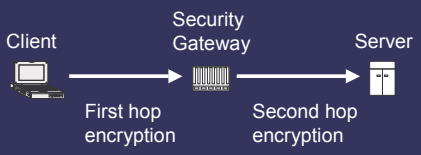
Network Security Architectures Part 2 Formalization and Testing

Summer School on Software Security Theory to Practice

Carl A. Gunter
University of Pennsylvania
Summer 2004

End-to-End Security and Mandatory Tunnels

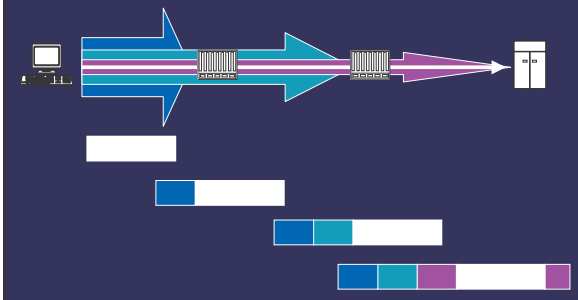


Examples: WTLS, cdma2000, L2TP, Palm VII

Goals for a Security Protocol

1. If client C receives content from server S, then this is authorized by the policies of S and all of the security gateways between C and S
2. If C receives content from S, then this content is encrypted and authenticated from end-to-end between C and S
3. Simple setup and low-overhead enforcement

IPSec Strategy



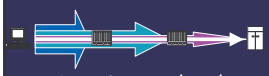
Encapsulation

- AH headers for authentication and authorization of traversal. Use tunnel mode.
- ESP header for authentication and confidentiality of end-to-end communication. Use transport mode.

Drawbacks to IPSec Solution

- Requires complex configuration using nested tunnels to establish security associations between client, gateways and server
- Encrypts the TCP header limiting use of VJC and other similar compression techniques
- Setup is relatively costly as session keys must be exchanged
- Nested headers introduce significant bandwidth overhead

IP SEC Header Overheads for 576 Byte Packets



Security overhead =

$$\frac{(4.50 + 7.61t)}{(60.8 - 5.25t)}$$

# SGs	TCP	TCP + VJC
0	7%	17%
1	22%	31%
2	39%	49%
3	61%	70%
4	88%	97%

Evidence of Problems

- Experimental: FreeBSD IPSec showed an overhead of 46% with two gateways
- Standards activity: secure L2TP overheads were so severe a standard was developed specifically to reduce them. Default security with one gatekeeper yielded this:

A Goodloe, C Gunter, T Hiller, P McCann, M McDougall

Case Study: Layer 3 Accounting (L3A)

- Motivating problem from wireless security
- Solution by composing secure tunnels
- Maude model
- Problems
- Future work

A Goodloe, C Gunter, MO Stehr

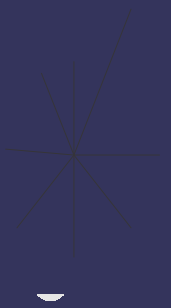
Wireless Security

- Why is wireless security any different from wired security?
  - Resource constraints
  - Increased risk to confidentiality
  - Value of the network link

Wireless Security Efforts

- Layer 1 (Physical)
  - Spread spectrum
- Layer 2 (Link)
  - 802.11x – 802.11(b) WEP, 802.11(g)
  - CDMA 2000
  - GPRS

802.11/WEP



ERROR: ioerror
OFFENDING COMMAND: image

STACK:

/