

An Efficient and Privacy-Aware Method for Revealing Network Covert Channels

**M. Zuppelli, L. Caviglione,
C. Pizzi, M. Repetto**

National Research Council of Italy



GUARD



imati

Covert Channels

- Stegomalware uses information hiding to:
 - Elude well-known detection techniques
 - Orchestrate an attack
 - Exfiltrate sensitive data
 - ...
- Covert channels mainly exploit:
 - Host resources (CPU, memory usage, etc.)
 - Traffic (HTTP, DNS, etc.)
- Challenges:
 - Unknown a priori
 - Threat-dependent
 - Scalability
 - Privacy

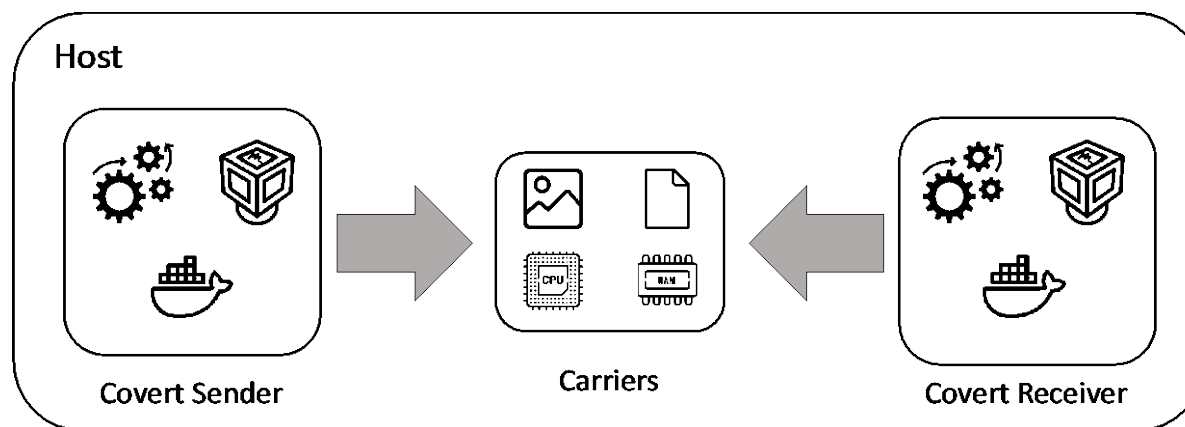


Figure 1. Local covert channel.

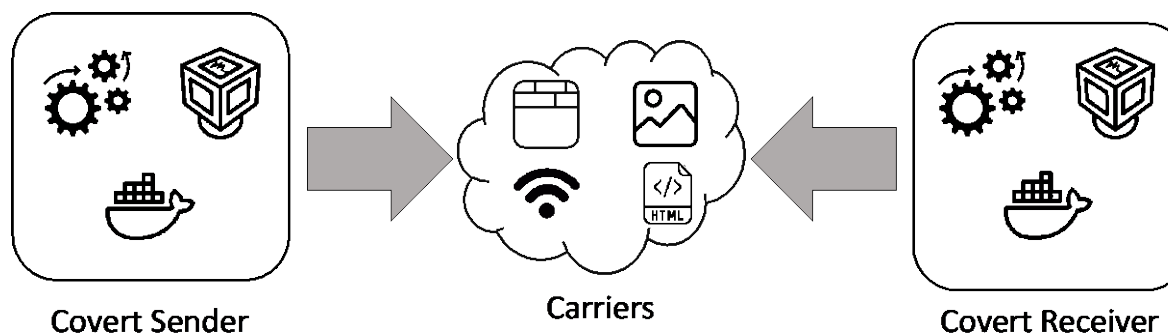


Figure 2. Network covert channel.

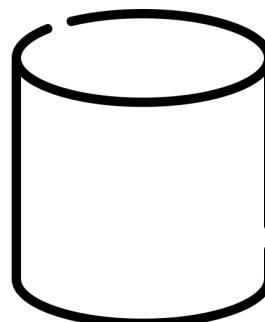
extended Berkeley Packet Filter

- eBPF leverages code-augmentation features of the Linux kernel.
- Programs are executed when the kernel hits certain hook points.

- Privacy-aware.
- Easily extensible.
- Memory bounded.



read()



eBPF Maps

write()



eBPF

Sockets

TCP/IP

...

Kernel

Process

sendmsg()

recvmsg()

Syscall

Figure 3. eBPF overview.

Data Collection for Network Covert Channels

- Organization of the eBPF map: the whole range of values of a field is split into B equally-spaced bins. Each bin has a corresponding counter.
- Goals:
 - It guarantees privacy
 - It can be adapted to many protocols
 - Larger fields can be mapped into a smaller space

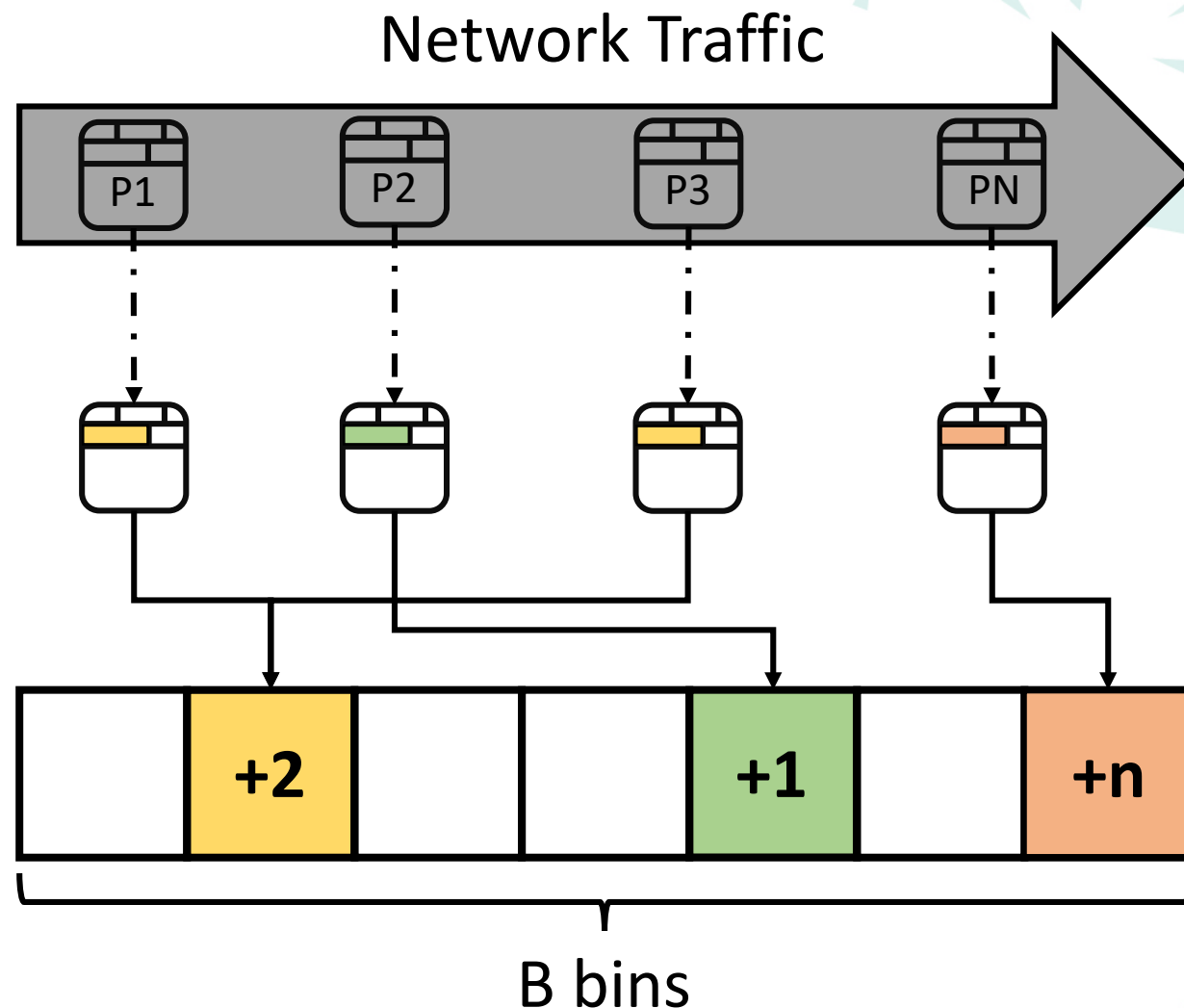


Figure 4. eBPF map organization.

Metrics and Detection

- Reveal of covert channels, by producing:
 - “new” metrics
 - a “pictorial” status of the network traffic (e.g., heatmaps)
- Example detection - IPv6 use case:
 - Comparison between an estimate of active IPv6 flows and third-party measurements
 - Temporal evolution of heatmaps

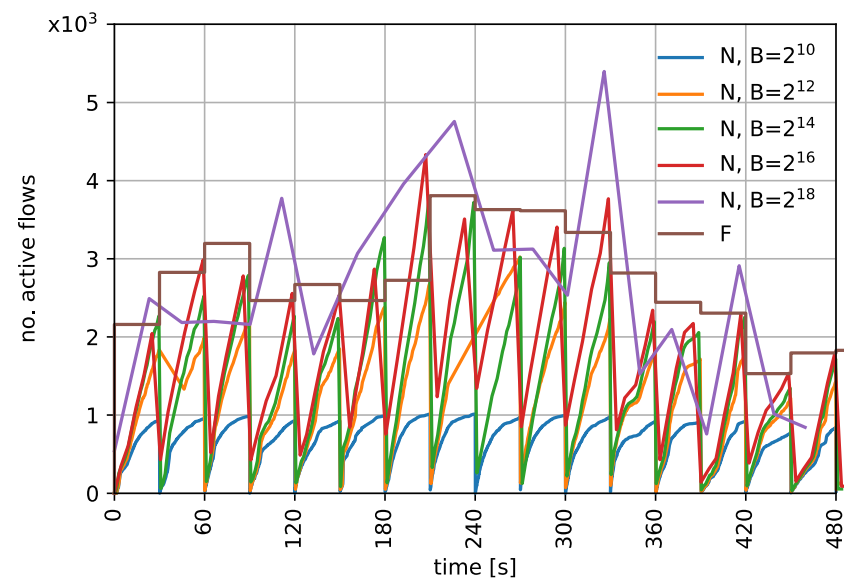


Figure 5. eBPF measurement example.

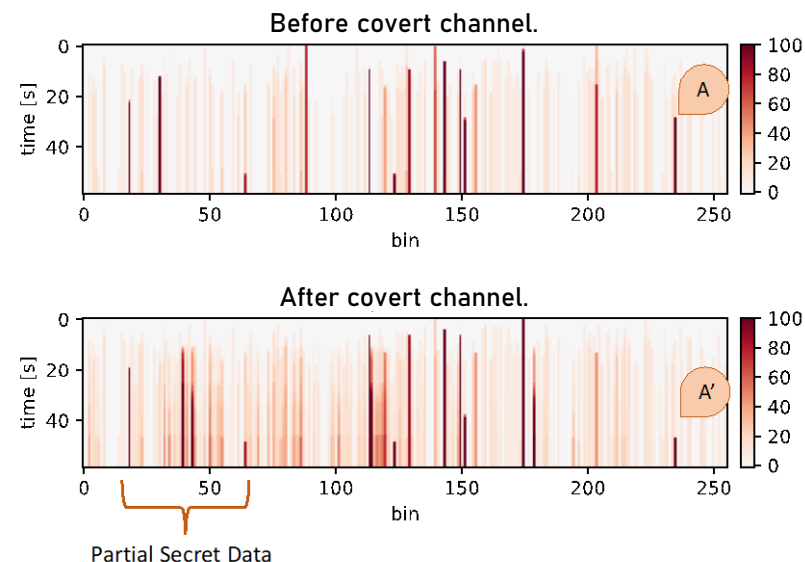


Figure 6. Temporal evolution of the bins.

Conclusions

- Covert channels can target both host resources and network packets.
- eBPF guarantees the visibility on the entire host.
- Our framework ensures:
 - Privacy-awareness
 - Efficiency
 - Extensibility and scalability
- Current research goals:
 - Comparison with other security tools
 - Use of the eBPF framework to deal with other threats