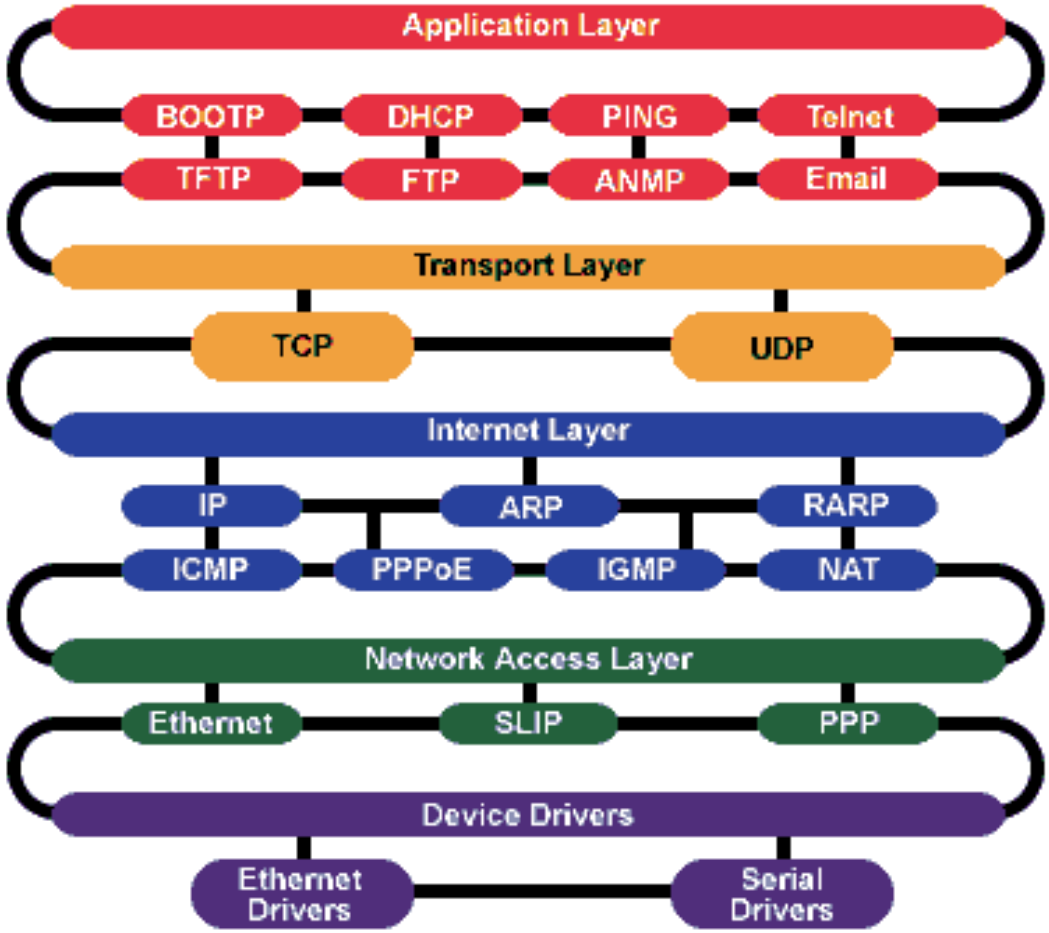


Real Covert channel based on IPv4ID



Unknown

Opportunities for the creation of covert channels exist at all layers in the TCP/IP protocol stack.



Covert Channels in Protocols Analytical base

HOW

Traditional Analysis based on:

- Authoritative definition

Extension to the Traditional Analysis

- Implementations
- Interferences produced from the context where the protocol is running

University of St Andrews

Thank you

David Llamas

PhD Student

University of St Andrews
School of Computer Science
Distributed Systems and Networks research group
North Haugh, St Andrews
Scotland, UK

For further information just *google* me or kruptos