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
Incoming packet processing

TCP  UDP  ..........  ICMP

IP_Input()  IPSec

Network
Outgoing packet processing

User Process

TCP

UDP

ICMP

Policy Database

IP_Output()

Network

IPsec
Some performance measurements

MBit/sec

None  DES  3DES  CAST128  Blowfish

- SHA1
- MD5

- 96
- 10.2 9.7
- 6.6 6.4
- 12.5 11.9
- 13.3 12.3

Algorithms
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