IPsec – IKE
Internet Key Exchange Protocol

BİL 448/548

Internet Security Protocols

Ali Aydın Selçuk

IPsec

- Cryptographic protection of the IP traffic, transparent to the user
- Main components:
  - Internet Key Exchange (IKE): IPsec key exchange protocol
  - Authentication Header (AH): Authentication of the IP packet (optional)
  - Encapsulating Security Payload (ESP): Encryption/authentication of the IP packet (optional)

Session Key Establishment

- Packets are authenticated/encrypted with a session key.
- Session keys are exchanged using the long term keys (public or symmetric keys).
- Compromise of a session key should not compromise other sessions.
- Desired features:
  - Freshness guarantee
  - Perfect forward secrecy
  - DoS protection

Freshness Guarantee

- Key replay attack

  An attacker who has broken a past session key can try to replay the same key exchange protocol messages, establish the same session key, and impersonate the client (or server).

- “Freshness guarantee”

  If both parties contribute something to the established session key, key replay attacks won’t be possible.

Perfect Forward Secrecy

- PFS: Compromise of some secret key (session or long term) doesn't compromise other keys.
- Non-PFS examples:
  - Kerberos (key exchange with a KDC)
  - SSL session key transport with RSA encryption
- PFS example: DH with RSA signatures
- By-product: "Key escrow" prevention

  Conversations can't be decrypted by authorities holding copies of long-term private keys.

“Denial of Service” Protection

- DoS attacks: Depleting a server’s resources (memory, CPU, or bandwidth) by overwhelming it with bogus requests (TCP SYN, ICMP, etc.).
- If attacker can make server do PKC op (RSA, DH, etc.) by just initiating a session, DoS is made easy (by CPU depletion).
- Protection:
  - cookies
  - puzzles

DoS Protection – Cookie Solution

- Server responds to session requests with a random number (cookie).
  Initiator has to respond back with that cookie to continue
- Attacker would have to either
  - reveal its address
  - or, abort the attack
- Stateless cookies: cookie is H(IP addr, secret K); server doesn’t have to remember it.

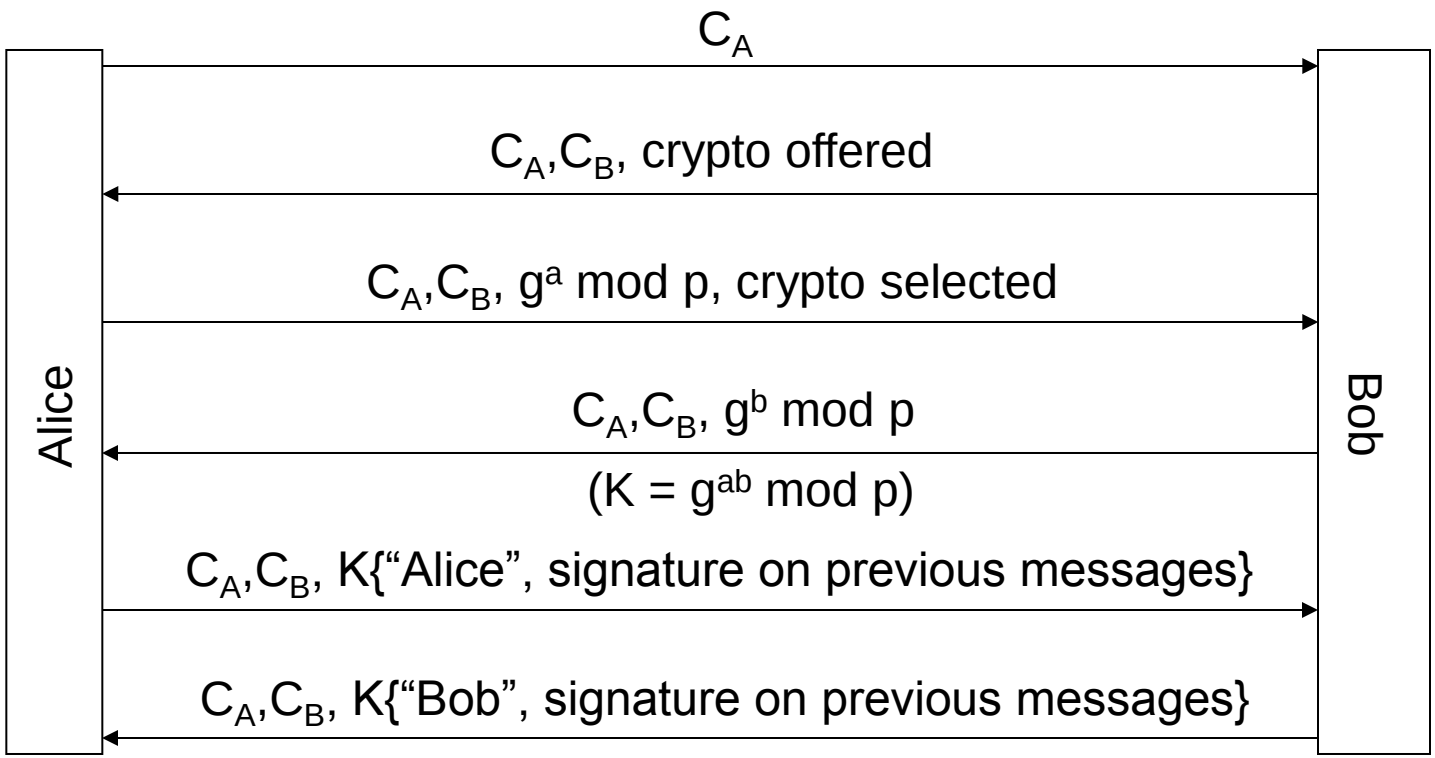
DoS Protection – Puzzle Solution

- Server requires initiator to solve a puzzle
  E.g., MD5(x) = …, x = ?, for an n-bit x.
- Solving is slow, verification fast.
- Can be made adaptive to increasing load. (how?)
- Can be made stateless. (how?)
- Can be used against spam as well

History of IKE

- Early contenders:
  - Photuris: Authenticated DH with cookies
  - SKIP: Authenticated DH with long-term exponents
  - ISAKMP: A protocol specifying only payload formats & exchanges (i.e., an empty protocol)
- Oakley: Modified Photuris; can work with ISAKMP
- IKE: A particular Oakley-ISAKMP combination
- The whole process and the resulting protocols are just too complex.

Photuris



C_A: Alice’s cookie; for connection ID

C_B: Bob’s cookie; against DoS

Photuris – Features

- DoS protection by cookies
  (note: C_B can be stateless)
- Authentication & integrity protection of the messages by a combined signature at the last rounds
- Identity hiding from passive attackers (How?)

IKE/ISAKMP Phases

Phase 1:

- does authenticated DH, establishes session key & "ISAKMP SA"
- two possible modes: Main & Aggressive
- two keys are derived from the session key:
  SKEYID_e: to encrypt Phase 2 messages
  SKEYID_a: to authenticate Phase 2 messages

Phase 2:

- IPsec SA & session key established; messages encrypted & authenticated with Phase 1 keys
- Additional DH exchange is optional (for PFS)

Phase 1 Exchange

Two possible modes:

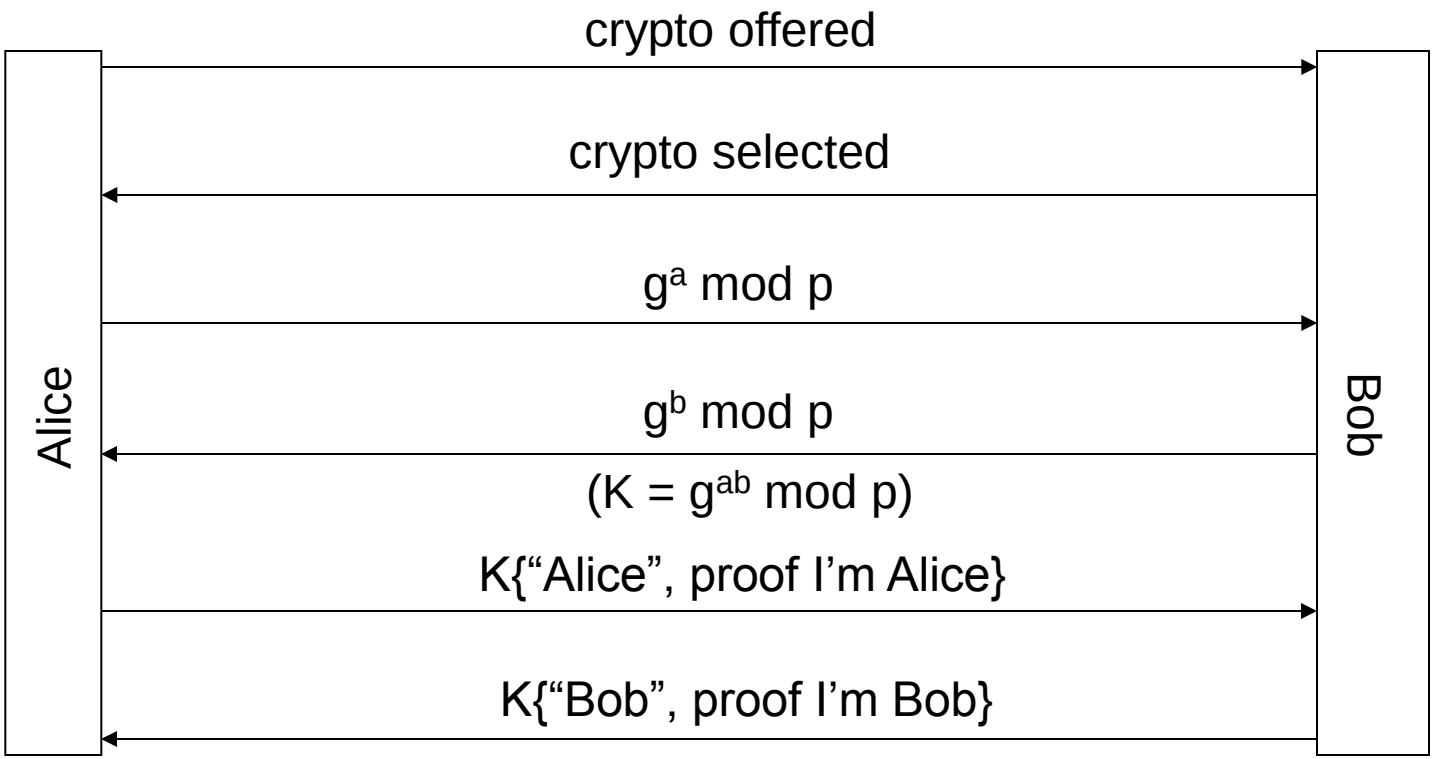
- Main mode: 6 rounds; provides identity hiding
- Aggressive mode: 3 rounds

Types of authentication:

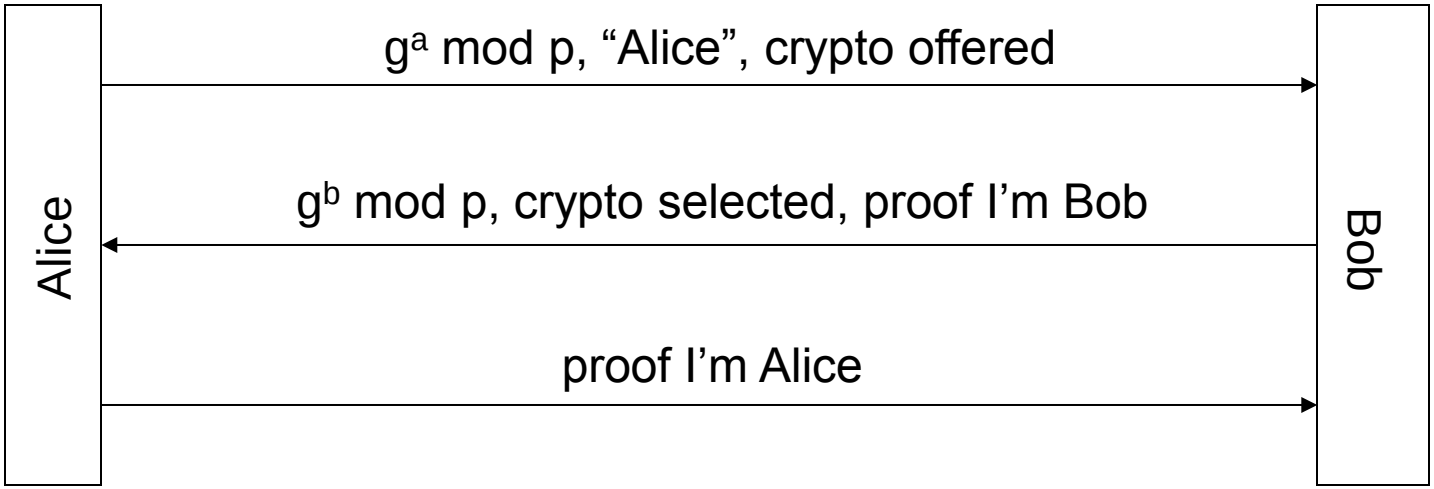
- MAC with pre-shared secret key
- digital signatures
- public key encryption
  - original: all public key encryption
  - revised: public + secret key encryption

(Each type has its benefits; but is it worth the complexity?)

Phase 1 – Main Mode (generic)



Phase 1 – Aggressive Mode (generic)



Phase 1 Issues & Problems

Crypto parameters:

Alice presents all algorithm combinations she can support

(may be too many combinations)

Authentication:

- certain fields (why not all?!) of the protocol messages are hashed & signed/encrypted in the final rounds
- not included: Bob's accepted parameters (problematic)

Cookies & Statelessness:

- Cookie protection: similar to Photuris cookies
- Bob is no longer stateless (problematic) since "crypto offered" must be remembered from message 1.

Phase 1 Issues (cont'd)

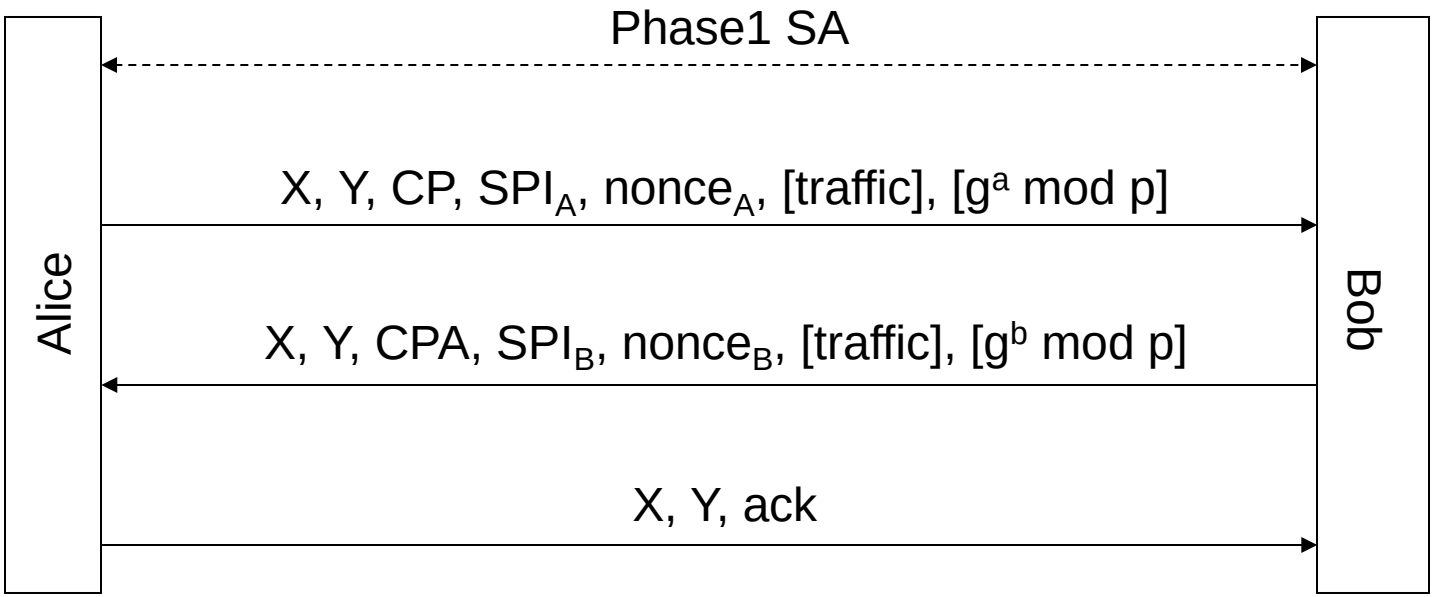
Complexity:

- 8 different protocols are defined (2 modes, each with 4 types of authentication)
- Unnecessarily flexible and complex

Phase 2 Exchange

- Establishes IPsec SA & session key
- Runs over the IKE SA established in Phase 1. (message are encrypted/authenticated with Phase 1 keys)
- Key generation: based on Phase 1 key, SPI, nonces.
- DH exchange: Optional (for PFS).
- IPsec Traffic Selector: Established optionally. Specifies what traffic is acceptable. (e.g., What port numbers are allowed to use this SA.)

Phase 2



- X: pair of cookies generated in Phase 1
- Y: session identifier
- traffic: IPsec traffic selector (optional)

IKEv2 Protocol

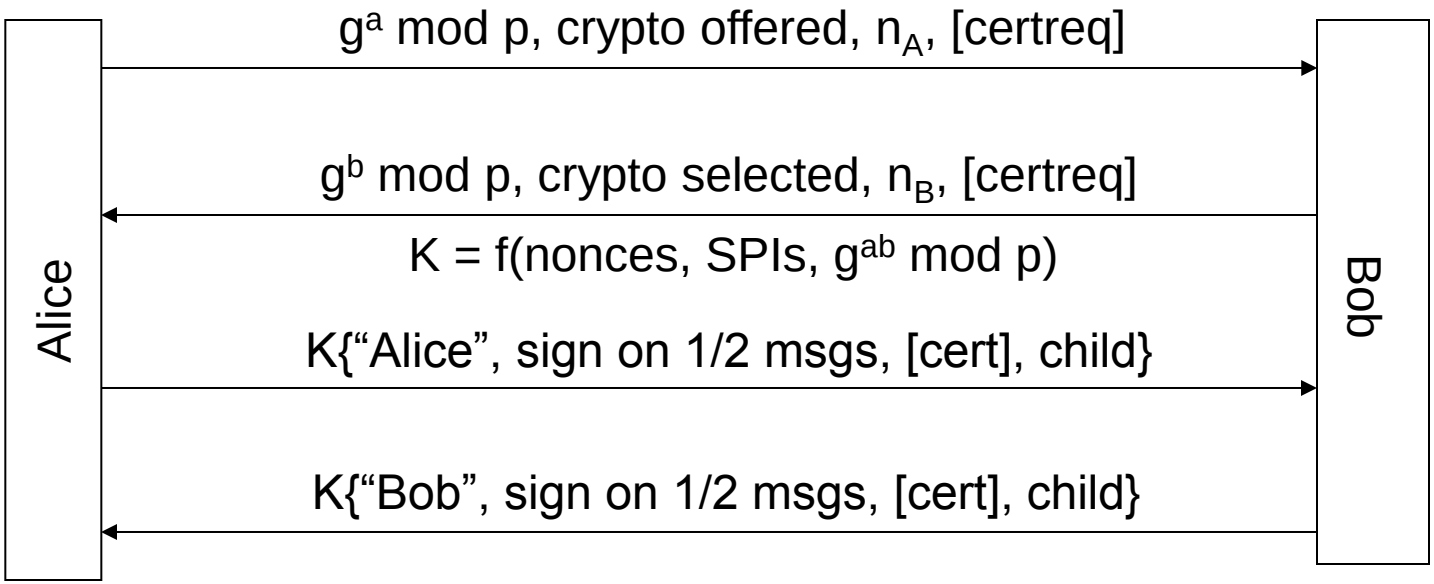
Initiated by Perlman & Kaufman, with the aims of

- simplifying IKEv1
- fixing the bugs
- fixing the ambiguities
- while remaining as close to IKEv1 as possible. (“no gratuitous changes”)

IKEv2 – Main Features

- Modes of authentication, only by
  - public key signatures
  - pre-shared keys (PSK)
- IKE SA + IPsec SA are established in the same protocol, in 4 messages. (~ Phase 1)
- Additional child SAs, only if needed (~ Phase 2)
- DoS protection optional, via cookies (stateless).
- Crypto negotiation is simplified
  - support for “suites”
  - “any of these enc., with any of these hash...”

IKEv2 – The Exchange Protocol

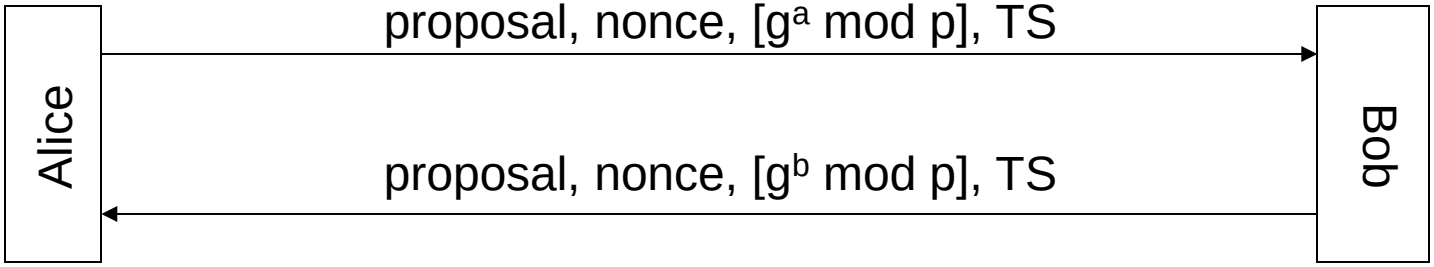


- Bob can optionally refuse the first message and require return of a cookie.
- Adds extra 2 messages.

IKEv2 – The Exchange Protocol (cont'd)

- DoS protection: Optional; by Bob responding the first message with a (stateless) cookie.
- Originally, designed with 3 rounds. Later 4 rounds is agreed on:
  - Initiator needs a 4th message anyway to know when to start the transmission.
  - Extra msgs for cookie exchange can be incorporated into 4 msgs, if Alice repeats msg.1 info in msg.3
- Preserves identity hiding from passive attackers.

IKEv2 – Child SA Creation



- proposal: crypto suites, SPI, protocol (ESP, AH, IP compression)
- TS: Traffic selector
- Derived keys: Function of IKE keying material, nonces of this exchange, plus optional DH output.

Other IKEv2 Features

Reliability:

- All messages are request/response.
- Initiator is responsible for retransmission if it doesn't receive a response.

Traffic selector negotiation:

- IKEv1: Responder can just say yes/no.
- IKEv2: Negotiation ability added.

Rekeying:

- Either side can rekey at any time.
- Rekeyed IKE-SA inherits all the child-SAs.