Transparent Network Security Policy Enforcement

Jason L. Wright
Network Security Technologies, Inc. (NETSEC)
jason@openbsd.org

Angelos D. Keromytis
Distributed Systems Lab, University of Pennsylvania
angelos@openbsd.org

Overview

- OpenBSD bridge
- Transparent firewall
- Layer-2 filtering
- LAN extension (IPsec bridge)

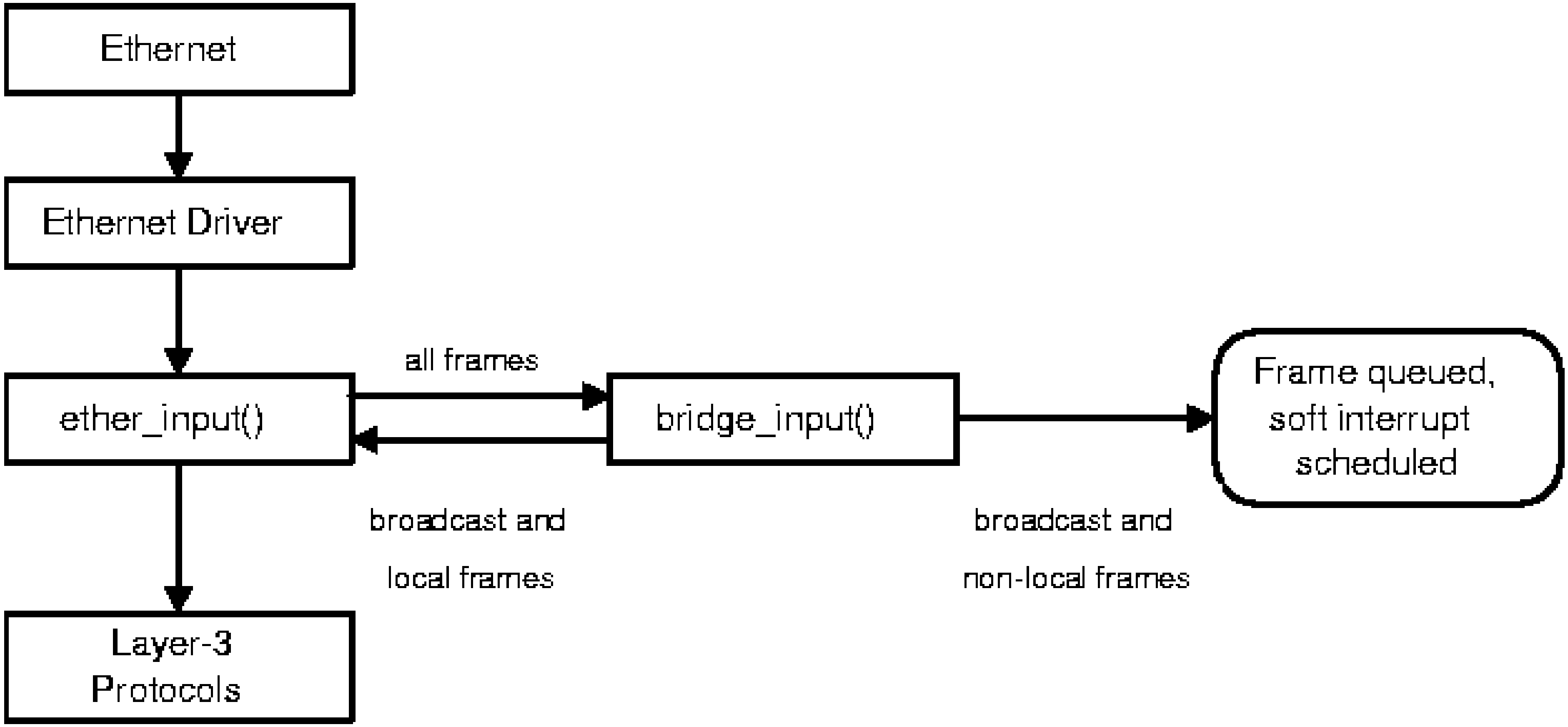
Other uses...

- Bump-in-the-wire
- Distributed firewalls

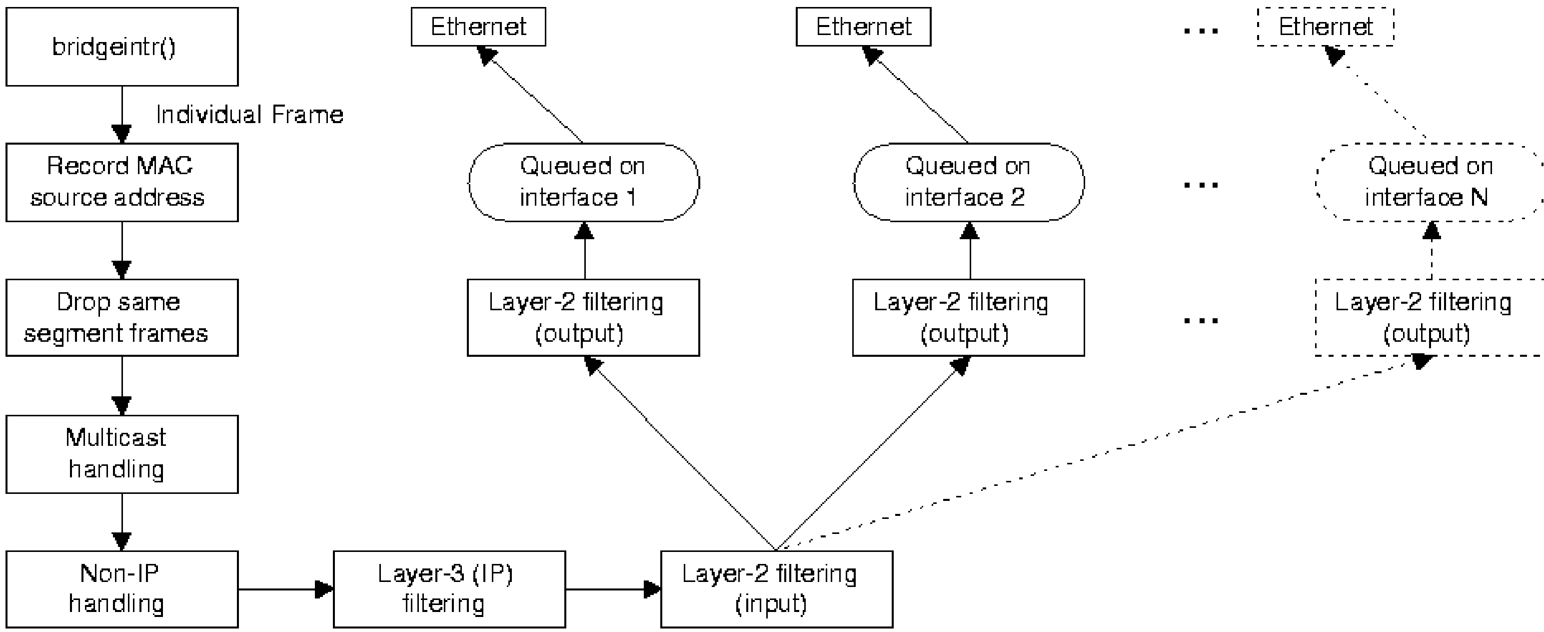
Bridge Implementation

- What is a bridge?
  - Address cache
  - Learning
  - Discovery
- OpenBSD bridge
  - Implemented as a virtual interface
  - Member interfaces as ports
  - Multiple independent bridged networks per host

Input Processing



Output Processing



Layer-2 Filtering

- Prevent ethernet address spoofing
- Static address cache entries
- Tunable MAC discovery
- Tunable MAC address learning
- Tunable multicast/broadcast handling
- IPF-like rules for Layer-2 MAC addresses

Layer-3 Filtering

- Uses standard packet filter mechanism (IPF) for Layer-3 filtering
  - Code and knowledge reuse
- Divert frames that pass Layer-2 filters to Layer-3
  - Some packet-cooking necessary
- Frames are forwarded iff they pass both filtering mechanisms

Result: Invisible firewall

Problems this solves

- Firewalls themselves can be subject to attack since they are exposed
- Sometimes at the wrong layer
- Minimizes topology changes
- No changes necessary to the protected hosts
- "Personal firewalls"
  - Plug-n-play
  - Useful in home-networking

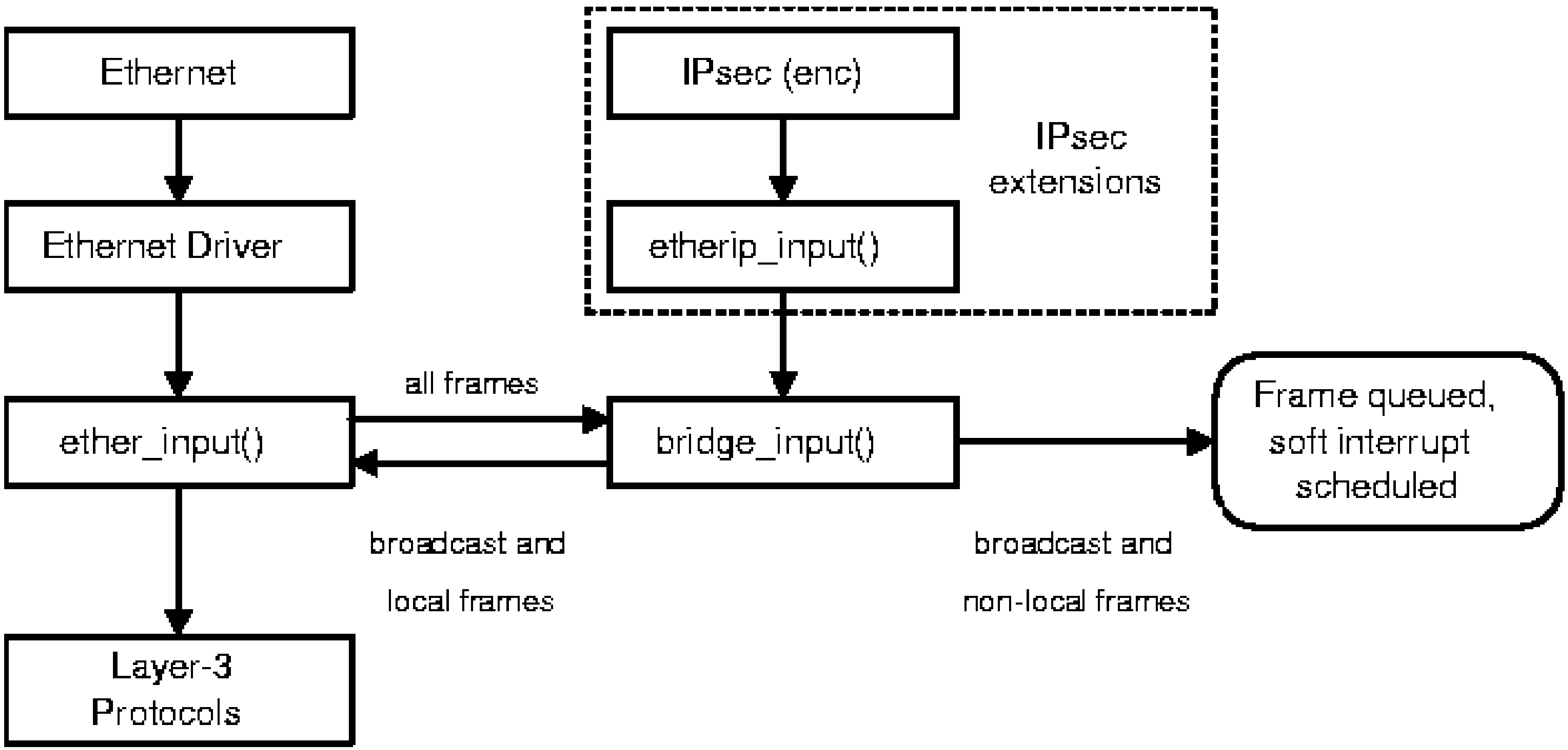
LAN extension

- Extend LAN over WAN
  - Nice for telecommuters
  - No routing/addressing voodoo needed
- Needed pieces
  - Mechanism to capture all frames -- Bridge
  - Encapsulation mechanism -- IPsec

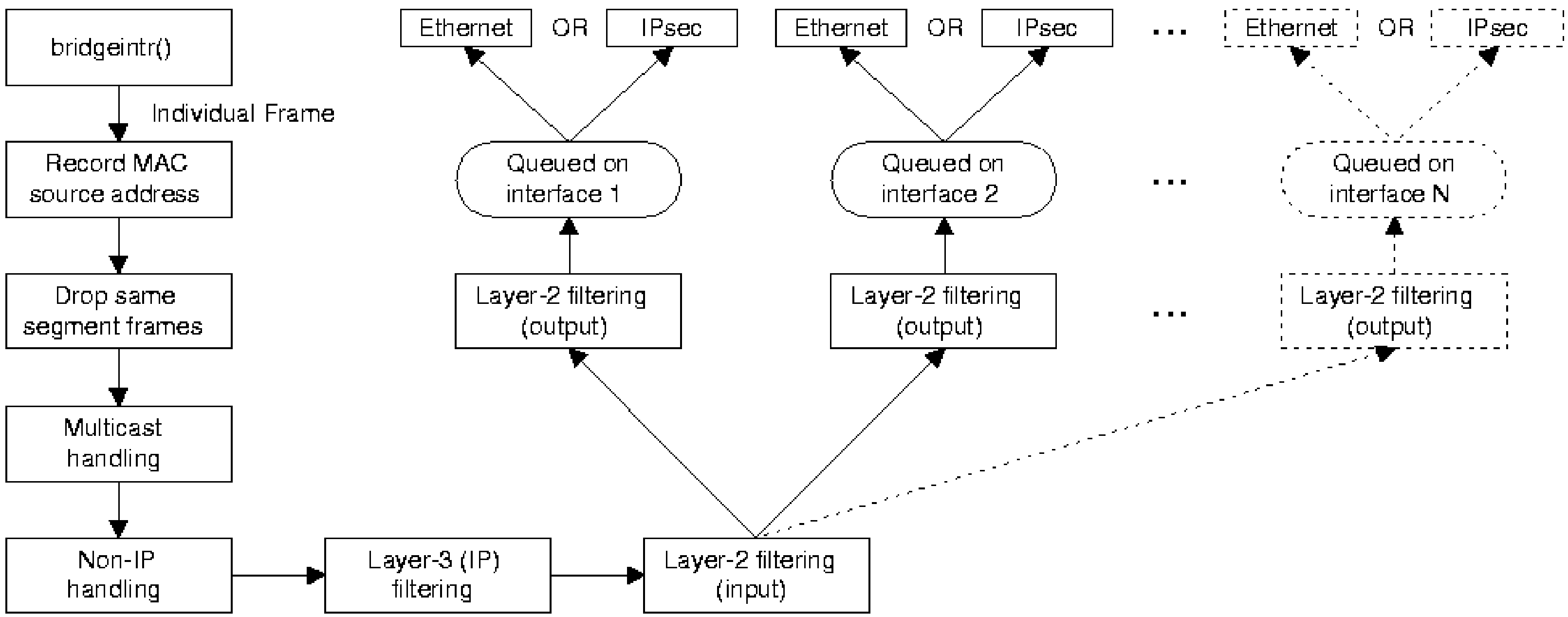
LAN extension implementation

- encapsulation (enc) interface
  - Virtual interface with IPsec Security Association (SA) attached
  - Originally used just for debugging
- Bridge Changes
  - Allow "enc" interfaces as members
  - Changes to allow member interfaces without MAC addresses
- Do Ethernet-in-IP over IPsec

Modified Input Processing



Modified Output Processing



Future/Current Work

- Desirable to have IPsec everywhere
  - Not possible to add to all systems
- Interim solution: bump-in-the-wire
  - Separate box (bridge) does IPsec on behalf of end-host
  - Pretends to be end-host when negotiating SAs
  - isakmpd changes needed

Conclusion

Where to find the code:

OpenBSD 2.7 - http://www.openbsd.org/

Acknowledgements:

The authors would like to thank Theo de Raadt, Jonathan Smith, and Suzanne Lea for suggestions and support during development.

Disclaimer

OpenBSD is based in Calgary, Canada. All individuals doing cryptography related work do so outside countries that have limiting laws.