IK2206 – Internet Security and Privacy
Chapter 18 – IPsec: IKE

18.1 Photuris (READ)

- How does Photuris provide defence against DoS attacks?

  The first exchanged messages are stateless cookies. An active attacker can send as much cookies as he wants – the only thing happening on his victim is that it stores the received cookie and responds with another cookie.

- How does Photuris provide identity hiding?

  By first doing an anonymous Diffie-Hellmann and using an initial stateless cookie.

- Why do you think Alice and Bob signs messages 5 and 6? (Hint: see section 16.12 about downgrade attacks)

18.2 SKIP (READ BRIEFLY)

18.3 History of IKE (READ BRIEFLY)

18.4 IKE Phases (READ)

- What is the idea behind having two phases in IKE? The author's seem to prefer a design with only a single phase. Do you agree?

  Phase 1 does mutual authentication and establishes session keys. Then using the keys established in phase 1, multiple phase-2 SAs between the same pair of entities can be established.

  Theory is that although the phase-1 exchange is necessarily expensive, the phase-2 exchanges can then be simpler and less expensive because they can use the session key created out of the phase-1 exchange.

  You can set up multiple connections with different security properties, such as integrity-only encryption with a short key, or encryption with long key. The author disagrees with this since it would seem logical to use the strongest protection needed by any of the traffic.

- In which phase is the ESP/AH SA created?

  An ESP or AH SA would be established through phase 2

18.5 Phase 1 IKE (READ)

18.5.1 Aggressive Mode and Main Mode

- Does Aggressive Mode provide endpoint identity hiding? Does Main Mode? How come there is a difference?

  Main mode provides endpoint identity hiding. If the main mode is used, in messages 5 and 6 each side reveals its identity encrypted with the Diffie-Hellman value agreed upon in message 3 and 4.

- In aggressive mode Trudy could launch a "downgrade attack" by sending a refusal message back to Alice. How should Alice proceed if she receives a message where her proposed crypto is refused?

  Alice should attempt to reconnect with main mode, rather than retry aggressive mode with a weaker cryptographic choice.

18.5.2 Key Types

- How come there are 8 variants to do an IKE phase 1 exchange? How many of these variants are based on public key cryptography?

  There are 4 authentication methods (original public key encryption, revised public key encryption, public key signature and pre-shared secret key encryption), and for each authentication method, a main mode protocol and an aggressive mode protocol can be used. Variants based on pre-shared secrets might make sense because secret keys are higher performance and might be easier to configure. The original public key encryption method is only there for backward compatibility.
  But why have both public key encryption and public key signature (a public key pair whose usage is restricted to signing and signature verification) methods?
  If Alice's encryption key was escrowed, and her signature key was not, then using the signature key offers more assurance that you are talking to Alice rather than the escrow agent.
  Six of them are based on public key cryptography (original public key encryption, revised public key encryption, public key signature) and for each are the two modes (main, aggressive) available.

- Assume we could skip aggresive mode, and only support the "pre-shared" key and signature key types, how many variants would remain?

  Two variants ???

18.5.3 Proof of Identity (READ BRIEFLY)

Is IKE subject to downgrade attacks?

In IKE the proof of identity is different for each key type, and each consist of some hash of the key associated with the identity, the Diffie-Hellman values, nonces, the cryptographic choices Alice offered. IKE does not prevent a downgrade attack as not the whole previous message is hashed. This will be most likely fixed in a later version of IKE.

-

18.5.4 Cookie Issue

- IKE does not support stateless cookies. How could it have been fixed?

  Bob isn't stateless since he has to remember the cipher suites that Alice supports. If Alice would retransmit them in later messages, Bob could be stateless.

- SKIP the part of 18.5.4 concerning cookie issues related to connection identifiers.

18.5.5 Negotiating Cryptographic Parameters

- With IKE, every choice takes 20 bytes to specify {4 bytes for a header and 4 bytes for each of encryption, hash, authentication, and Diffie-Hellman, as described by Perlman's and Kaufman's paper.} TLS/SSLv3 uses a set of pre-defined cipher suites (see section 19.10), and two bytes is required to specify a suite. Which do you prefer?

  It is more efficient to provide predefined suites otherwise Alice would have to specify 81 (3^4) suite choices to Bob.

18.5.6 Session Keys

- Does IKE negotiate different keys in each direction? Why would it be good to have different keys in each direction?

  IKE phase 1 establishes 2 session keys: an integrity key and an encryption key for the purpose of integrity-protecting and encrypting. IKE doesn't establish 4 session keys(integrity and encryption for each direction), since cryptographers generally recommend using different keys in the two direction in order to avoid dictionary attacks.

- Read the first paragraph of this section (providing the answer to the question above. SKIP the rest of the section.

18.5.7 Message IDs (READ BRIEFLY)

18.5.8 Phase 2/Quick Mode (READ BRIEFLY)

- More on IKE Phase 2 in section 18.6

18.5.9 Traffic Selectors

- Is it possible to have use different SAs between different traffic flows between the same machines?

IPsec allows each side of a phase 2 SA to restrict the traffic sent on that SA, by IP address, protocol type and/or TCP/UDP port. This is done by having the phase 2 initiator give a proposal for what IPsec calls a "traffic selector". The other side can either accept it exactly as specified, or refuse.

18.5.10 The IKE Phase 1 Protocols

- READ BRIEFLY the subsections 18.5.10.1-8.
- As stated before, having so many alternatives is overly complex.
- For each (or some) of the protocols, try to find out if (and how) they support:
  - identity hiding
  - resistance to downgrade attacks
  - perfect forward secrecy
- Compare the original and revised public encryption key modes. Why was the protocols revised?

  The original mode has the problem that in message 3 there are two fields separately encrypted with Bob's public key, so two private key operations are necessary to decrypt it.

  The public encryption protocol was revised to require only a single private key operation on each side.

- Why does the public encryption key modes more problems than the signature key modes concerning how to exchange certificates (public keys)?

  There is no way for either Alice or Bob to ask the other side to send them their certificate.

- What are the problems with the Shared Secret Main Mode?

  This is the most broken mode. In this mode Alice's identity has to be her IP address.

18.6 Phase-2 IKE: Setting Up IPSec SAs (READ)

- In Phase-2 Alice and Bob negotiate everything to setup an IPSec SA, e.g., use of AH or ESP, and cipher protocols and keys for AH/ESP. From the text and Fig 18-12, are you able to get a rough understanding of how this is accomplished?

The phase-2 exchange sends nonces and other information which gets shuffled into the SKEY-SEED computed in the IKE SA to compute integrity and encryption keys for the IPSec SA.

All messages in Quick Mode (Phase-2 IKE) are encrypted with the Phase 1 SA's encryption key Kenc and integrity protected with the Phase 1 SA's integrity key Kint

This exchange agrees upon parameters and encryption and/or integrity keys for each direction, to be used by the created IPsec SA.

18.7 ISAKMP/IKE Encoding (SKIP)