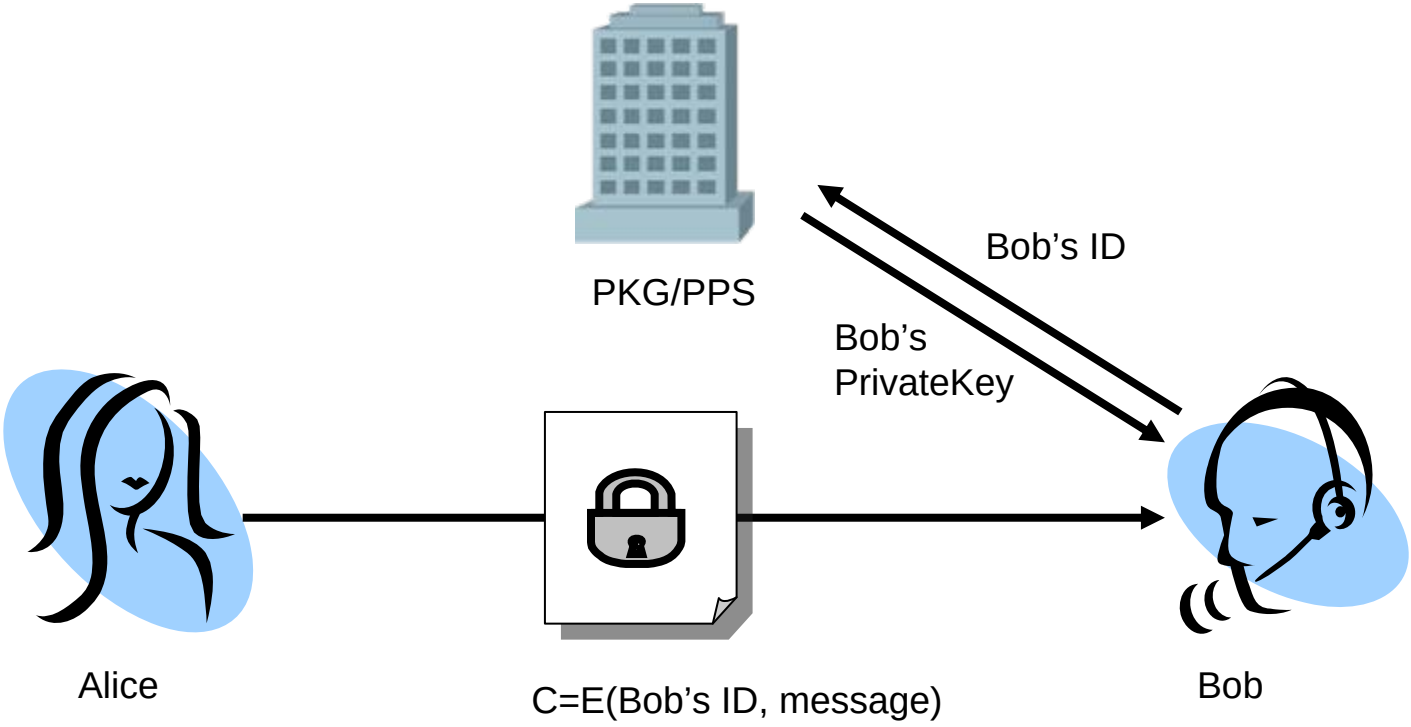
Identity-Based Encryption (IBE) Cipher Suites for Transport Layer Security (TLS)

draft-huang-tls-ibe-00

Min Huang
HuaweiSymantec
July,2009

Identity-Based Encryption (IBE)

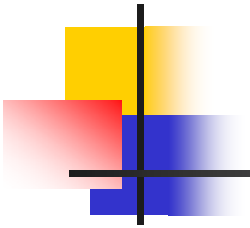


Benefit from IBE

- IBE has been standardized by IETF(RFC5091,RFC5408,RFC5409),IEEE(P1363.3),etc.
- One more choice for TLS
  - Key exchange
  - Client and server authentication
- Public key = Identity
  - No certificate => No certificate management
    - An example with short-lived public keys: Bob@gmail.com|valid period
- Shorter key length, less encrypting time
  - Based on pairing, efficiency similar to ECC,160bits IBE provides the same security level as 1024 bits RSA

IBE for TLS mechanism

- Key-exchange Method
  - A new key-exchange method is introduced. All of the key exchange methods which transmit encrypted premaster secret using public-key encryption can be replaced by the method based on IBE public-key encryption.
- Client and Server Authentication
  - An authentication method allowing the users to compute digital signatures using their private keys from the PKG. Each side can validate the signature with the public key of the other side.



IBE for TLS Process

-Cipher suite negotiation

-Public Parameter set negotiation

-Sending the PreMasterSecret encrypted by IBE

-Client Authentication

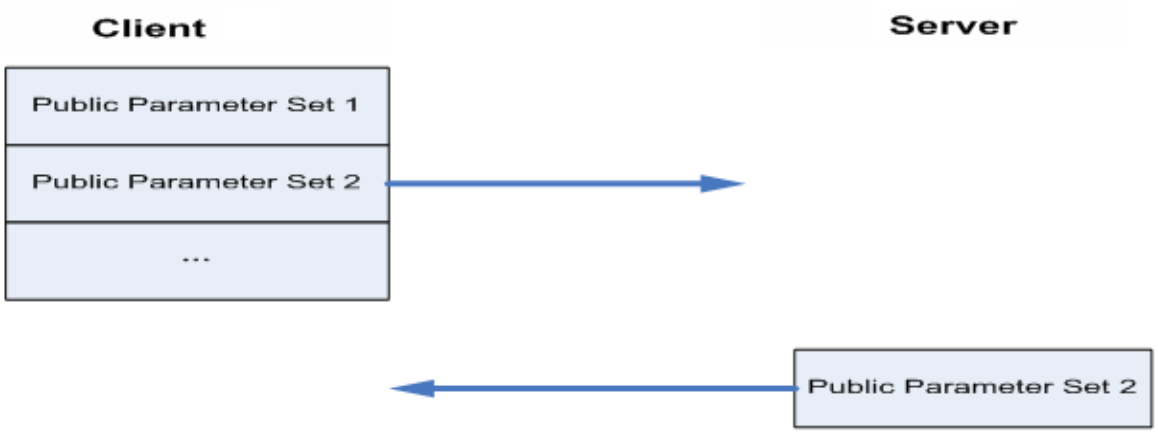
CipherSuite

- ClientHello
  - this message should contain IBE cipher suites(IANA consideration) (described in -00 version)

    CipherSuite TLS_IBE_WITH_NULL_MD5
    CipherSuite TLS_IBE_WITH_NULL_SHA
    CipherSuite TLS_IBE_WITH_NULL_SHA256
    CipherSuite TLS_IBE_WITH_RC4_128_MD5
    CipherSuite TLS_IBE_WITH_RC4_128_SHA
    CipherSuite TLS_IBE_WITH_3DES_EDE_CBC_SHA
    CipherSuite TLS_IBE_WITH_AES_128_CBC_SHA
    CipherSuite TLS_IBE_WITH_AES_256_CBC_SHA
    CipherSuite TLS_IBE_WITH_AES_128_CBC_SHA256
    CipherSuite TLS_IBE_WITH_AES_256_CBC_SHA256
- The CipherSuite in blue will be deleted in -01 version (because MD5,RC4 are thought not secure enough nowadays)

Public Parameter Negotiation

- Mechanism 1



  - Client sends public parameter sets list client trusts via ClientHelloExtension
  - Server chooses one set from the trusting list and replies to the client via ServerHelloExtension
  - Advantage: Client sends what it trusts, so it can avoid compromised server sends forged public parameter
  - Disadvantage: ClientHello Message with trusting public parameters set list may be large, but suitable for a domain with the number of PKG is not large

Public Parameter Negotiation

- Mechanism 2

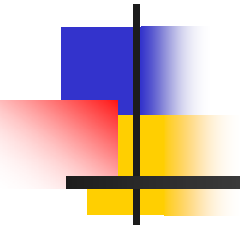
  - Server sends one public parameter set to client by ServerCertificate
  - Similar to PKI mechanism, server sends its certificate in PKI, but sends Public Parameter set and its ID in IBE
  - It needs signature attached to avoid forged Public Parameter

Client Authentication (optional)

- Certificate Request
  - Add a new type of ClientCertificate
- Client Certificate
  - An Empty message
- Certificate Verify
  - The client computes its signature over all handshake messages sent or received starting at client hello and up to but not including this message. It use the client IBE-based private key

Open issue

- Is there anyone interested in this proposal?
- Anyone interested in co-author with me?



Thank you

huangmin@huaweisymantec.com