Arguments Against IPSEC

("The Con Arguments")

Bob Braden
USC/ISI

Network and Distributed System Security Symposium '99
San Diego, CA
Feb 4-5, 1999

Disclaimer, etc.

Honesty time...

o I am not an IPSEC expert.

In fact, I am not an expert in any branch of computer security!

But I do know something about end-to-end protocol issues in the Internet, and IPSEC is an end-to-end protocol

o I want to acknowledge chats with Cliff Neumann and Brian Tung, who ARE security experts.

o I am really only a simulated foe of IPSEC.

Back in the early 1980s, Steve Kent convinced me that IPSEC would be a Good Thing, and I still believe it.

o I am sure the other speakers and the audience will keep me honest!

OUTLINE

- Historical Perspective
- IPSEC Downsides
- Conclusions
- A Parting Shot

Historical Perspective

o Roughly 15 years ago, IPSEC was invented to provide a common security service that preserves the 'end-to-end connectivity' of of IP and TCP.

End-to-end connectivity is fundamental to the Internet religion -

-- Relays are *BAD*.

-- The IAB did not want application-level gateways or firewalls to degenerate the Internet into a *Bitnet*.

o Since then, IPSEC protocol has "matured", and all of you over 50 know what that means about its bulk!

For example, "End" now has several alternative definitions in IPSEC, to accommodate the security gateways and VPNs that are popular today.

The Downsides of IPSEC

1. IPSEC breaks a lot of things, or makes them harder, because it operates in the Internet layer (layer 3.5).

2. IPSEC makes network security harder.

3. IPSEC adds complexity to the IP layer.

4. IPSEC prevents reasonable application-specific optimization, worsening the security performance problem.

And I will claim one more downside of IPSEC that is too scandalous to put here; I will save it for a Parting Shot.

1. IPSEC Breaks a Lot of Things

(1a) When used for encryption, IPSEC hides information that may be important or even vital for network operation -- especially, it hides the transport layer header.

(1b) When used only for integrity, IPSEC prevents legitimate and useful rewriting of protocol headers “within” the network.

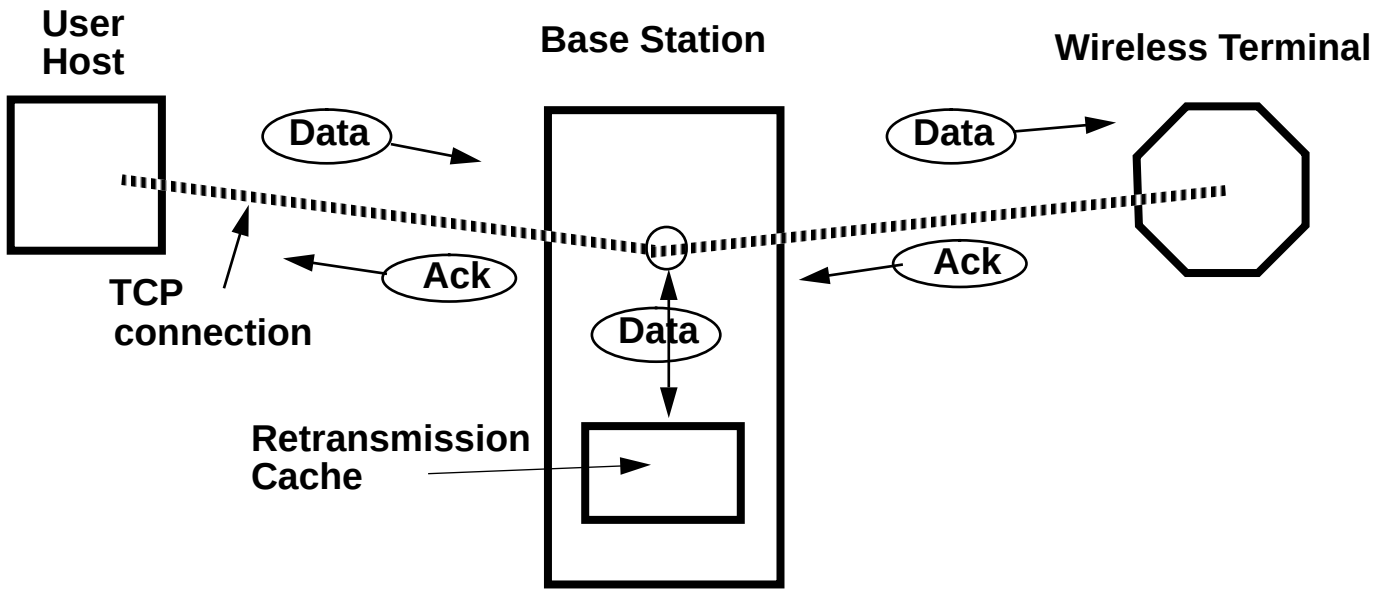
1a. Hiding the Transport Layer

Encryption of the transport layer interferes with:

- **o Network Management.**
  - **>> Network managers want to understand the traffic flows.**
  - **>> E.g., RMON2 MIB can gather information on per-port usage.**
- **o TCP performance enhancements**
  - **>> ACK “snooping” for wireless**
  - **>> ACK pacing for efficient satellite hop**

Ironically, these enhancements (see following slides) were designed to preserve End-to-End TCP semantics.

Example: ACK Snooping

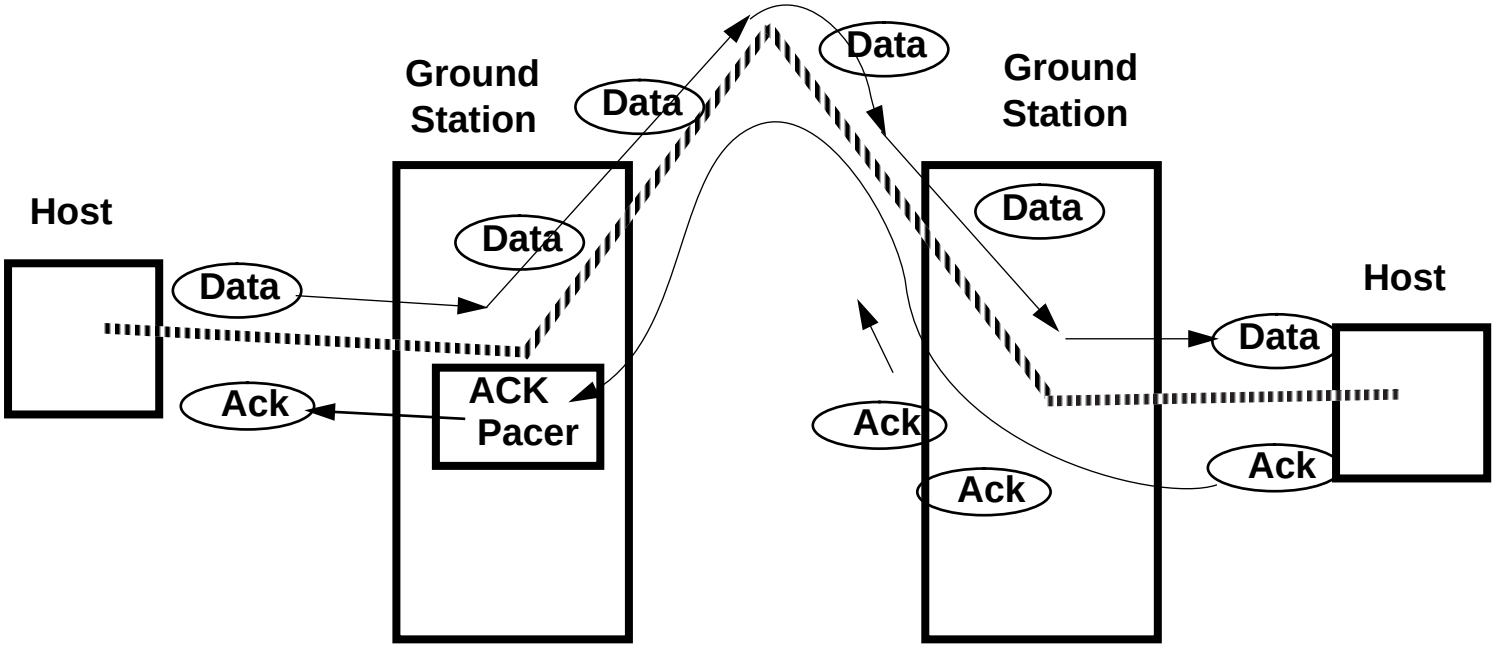


Snooper in Base Station:

* Caches data packets for possible retransmission
* Detects loss by counting duplicate ACKs from wireless terminal.
* Swallows these dupe ACKs and retransmits locally.

If no loss, or if slow-start: normal end-to-end operation.

Example: ACK Pacing



Objective: Fill satellite pipe despite limited buffering in terrestial routers.

Proposed solution: pace returning ACKs to limiting data rate along path.

1a. Hiding the Transport Layer

Encryption interferes with:

o Network Management

o TCP performance enhancements

o Fine-grained QoS (Quality of Service)

Integrated Services: TCP/UDP port numbers needed to define flows.

Differentiated Services: May need port numbers at "edge" of network.

o Knowledge of a transport protocol (e.g., RTP) that is "shimmed" on top of UDP.

Rewriting Protocol Headers

is used for:

- **o NAT boxes *[Some would regard breaking NAT as a win]***
- **o Transport-layer header compression**
- **o Hidden Web proxies**
- **o ? (In the future)**

2. Harming Network Security

o Intrusion detection may be more difficult, more limited.

o The CPU cost of IPSEC cryptography will make denial-of-service attacks much easier.

3. The Complexity Burden

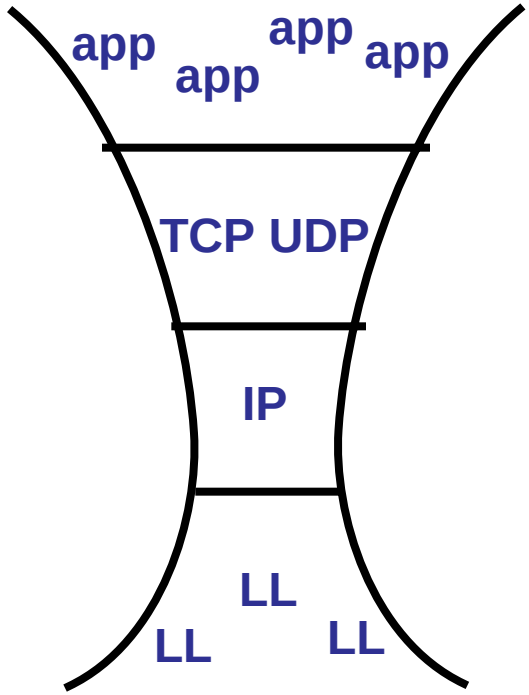
"IP over Everything, and Everything over IP" [VCerf]

The simplicity of the IP layer is widely regarded as a major virtue (cf. recent "dumb network" discussion)

Steve Deering gives a talk entitled "Watching the Weight of the Protocol Hour-Glass".

IPSEC adds significant complexity to the IP protocol layer.

The Internet protocol suite is still evolving. IPSEC will interact with, and add complexity to, each new change or extension.



4. App-Level Security Optimization

Comparing IPSEC with application-level security:

substantial wins, and substantial losses.

o Common IPSEC service ==> WIN for IPSEC

o IPSEC cannot optimize for application requirements

==> LOSS for IPSEC.

Conclusions

Is IPSEC a Good Thing?

Compared to What?

- **o Link-layer security?**
- **o Transport-layer security?**
- **o Application-layer security?**

We don't really know the answers about IPSEC yet.

- **-- IPSEC deployment and use is still (I believe) quite sparse.**
- **-- We don't have a lot of experience with IPSEC's:**
  - **o Performance costs**
  - **o Management complexity and costs**
  - **o Key management complexity and costs**

Parting Shot

The decision to require IPSEC in IPv6 was audacious.

It is conceivable that this IPSEC requirement might delay the deployment of IPv6.

The alternative to IPv6 is NATs and address-space wars. It would be a grim irony if IPSEC contributed to such a result.