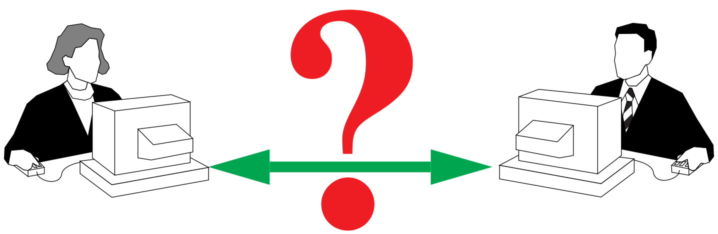
ENskip

(Simple Key-Management For Internet Protocols)

Michael Hauber, Christian Schneider
Germano Caronni



Computer Engineering
and Networks
Laboratory

Architectures

- Solaris
- IRIX
- NetBSD
- NeXTstep

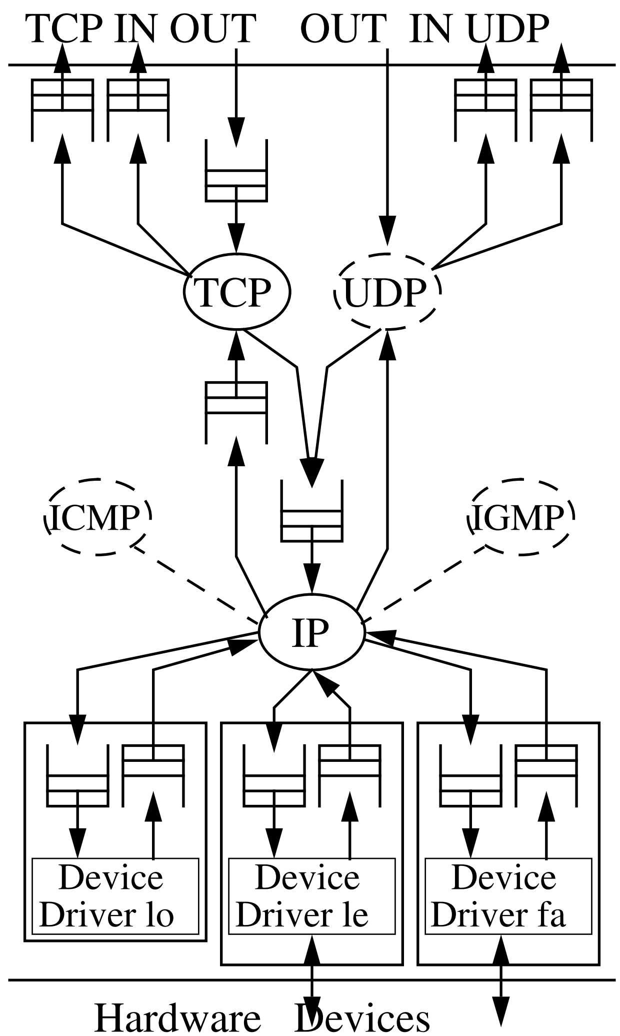
Features

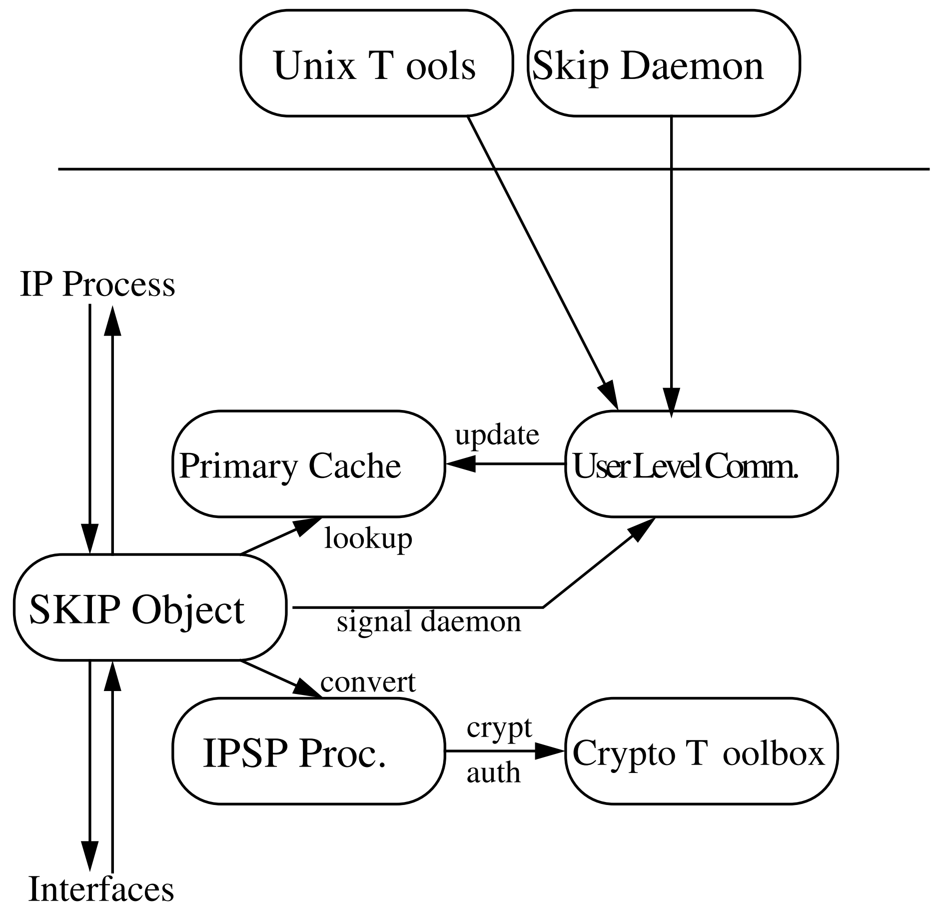
- Network layer
- Transport layer
- Encryption
- Authentication
- Sequencing

Algorithms

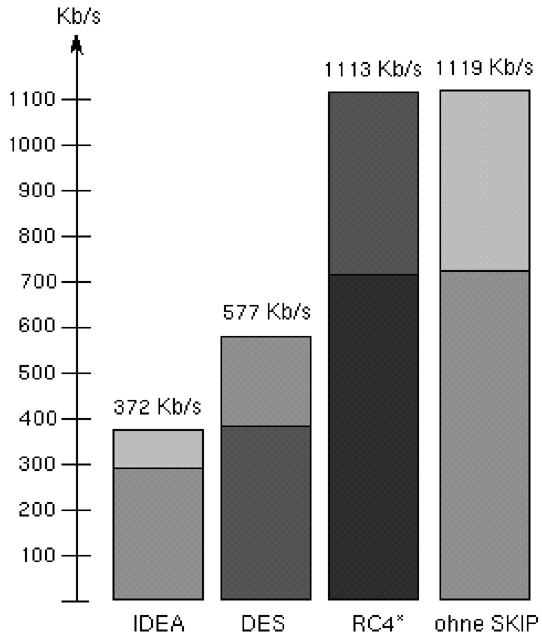
RC4*, DES, 3-DES, IDEA, MD5

System Architecture

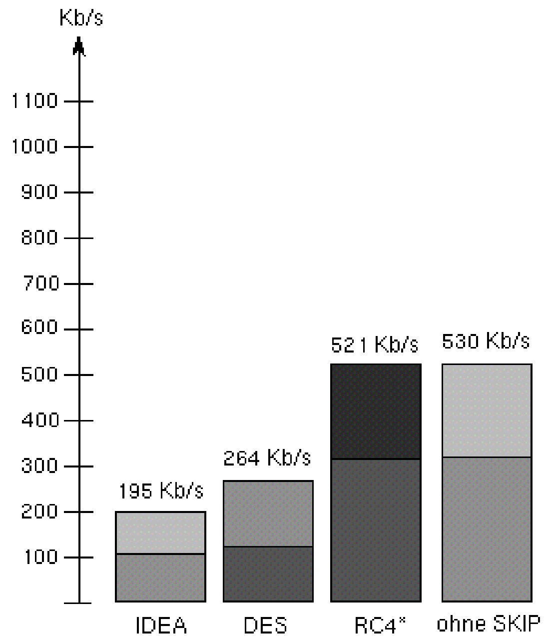




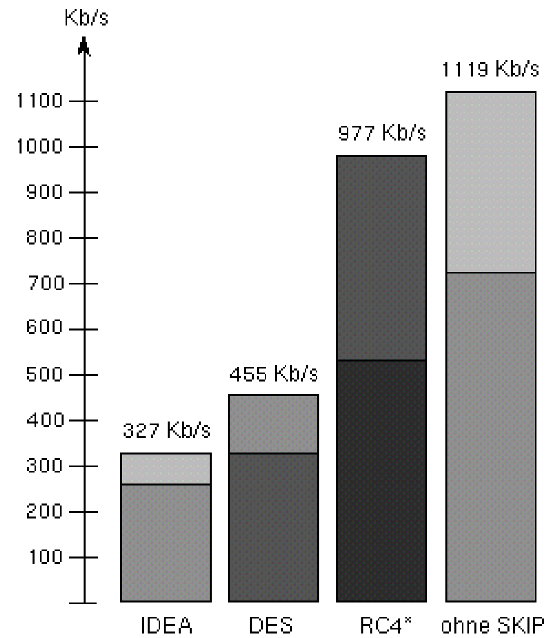
Performance



Encryption only, 1k



Encryption only, 128 bytes



Crypt & Auth, 1k

Computer Engineering and Networks Laboratory

ETH

Future work

- Compatibility with other SKIP implementations
- DH public key operations
- Conformance to new draft
- Public key distribution & acquisition
- Linux SKIP version
- Bringing security up to application layer

Availability

ENskip Software is freely available

ftp://ktik0.ethz.ch/pub/packages/skip

Mailing list “skip-info@tik.ee.ethz.ch”

To: listproc@tik.ee.ethz.ch

Body: subscribe skip-info <Your Name>

Contact address

{skip,caronni}@tik.ee.ethz.ch

Questions?