NRL IPv6+IPsec

Craig Metz

June 17, 1998

IPsec at NRL

- NRL involved in IPsec from the start.

- Emphasis on end-to-end host use.

Features: PF_KEY

- Puts key management in user space.

- Allows different protocols to be used.

Features: API

- Allows applications to be aware of security.

- Coming: Far more robust API.

Features: Policy

- Allows many apps to use security without modifications.

- Allows sysadmins to have system-wide security controls.

Features: Policy

- Moving bits is easy; getting the policy engine right is hard.

- Coming: Better internals, support for extremely robust policies. First cut looks like a firewall.

Implementation

- Free implementation for BSD/OS and NetBSD. Included in the box with BSD/OS 4.0.

- Partial Linux support now, complete coming soon.

Implementation

- `http://web.mit.edu/network/isakmp`

- Our releases are export controlled. Third parties have created “export” versions.

Future Directions

- Hardware crypto suited for IPsec.

- Put the pieces together to build a whole solution.