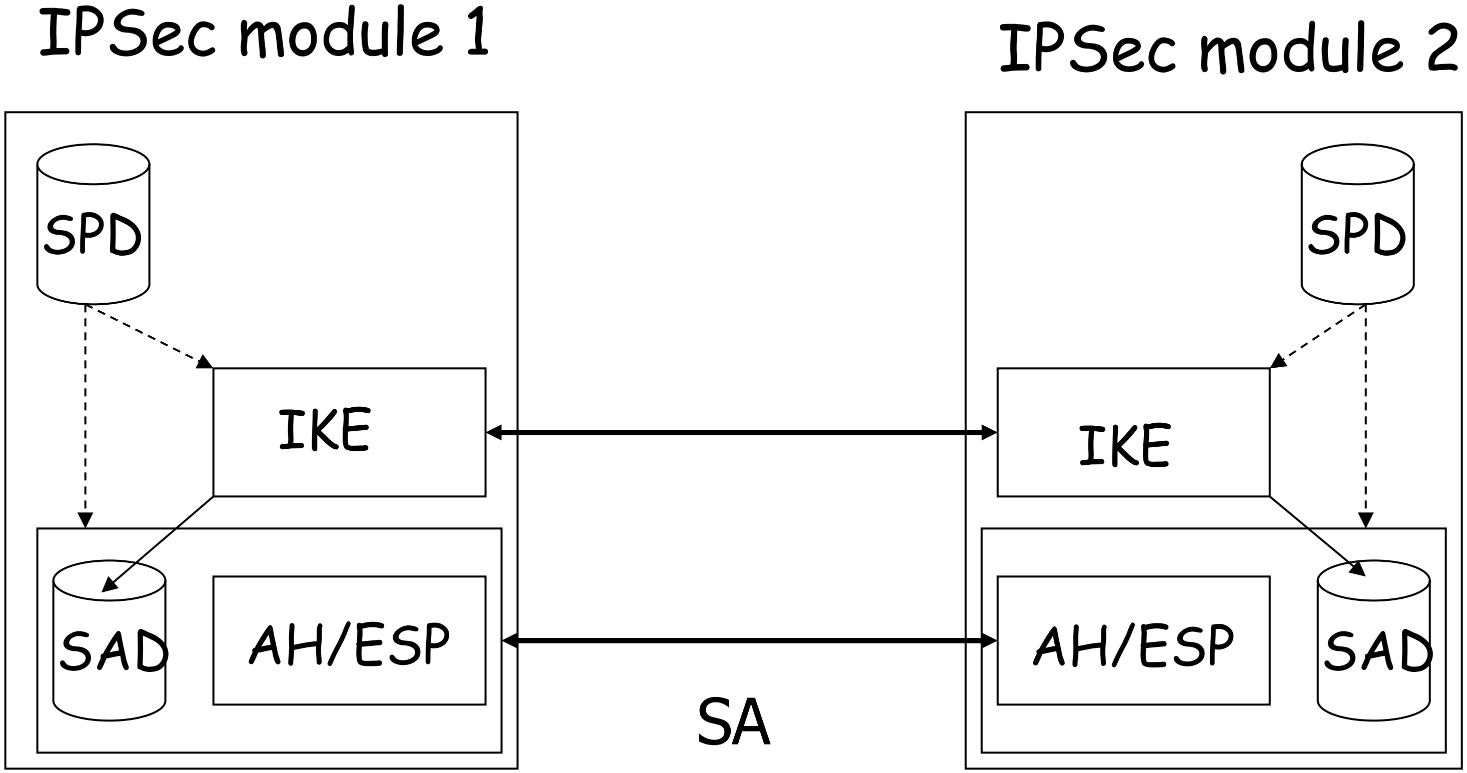
IKEv2: IPSec Key Management Protocol

Lecture 20

Acknowledgement: Slides from Vincent Luk, revised by Cunsheng Ding

IP Security Architecture



SAD: Security Association Database

IKE: Internet Key Exchange

SPD: Security Policy Database

Outline

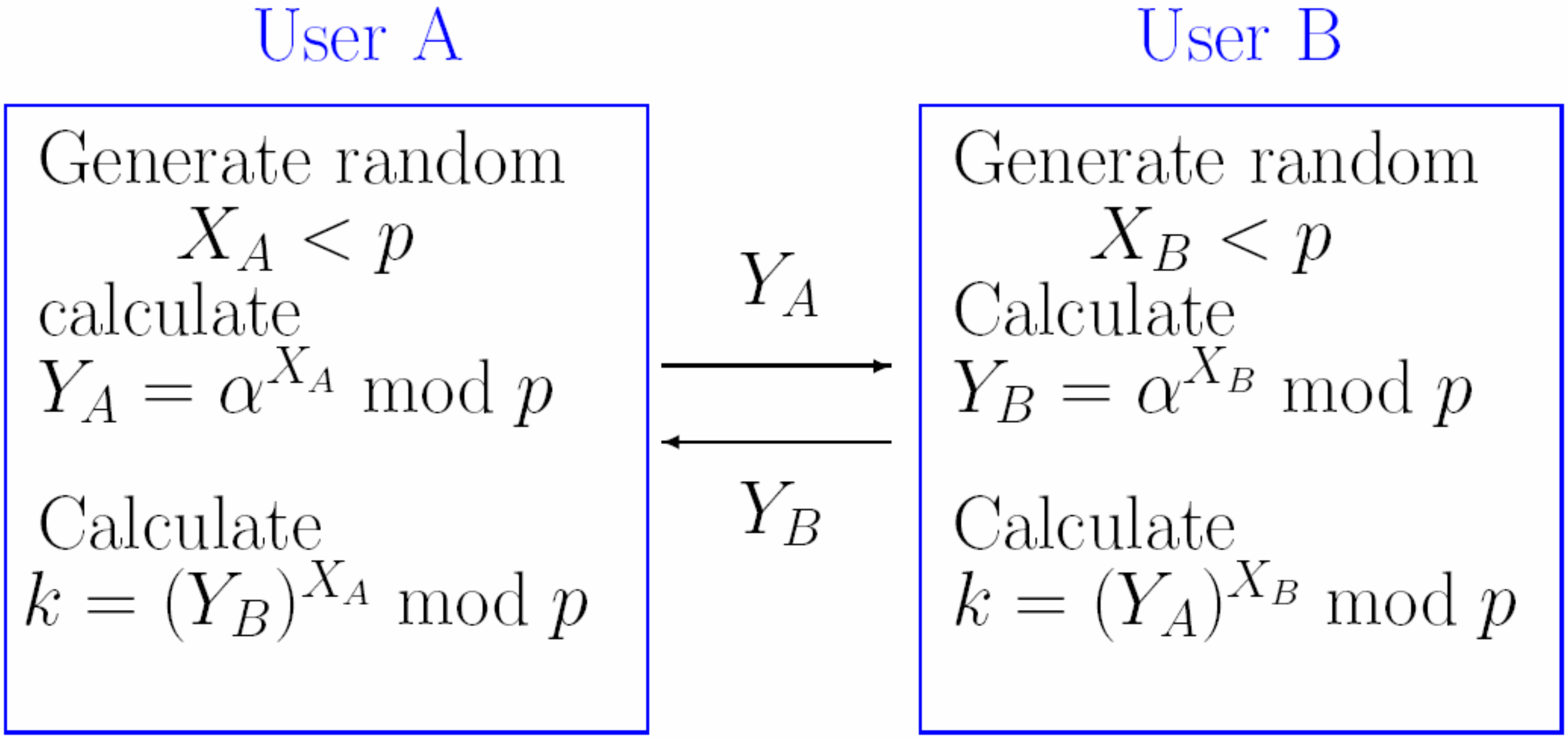
- Motivations of Automated Key Management
- Key Concepts
  - Diffie-Hellman Key Exchange Protocol
  - Perfect Forward Secrecy
  - Pseudo-Random Function (PRF)
- IKEv2
  - Authentication and Key Generation
  - Cryptographic Algorithm Negotiation
  - Re-keying
- Some Comments on IKEv2

Why Automated Key Management?

- Have to configure keys used in AH & ESP.
- Manual Techniques
  - Simplest
  - Practical in small and static environment
  - Human intervention, mis-configurations easily
  - Do not scale well
  - Static key not good for security

Revision: Any problem about DH?

Diffie-Hellman Key Exchange Protocol



User A

Generate random
$X_A < p$
calculate
$Y_A = \alpha^{X_A} \bmod p$

Calculate
$k = (Y_B)^{X_A} \bmod p$

$\xrightarrow{Y_A}$

$\xleftarrow[Y_B]{}$

User B

Generate random
$X_B < p$
Calculate
$Y_B = \alpha^{X_B} \bmod p$

Calculate
$k = (Y_A)^{X_B} \bmod p$

Diffie-Hellman in Practice

- Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
  - 768-bit modulus and primitive root 2.
  - 1024-bit modulus and primitive root 2.
  - Two elliptic curve DH parameters (details omitted here)
  - 1536-bit MODP Group
  - 2048-bit MODP Group
  - 3072-bit MODP Group
  - 4096-bit MODP Group
  - 6144-bit MODP Group
  - 8192-bit MODP Group

Perfect Forward Secrecy (PFS)

- Refers to the notion that the compromise of a single session key will not compromise other session keys.
- Any key should not be derived from any predecessor key

Pseudo-Random Function (PRF)

- PRF function takes a variable length key, variable length data, and produces a fixed length output
  - e.g., slightly modified HMAC
- For generating keying material and the authentication of IKE
- In RFC4307: Recommended PRF

PRF_HMAC_SHA1	MUST	RFC2104
PRF_HMAC_MD5	MAY	RFC2104
PRF_AES128_CBC	SHOULD+	AES-PRF

- Technical details of these PRFs are omitted here.

PRF+

prf+ (K,S) = T1 , T2 , T3 , T4 , ...

where:

T1 = prf (K, S | 0x01)

T2 = prf (K, T1 | S | 0x02)

T3 = prf (K, T2 | S | 0x03)

T4 = prf (K, T3 | S | 0x04)

...

where

| means concatenation

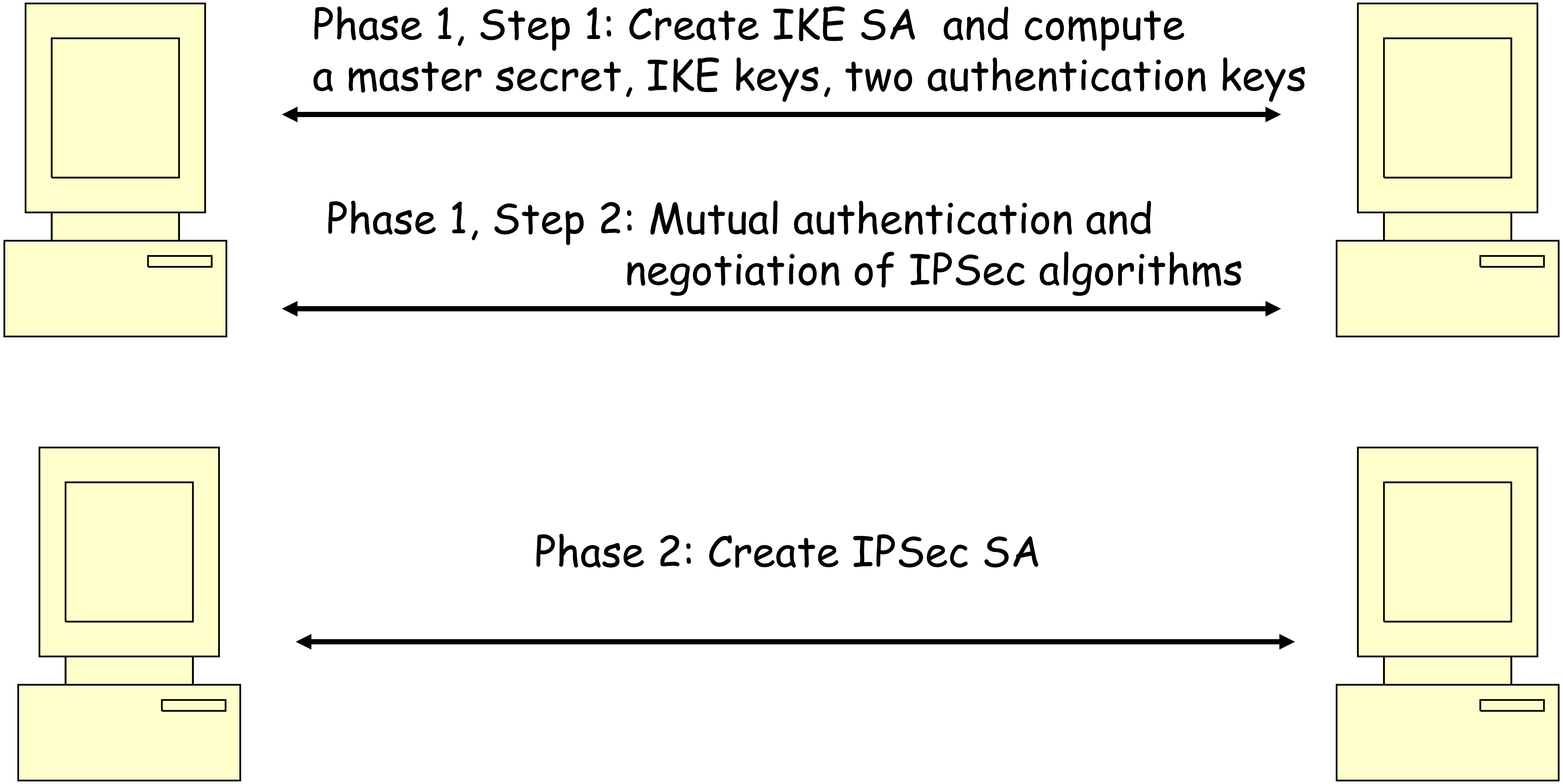
0x01 etc. are constants

A number of Ti's are computed iteratively as needed

Outline

- Motivations of Key Management
- Key Concepts
  - Diffie-Hellman Key Exchange Protocol
  - Perfect Forward Secrecy
- IKEv2
  - Authentication and Key Generation
  - Cryptographic Algorithm Negotiation
  - Re-keying
- Some Comments on IKEv2

IKEv2 Outline



Phase 1, Step 1: Create IKE SA and compute a master secret, IKE keys, two authentication keys

Phase 1, Step 2: Mutual authentication and negotiation of IPSec algorithms

Phase 2: Create IPSec SA

IKEv2 Protocol

Phase 1, Step 1: IKE_SA_INIT

- Negotiate IKE algorithms (Ciphers, Hash algorithms, DH group)
- Compute four secret keys for IKE
- Compute master secret k_d for computing IPSec keys in Phase 2.
- Compute two mutual authentication keys for Step 2 of Phase 1 below.

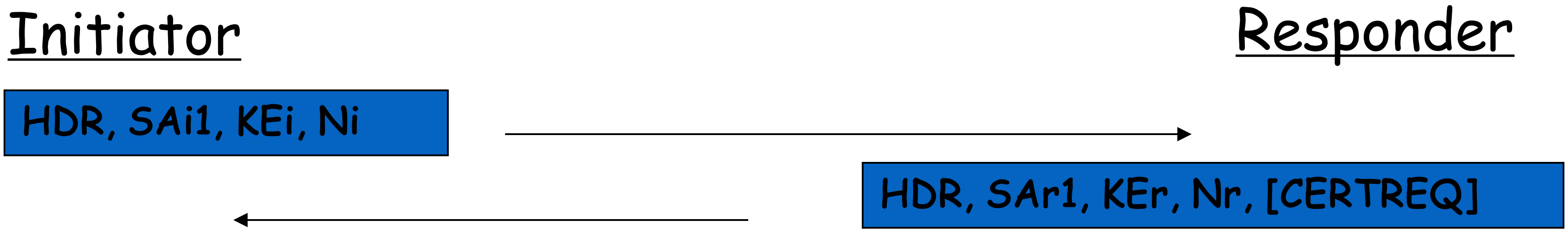
Phase 1, Step 2: IKE_AUTH

- Mutual authentications (two choices)
- Negotiation of IPsec algorithms (piggybacked here)

Phase 2: CREATE_CHILD_SA

- Setup IPSec security associations

Phase 1.1: IKE_SA_INIT (1)



Initiator

Responder

HDR, SAi1, KEi, Ni

HDR, SAr1, KEr, Nr, [CERTREQ]

- HDR (IKE header)
  - Version number
  - SPIi: A value chosen by the initiator to identify this IKE security association.
  - ……
- SAi1
  - Supported Crypto algms of initiator for the IKE_SA (DH group, encrpt, authen algor for protecting the messages in Phase 1.2 and Phase 2, prf)
- KEx
  - Diffie-Hellman Values

- Nx
  - Nonce of Init./Responder
  - Used for authentication & computing secret keys
- SAr1
  - Expressed the choice based on SAi1
- [CERTREQ]
  - Optional request that decides a mutual authentication method

Phase 1.1: IKE_SA_INIT (2)

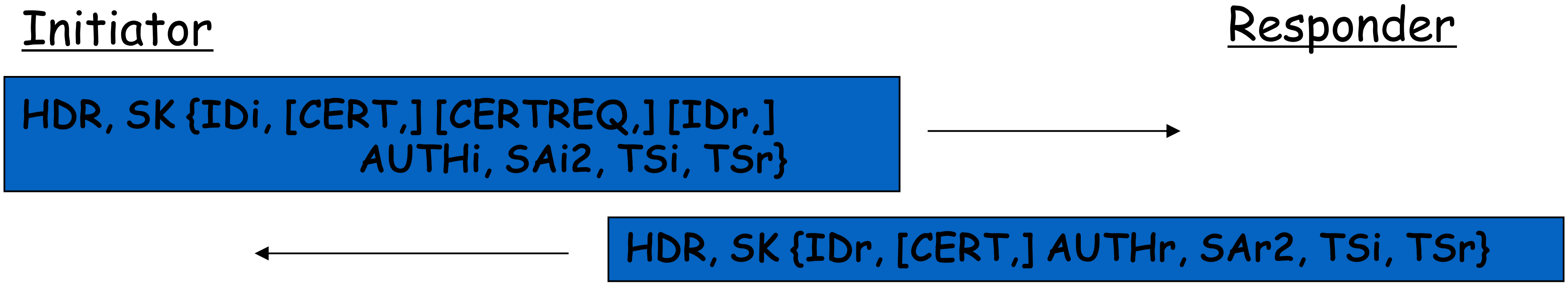
- After exchanging two messages, each party can generate SKEYSEED based on the values in KEi and KEr by DH
  - SKEYSEED=prf(Ni | Nr, g^(s_is_r)) [Remark: s_i the secret of I]

    Nonces add the freshness to the key materials.
  - {SK_d | SK_ai | SK_ar | SK_ei | SK_er | SK_pi | SK_pr} =

    prf+ (SKEYSEED, Ni | Nr | SPIi | SPIr)

    The prefix of output of the function prf+ is cut into pieces as different keys
- SK_d is the master secret that will be used to compute IPSec SA keys later in Phase 2.
- Messages in Phase 1.2 and Phase 2 will be encrypted and integrity protected by SK_ai, SK_ei, SK_ar, SK_er respect.
- SK_pi and SK_pr are pre-shared secret keys for authentication in Phase 1.2 (technical details of this authentication method are given later).

Phase 1.2: IKE_AUTH (1)



Initiator

Responder

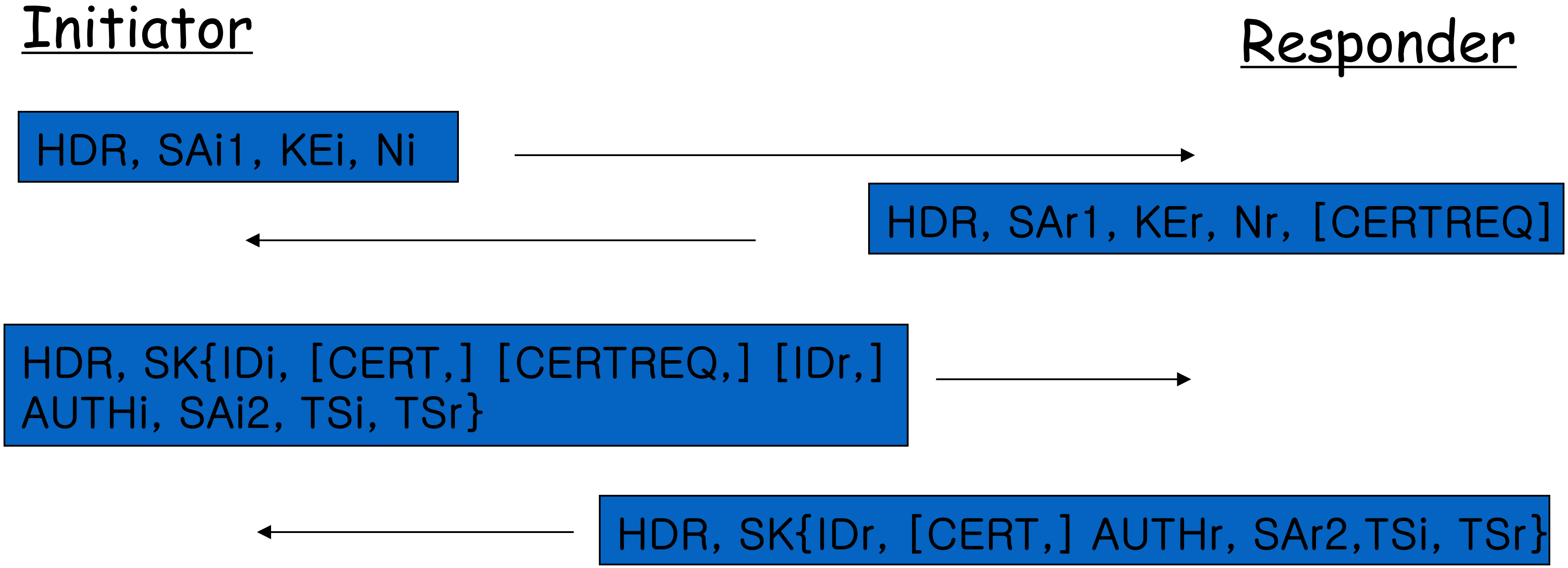
HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTHi, SAi2, TSi, TSr}

HDR, SK {IDr, [CERT,] AUTHr, SAr2, TSi, TSr}

- {...}
  - indicated payloads are encrypted and integrity protected using that direction's SK_e & SK_a and the IKE encryption and auth algorithms
- IDi, IDr
  - For authentication by preshared secrets (SK_pi, SK_pr) (details given later)
- AUTHx
  - Preshared secrets (SK_pi, SK_pr) (details given later)
  - Digital signature (details given later)

- SAi2/SAr2 piggybacked here
  - For CREATE_CHILD_SA
  - They contain only algorithms
- TSx
  - Traffic Selector Info (IP Add + Port)
  - It defines which traffic to be protected by SAi2, SAr2
  - It contains protocol, port range, address range
  - TSi = (0, 0-65535,192.0.2.202-192.0.2.202)
  - TSr = (0, 0-65535,192.0.2.0-192.0.2.255)

The Whole Picture of Phase 1



Initiator

Responder

HDR, SAi1, KEi, Ni

HDR, SAr1, KEr, Nr, [CERTREQ]

HDR, SK{IDi, [CERT,] [CERTREQ,] [IDr,] AUTHi, SAi2, TSi, TSr}

HDR, SK{IDr, [CERT,] AUTHr, SAr2,TSi, TSr}

Remark 1: [CERTREQ] means authentication with digital certificate.
Remark 2: "SK{}" means encryption using the keys sk_{ei} and sk_{er} .
Remark 2: SAi2 and SAr2 are negotiations of IPSec SA algorithms, piggybacked
in this authentication step.

Mutual Authent. by AUTH (2)

- Digital Signature Based
  - Requires individual [CERT] exist in both messages
  - [CERTREQ] indicates to use certificate authentication
  - Initiator signs the 1st message appended by Nr and prf(SK_pi, IDi)
  - responder signs the 2nd message appended by Ni and prf(SK_pr, IDr)
- Pre-shared Key (SK_pi, SK_pr)
  - HMAC using negotiated prf function
  - AUTHx = prf(prf(Shared Secret, "Key Pad for IKEv2"), <InitiatorSignedOctets> or <ResponderSignedOctets>)
  - "InitiatorSignedOctets" invoves: 1st message in Phase 1.1, Nr, IDi, prf(SK_pi, IDi)
  - "ResponderSignedOctets" is similar.

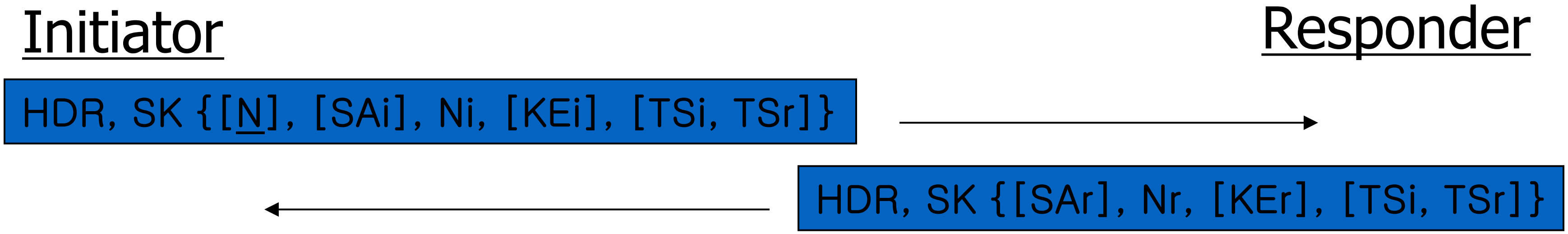
CHILD_SA Negotiations in IKE_AUTH

- Establishment of CHILD_SA is piggybacked in IKE_AUTH

- Initiator proposes SAi2 in message 3
- Responder answers SAr2 in message 4

- Traffic protected by the SA is also negotiated through traffic selectors (TSi, TSr)

Phase 2: CREATE_CHILD_SA



Initiator

Responder

HDR, SK {[N], [SAi], Ni, [KEi], [TSi, TSr]}

HDR, SK {[SAr], Nr, [KEr], [TSi, TSr]}

- [N]: Indication negotiation of new IPSec SA
- [KEx]
  - Diffie-Hellman value, different from those in Phase 1.1
  - Used only when PFS is required. In this case, they will be used in computing new IPSec keys
- [TSx]
  - Traffic Selector Negotiations for new IPSec SA
  - Used only when [N] is used
- If [N] is not used, this is the 1st IPSec SA creation under this IKE SA
- The protection SK{} here is by the IKE SA negotiated before.
- Ni and Nr should be different from those in Phase 1.1. They and SK_d are used to compute IPSec secretr keys.

- An established IKE SA may be used to create many IPSec SAs and may be used for a long time.
- A set of IPSec algorithms was already negotiated in Phase 1.2. However, if a new IPSec SA should be created, then [N] is used to indicate this. At the same time, new [KEi] and [TSi, TSr] (different from those in Phase 1.2) may be negotiated.
- The Ni and Nr here are different from those in Phase 1.1, and will be used to compute IPSec secret keys.

Finally, Keys for AH or ESP

- After CREATE_CHILD_SA, the key(s) for AH or ESP will be generated!
- KEYMAT = prf+(SK_d, Ni | Nr)
  - Ni and Nr are the new nonces in Phase 2
  - They are independent of the two nonces in Phase 1
  - KEYMAT is cut into pieces as AH and/or ESP keys
- For stronger PFS
  - KEYMAT = prf+(SK_d, g^(s_i s_r) (new) | Ni | Nr) ,
  - Where g^s_i and g^s_r are the new DH values in Phase 2, SK_d is the old one Phase 1, Ni and Nr are new ones in Phase 2.
  - KEYMAT is cut into pieces as AH and/or ESP keys

Outline

- Motivations of Key Management
- Key Concepts
  - Diffie-Hellman Key Exchange Protocol
  - Perfect Forward Secrecy
  - Pseudo-Random Function (PRF)
- IKEv2
  - Authentication and Key Generation
  - Cryptographic Algorithm Negotiation
  - Re-keying
- Improvements over IKE (v1)
- Some Comments on IKEv2

Cryptographic Algorithm Negotiation

- "SA" payload consists of one or more proposals:
  - IPSec protocols: IKE, ESP, AH
  - Cryptographic algorithms associated with each protocol
  - A prf function may be included
- The responder answers this choice based on the proposals proposed by the Initiator

Re-keying

- Secret keys of IKE, ESP and AH should be only used in a limited amount of time.
- After SA lifetime expires, re-keying has to be done.
- Either side thinks that an SA has been used for enough time, it negotiates a new SA.
- After the new SA is setup, delete the old one.

Outline

- Motivations of Key Management
- Key Concepts
  - Diffie-Hellman Key Exchange Protocol
  - Perfect Forward Secrecy
- IKEv2
  - Authentication and Key Generation
  - Cryptographic Algorithm Negotiation
  - Re-keying
- Comments about IKEv2

Some Comments on IKEv2

- It's debatable to keep the Phase I & II architecture
- Still over-flexible in terms of
  - Optional choice of PFS in CREATE_CHILD_SA
- A revised version of IKEv2 was leased in 2014 and is available in: https://tools.ietf.org/html/rfc7296
  - It is now a standard.
- A "minimal" version of March 2016 can be found in:

https://datatracker.ietf.org/doc/rfc7815/

References

- Bellovin, S., “COMS W4180 Session 11 IP Sec” http://www.cs.columbia.edu/~smb/classes/f06/l10.pdf
- Lee, Kyesang., “Internet Key Exchange version 2 (IKEv2) protocol”, http://seclab.cs.ucdavis.edu/-seminars/IKEv2.ppt
- Paterson, K., “A Cryptographic Tour of the IPsec Standards”, http://eprint.iacr.org/2006/097.pdf
- Perlman, R., Kaufman, C., “Key exchange in IPSec: analysis of IKE”, IEEE Internet Computing, Vol. 4 Issue: 6, Nov.-Dec. 2000, pp. 50 –56.
- Harkins, Kaufman, Kivinen, Kent, Perlman, “Design Rationale for IKEv2”, www3.ietf.org/proceedings/02jul/I-D/draft-ietf-ipsec-ikev2-rationale-00.txt