OpenBSD IPsec Implementation

Angelos D. Keromytis
University of Pennsylvania

Niels Provos, John Ioannidis

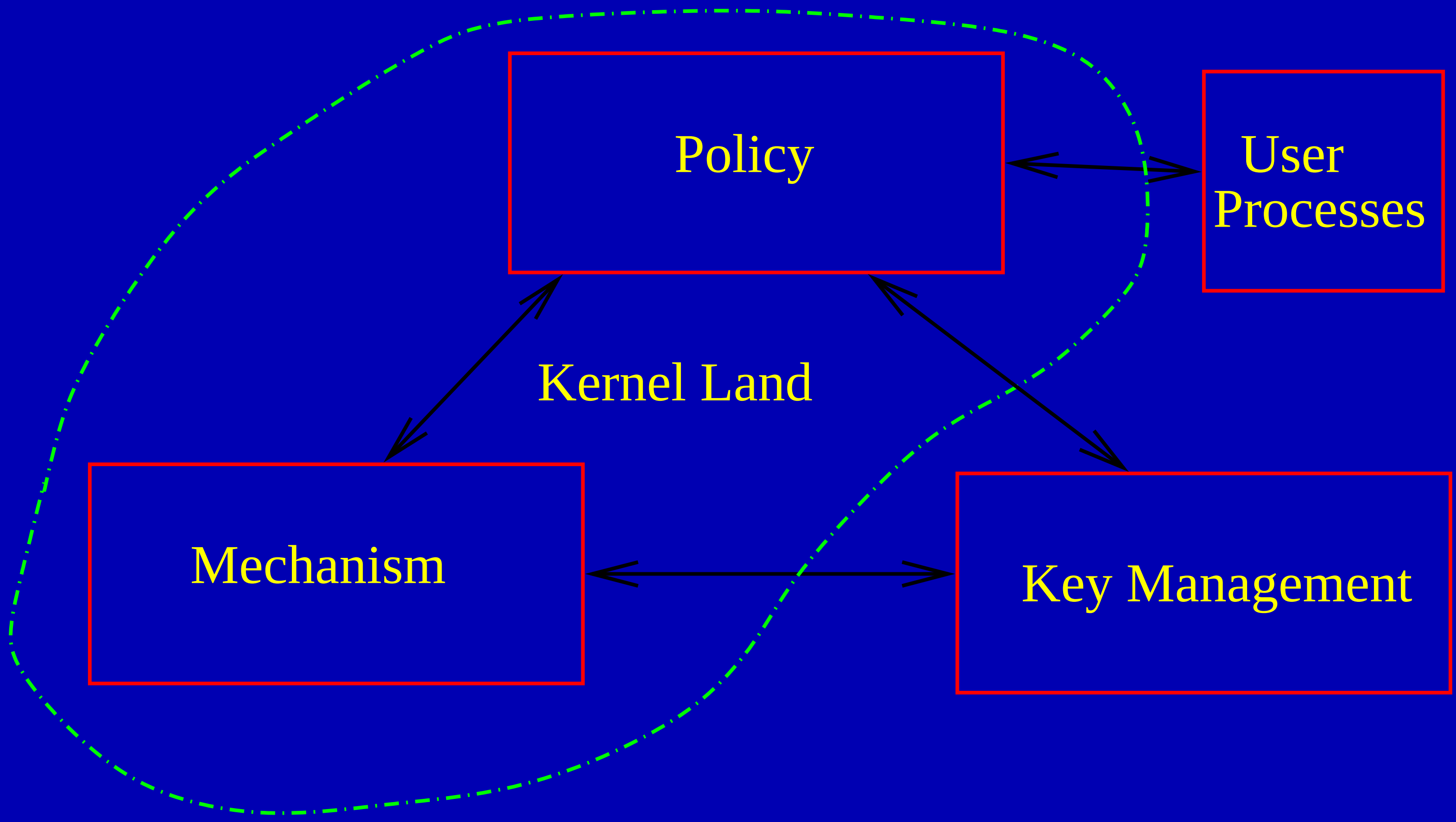
Background

- Based on BSD/OS code by John Ioannidis
- Ported to NetBSD and then OpenBSD
- Coded entirely outside the US
- Working on FreeBSD port
- Integration, key management, automatic keying, user tools

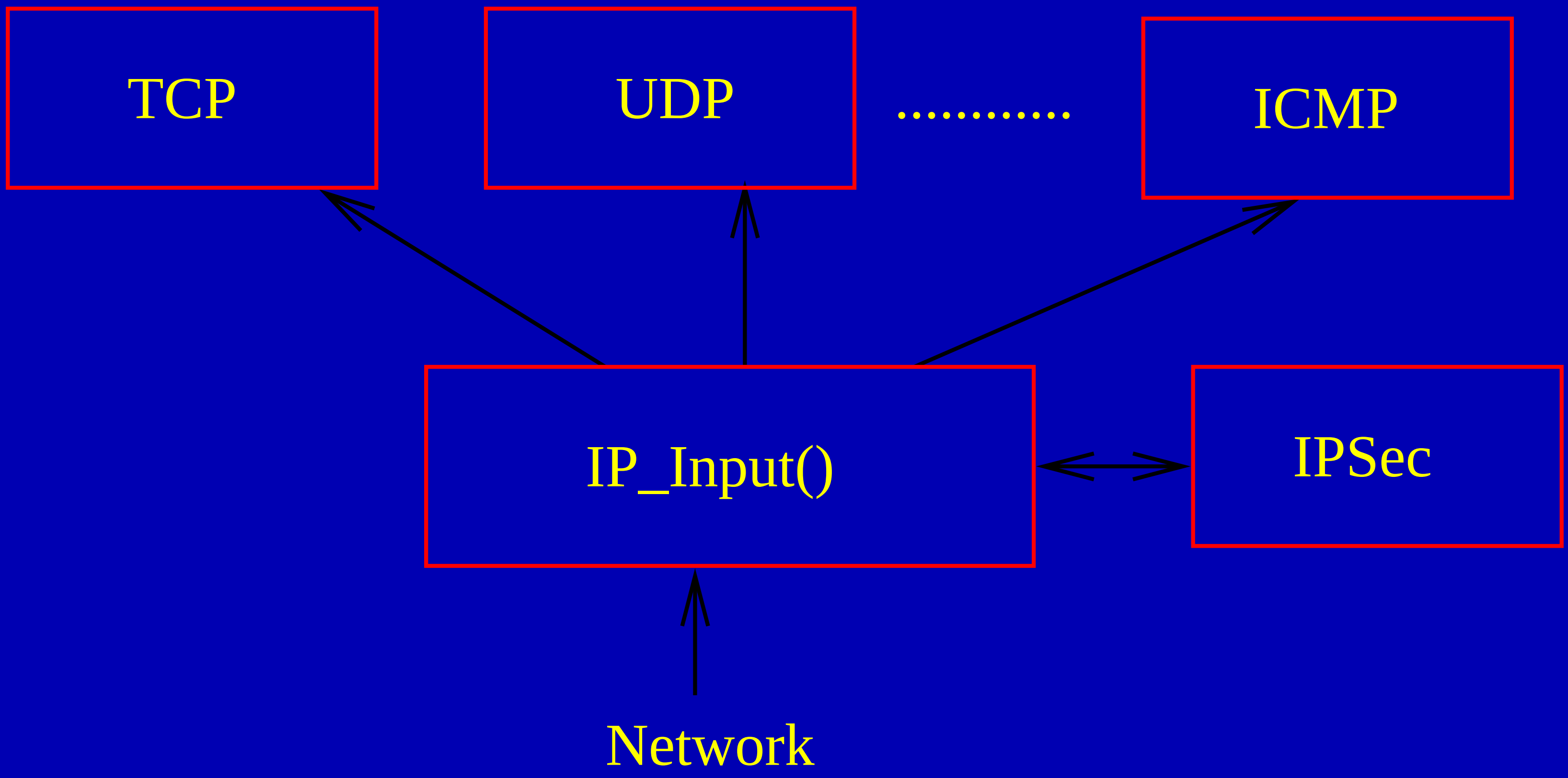
What can it do

- RFC 1829/1851 ESP (DES, 3DES)
- RFC 1828/1852 AH (MD5, SHA1)
- New-style ESP (DES, 3DES, Blowfish, CAST128)
- New-style AH (MD5, SHA1, RIPEMD160)
- Transport and tunnel mode
- Trivial to add new transforms
- Photuris for automatic keying
- setsockopt() API for per-connection/per-user keying

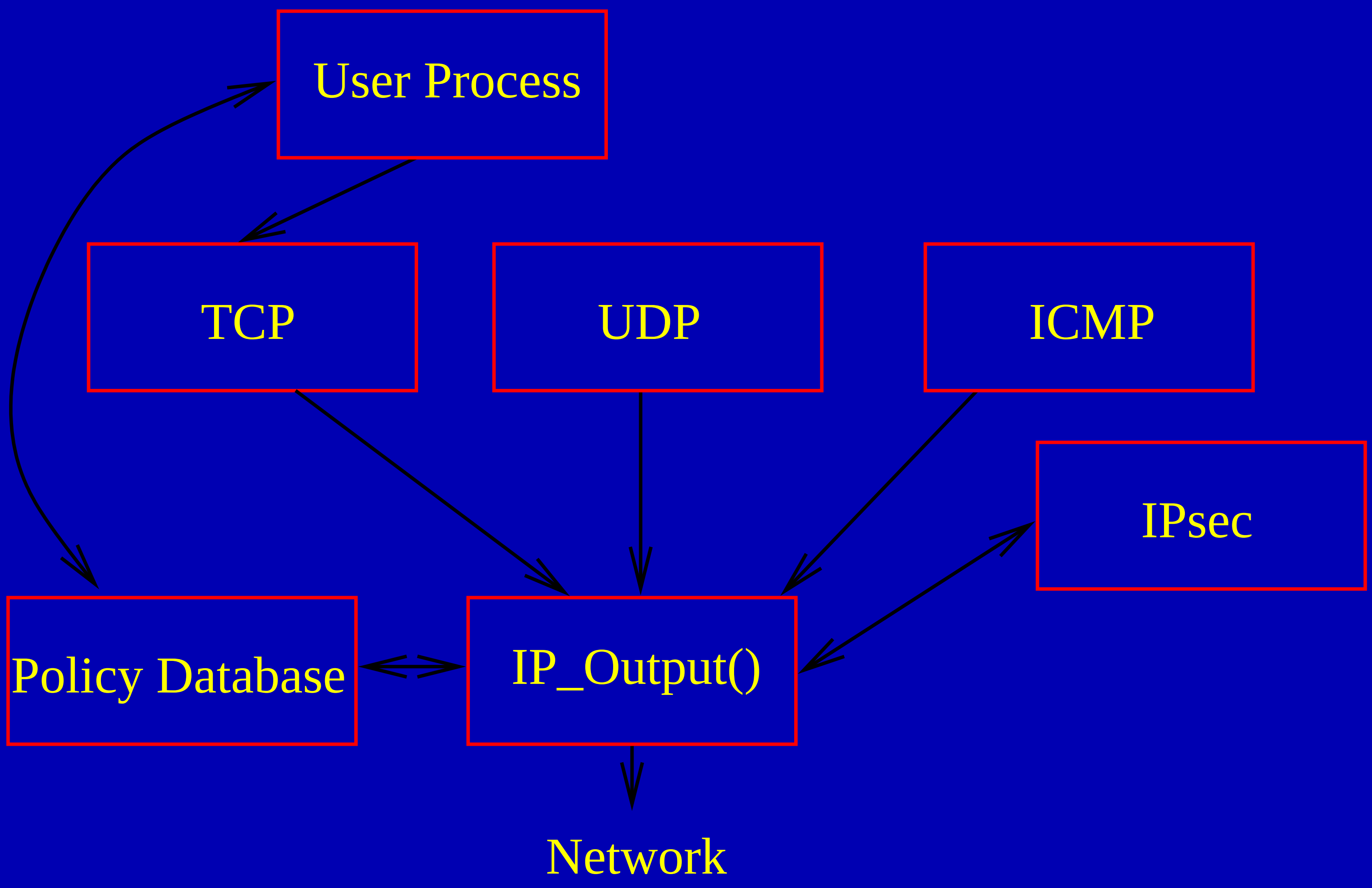
Grand view


Policy
User Processes
Kernel Land
Mechanism
Key Management

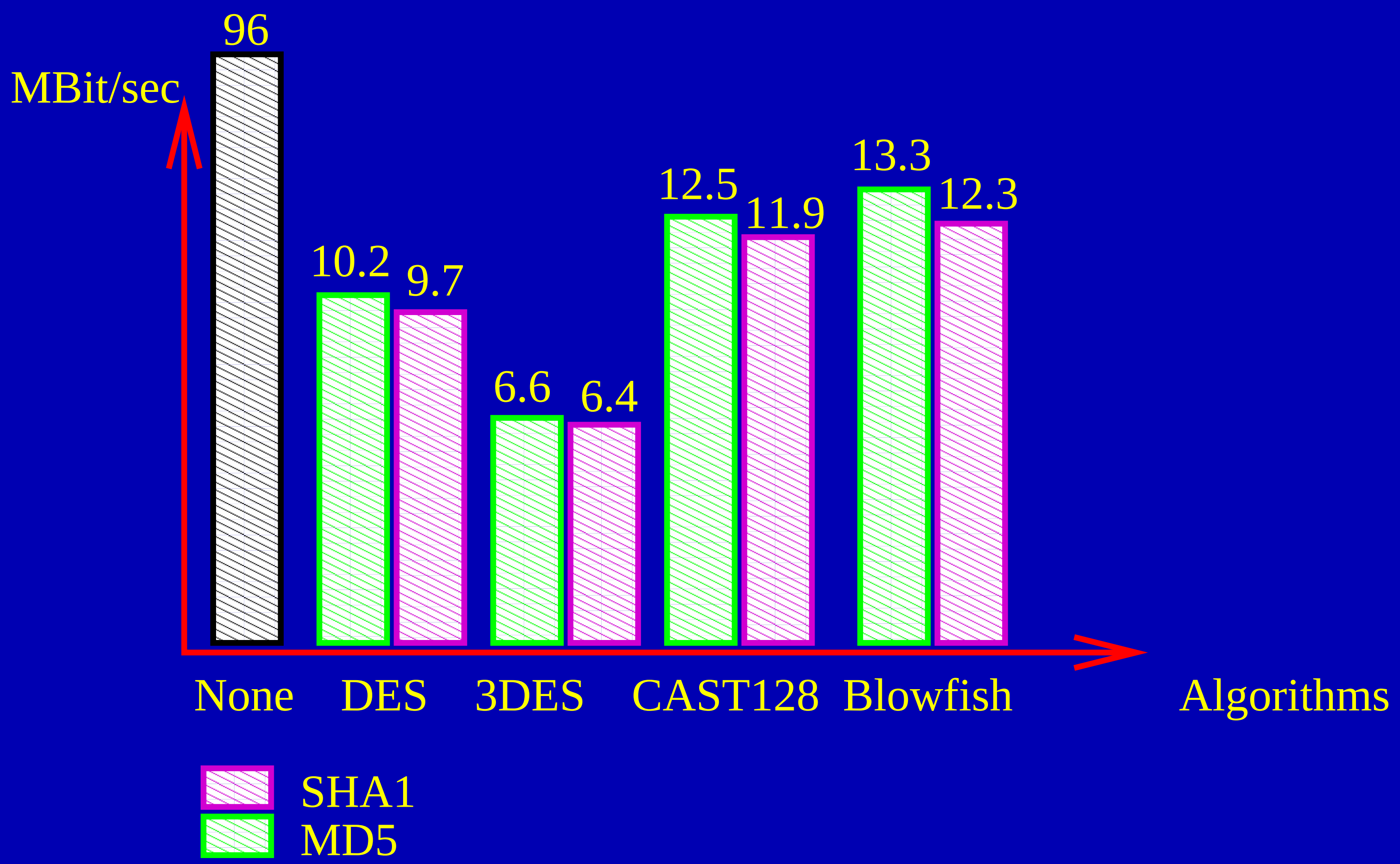
Incoming packet processing



Outgoing packet processing



Some performance measurements



What's coming

- Integration in userland tools
- Centralized policy specification for servers
- DNSSEC support for Photuris
- http://www.openbsd.org/
- angelos@openbsd.org, provos@openbsd.org