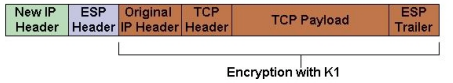
Performance-aware Security for Unicast Communication in Hybrid Satellite Networks

Ayan Roy-Chowdhury and John S. Baras

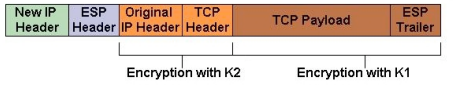
- TCP Performance Enhancing Proxy (PEP) server used to mitigate the negative impact of satellite link propagation delay on TCP performance.
- HTTP Proxy server used to reduce the effect of satellite link delay on HTTP protocol/web browsing.
- IPSEC disables the functionality of TCP PEP and HTTP proxy.
- SSL/TLS for secure web browsing disables functionality of HTTP proxy.

How to enable security similar to IPSEC and SSL in hybrid satellite networks, while preserving functionality of TCP PEPs and HTTP proxy?

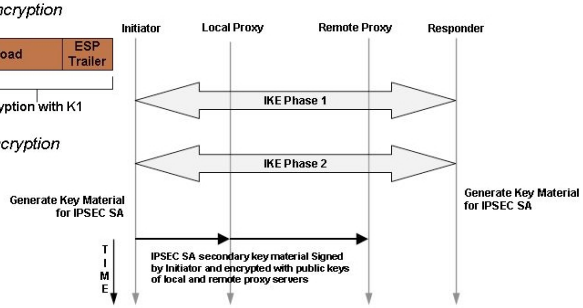
Network Layer Security: Layered IPSEC (LES) with modified IKE



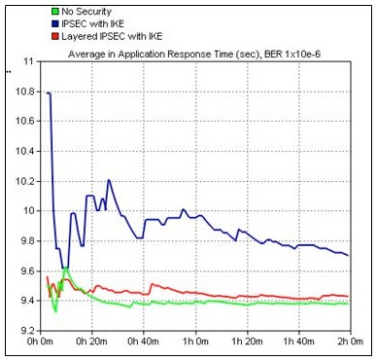
Original IPSEC ESP Tunnel Mode Encryption



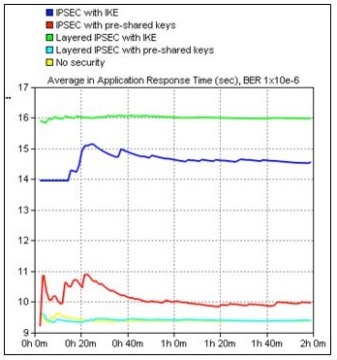
Layered IPSEC ESP Tunnel Mode Encryption



- Can co-exist with TCP PEPs in hybrid satellite networks.
- Modify Internet Key Exchange (IKE) to use with layered IPSEC: two additional keys for encryption and authentication of IP and TCP headers – the secondary keys.



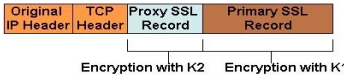
Custom application response time



Effect of IKE handshake on response time

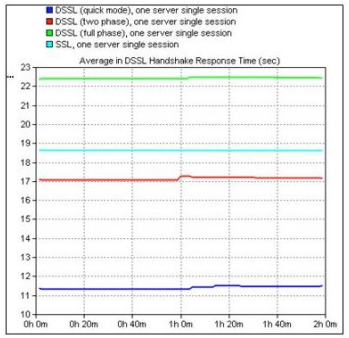
Transport Layer Security: Dual-mode SSL (DSSL)

DSSL Primary and Secondary Modes

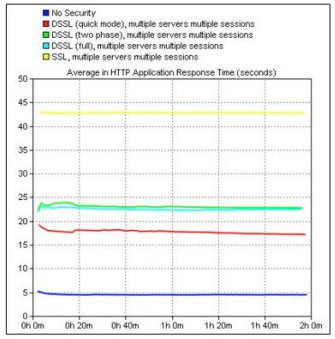


Three versions with varying handshake times:

- DSSL full – 5 stages in handshake
- DSSL two-phase – only first two handshake stages
- DSSL quick mode – only stage 2 of *full* mode



DSSL handshake response times



HTTP Response Times

Further information: University of Maryland Invention Disclosure IS-2008-134, Office of Technology Commercialization, University of Maryland College Park.