# Netlink interface for the Connection Tracking System

Pablo Neira Ayuso

6 de octubre de 2005

# Index

# Background

## Conntrack interface:

- Lack of an appropiate interface for userspace programs
- Limitations of /proc (dumping)

## Netlink Sockets:

- A messaging system to control and provide asynchronous event notification amongst the different networking modules in Linux (Jamal's Beyond Sofnet)
- RFC 3549 - Linux Netlink as an IP Services Protocol

# Background

## Conntrack interface:

- Lack of an appropiate interface for userspace programs
- Limitations of /proc (dumping)

## Netlink Sockets:

- A messaging system to control and provide asynchronous event notification amongst the different networking modules in Linux (Jamal's Beyond Sofnet)
- RFC 3549 - Linux Netlink as an IP Services Protocol

# Background

## Conntrack interface:

- Lack of an appropiate interface for userspace programs
- Limitations of /proc (dumping)

## Netlink Sockets:

- A messaging system to control and provide asynchronous event notification amongst the different networking modules in Linux (Jamal's Beyond Sofnet)
- RFC 3549 - Linux Netlink as an IP Services Protocol

# ctnetlink

version 0.90:

- Userspace programs don't use kernel structures anymore
  - Every structure has been split in netlink attributes
  - Backward compatibility assured
- Features:
  - Conntrack table and Expectation list dumping and flushing
  - Event Notification via Event API
  - Accounting: reset counters
  - Creation, Deletion and Modification of conntracks
  - Expectations: Creation and Deletion

# ctnetlink

version 0.90:

- Userspace programs don't use kernel structures anymore
  - Every structure has been split in netlink attributes
  - Backward compatibility assured
- Features:
  - Conntrack table and Expectation list dumping and flushing
  - Event Notification via Event API
  - Accounting: reset counters
  - Creation, Deletion and Modification of conntracks
  - Expectations: Creation and Deletion

# ctnetlink

version 0.90:

- Userspace programs don't use kernel structures anymore
  - Every structure has been split in netlink attributes
  - Backward compatibility assured
- Features:
  - Conntrack table and Expectation list dumping and flushing
  - Event Notification via Event API
  - Accounting: reset counters
  - Creation, Deletion and Modification of conntracks
  - Expectations: Creation and Deletion

# ctnetlink TODO

Still pending issues:

- Private protocol information handlings
- Netlink event messages listened by nobody: performance drop
- conntrack ID: we're back to unsigned int

# ctnetlink TODO

Still pending issues:

- Private protocol information handlings
- Netlink event messages listened by nobody: performance drop
- conntrack ID: we're back to unsigned int

# userspace libraries TODO

Still pending issues:

- Implement libconntrack (from libct.c)
- fix the testsuite

# userspace libraries TODO

Still pending issues:

- Implement libconntrack (from libct.c)
- fix the testsuite

# conntrack tool TODO

Still pending issues:

- Kill conntracks by ID
- Set connmark
- Dump ip_conntrack_count
- top-like display

# conntrack tool TODO

Still pending issues:

- Kill conntracks by ID
- Set connmark
- Dump ip_conntrack_count
- top-like display