TLS-PSK with NULL Encryption

Uri Blumenthal
Security Architect
Communications Technology Lab
Intel Corporation

July 11, 2006

TLS-PSK-WITH-NULL-SHA

Why

- For our product(s) we need TLS to protect communications
  - Requirements include Pre-Shared Keys (so TLS-PSK, RFC 4279)
  - Requirements also include ability to run in cipher-controlled places
    - Some countries place restrictions on encryption
    - Some corporate policies limit encryption usage on their Intranets

What

- To address the need, augment RFC 4279 by adding three suites
  - Everything's the same except encryption algorithm defined is NULL

• Pre-shared symmetric key	TLS-PSK-WITH-NULL-SHA
• RSA-encrypted contribution to key	TLS-RSA-PSK-WITH-NULL-SHA
• Diffie-Hellman contribution to key	TLS-DHE-PSK-WITH-NULL-SHA

  - Same security considerations as in RFC 4279 *plus – no confidentiality* ☺