Transport-Friendly ESP

or

Layer Violation for Fun and Profit

Steven M. Bellovin
smb@research.att.com
http://www.research.att.com/~smb

Mailing List

Subscription:

```
mail majordomo@research.att.com
subscribe tf-esp
```

Archives

```
mail majordomo@research.att.com
get tf-esp tf-esp
```

Agenda

1530 Introduction, administrivia, agenda-bashing

1540 Hari Balakrishnan

1545 Shivkumar Kalyanaraman, Packeteer

1555 Spencer Dawkins, PILC/PEP

1605 Yongguang Zhang, TCPPEP

1615 Jerry Freedman

1620 Bob Monsour, Compression

1625 Rodney Thayer, "When You Don’t Need TF-ESP"

1640 More of the loyal opposition

1700 Steve Bellovin, "How to do TF-ESP"

1710 Discussion

1730 Food and/or drink

Purpose

Our primary goal for today is to understand the problem. Is tf-esp needed? Can the same goals be achieved in other ways?

We’ll also discuss the basic constraints on a solution. We will not try to do any real technical designs at this point.

Why Leak Information?

- Traffic-shaping
- Wireless spoofing
- Traffic monitoring
- Firewalls
- Other uses we’ll hear about today.

Why Not SSL or TLS?

- SSL does’t work for UDP.
- SSL doesn’t protect headers from modification, leading to possible DoS attacks.
- SSL requires changes to all applications.
- SSL isn’t amenable to hardware implementations.
- SSL can’t easily do VPNs.

But...

- Yes, it’s a layer violation
- Yes, it leaks some information
- Maybe there’s a better way to solve our problems

Can Midpoints Modify the Packet?

- How do we distinguish helpful modifications from man-in-the-middle attacks?
- Each such proposal requires careful, in-depth analysis.
- Basic test: is it worse if the attacker rewrites a field than if the packet is dropped completely?
- No such proposals are currently on the table for this group.

Ground Rules

- We can’t modify ESP
- We can define a new protocol type
- We can negotiate use of this protocol via IKE

TF-ESP Choices

- Separate "disclosure header"
- Modified ESP header with cleartext fields
- Resulting header must be recognizable by and comprehensible to a context-free midpoint node

Disclosure Header

- Separate copy of some information
  - Note -- receiving host must verify that copies match
- Redundancy is ugly
- But -- can disclose **exactly** what is needed
- N.B. -- probably needs to be integrity-protected.

Modified ESP Header

- Tricky -- watch out for encryption blocksize
- Want ciphertext and plaintext to be on 8-byte boundaries.(Maybe even 16-byte boundary for AES.)
- Fundamental assumption: interesting stuff to leak is all near the beginning of the headers; sensitive stuff is at the end.
  - Example: better not expose the TCP checksum.