Network Security Architectures
Part 2 Formalization and Testing

Summer School on Software Security
Theory to Practice

Carl A. Gunter
University of Pennsylvania
Summer 2004

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

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.

<table>
<thead>
<tr>
<th>IP</th>
<th>AH</th>
<th>IP</th>
<th>AH</th>
<th>ESP</th>
<th>TCP</th>
<th>payload</th>
<th>ESP</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>24</td>
<td>20</td>
<td>24</td>
<td>8</td>
<td>20</td>
<td></td>
<td>16</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th># SGs</th>
<th>TCP</th>
<th>TCP + VJC</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7%</td>
<td>17%</td>
</tr>
<tr>
<td>1</td>
<td>22%</td>
<td>31%</td>
</tr>
<tr>
<td>2</td>
<td>39%</td>
<td>49%</td>
</tr>
<tr>
<td>3</td>
<td>61%</td>
<td>70%</td>
</tr>
<tr>
<td>4</td>
<td>88%</td>
<td>97%</td>
</tr>
</tbody>
</table>

Security overhead = (4.50 + 7.61t) / (60.8 - 5.25t)

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:

<table>
<thead>
<tr>
<th>IP</th>
<th>ESP</th>
<th>UDP</th>
<th>L2TP</th>
<th>PPP</th>
<th>IP</th>
<th>ESP</th>
<th>TCP</th>
<th>Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ESP</td>
</tr>
</tbody>
</table>

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:
/