ANSI X9.44 and IETF TLS

Russ Housley and Burt Kaliski
RSA Laboratories

November 2002

Introduction

- ANSI X9.44 specifies key establishment schemes based on the RSA algorithm
  - currently in draft form
- Schemes selected to *reflect* and *guide* industry practice
- NIST key management FIPS intended to adopt X9.44 and other X9 standards

Reflecting and Guiding

- X9.44 reflects industry practice where appropriate for banking/FIPS:
  - S/MIME key transport with PKCS #1 v1.5
  - TLS handshake with PKCS #1 v1.5, SHA-1, MD5
- Also guides toward new techniques:
  - S/MIME key transport with RSA-KEM
  - TLS handshake with RSA-KEM, SHA-256 and above
- Focus on key establishment, not session encryption

TLS Handshake: Crypto Recap

- Ciphertext = Encrypt (Server Public, Premaster)
- Master = KDF (Premaster, Nonces)
- Session = KDF (Master, Nonces)
- Tag = MAC (Master, Handshake Messages)

TLS Handshake Crypto Today

- Encrypt = PKCS #1 v1.5 Block Type 02
- KDF = TLS PRF
  - PRF (secret, label, seed) =
    HMAC-MD5 (S1, label + seed) ⊕
    HMAC-SHA-1 (S2, label + seed)
  - S1 is first half of secret; S2 is second half
- MAC = TLS PRF

Security Analysis

- PKCS #1 v1.5 encryption has vulnerabilities, but TLS handshake has countermeasures
- Jonsson-Kaliski result (Crypto 2002):
  - TLS handshake security (loosely) related to *gap-partial-RSA assumption*
  - relies only on SHA-1 security, not MD5
- Analysis has helped support X9F1 acceptance of TLS, despite PKCS #1 v1.5 vulnerabilities
  - SSLv3 currently out; security relies on SHA-1 & MD5

X9.44-Recommended Enhancements

- Encrypt = Raw RSA
  - Premaster as long as RSA modulus
- KDF = IEEE P1363a KDF2
- MAC = HMAC
  - both based on SHA-1 or higher

Note: No architectural changes required

Rationale for Enhancements

- Raw RSA + KDF2 ≈ Shoup's RSA-KEM
  - Security related to *ordinary* RSA assumption
  - Intuition: Attacker must know full input to RSA in order to compute master secret
- KDF2, HMAC more standard, support larger hash sizes

Client Authentication

- Sign (Client Private, Handshake Messages)
- Today: PKCS #1 v1.5 variant
- Enhancement: RSA-PSS (or other X9-approved signature scheme)

Next Steps

- TLS WG:
  - Consider X9.44 direction
- X9F1:
  - Incorporate TLS WG feedback
- Joint:
  - Draft TLS cipher suites for new algorithms, e.g., SHA-256, reflecting guidance

More Information

- Russ Housley
  - rhousley@rsasecurity.com
  - +1 703 435 1775
- Burt Kaliski (editor, ANSI X9.44)
  - bkaliski@rsasecurity.com
  - +1 781 515 7073
- Next ANSI X9F1 meeting:
  January 29-30, 2003 by teleconference