```
Aug 16 09:20:07.561: ISAKMP: (0):processing KE payload. message ID = 0
Aug 16 09:20:07.561: ISAKMP: (0):processing NONCE payload. message ID =
Aug 16 09:20:07.563: %CRYPTO-6-IKMP_CRYPT_FAILURE: IKE (connection id 0
to decrypt (w/RSA private key) packet
Aug 16 09:20:07.564: ISAKMP: (0):Input = IKE_MESG_INTERNAL, IKE_PROCESS
E
Aug 16 09:20:07.564: ISAKMP: (0):Old State = IKE_R_MM3  New State = IKE

Aug 16 09:20:07.564: ISAKMP: (0):: incrementing error counter on sa, attempt 1 o
f 5: reset_retransmission
Aug 16 09:20:07.564: ISAKMP: (0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_ERROR
Aug 16 09:20:07.564: ISAKMP: (0):Old State = IKE_R_MM3  New State = IKE_R_MM2

Aug 16 09:20:07.847: ISAKMP: (0):purging SA., sa=7F5BCC501070, delme=7F5BCC50107
0
Aug 16 09:20:08.565: ISAKMP: (0):retransmitting phase 1 MM_SA_SETUP...
                            incrementing error counter on sa, attempt 2 o
```

RUB

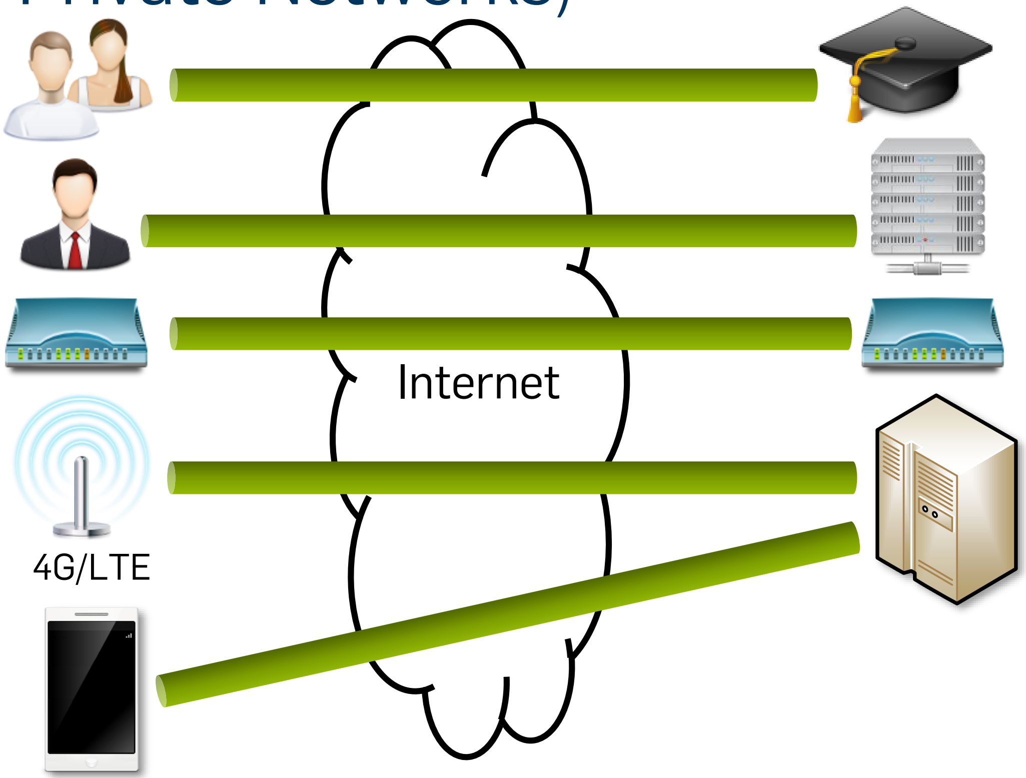
THE DANGERS OF KEY REUSE: PRACTICAL ATTACKS ON IPSEC IKE

Dennis Felsch [1], Martin Grothe [1], Jörg Schwenk [1], Adam Czubak [2], Marcin Szymanek [2]

[1]: Ruhr University Bochum, Germany [2]: University of Opole, Poland

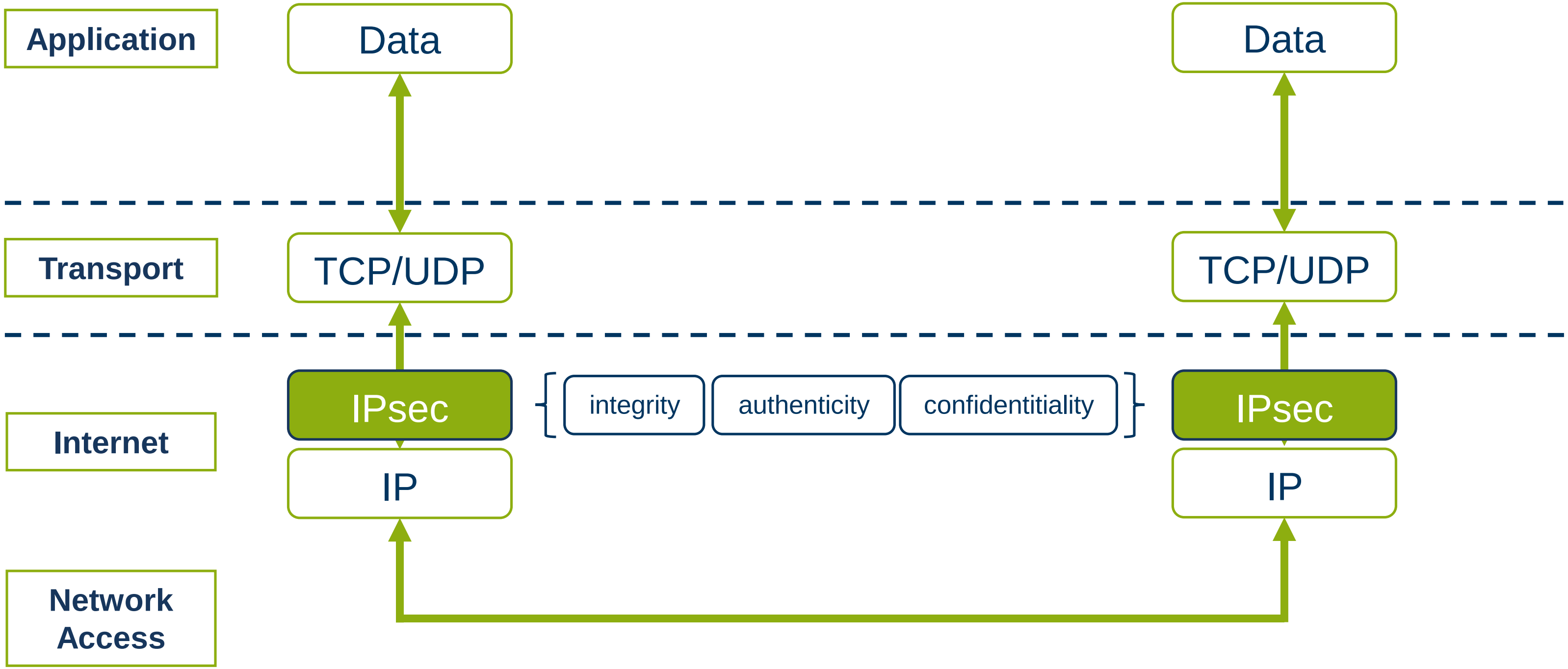
27TH USENIX SECURITY SYMPOSIUM 08/16/2018

VPNs (Virtual Private Networks)



Icons from KDE Oxygen theme licensed under GNU LGPLv3, http://www.kde.org/

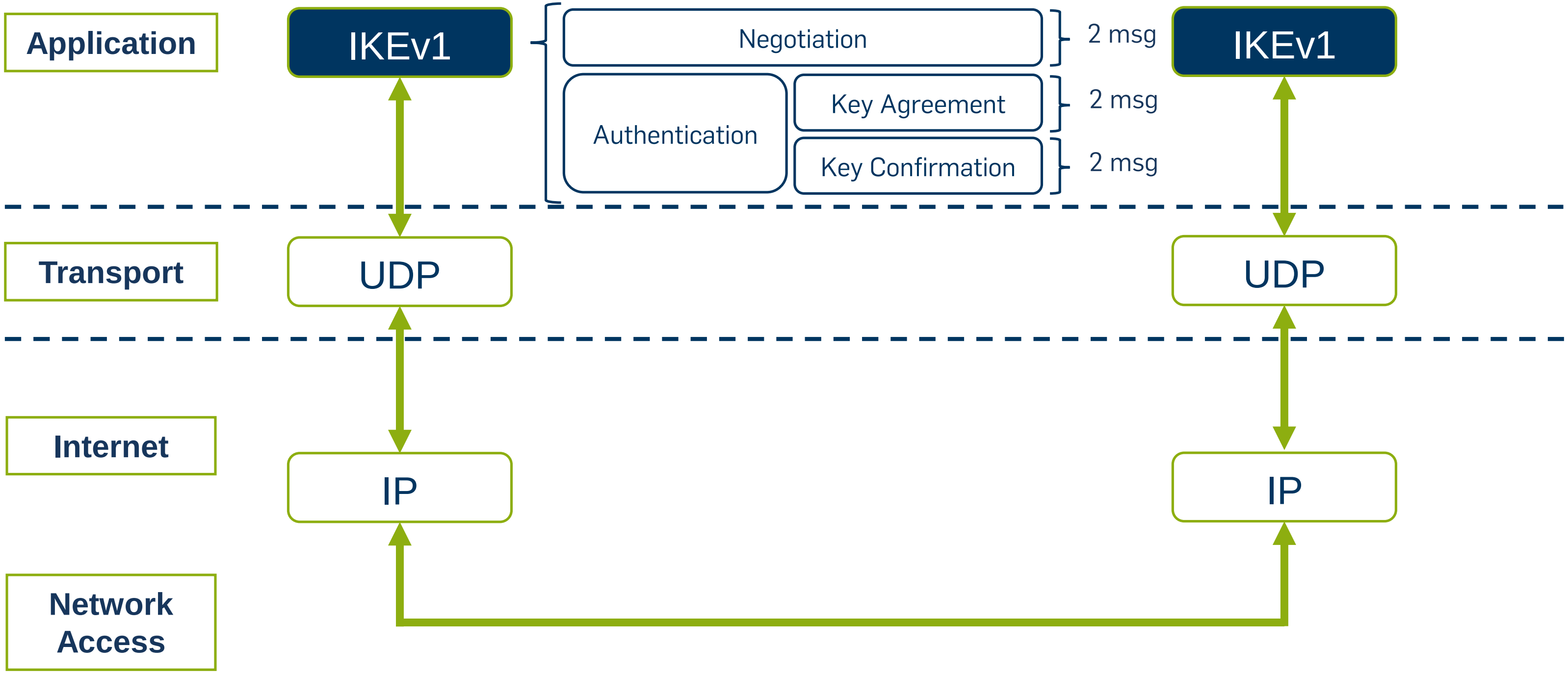
IPsec (Internet Protocol Security)



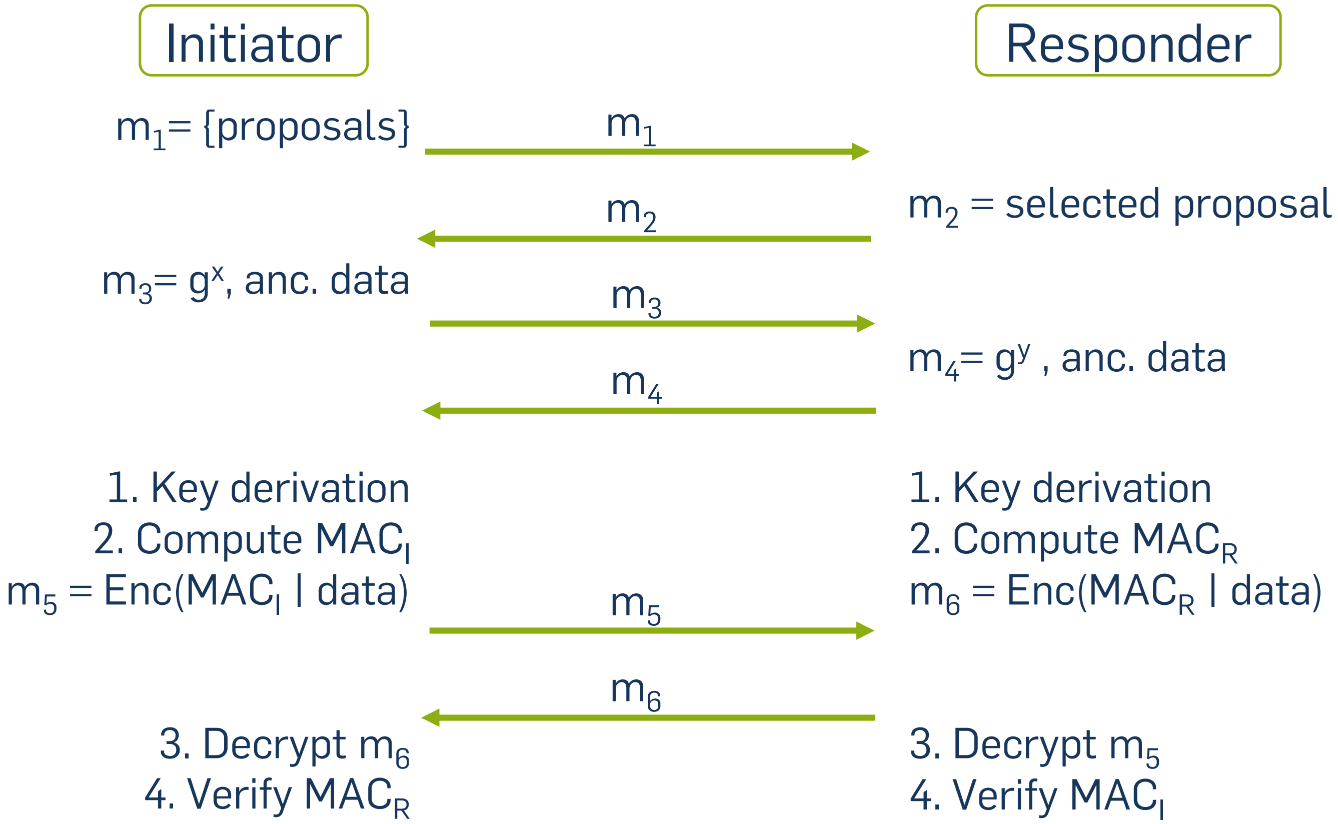
IKE (Internet Key Exchange)

- The handshake protocol of IPsec
- Standardized in two major versions
  - IKEv1: Published in 1998, declared obsolete by the IETF
    - nevertheless included in all implementations
  - IKEv2: Published in 2005, current version

IKEv1


Application
IKEv1
Negotiation
2 msg
IKEv1
Authentication
Key Agreement
2 msg
Key Confirmation
2 msg
Transport
UDP
UDP
Internet
IP
IP
Network Access

IKEv1 Protocol Flow



Initiator

Responder

m_1= {proposals}

m_1

m_2

m_2 = selected proposal

m_3= g^x, anc. data

m_3

m_4= g^y , anc. data

m_4

1. Key derivation
2. Compute MAC_I

m_5 = Enc(MAC_I | data)

1. Key derivation
2. Compute MAC_R

m_6 = Enc(MAC_R | data)

m_5

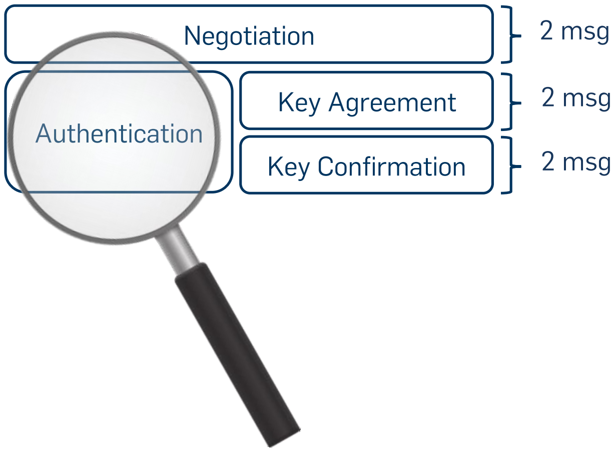
m_6

3. Decrypt m_6
4. Verify MAC_R

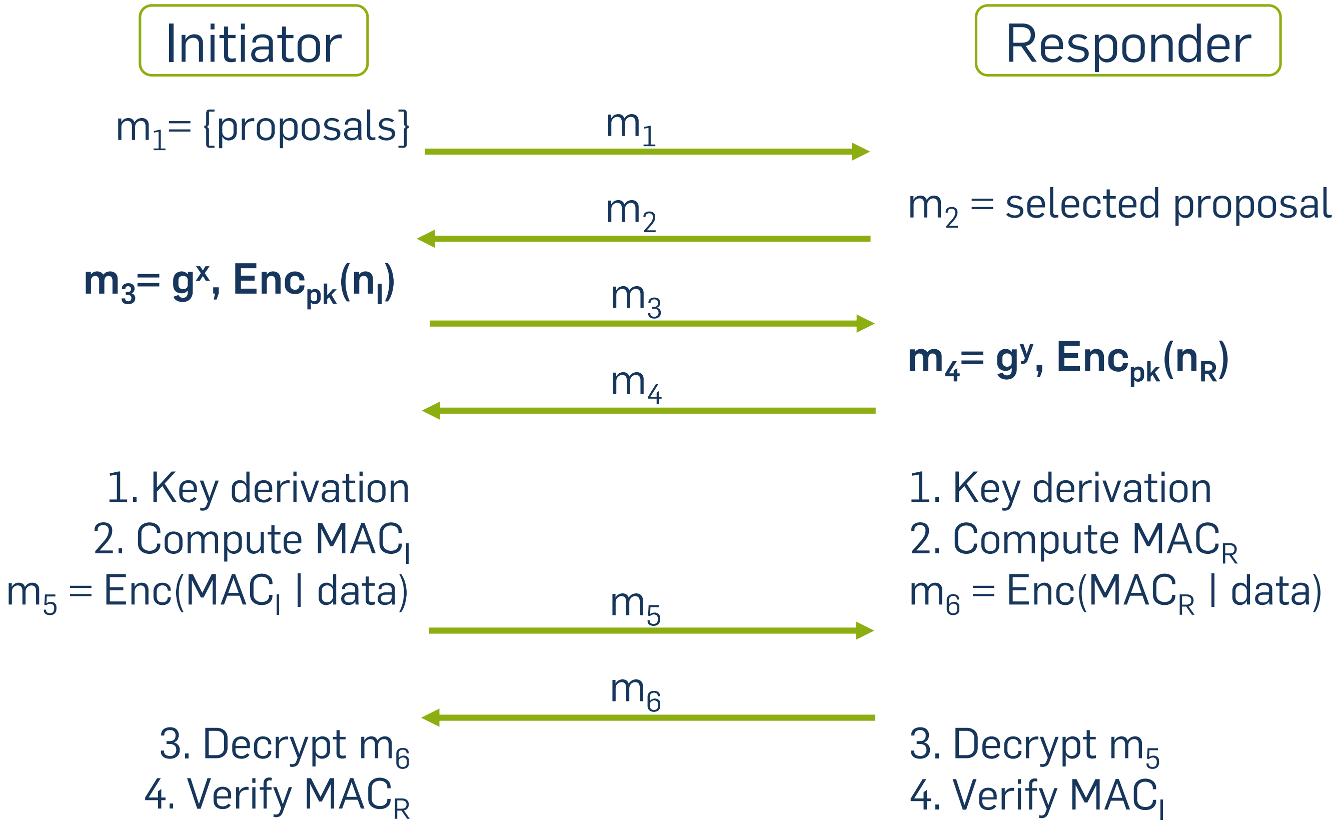
3. Decrypt m_5
4. Verify MAC_I

IKEv1 Authentication Methods

1. PSK (Pre-Shared-Key)
2. Digital Signatures
3. Public Key Encryption (PKE)
4. Revised Public Key Encryption (RPKE)



IKEv1 Protocol Flow With PKE Authentication



Initiator

Responder

m_1= {proposals}

m_1

m_2

m_2 = selected proposal

$\mathbf{m_3= g^x, Enc_{pk}(n_I)}$

m_3

$\mathbf{m_4= g^y, Enc_{pk}(n_R)}$

m_4

1. Key derivation
2. Compute MAC_I

m_5 = Enc(MAC_I | data)

1. Key derivation
2. Compute MAC_R

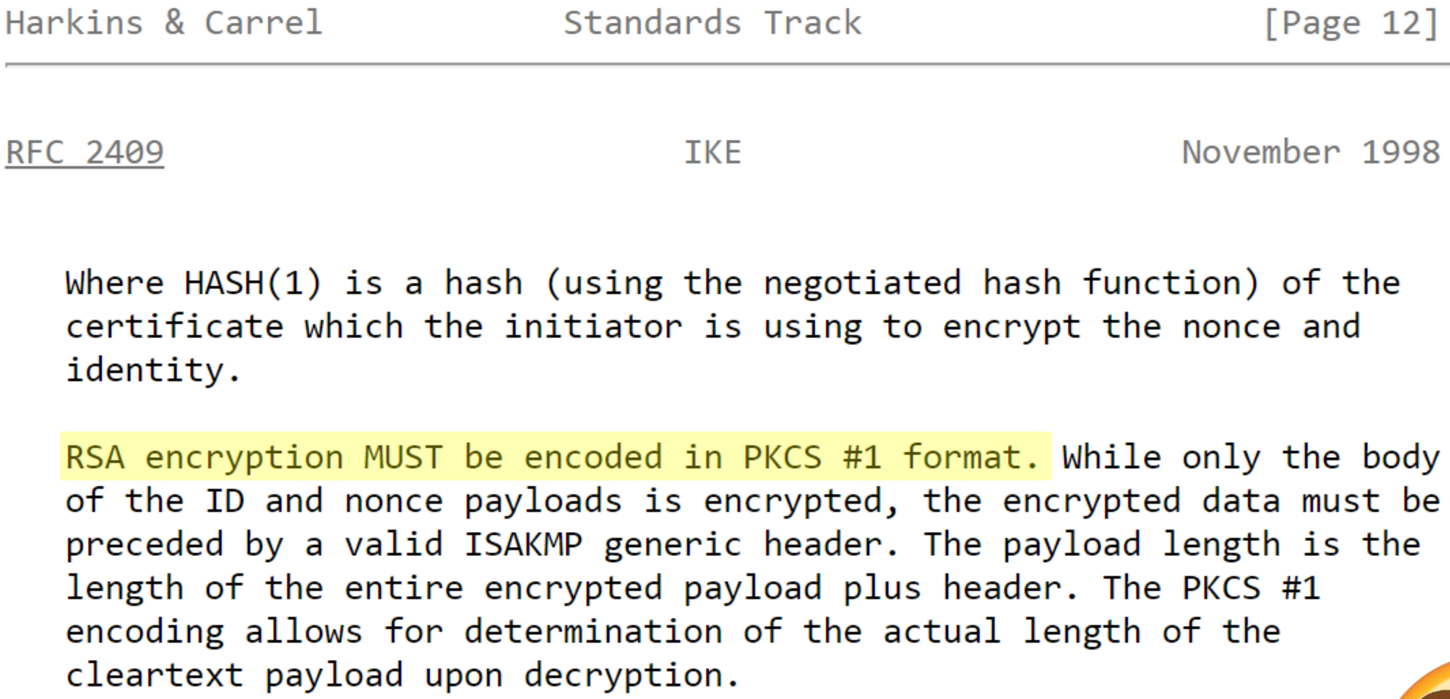
m_6 = Enc(MAC_R | data)

m_5

m_6

3. Decrypt m_6
4. Verify MAC_R

3. Decrypt m_5
4. Verify MAC_I



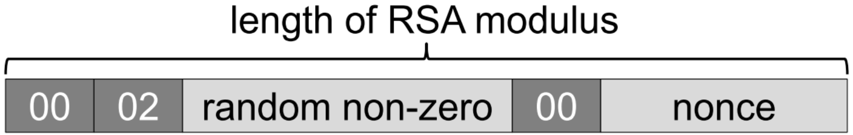
```
Harkins & Carrel            Standards Track                   [Page 12]

RFC 2409                          IKE                     November 1998


   Where HASH(1) is a hash (using the negotiated hash function) of the
   certificate which the initiator is using to encrypt the nonce and
   identity.

   RSA encryption MUST be encoded in PKCS #1 format. While only the body
   of the ID and nonce payloads is encrypted, the encrypted data must be
   preceded by a valid ISAKMP generic header. The payload length is the
   length of the entire encrypted payload plus header. The PKCS #1
   encoding allows for determination of the actual length of the
   cleartext payload upon decryption.
```

What if implementations contained Bleichenbacher oracles?

More Bleichenbacher:
Return Of Bleichenbacher's
Oracle Threat (ROBOT)
Pwnie Award winner
This afternoon, Track 2

Bleichenbacher's Attack In Two Slides

- Padding oracle attack
- RSA PKCS#1 v1.5 encryption padding:

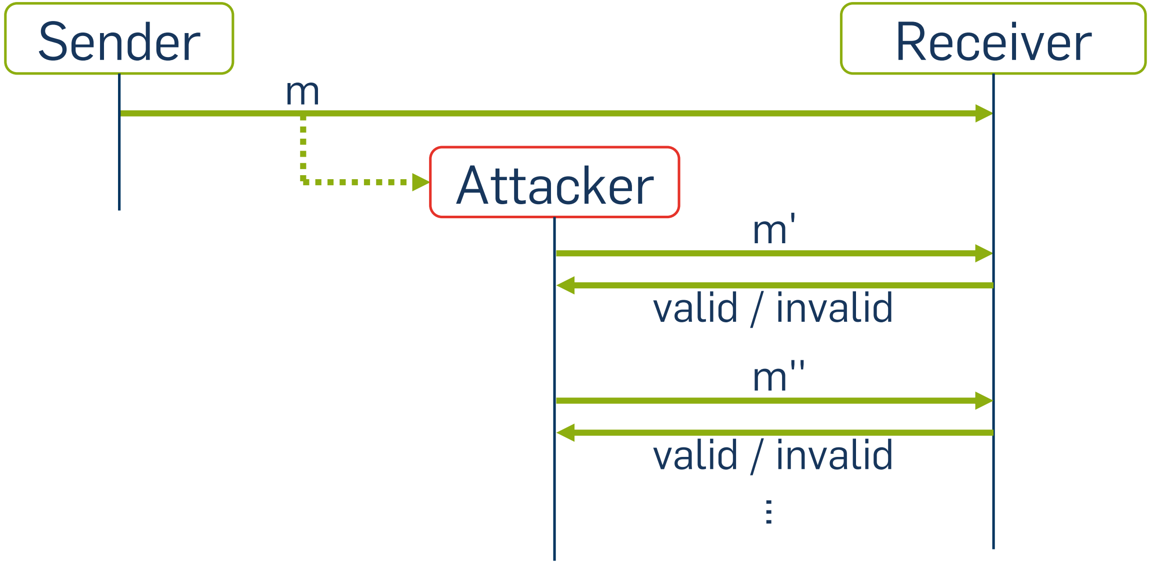


length of RSA modulus

00	02	random non-zero	00	nonce

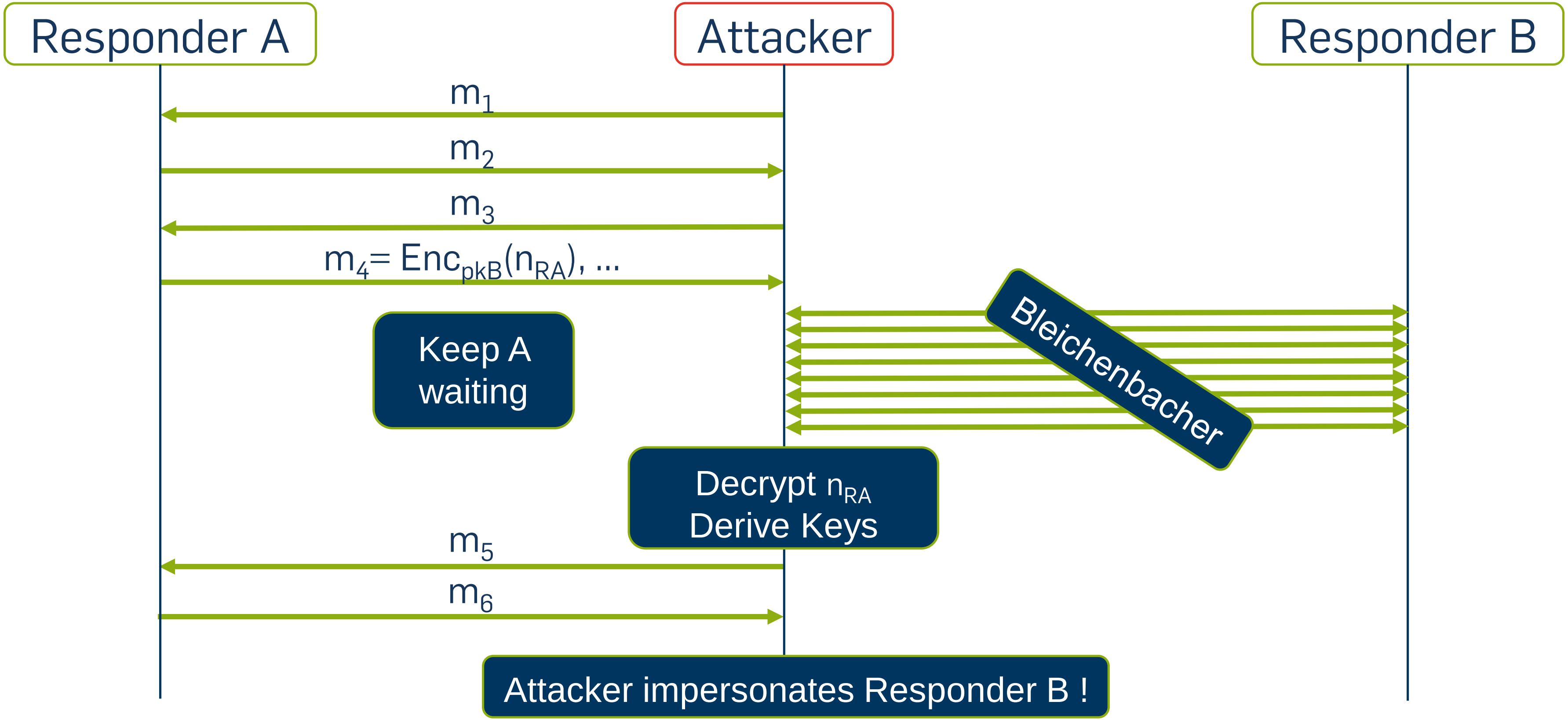
- Attack requires oracle that tells if padding is valid

Bleichenbacher‘s Attack In Two Slides



- Leaks the plaintext of message *m* to the attacker

Attack Idea On IKEv1 With PKE Authentication



Where To Find The PKE And RPKE Modes?

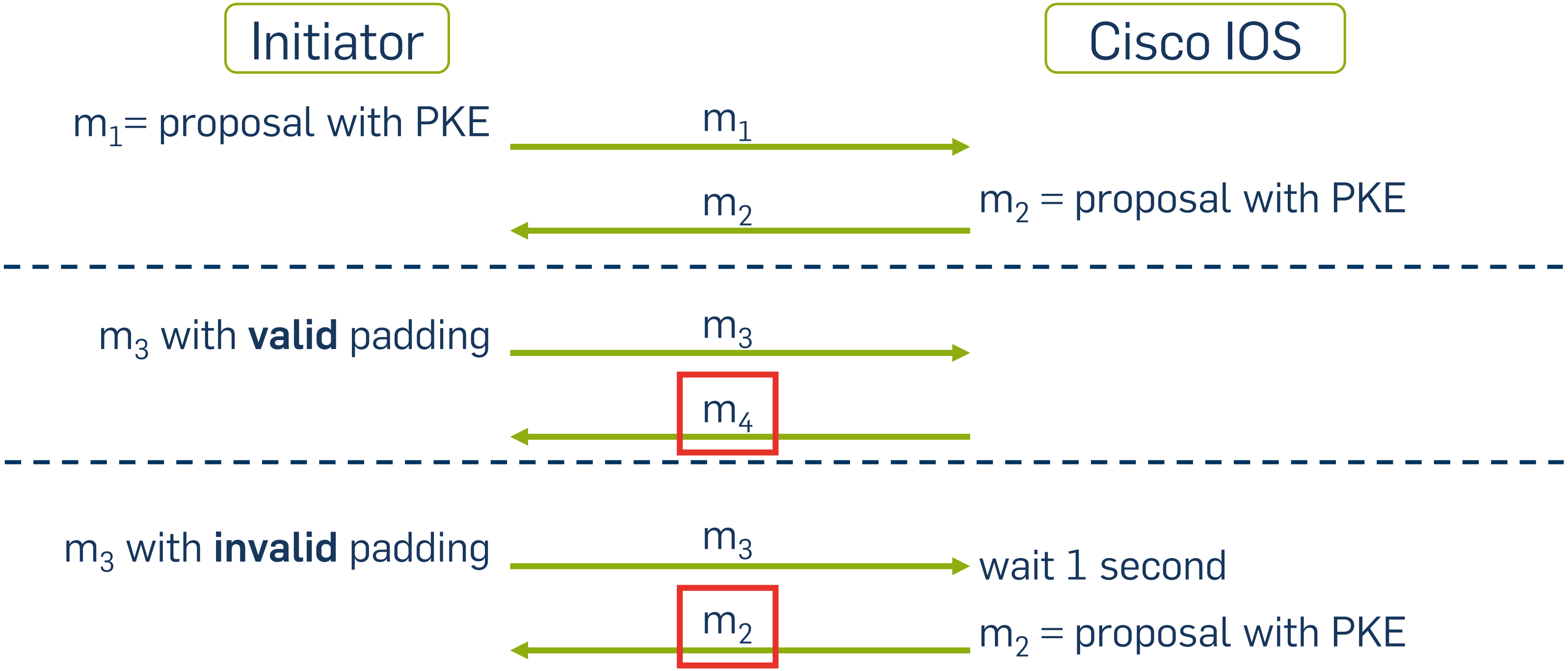
- Cisco includes PKE authentication in IOS
- Huawei includes RPKE in some security appliances
- Implementations in Clavister's cOS and ZyXEL's ZyWALL USG devices broken

Where To Find The PKE And RPKE Modes?

Case Study: Bleichenbacher Oracle In Cisco IOS 1/3

- Test device:
  - Cisco ASR 1001-X router
  - IOS XE 03.16.02.S

Case Study: Bleichenbacher Oracle In Cisco IOS 2/3



Initiator

Cisco IOS

m_1= proposal with PKE

m_1

m_2

m_2 = proposal with PKE

m_3 with **valid** padding

m_3

m_4

m_3 with **invalid** padding

m_3

wait 1 second

m_2

m_2 = proposal with PKE

Case Study: Bleichenbacher Oracle In Cisco IOS 3/3

- IOS cancels IKEv1 handshake after 60 seconds at the latest
- Public key 1024 bits ⇒ ~850 responses per second
- $60 \cdot 850 = 51{,}000$ requests per handshake

- Empirical study with a simulator:
  26 % of attacks require less than 51,000 requests

Cisco IOS – Simulator vs. Real Hardware

- Cisco's IKE handshake implementation is not optimized for throughput
- Cryptographic calculations for IKE are done by CPU
- m_1/m_2 negotiations take a lot of time

- Decryption attack with 19,000 requests took 13 minutes

Cisco IOS – Is An Attack Realistic?

- A too slow attack does not permanently lock out attackers
- Still dangerous if the victim has deployed multiple responders sharing one key pair
    - e. g. for load balancing

Bleichenbacher Oracles In (R)PKE Implementations

- Cisco: CVE-2018-0131
- Huawei: CVE-2017-17305
- Clavister: CVE-2018-8753
- ZyXEL: CVE-2018-9129

- Patches are available!

Key Reuse

- Maintaining individual key pairs for all variants of IKE?
- Common practice: A single RSA key pair
- Actual security depends on
  - cross-ciphersuite,
  - cross-version, and
  - cross-protocol security

Bleichenbacher's Attack & Signatures

- For RSA:
  - A decryption & creating a signature is the same operation
- **Bleichenbacher's attack can forge a signature**

Attack Against IKEv2 With Signatures

- Signature Based Authentication
  - Supported by IKEv1 and IKEv2
  - IKEv2 on Cisco router: 4 minutes time

- For Cisco: Simulation succeeds in 22% of attacks
- Real hardware again lacks performance

Additional Contributions In The Paper

- A dictionary attack against PSK authentication in main mode (CVE-2018-5389)
- Message flow diagrams of all IKE variants
- Description of the oracles in Huawei’s, Clavister’s, and ZyXEL’s implementations
- Description of our parallelized Bleichenbacher attacker

Questions?

Dennis Felsch

Ruhr University Bochum
Horst Görtz Institute for IT-Security
Chair for Network and Data Security

dennis.felsch@rub.de
@dfelsch

https://web-in-security.blogspot.de