



A bridge as a representative exemplified on ISAKMP

Franjo Severinac
University of Hamburg
13.07.2006



A bridge as a representative exemplified on ISAKMP

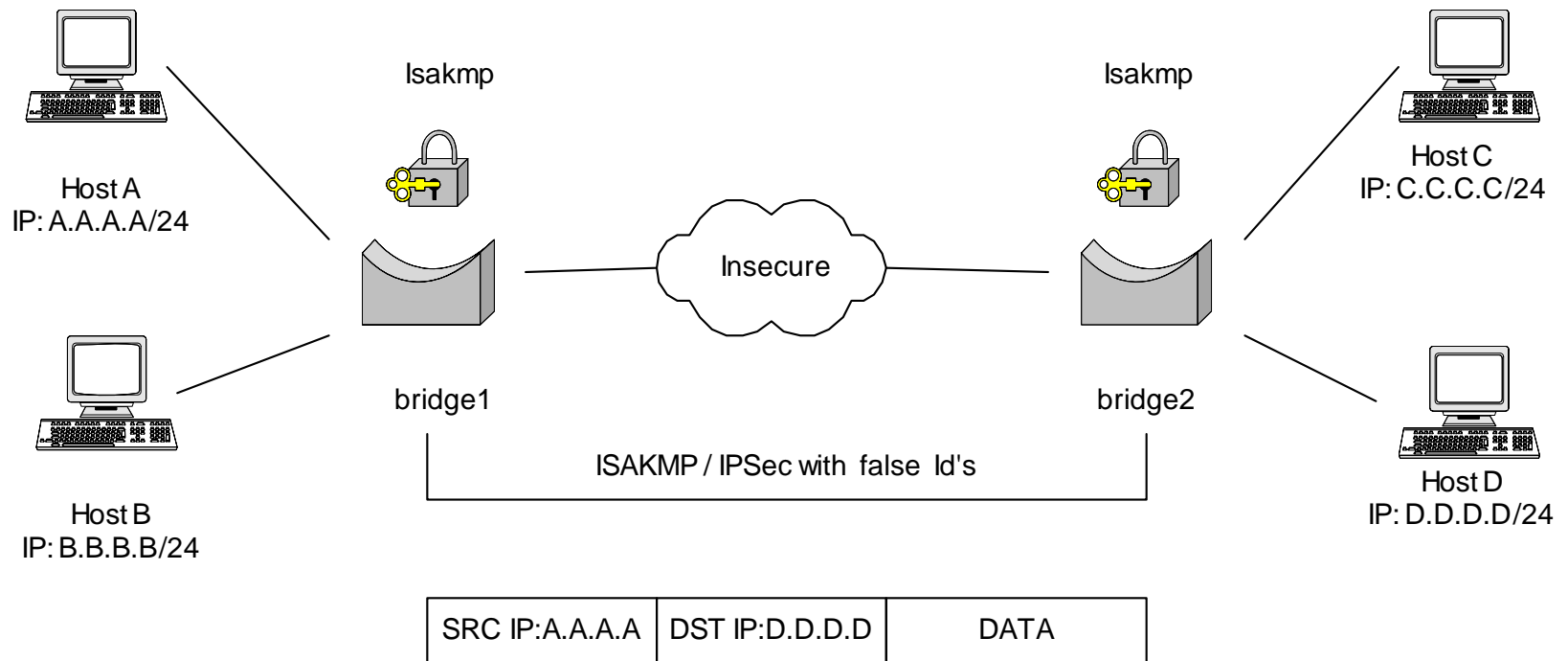
1.) What is the idea/goal?

- goal
- Basics
 - Network bridge
 - Representative
 - ISAKMP

2.) Theory

- TCP/IP Reference-model
- Changes to be done
- Generalisation

Goal





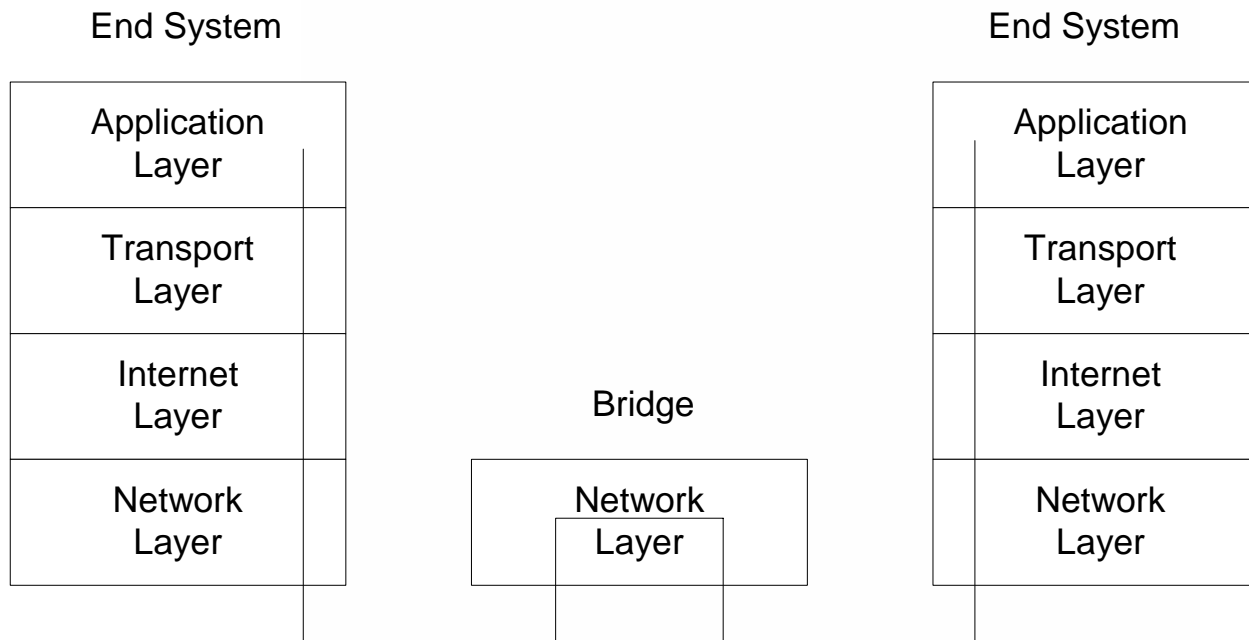
Basics: network bridge

- logical link between interfaces
- forwarding decision based on learned Mac addresses
- OpenBSD provides further functionality:
 - ability to act as a transparent filter for ip datagramms
 - possibility to perform Ipsec-processing according to policies set



Basics: network bridge

TCP/IP Reference-model





Basics: representative

Definition representative:

A representative is an entity, authorized by another entity, to perform actions instead of itself.

---> bridge authorized by network admin

Definition identity:

Identity can be seen as the sum of the characteristics which distinguish an individuum from others.

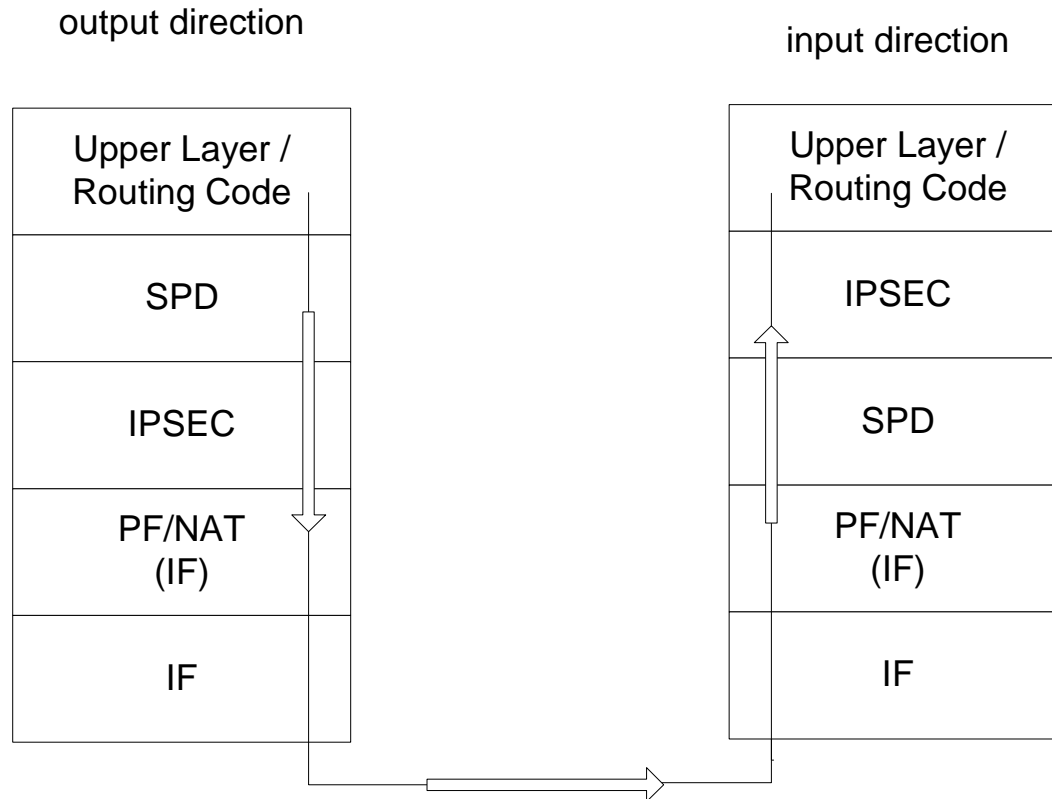
--- > keying material, IP & Mac address



Basics: ISAKMP

- Internet Security Association and Key Management Protocol (ISAKMP) serves for administration of keys used by IPsec
- Uses Diffie-Hellman (DH) to generate/exchange keys through insecure networks
- Works in two phases
- Participants need to authenticate (PSK, Certificates)

Packet flow through TCP/IP stack





TCP/IP Reference - model

- Which layer has what functions?
- How are identities defined at the layers?
- How packets flow through the TCP/IP stack?



TCP/IP Reference - model

- What changes have to be done in
 - Network Layer / Internet Layer / Transport Layer ?
 - ISAKMP ?
 - General configuration ?
- How these changes violate the TCP/IP Reference-model?
- Can the representation functionality be generalized to all applications?



??? Questions ???
