

Discussione Tesi di Laurea

*Nascondere in piena vista:
un'introduzione operativa ai canali occulti nelle reti*

Candidato – Davide Fiocchi

Relatore – Prof. Franco Callegati

Alma Mater Studiorum - Università di Bologna

Prima Sessione di Laurea

Anno Accademico 2024-2025

Canali nascosti di rete

Definizione

Un **Network Covert Channel** è un canale di comunicazione che permette di trasmettere informazioni attraverso una rete in modo non autorizzato e/o non previsto.

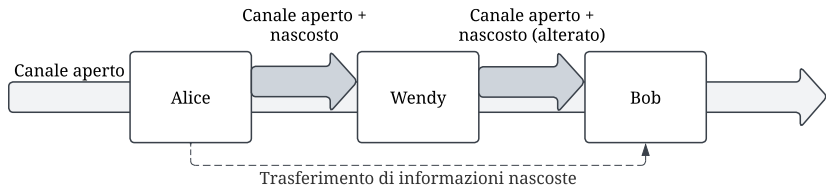


Figura: il problema del prigioniero introdotto da [Simmons, 1984].

In pratica

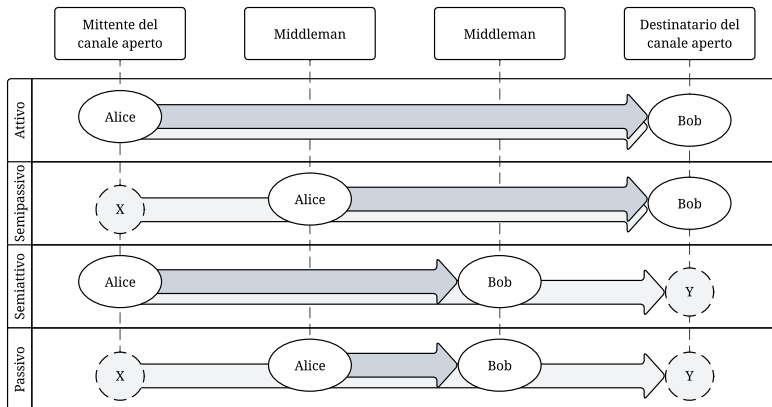
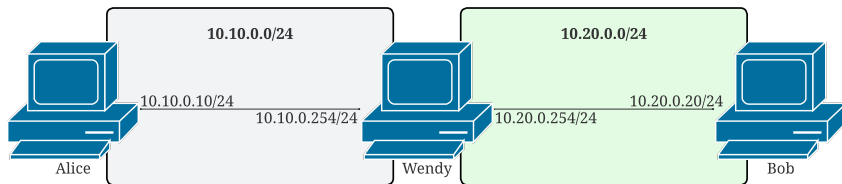


Figura: alcuni scenari di utilizzo dei canali nascosti.

Setup sperimentale

o come osservare l'invisibile

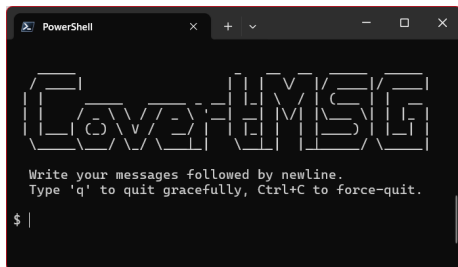
È stato realizzato un semplice framework per la generazione e l'analisi di traffico proveniente da una comunicazione mediante covert channels.



Ambiente virtualizzato (Docker):

- **Alice** e **Bob** comunicano attraverso un canale nascosto;
- **Wendy** agisce da router per il traffico tra Alice e Bob, registrando i messaggi in transito.

Covert Messenger



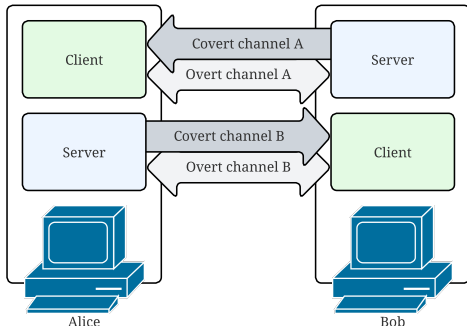
Un applicativo da riga di comando scritto in Python, che permette di realizzare scambi di messaggi attraverso diversi tipi di covert channels.

Message-driven Model-View-Controller

- ogni canale nascosto è implementato da un **model**;
- il **controller** funge da **message box**;
- l'utente interagisce con la **view**.

Proof of concept:

alcuni canali nascosti in **HTTP**

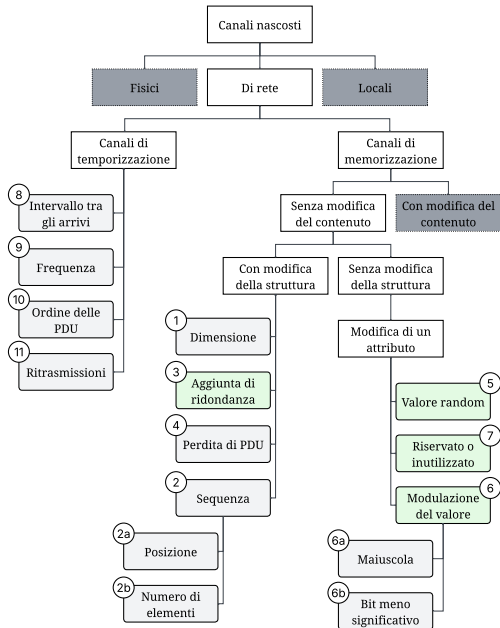


[Graniszewski et al., 2018]

- **Trailer (HTTP/1.1):** sfrutta l'header opzionale "Trailer", il cui contenuto non è vincolante.
- **Whitespace (HTTP/1.1):** utilizza sequenze di caratteri di spazio e tabulazione all'interno dei valori degli header.
- **Padding (HTTP/2):** codifica un bit scegliendo tra due modi equivalenti di specificare l'assenza di padding.

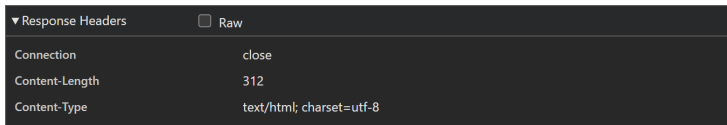
Appendice A

[Wendzel et al., 2015]

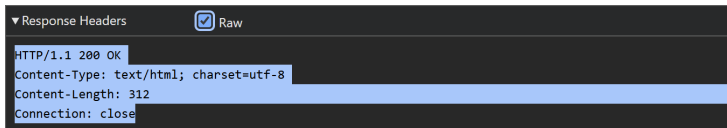


Appendice B

Visualizzazione nel browser del canale nascosto Whitespace



(a) Browser basato su *Chromium*, visualizzazione compatta.



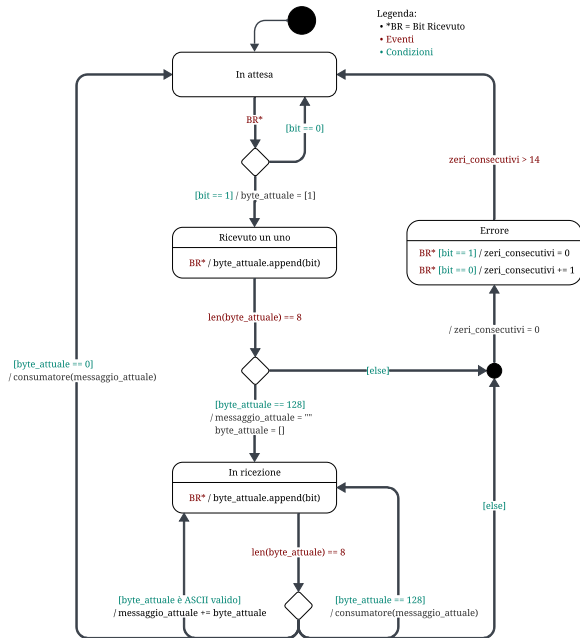
(b) Browser basato su *Chromium*, visualizzazione raw.



(c) *Firefox*, visualizzazione raw.

Appendice C

Macchina a stati finiti





Gustavus J. Simmons (1984)

The Prisoners' Problem and the Subliminal Channel.

In: David Chaum (Ed.), *Advances in Cryptology: Proceedings of Crypto 83*, Springer US, Boston, MA, pp. 51–67.

https://doi.org/10.1007/978-1-4684-4730-9_5



Waldemar Graniszewski, Jacek Krupski, Krzysztof Szczypiorski (2018)

SOMSteg – Framework for Covert Channel, and its Detection, within HTTP
J. Univers. Comput. Sci. 24(7), 864–891.

<https://doi.org/10.3217/jucs-024-07-0864>



Steffen Wendzel, Sebastian Zander, Bernhard Fechner, Christian Herdin (2015)
Pattern-Based Survey and Categorization of Network Covert Channel Techniques.

ACM Computing Surveys, 47, 50:1–26.

<https://doi.org/10.1145/2684195>