Camellia Cipher Suites for TLS

<draft-kato-tls-rfc4132bis-00.txt>

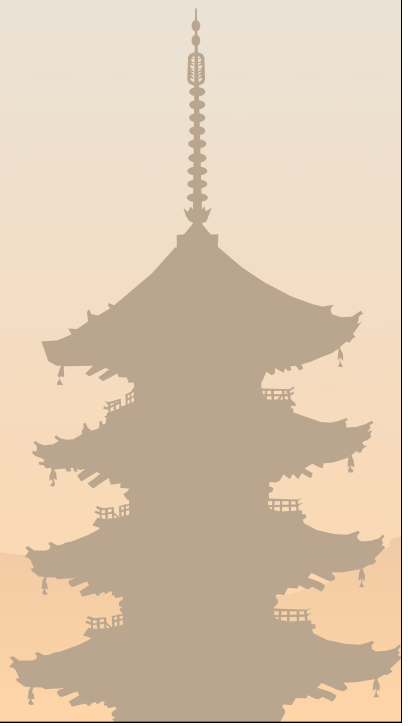
Akihiro KATO

IETF 71th March 2008

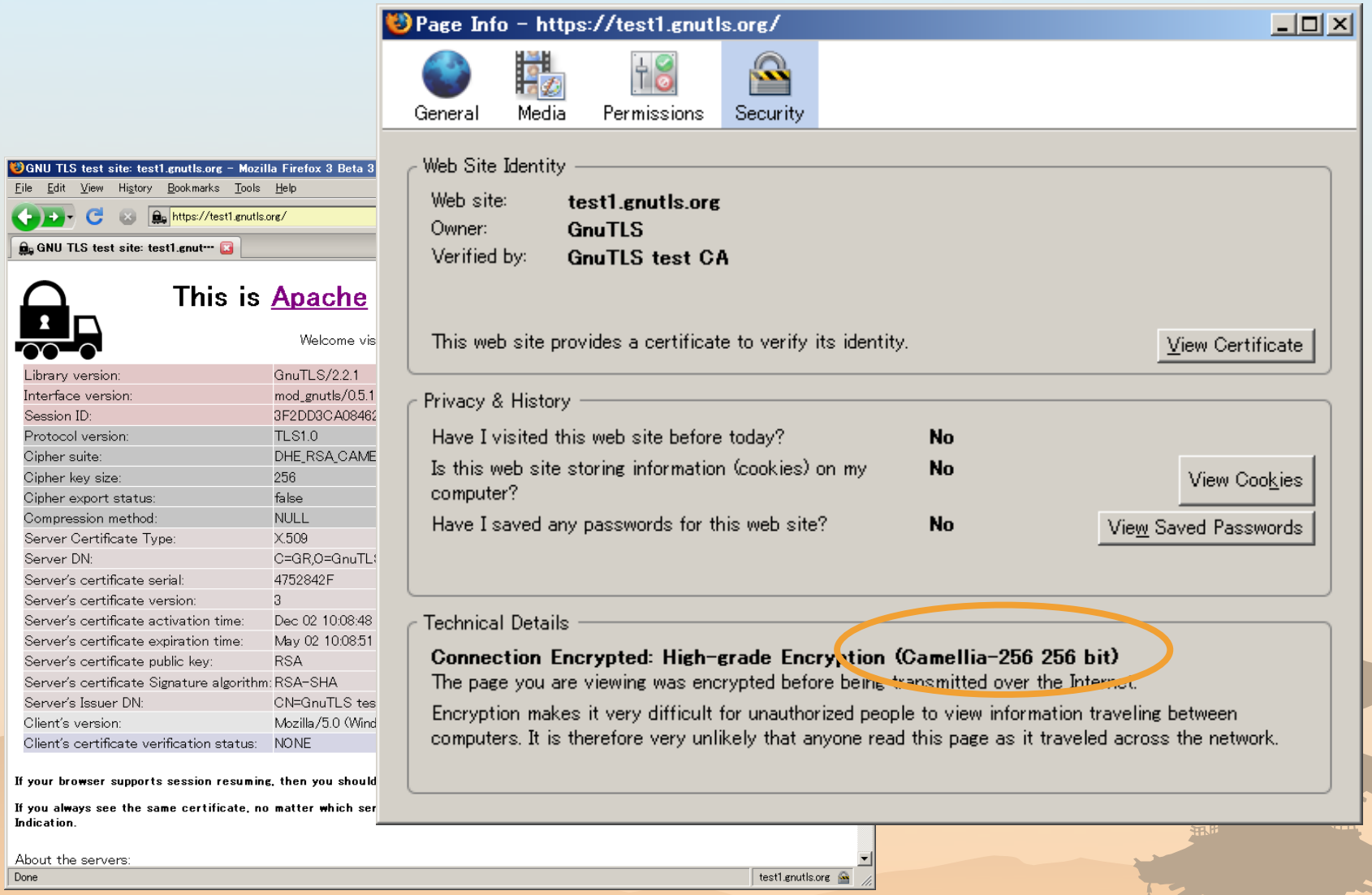
TLS Working Group

Back Ground

- RFC4132 Published July 2005
- Adapted several FOSS
  - OpenSSL 0.9.8c or later
  - GnuTLS
  - Firefox3
  - IPsec Stack (Linux, FreeBSD)



Connect to GnuTLS Test Server by



Proposed New Cipher Suites

RSA_WITH_CAMELLIA_128_CBC_SHA256	RSA_WITH_CAMELLIA_128_CBC_SHA256
DH_DSS_WITH_CAMELLIA_128_CBC_SHA256	DH_DSS_WITH_CAMELLIA_128_CTR_SHA256
DH_RSA_WITH_CAMELLIA_128_CBC_SHA256	DH_RSA_WITH_CAMELLIA_128_CTR_SHA256
DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256	DHE_DSS_WITH_CAMELLIA_128_CTR_SHA256
DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	DHE_RSA_WITH_CAMELLIA_128_CTR_SHA256
DHE_anon_WITH_CAMELLIA_128_CBC_SHA256	DHE_anon_WITH_CAMELLIA_128_CTR_SHA256
RSA_WITH_CAMELLIA_256_CBC_SHA384	RSA_WITH_CAMELLIA_256_CTR_SHA384
DH_DSS_WITH_CAMELLIA_256_CBC_SHA384	DH_DSS_WITH_CAMELLIA_256_CTR_SHA384
DH_RSA_WITH_CAMELLIA_256_CBC_SHA384	DH_RSA_WITH_CAMELLIA_256_CTR_SHA384
DHE_DSS_WITH_CAMELLIA_256_CBC_SHA384	DHE_DSS_WITH_CAMELLIA_256_CTR_SHA384
DHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	DHE_RSA_WITH_CAMELLIA_256_CTR_SHA384
DHE_anon_WITH_CAMELLIA_256_CBC_SHA384	DHE_anon_WITH_CAMELLIA_256_CTR_SHA384
RSA_WITH_CAMELLIA_256_CBC_SHA512	RSA_WITH_CAMELLIA_256_CTR_SHA512
DH_DSS_WITH_CAMELLIA_256_CBC_SHA512	DH_DSS_WITH_CAMELLIA_256_CTR_SHA512
DH_RSA_WITH_CAMELLIA_256_CBC_SHA512	DH_RSA_WITH_CAMELLIA_256_CTR_SHA512
DHE_DSS_WITH_CAMELLIA_256_CBC_SHA512	DHE_DSS_WITH_CAMELLIA_256_CTR_SHA512
DHE_RSA_WITH_CAMELLIA_256_CBC_SHA512	DHE_RSA_WITH_CAMELLIA_256_CTR_SHA512
DHE_anon_WITH_CAMELLIA_256_CBC_SHA512	DHE_anon_WITH_CAMELLIA_256_CTR_SHA512

Issues and Questions

- Explosion of Cipher suites
  - Eliminate CTR, SHA384 or SHA512
    - 36 New Cipher suites→ 12 New Cipher suites
- SHA-384 vs. SHA512
  - NIST SP 800-57 said “256bit security for HMAC are HMAC-256, HMAC-384, HMAC-512”
  - TLS spec takes 384

What's Next?

- Shrink Cipher suites
- Take in comments
- Fix errors
- Submit A.S.A.P to I-D repository

Questions and comments?