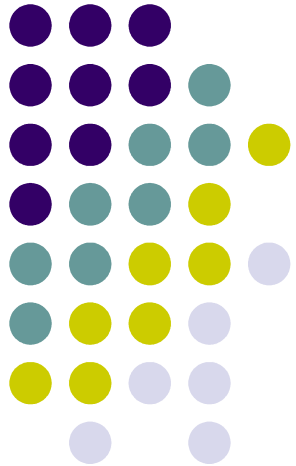
IP Covert Timing Channels: Design and Detection

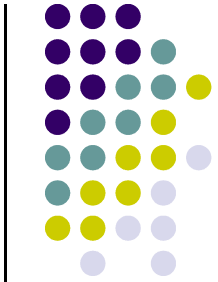
By

Serdar Cabuk, Carla E. Brodley, Clay Shields.



Outline

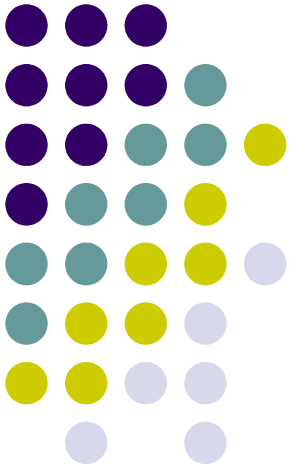
- Positive Traits
- Problems
- Questions
- Extensions
- Other Covert Channels
- Discussion



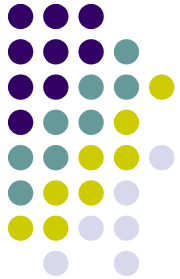
Positive Traits

- What are the redeeming qualities and/or contributions of this paper?

Problems

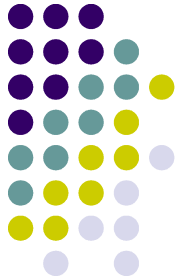


Acceptable Test Scenario #1



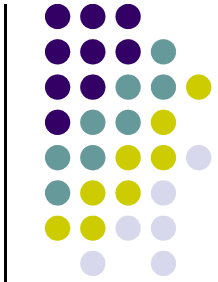
- Team 1 builds the covert channel and generates 3 logs, gives them to team 2.
- Team 2 does not know which or even if the logs have a covert channel.
- Team 2 tries to detect the covert channel.

Acceptable Test Scenario #2



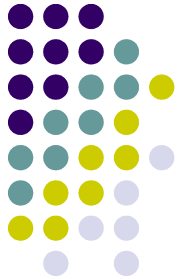
- Team 1 builds the covert channel and generates 3 logs, gives them to Team 2.
- Team 2 knows at least one log contains a covert channel, but not which log(s).
- Team 2 tries to detect the covert channel.

Testing Methodologies



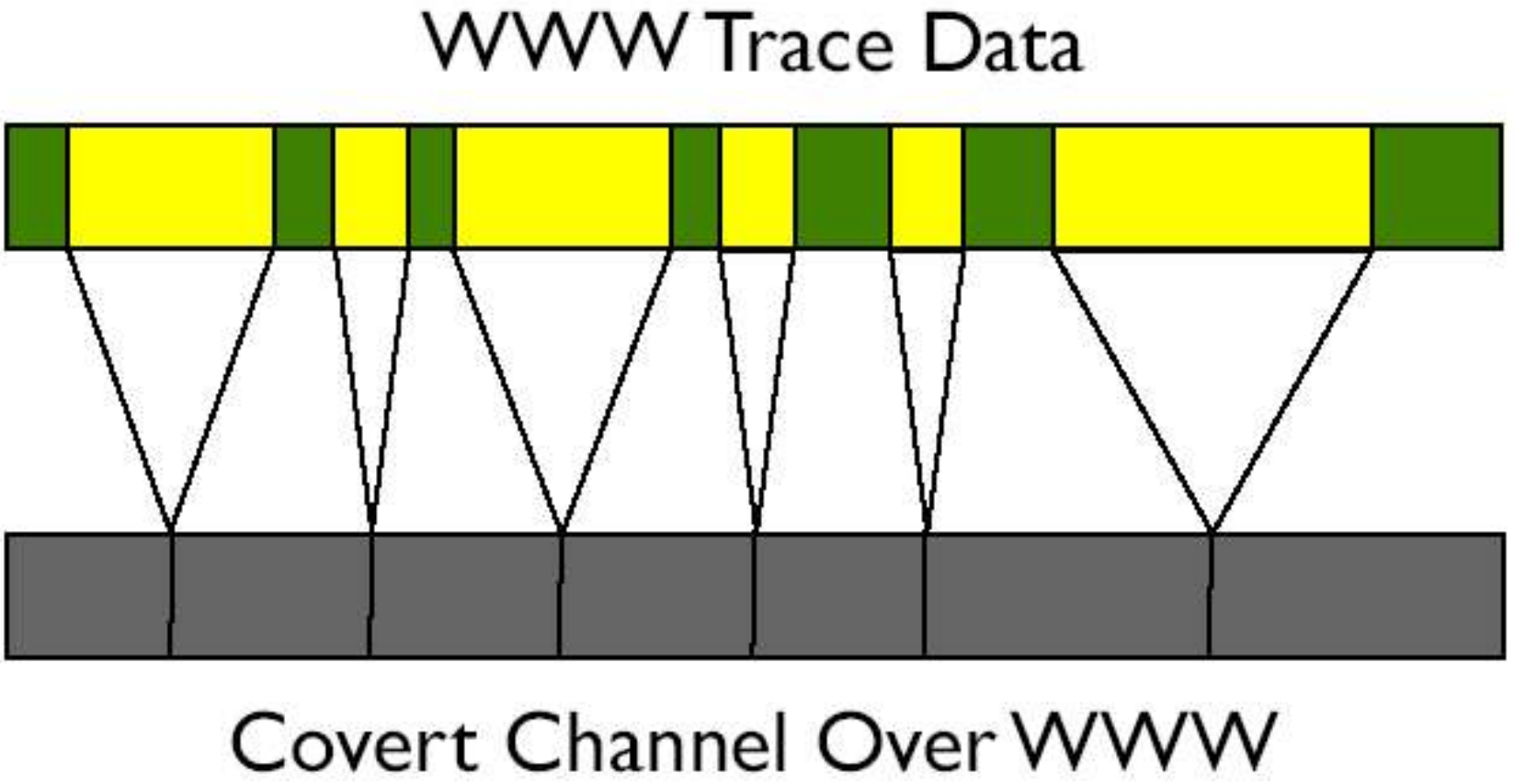
- Double Blind? No
  - Ideal, but not really plausible in computer science.
- Single Blind? No
- Eyes wide open? Of course.
  - A preferred method would be to make all data sets public to have them more openly scrutinized and tested.

Noise introduction

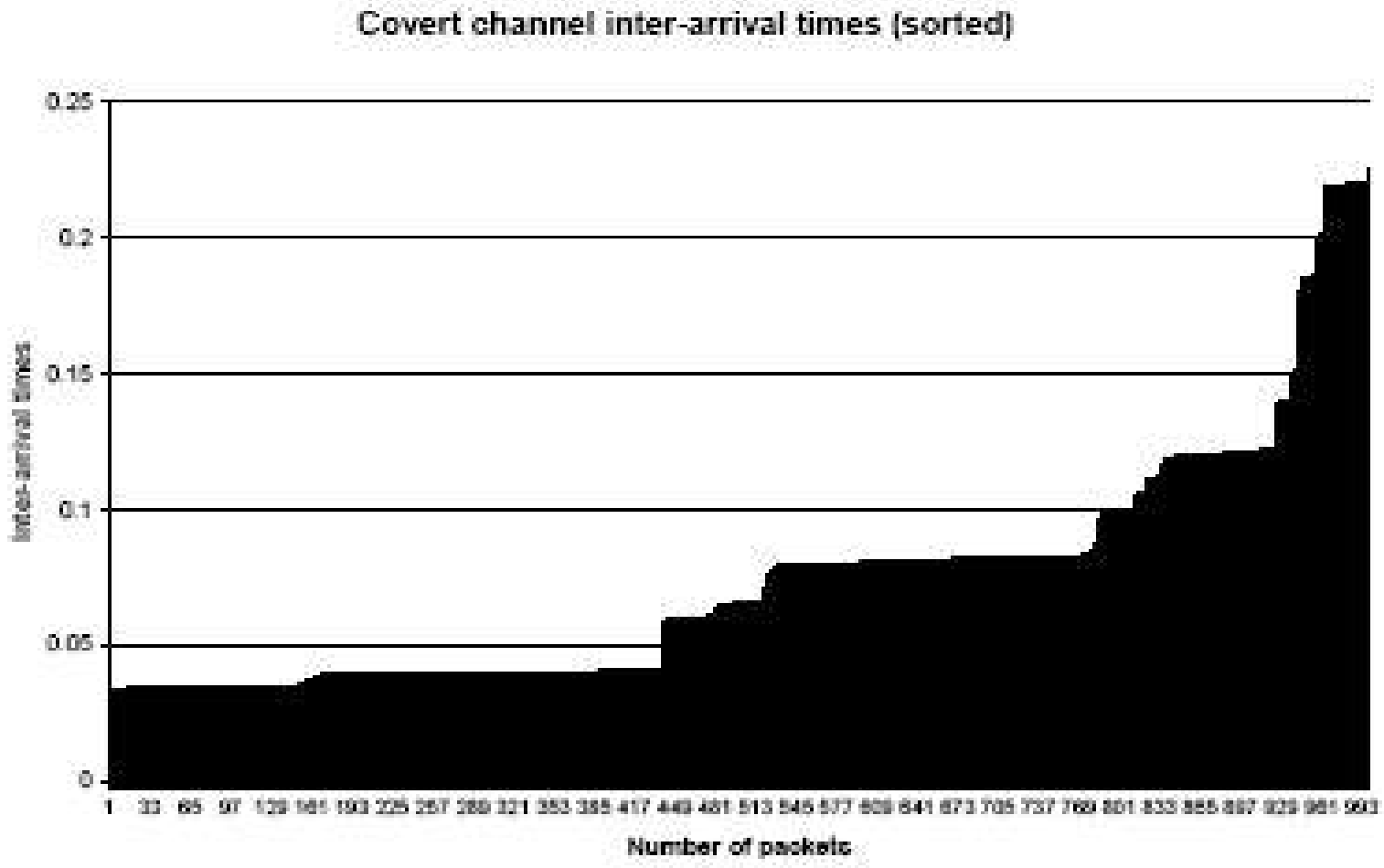


- What is the goal of introducing noise in Covert Channel III?
  - To introduce irregularity
  - To try to defeat e-similarity

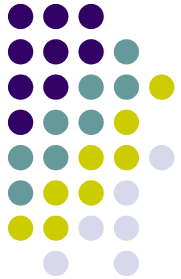
Noise introduction (cont)



Graphs and Data

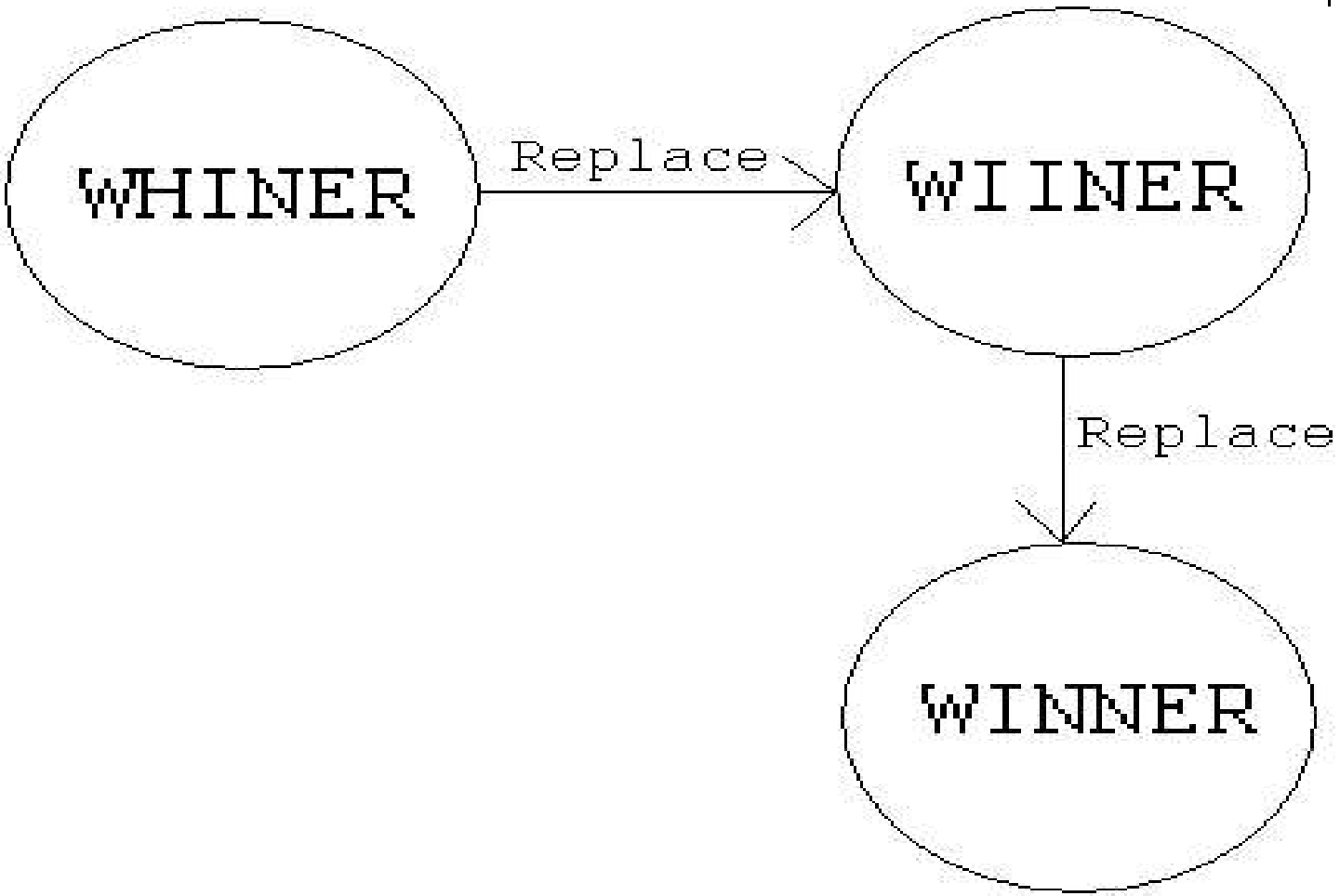


Edit Distance Better Explained

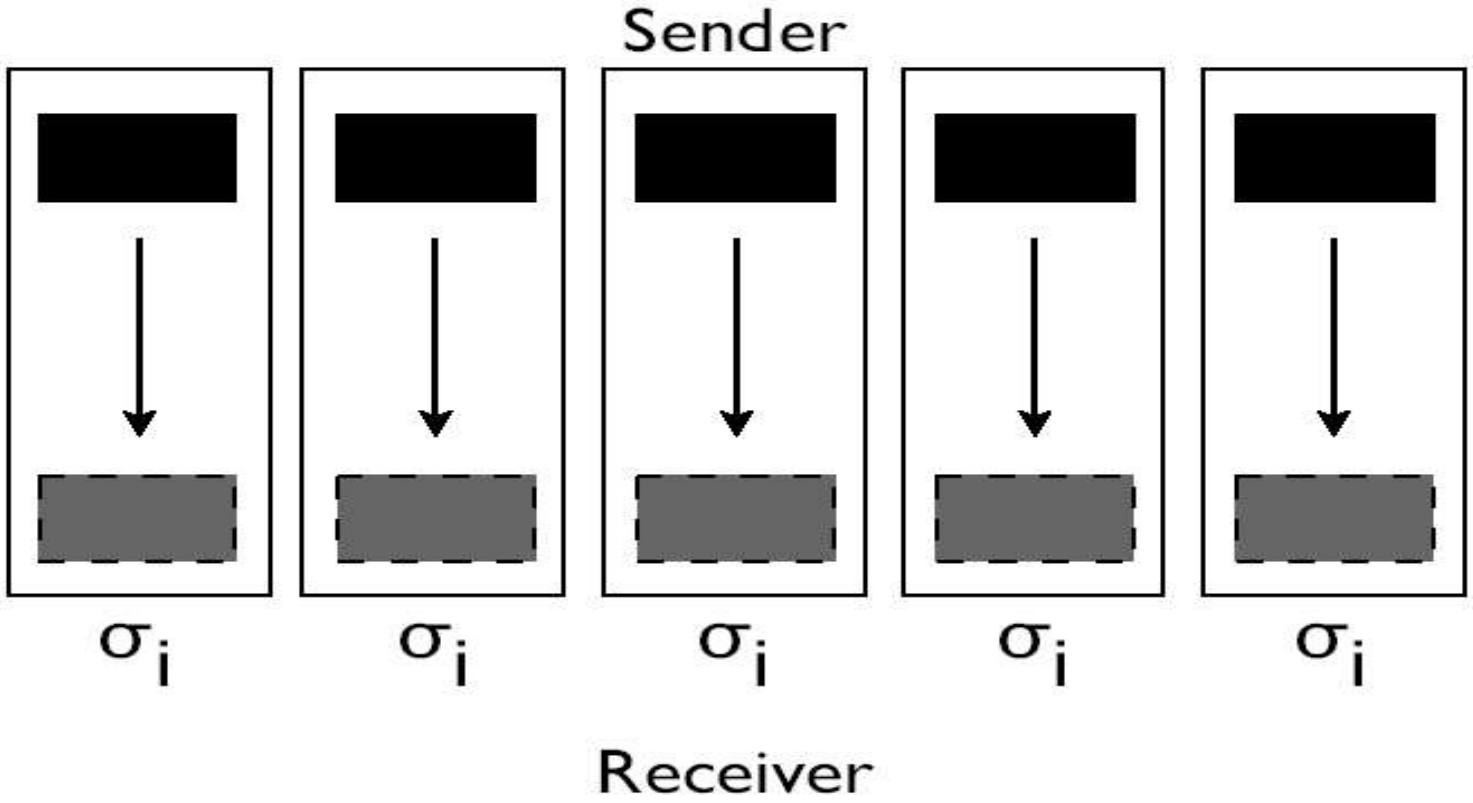


- Four operations: Insert, Delete, Replace, Match.
- *Edit distance* = number of the above operations preformed

Edit Distance Example



Edit Distance in this Paper



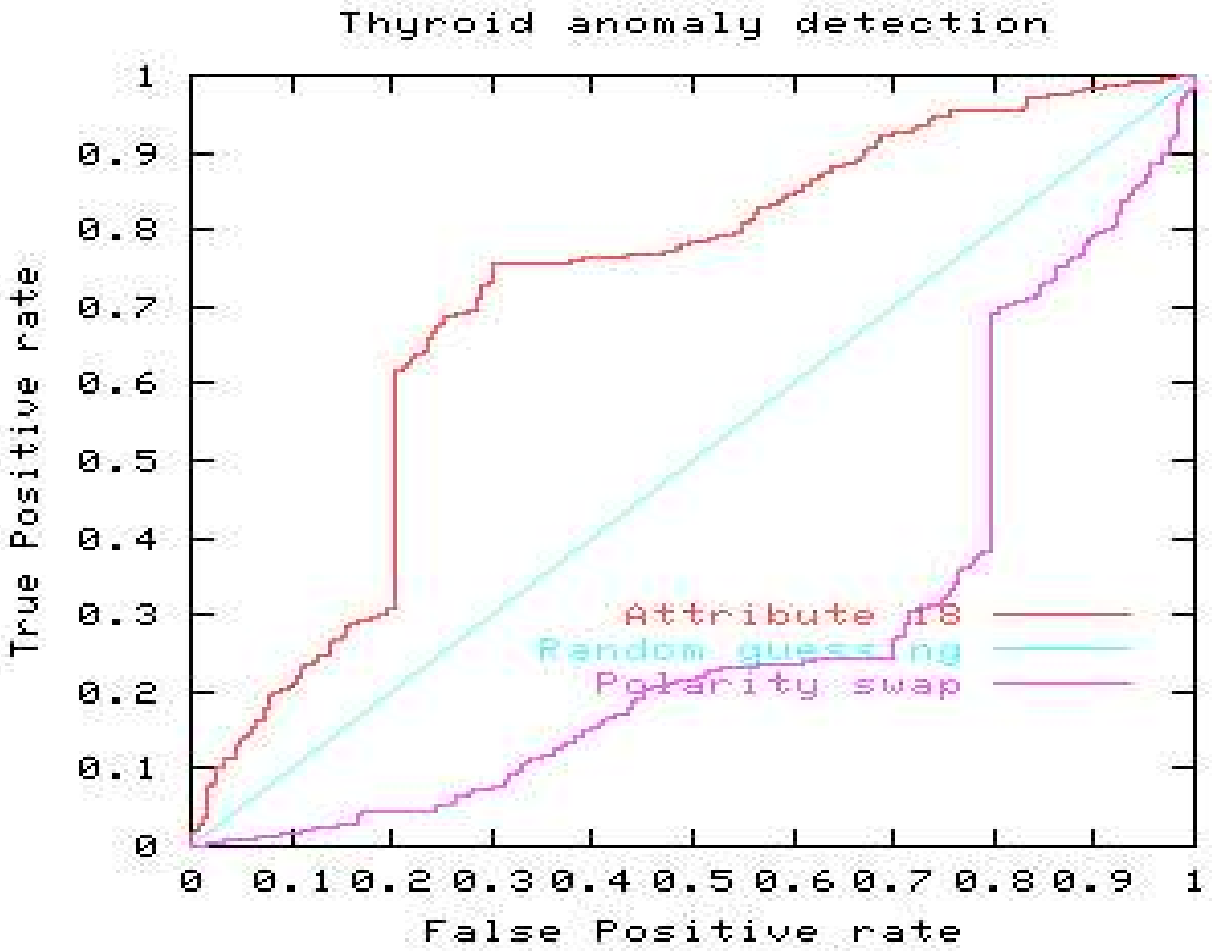
σ_i is computed as the edit distance of each frame

False Positive Rates

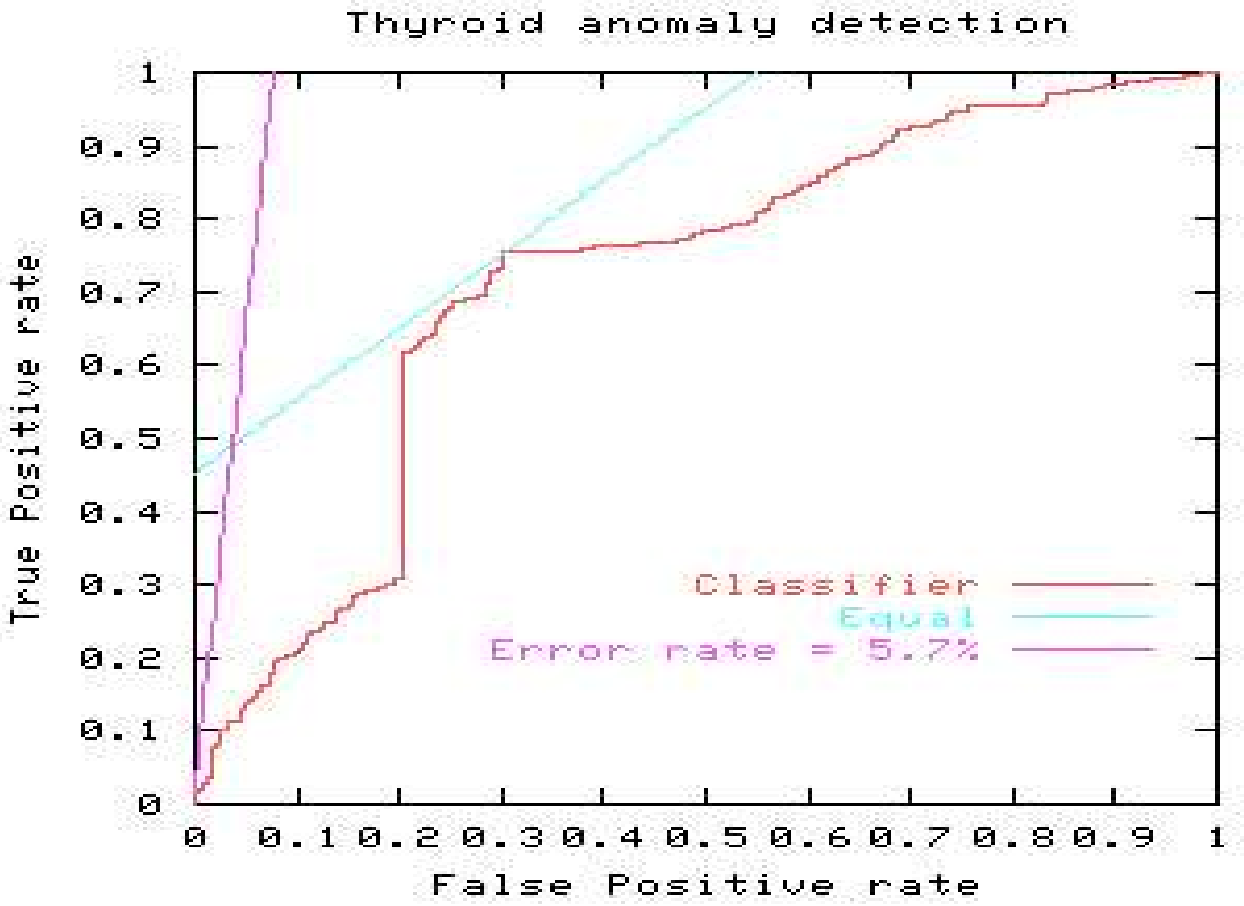
WWW	Threshold	FP	Cov-I	Cov-II	Cov-III(10%)	Cov-III(25%)	Cov-III(50%)
	$\mu + 2\sigma$	10.0	0.0	0.0	86.6	100.0	100.0
	$\mu + 1.5\sigma$	10.0	0.0	0.0	0.0	53.0	86.6
	$\mu + 1\sigma$	10.0	0.0	0.0	0.0	0.0	86.6
	$> Max$	10.0	0.0	0.0	0.0	20.0	86.6
FTPD	Threshold	FP	Cov-I	Cov-II	Cov-III(10%)	Cov-III(25%)	Cov-III(50%)
	$\mu + 2\sigma$	10.0	0.0	66.7	86.6	100.0	100.0
	$\mu + 1.5\sigma$	10.0	0.0	0.0	0.0	80.0	93.3
	$\mu + 1\sigma$	30.0	0.0	0.0	0.0	6.7	93.3
	$> Max$	10.0	0.0	0.0	0.0	33.3	86.6

- Seemingly high false positive rates
- Lack of an equal error rate and ROC curve make the reported false positive rates useless.

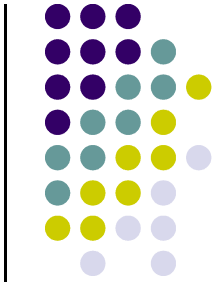
False Positive Rates (cont)



False Positive Rates (cont)

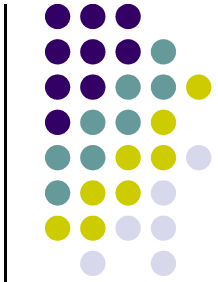


Compression



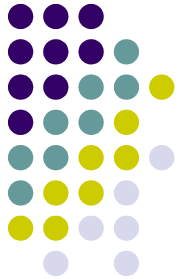
- How does compression impact their detection methods?
  - How does compression affect inter-arrival time?

On the limits of compression



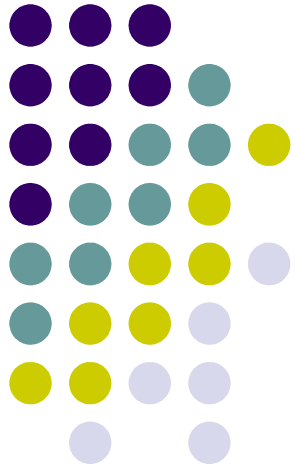
- How do we design an ideal covert channel?
  - Does this necessarily mandate error connection strategies?
  - How does this interplay with compression?

Revisited Assumptions

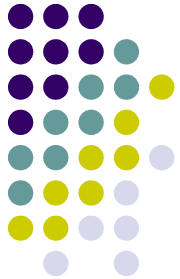


- Any reasonable covert timing channel has to have regularity
  - Random function/seed
- IP traffic is irregular and thus can be distinguished from regular covert traffic.
  - Research shows IP traffic can be regular. View [5].

Questions

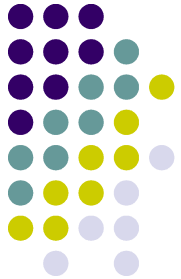


Real Threat?



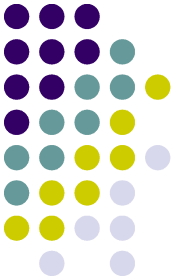
- Is this a feasible threat? Why or why not?
- Do we need to make covert channel resistant protocols and schemes?
  - How could we?
- Is there a bound on the acceptability of information leakage?

Class Questions



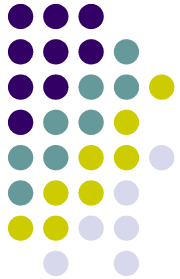
- Is edit distance more appropriate than Hamming distance in this setting?
  - If so, why?
- Why do they use a unidirectional channel?

Extensions



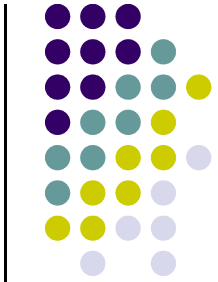
- “Quantifying how error-correction can be used to mitigate network congestion and improve channel accuracy.”

Extensions (cont)



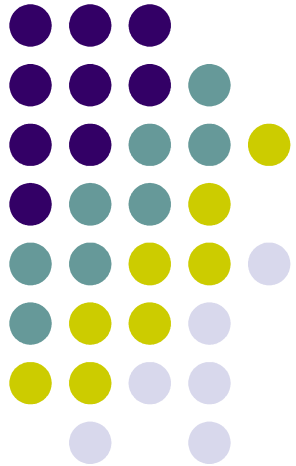
- Looking at the creation of a covert channel in a completely realistic environment. Hide the covert channel in a real distribution by monitoring traffic
  - Are there protection methods that would detect covert channels trying to blend into distributions?

Extensions (cont)

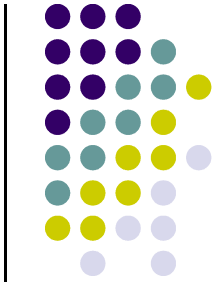


- Can you find a statistical measure that can be proved to be invariable under an entire (non-trivial) class of attacks?

Other Forms of Covert Channels

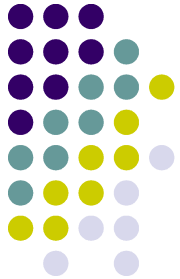


HTTP Covert Channel



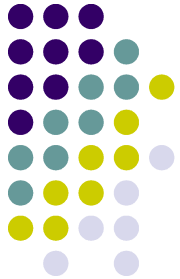
- Paper entitled *New Covert Channels in HTTP* by Mathias Bauer [2]
- Uses HTTP to spread information between sites (cookies, meta tags)
- Universal Re-encryption
- Potentially faster communication speeds
- Clients spreading information offer cover

Packet Sorting Channel



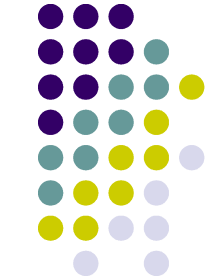
- For every n objects, they can be ordered n! ways
- Can encode information using this by picking specific orderings.
- 2 shared keys: K and k
  - K is the length of the packet sequence (IE 24 packets are to be sent)
  - k is a parameter to the toral automorphism (really fancy PRNG)

Packet Sorting (cont)



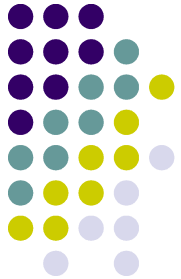
- There is a final private key that determines which sequence is used
- If Alice encodes a message to Bob
  - Bob generates every sequence for every possible final key
  - Picks the one that matches, the final key contains the covert message

Subliminal Channel (Broadband)



- ElGamal Signatures
  - R = g^k mod p (where p is a big prime)
  - S = (M – xr) / k (mod p -1) : M is the message, x is the signer's private ke, k is a random value
- Subliminal channel (Horribly trivial)
  - 1.) Give the recipient the signing key, x
  - 2.) Make "k" a covert message
  - 3.) The recipient recovers k by algebra and has the message

Subliminal Channel (Narrow band)



- Suppose the signer wishes to convey 10 bits of information
- The signer can try values of k until he/she gets lucky (on average, 1000 tries)
- K is again recovered by algebra

References

- [1] S. Cabuk, C. Brodley, R. Forte, C. Shields. "IP Covert Timing Channels: An Initial Exploration". *Proceedings of Computer and Communications Security, 2004.*

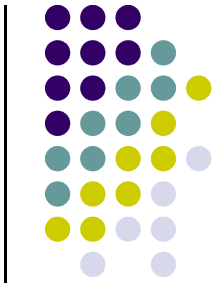
- [2] M. Bauer. "New Covert Channels in HTTP: adding unwitting Web browsers to anonymity sets". *Proceedings of the 2003 ACM workshop on Privacy in the electronic society*

References (cont)

- [3] K. Ahsan and D. Kundur. “Practical Data Hiding in TCP/IP”. *Proceedings Workshop on Multimedia Security at ACM Multimedia 2002*.

- [4] RJ Anderson, S Vaudenay, B Preneel, K Nyberg. “The Newton Channel”. *IEEE Journal of Selected Areas in Communications, 1998.*

References (cont)



- [5] V. Paxson, and S. Floyd. "Wide-Area Traffic: the Failure of Poisson Modeling." *IEEE/ACM Transactions on Networking*, 1995.