NETWORK INFORMATION HIDING

CH. 11: OVERALL CONCLUSION

Prof. Dr. Steffen Wendzel
Worms University of Applied Sciences

https://www.wendzel.de (EN) | https://www.hs-worms.de/wendzel/ (DE) @cdp_xe (Twitter)

Online Class: https://github.com/cdpxe/Network-Covert-Channels-A-University-level-Course/

Hochschule Worms
University of Applied Sciences

Conclusion

- Information Hiding faces inconsistency in its experimental methodology and its terminology/taxonomy.
  - **Patterns** and the **Unified Description Method** are means to improve the situation.
    - Both approaches (especially patterns) increasingly applied by the research community
  - Results of **Experimental Replication** underpins the need for better experimental testing.
- There is a lack of countermeasures when it comes to certain patterns.
  - Solution: Introduced **Countermeasure Variation**.
- When dealing with adaptive covert channels (NEL), current countermeasures such as static traffic normalizers do not perform well.
  - Solution: Introduced **Dynamic Wardens**.
- CPS/IoT Steganography is a new option ☺

Open Research Problems

- In general: development of sophisticated countermeasures is more challenging and more interesting than development of new hiding methods.
- We already know many hiding methods for several protocols. However, for **upcoming** network protocols, a covert channel analysis is a good idea (if described with e.g. the unified description method, so that results can be compared later).
- CPS steganography still in its infancies. Impact unclear.
- Scientific methodology (patterns, unified description method) will only work if applied by many researchers.
- Conducting additional replication studies.

Are there any questions?

THANK YOU FOR YOUR KIND ATTENTION.

PS. You can find my latest publications on my website, www.wendzel.de