Network Steganography

Florian Kemmer

Plymouth University

Unix Friends and User Campus Kamp
Furtwangen, 2014-04-11

About giving talks

You're not going to conferences to show off, but to receive valuable feedback from like-minded people in similar areas of research.

— *PhD student*

Who am I?

- MSc *Network Systems Engineering* at Plymouth University
- Worked one year in Academia
- BSc *Computer Networking* at HFU
- One term abroad at St. Pölten University of Applied Sciences

Contact
florian.kemmer@postgrad.plymouth.ac.uk
http://www.fkemmer.de

Table of Contents

Introduction

What is Steganography?

- Hiding information within other information
- Best explained with an example

Example: Spot the difference

(a) sha512: 20e37f[...]16aeae

(b) sha512: 27f6fb[...]65e956

Figure 1: `outguess -d message.txt -p100 angel_noSteg.jpg angel_steg.jpg`

Use cases for steganography

- Watermarking
- Hidden communication
- Information leakage
- Privacy Protection

Why would you use Steganography?

"Conventional cryptography is like shipping a safe in an armored car with a regiment of soldiers around it. Everyone knows that there's something secret inside."

– Description text of Wayner (2009)

Comparison

Cryptography

- Greek *kryptos* ("hidden" / "secret")
- Easy to discover
- Hard to break

Steganography

- Greek *steganos* ("protected" / "covered")
- Hidden in plain sight
- Doesn't attract attention
- If discovered, weakly protected

Network Steganography

General advantages

- Pictures (or other media) stored forever on the internet
- Widely available for forensic investigation
- Network traffic is rather volatile

Classic steganography

[Eth][IP][UDP/TCP][**PAYLOAD**]

- Payload gets modified as described before
- Protocols producing much traffic preferred
- Commonly used with VoIP
- Capacity depending on generated traffic

Header Modification

[Eth][IP][**UDP/TCP**][PAYLOAD]

- Using unused or unspecified data fields, e.g. in TCP Header
- Capacity depending on number of packets
- Easily defeated by *traffic normalisation*
- Hardly used

Packet Timing

- (unrequired) Retransmissions/duplicates
- Reordering
- **Inter-arrival times**

Network Covert Timing Channels

[Packet] Δt [Packet]

Active/Passive Covert Timing Channels

Active

- Actively generates traffic
- Easier to detect/harder to hide

Passive

- Doesn't generate traffic
- Throughput dependant on activity
- Highly hidden

On/Off timing channels

Idea

- Packet sent in interval: *1*
- No packet sent: *0*

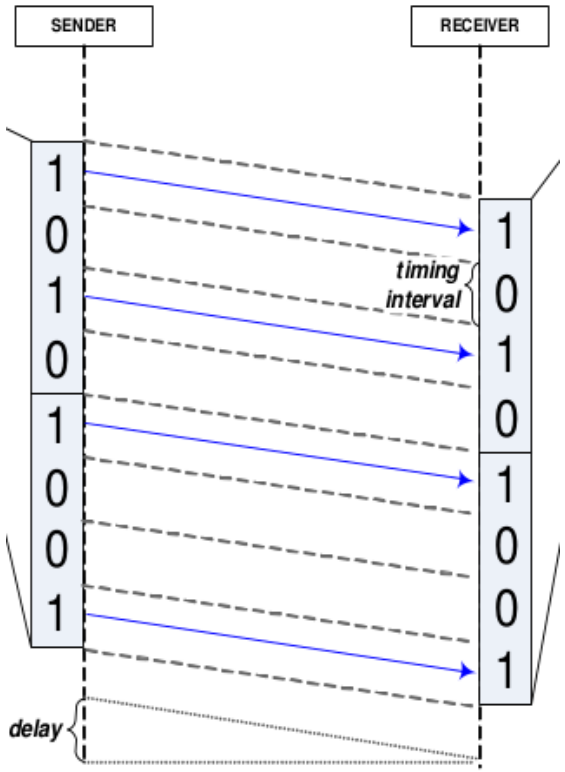

Figure 2: (Cabuk, Brodley and Shields, 2004)

Problems

- Synchronisation
- Long idleness for consecutive zeroes

"Morse code"

Idea

- Long-ish interval between two packets *1*
- Short-ish interval: *0*
- Non-binary codes possible

Problems

- Synchronisation
- Suspicious traffic pattern (see right)

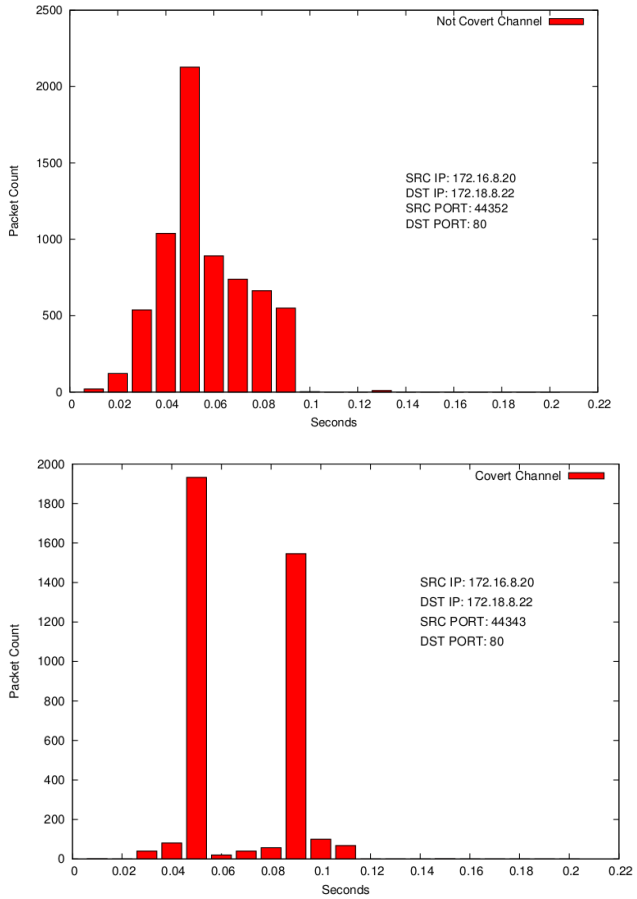

Figure 3: (Berk, Giani and Cybenko, 2005)

Timing is everything...

- Aiming is difficult
- Lots of things might happen on the way...

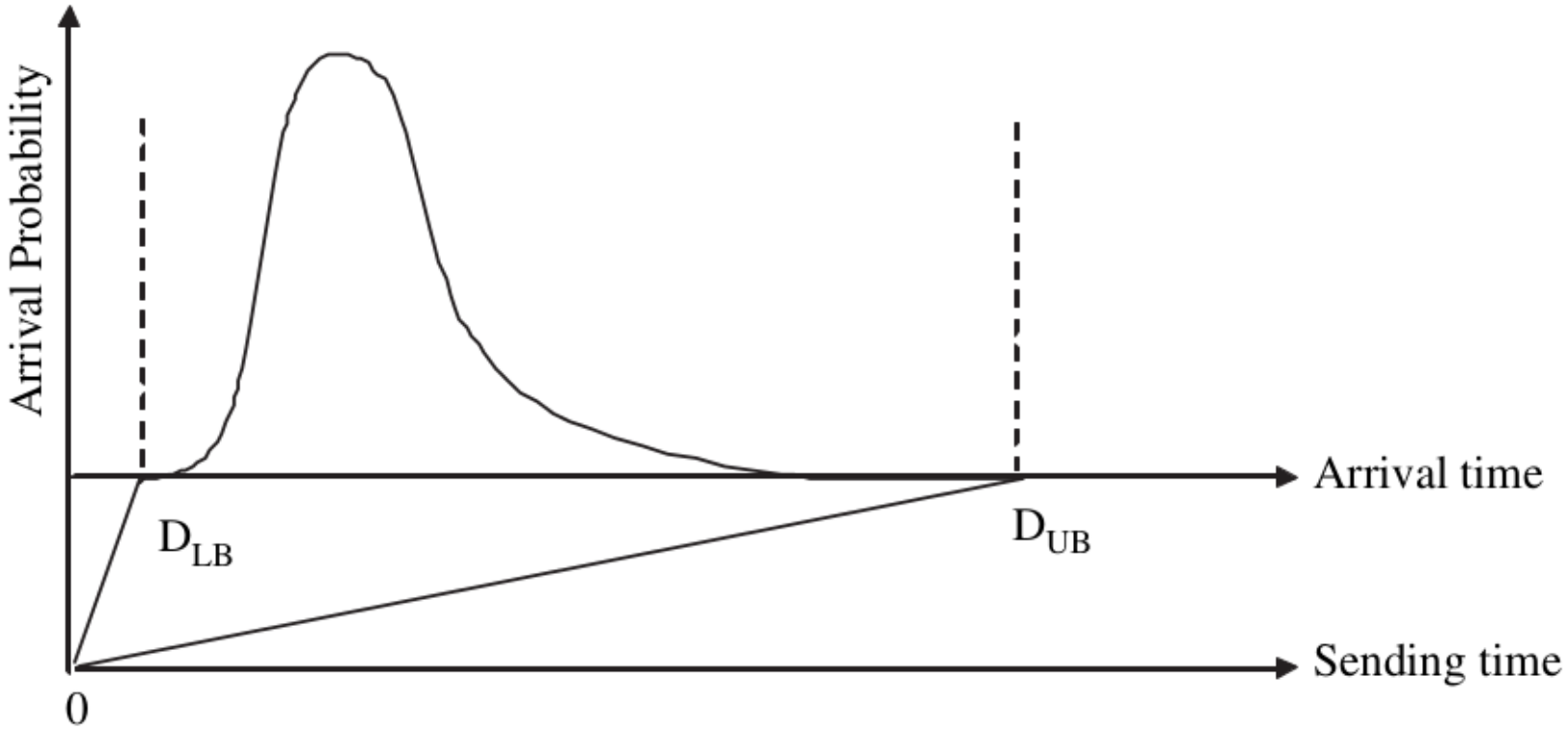

Figure 4: Packet delay in stable network according to Yao et al. (2009)

Defending Covert Timing Channels

Prevention

- Jamming delays
  Might affect legitimate traffic/users

Detection

- Shape based analysis
- Possibly able to trace origin

Summary

- Networks offer plenty of possibilities to hide messages
- Varying channel capacities
- Typically hard to detect
- Mainly researched in “Information Leakage”

Masters Project

Scenario description

- We're the good guys now!
- Fight censorship
- Cryptography doesn't work here
- Store hidden information in inter-arrival times

Differences to existing scenarios

- Two-way communication preferable
- Ability to generate traffic (less focus on bandwidth efficiency)
- Focus on fighting statistical analysis

Selection criteria for cover protocol

1. Large number of packets
2. Commonly used
3. TCP based
4. Independent of user action
5. Timely asymmetric
6. Bi-directional data-flow

Comparison of protocols (simplified)

	Packet number	*Commonly used*	*TCP based*	*User-independent*	*Asymmetric*	*Two-way*
"VoIP"	✔	✔				✔
SSH	✔	✔	✔		✔	✔
FTP	✔	✔	✔	✔	✔	✔

Table 1: Protocol Evaluation

Architecture (overview)

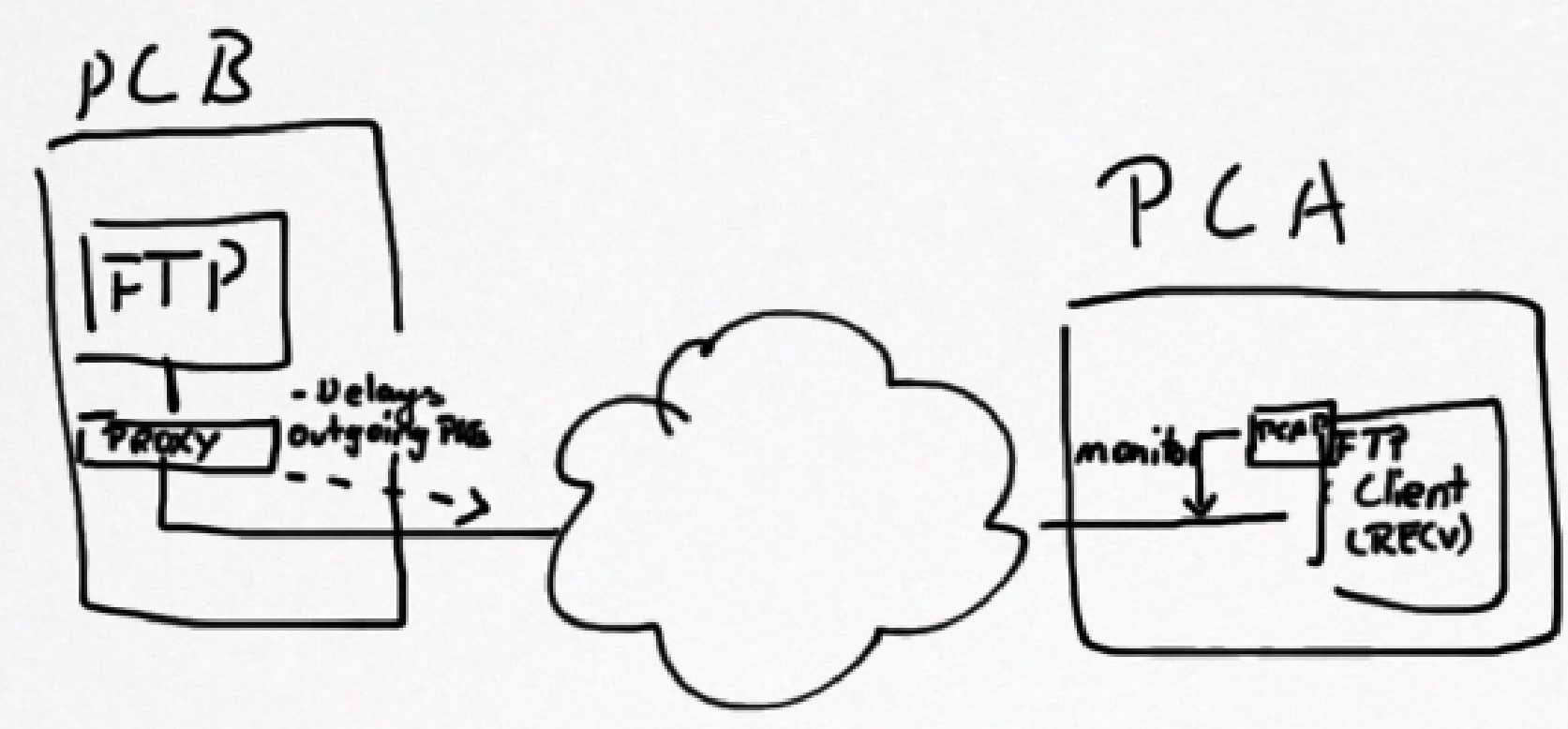

Figure 5: Architecture

FTP Proxy

- No need to write complete FTP server
- Admins can use their favourite server
- Can be moved away from original FTP server

FTP Proxy

- Intercepts FTP traffic
- Triggered by certain keywords (e.g. `RETR`, but not `LIST`)
- Delays returning packets according to $algorithm

FTP Client

- Standard client
- Separate monitor component (pcap) to extract incoming information

Expected ~~problems~~ challenges

- Jitter!
- Synchronisation
- Bandwidth/capacity

Conclusion

- Interesting and challenging field of research
- Still quite unexplored
- Looking forward to finishing exams and finally starting ;-)

Thank you!

Questions?

References I

Berk, V., Giani, A. and Cybenko, G. (2005). *Detection of Covert Channel Encoding in Network Packet Delays*. Department of Computer Science, Dartmouth College. URL: http://www.ists.dartmouth.edu/library/149.pdf.

Cabuk, S., Brodley, C. E. and Shields, C. (2004). "IP covert timing channels: design and detection". In: *Proceedings of the 11th ACM conference on Computer and communications security*, pp. 178–187.

Frith, D. (2007). "Steganography approaches, options, and implications". In: *Network Security* 2007.8, pp. 4–7. DOI: 10.1016/S1353-4858(07)70071-5. URL: http://linkinghub.elsevier.com/retrieve/pii/S1353485807700715 (visited on 26/11/2013).

References II

Lubacz, J., Mazurczyk, W. and Szczypiorski, K. (2012). "Principles and Overview of Network Steganography". In: *CoRR* abs/1207.0917.

Postel, J. and Reynolds, J. (1985). *File Transfer Protocol*. RFC 959 (INTERNET STANDARD). Updated by RFCs 2228, 2640, 2773, 3659, 5797, 7151. Internet Engineering Task Force. URL: http://www.ietf.org/rfc/rfc959.txt.

Walls, R. J., Kothari, K. and Wright, M. (2011). "Liquid: A detection-resistant covert timing channel based on IPD shaping". In: *Computer Networks* 55.6, pp. 1217–1228. DOI: 10.1016/j.comnet.2010.11.007. URL: http://linkinghub.elsevier.com/retrieve/pii/S1389128610003580 (visited on 23/02/2014).

References III

Wayner, P. (2009). *Disappearing cryptography: information hiding: steganography & watermarking*. 3rd ed. Amsterdam ; Boston: Morgan Kaufmann Publishers. 439 pp.

Yao, L., Zi, X., Pan, L. and Li, J. (2009). "A study of on/off timing channel based on packet delay distribution". In: *Computers & Security* 28.8, pp. 785–794. DOI: 10.1016/j.cose.2009.05.006. URL: http://linkinghub.elsevier.com/retrieve/pii/S0167404809000510 (visited on 12/12/2013).