ECN versus IPsec?

Steven M. Bellovin

`smb@research.att.com`

973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

What is IPSEC, and Why?

- Network-layer security protocol for the Internet.
- TCP- or UDP application-level retransmissions handle deleted or damaged packets.

  - Generally must modify protocol stack, kernel, or hardware; out of reach of application writers or users.

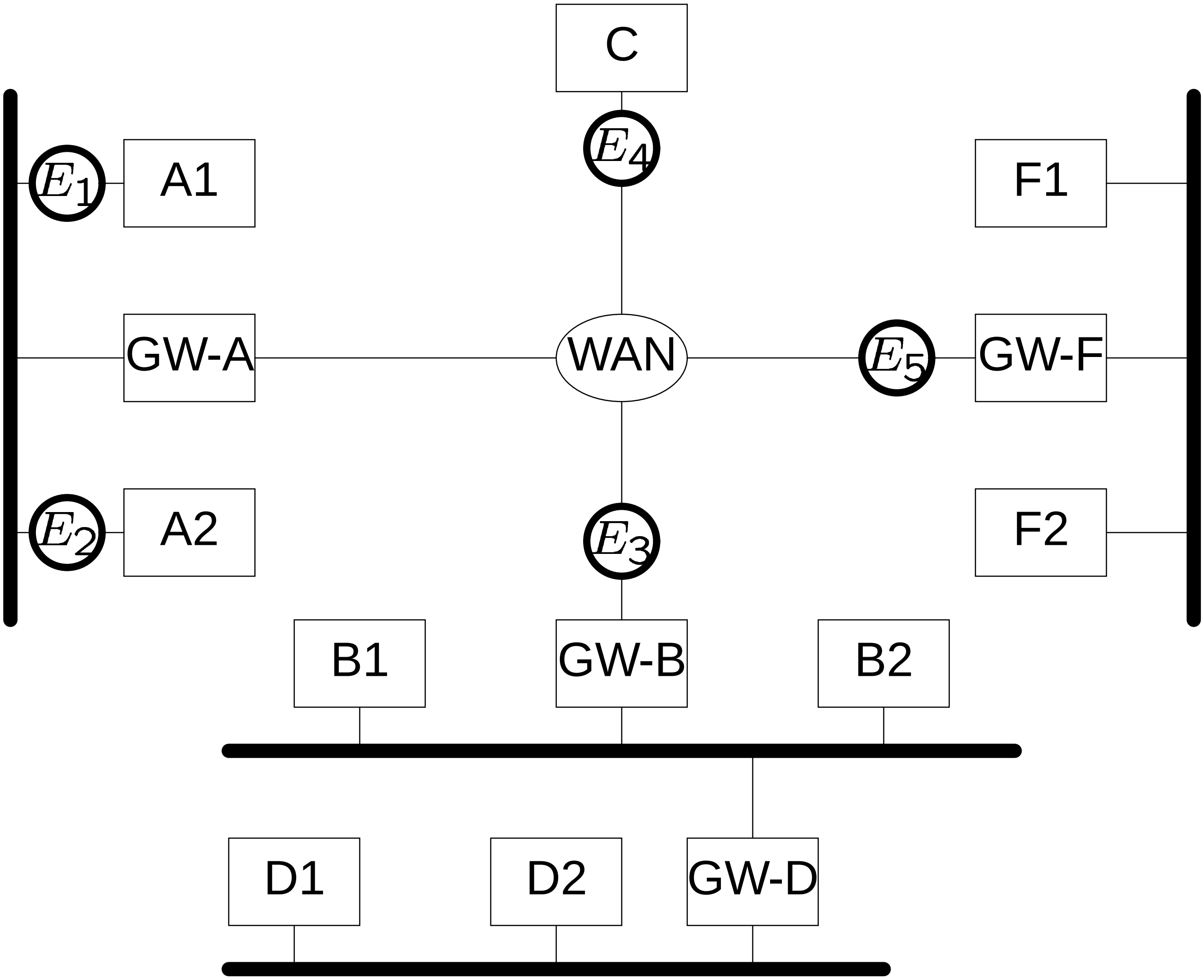
Basic Principles

- Nested headers
- Variable granularity of protection: user, host, network.
- Transparent to applications.

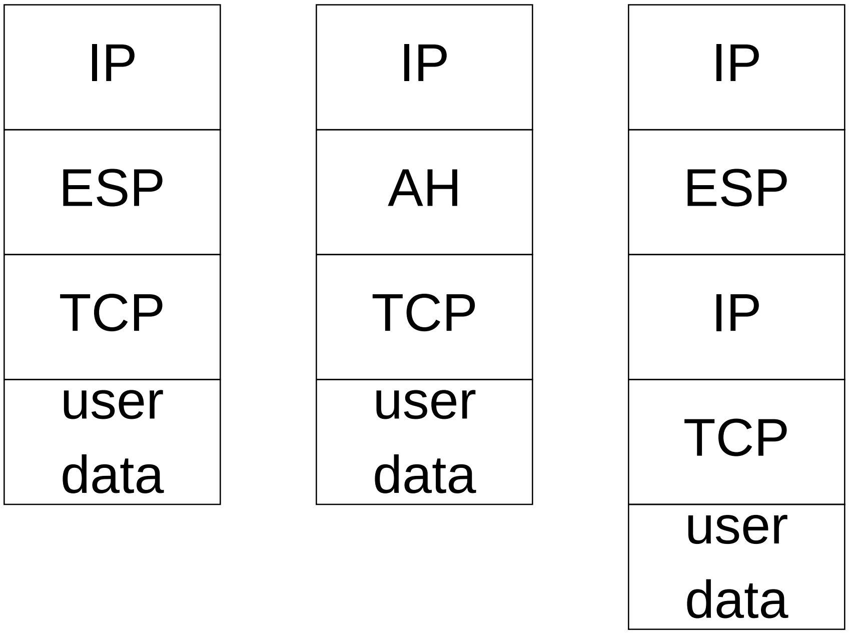
Design Rationale

- “Wasp-waist” protection.
- Maximum security leverage.
- Potential for end-to-end protection, while not requiring new higher-layer mechanisms to deal with corruption or deletion.
- Link-layer encryption doesn’t scale; application-level encryption is vulnerable to active attacks, traffic analysis, etc.

Uses



Packet Layouts



IP

ESP

TCP

user data

IP

AH

TCP

user data

IP

ESP

IP

TCP

user data

ESP versus AH

- ESP
  - Generally includes encryption, authentication, and replay prevention.
  - Any of the above can be omitted.
  - Strict layering.
- AH
  - Includes authentication and replay prevention.
  - Protects some of the preceeding IP headers.

  ⇒ Mutable IP fields excluded from AH calculation.

ECN Considerations – Transport Mode

- ToS field excluded from AH calculation; not examined for ESP.
- No impact in transport mode.

ECN Considerations – Tunnel Mode

- Original ToS field copied to outer IP header.
- Outer ToS field *not* copied back to inner header at tunnel termination.

Why It’s Done This Way

- A tunnel is a virtual wire.
- A goal of VPN-style IPsec is to protect the packet against outside influences.
- If the “wire” has certain properties, should the tunnel handler retain state and deal with it? Congestion control at the tunnel?
- Should we negotiate ToS field handling? Can an enemy exploit this? (That is, can an enemy cause worse behavior by modifying that field than simply dropping the packet?)