swIPe:
Network-Layer Security for IP

John Ioannidis
Columbia University
ji@cs.columbia.edu

Matt Blaze
AT&T Bell Laboratories
mab@research.att.com

Phil Karn
Qualcomm, Inc.
karn@qualcomm.com

BBQ

Motivation

- Internet is getting bigger and less friendly.
- Increasing demand from users for better security.
- Increased mobility of Internet users.
- Wireless networking.
- Application layer security does not adequately address the problems.

BBQ

Design Goals

- Should work over the existing Internet.
- Should not require adjunct hardware.
- Provide a smooth migration path.
- Multiple modes of operation.
- Transport and higher protocols unaffected.
- Decouple mechanism, policy, and key management.

BBQ

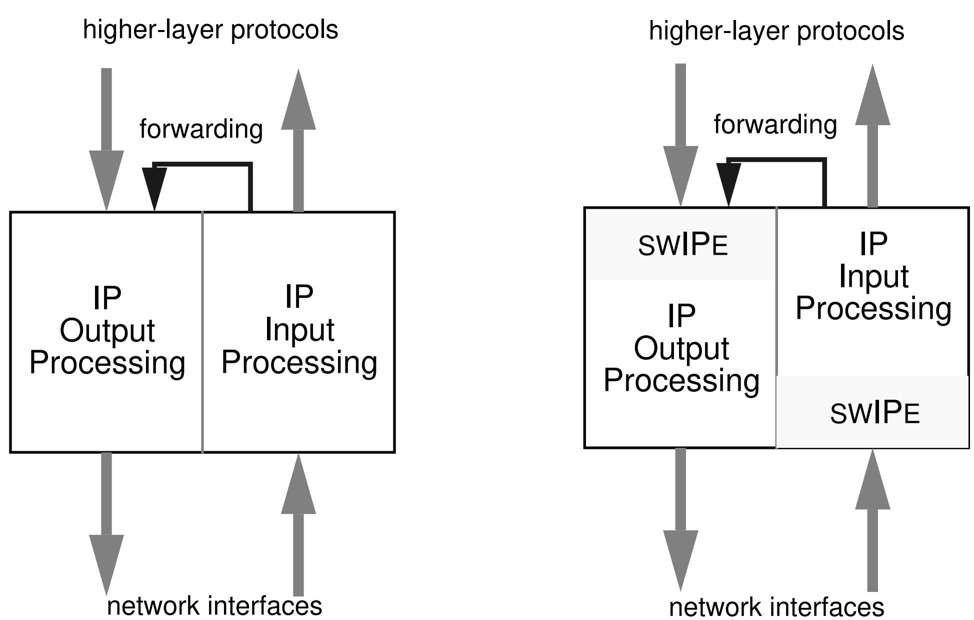
swIPe Overview

- Outgoing IP datagrams are signed and/or encrypted, encapsulated, and sent out.
- Incoming packets are decapsulated, then decrypted and/or authenticated prior to delivery to a higher-layer protocol
- "Policy engine" determines when swIPe-ing is done.
- Session key exchange and secure negotiation may use public key technology.
- Completely compatible with existing infrastructure.

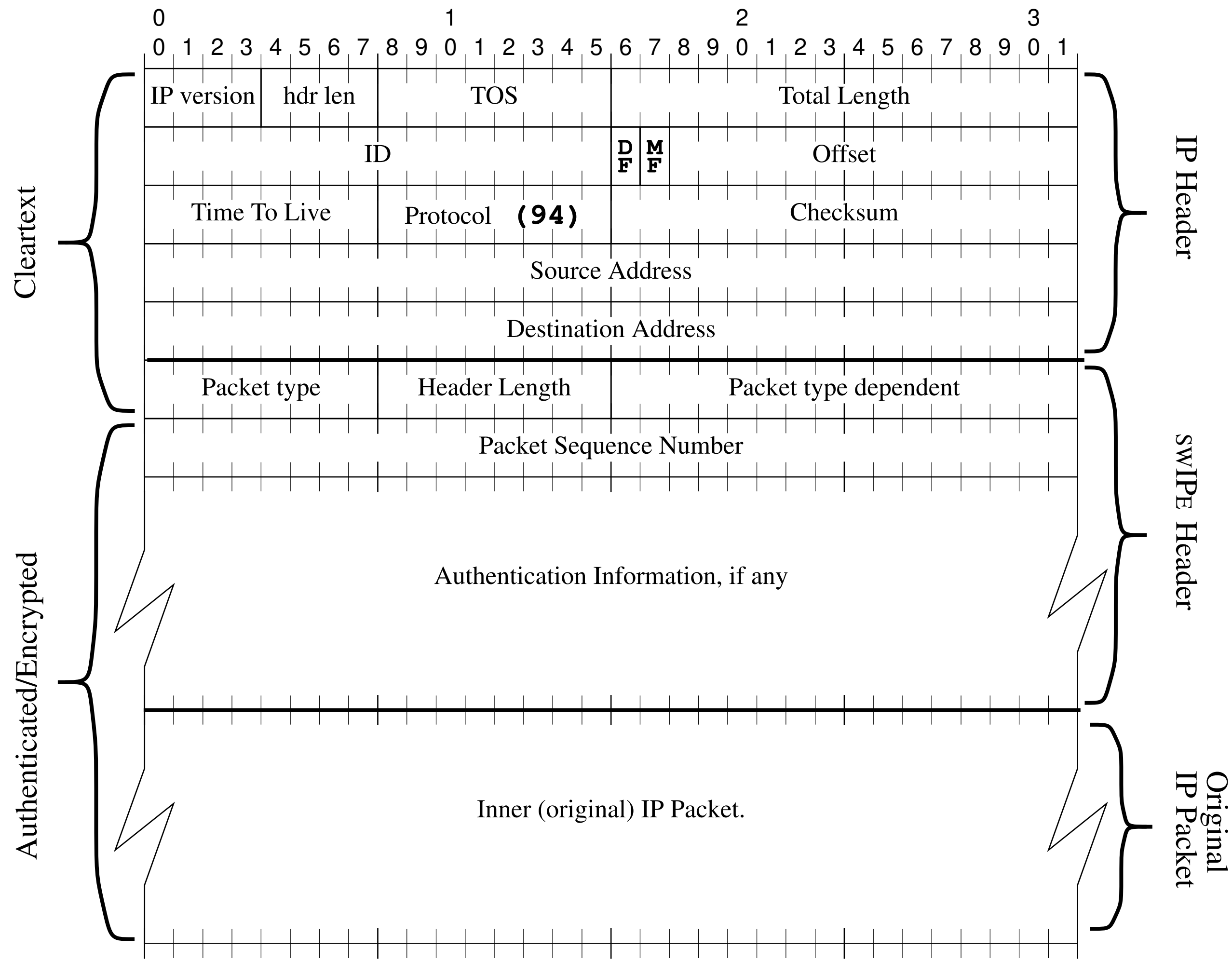
BBQ

swIPe: architecture:

without swIPe: with swIPe:

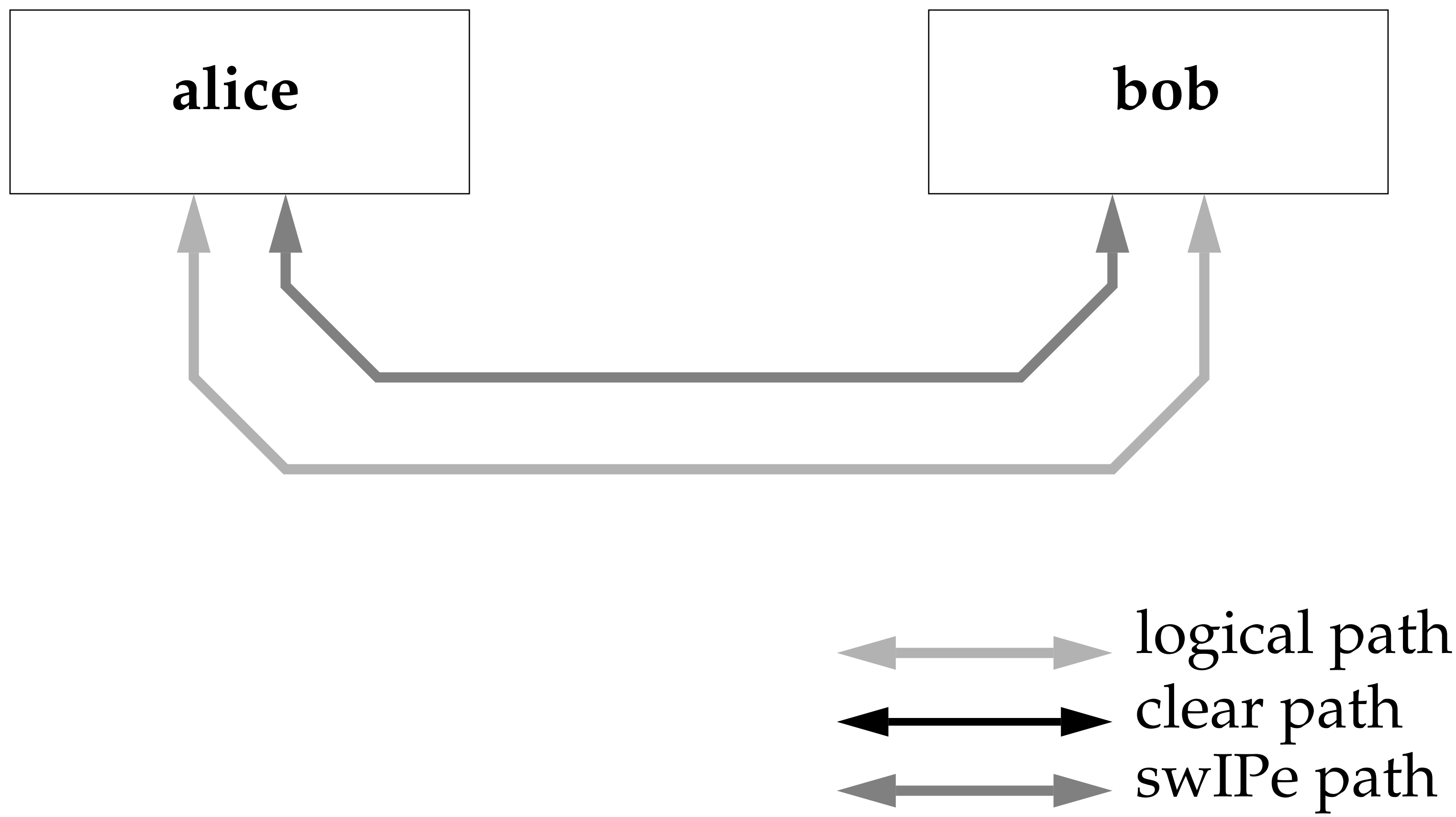


swIPe: packet format



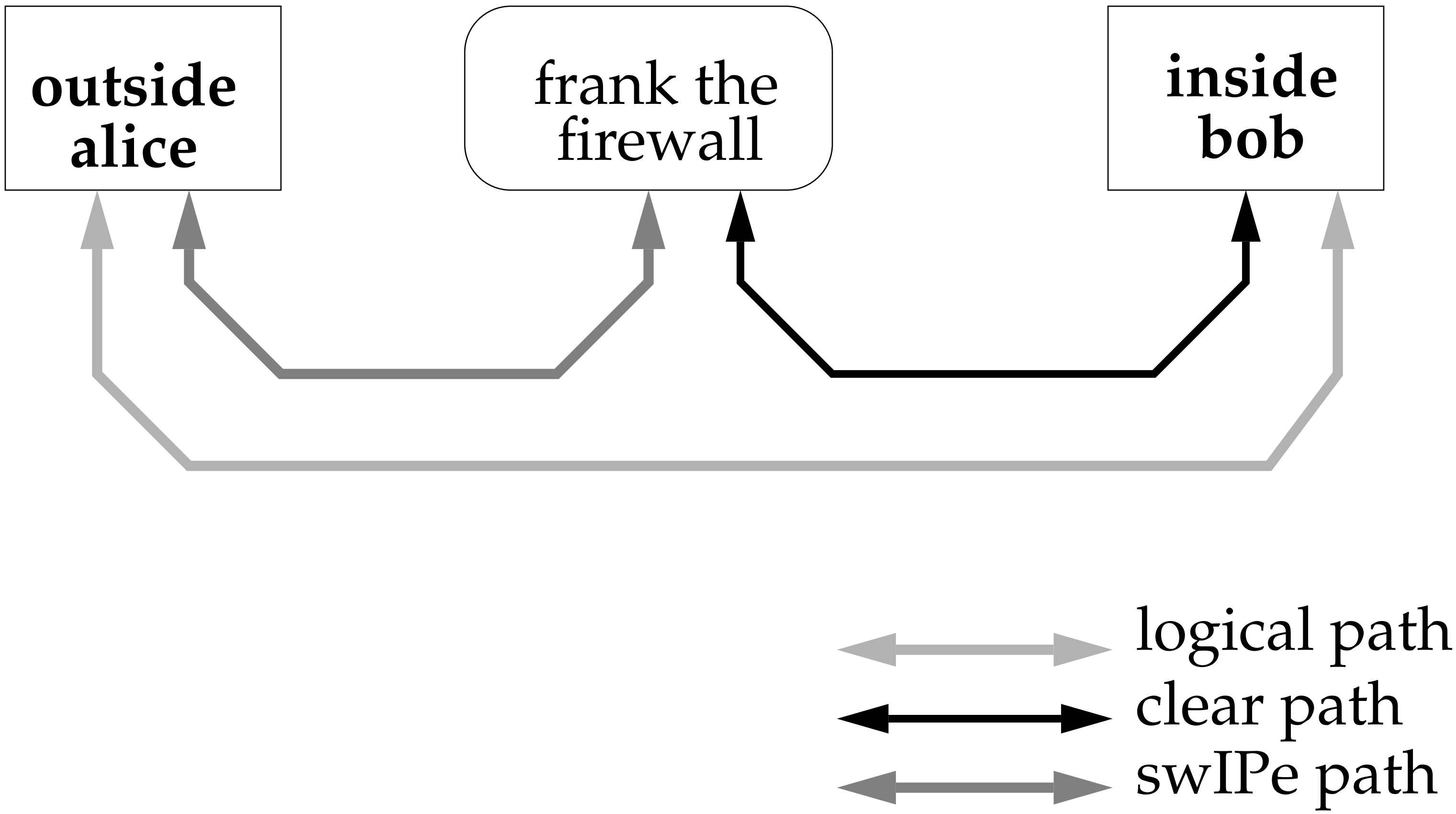
BBQ

swIPe example 1: end-to-end

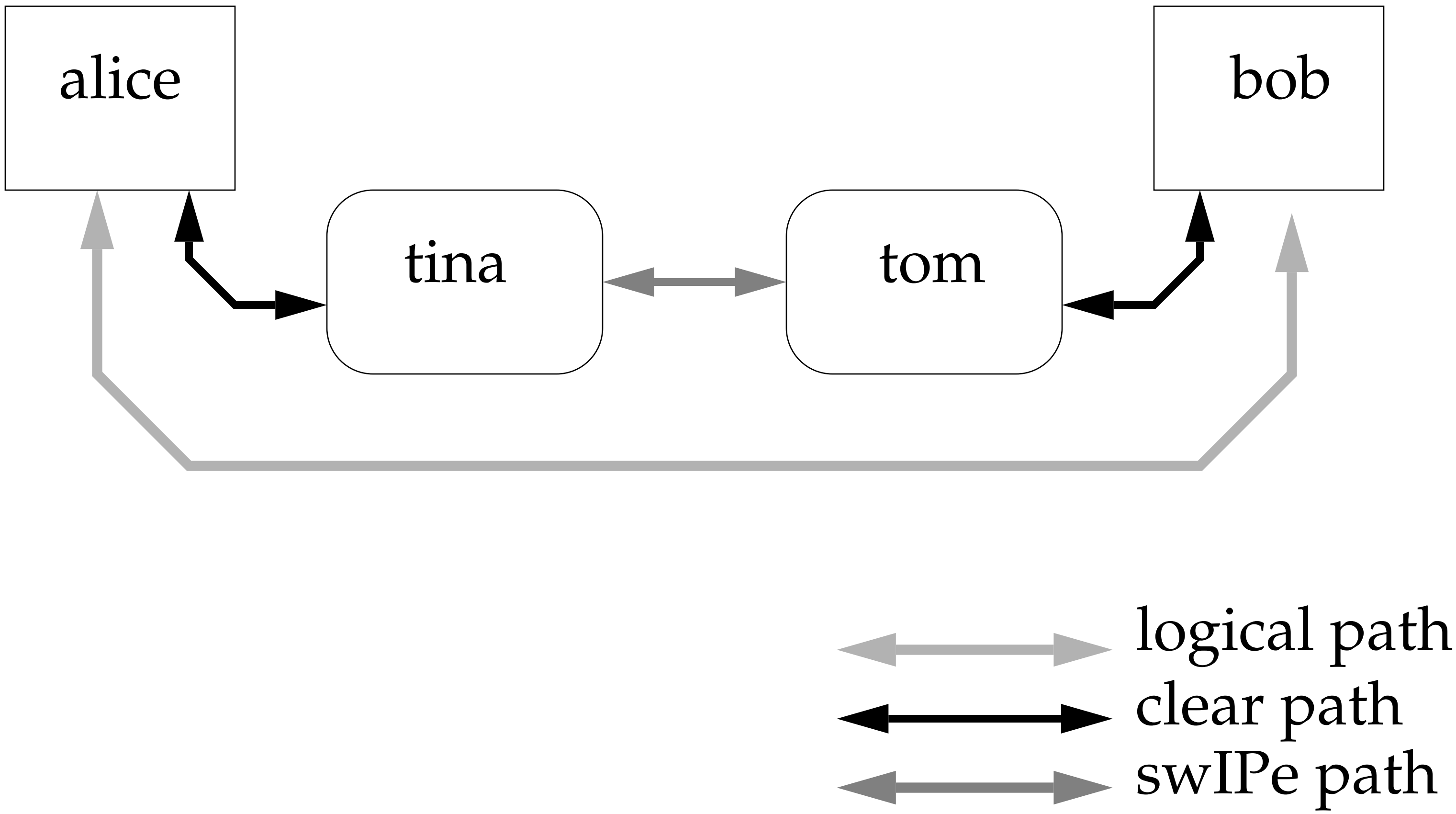


BBQ

swIPe example 2: secure router



swIPe example 3: secure bridging:



BBQ

Overhead

- Byte count:
  - 28-44 extra bytes, plus padding.
  - mostly noticeable on interactive-traffic slow links.
  - possibly amortized over very large MTUs.
- Timing (SparcStation2):
  - 1k packets: DES: 10ms; MD5: 1.1ms; proc: 0.2ms
  - DES and MD5 numbers scale linearly.
- Packets must be delivered almost in order.

Lessons Learned

- A&E feasible on a modern workstation or notebook.
- The interesting questions involve key management.
- A&E mechanism should be decoupled from enforcement policy and key management.
- Encapsulation allows easy deployment of multiple modes of operation.
- Implemented under SunOS 4.1.2, Mach 2.5, and BSD.

BBQ