Solutions to Selected Problems
Guide to Internet Cryptography

Companion Material

February 8, 2026

Preface

This document provides solutions to selected problems from the book *Guide to Internet Cryptography: Security Protocols and Real-World Attack Implications*. The material is intended for educational use in courses and self-study.

Book website: https://link.springer.com/book/10.1007/978-3-031-19439-9

1 Chapter 8: IPsec

Problem 8.1 SKIP

What is the equivalent of IKE in SKIP? How are the keys negotiated?

Solution

The equivalent of IKE is database access. Authentication of the DH shares is guaranteed be the authenticity of the results returned from the database(s).

Problem 8.2 IPsec: Architecture

Why is the SPD only needed to send an IPsec packet, not for receiving it?

Solution

When an IP packet is received, it is either unprotected or encrypted/authenticated with IPsec. So the basic policy how to process the IP packet is clear from its structure, and additional information on how to process it can be retrieved from the SAD by querying it with the SPI and the source IP address.

Problem 8.3 IPsec: Architecture

Assume that there is an entry in the SPD that all IP traffic to 136.135.134.132 UDP port 456 should be encrypted. What happens if no SA can be retrieved from the SAD for this target?

Solution

If there is no SA in the SAD for a policy given in the SPD, IKE must be invoked to negotiate the missing SA.

Problem 8.4 IPsec: ESP

An IP packet of 1281 bytes is the payload of IPsec ESP in Tunnel Mode. AES-CBC has been negotiated as the encryption algorithm. Which padding bytes must be added if minimum padding is used?

Solution

IPsec ESP Padding Calculation for AES-CBC

Given

- Original IP packet: 1281 bytes
- Encryption: AES-CBC (block size = 16 bytes)
- IPsec ESP Tunnel Mode with minimum padding

Calculation

Encrypted data includes:

$$\begin{aligned} \text{Size} &= \text{Original IP packet} + \text{Padding} + \text{Pad Length} + \text{Next Header} && (1) \\ &= 1281 + n + 1 + 1 = 1283 + n && (2) \end{aligned}$$

Block alignment requirement:

$$(1283 + n) \equiv 0 \pmod{16} \tag{3}$$

Padding needed:

$$1283 \bmod 16 = 3 \quad \Rightarrow \quad n = 16 - 3 = 13 \text{ bytes} \tag{4}$$

Padding Bytes (RFC 4303)

According to RFC 4303, padding bytes are filled sequentially starting from 1:

$$\text{Padding} = \texttt{01 02 03 04 05 06 07 08 09 0A 0B 0C 0D} \tag{5}$$

Complete ESP Trailer

```
Padding (13 bytes):  01 02 03 04 05 06 07 08 09 0A 0B 0C 0D
Pad Length (1 byte): 0D
Next Header (1 byte): 04 (for IPv4) or 29 (for IPv6)
```

Answer

Padding bytes: `01 02 03 04 05 06 07 08 09 0A 0B 0C 0D`
(13 bytes in hexadecimal)

Problem 8.5 IPsec: ESP

What type of authenticated encryption is used in IPsec ESP? Encrypt-and-MAC, MAC-then-Encrypt, or Encrypt-then-MAC [4]?

Solution

Encrypt-then-MAC.

Problem 8.6 IPsec: Tunnel Mode

Why must Tunnel Mode be used whenever an IPsec gateway is involved? Sketch an IPsec packet in Tunnel Mode that is sent from an IPsec-enabled host A to host B via an IPsec gateway G.

Solution

The gateway is not the final destination. Tunnel Mode encrypts the entire original IP packet (Src=A, Dst=B) and adds a new outer IP header (Src=A, Dst=G). After the gateway decrypts, it can see the inner destination (B) and route the packet correctly. Transport Mode wouldn't work because it doesn't preserve the original destination address.

Problem 8.7 STS Protocol

Please identify the mutual authentication protocol in the Station-To-Station protocol (STS). Please elaborate on the differences between STS and the signed Diffie-Hellman protocol (Figure 2.8).

Solution

Mutual authentication in STS is done with a certificate/verify protocol (but without certificates). X and Y are the challenges, and their hash values are signed. In STS, A also signs data from itself and from B, and vice versa. In Signed Diffie-Hellman, each party onlöy signs its own data.

Problem 8.8 Photuris

Do Photuris cookies protect against DDoS attacks carried out by a large botnet?

Solution

No, because no IP spoofing is needed in that case.

Problem 8.9 SKEME

Consider the following modification to the SCHEME protocol: Instead of X and Y, the ciphertexts c_I and c_R are included in the MAC computations. Can you still trust the key k_{sess}?

Solution

No. With this modification, SKEME would use an unauthenticated DHKE for key agreement, which is vulnerable to man-in-the-middle attacks.

Problem 8.10 SKEME

If we skip the SHARE phase in SCHEME and manually install a preshared key k_{mac} instead, would SCHEME still be secure? How many preshared keys would we need to enable session key establishment between any of the 4,000 hosts with this modified protocol?

Solution

Yes, it would be secure. The SHARE ohase is only needed to automatically install such a preshared key.
Each pair of hosts would need a different preshared key, and there are $4,000 \cdot 3,999$ pairs of hosts.

Problem 8.11 IKEv1

Try to assign each of the eight different variants of IKEv1 Phase 1 (Figure 8.28) to the most similar of the three protocols STS, Photuris, and SKEME.

Solution

MM/Sig: Photuris
AM/Sig: STS, because Photuris does not define a 3-message variant.
MM/PKE, AM/PKE, MM/RPKE, AM/RPKE: SKEME, because public-key encryption is used for authentication.
MM/PSK, AM/PSK: SKEME, because the SHARE phase could be replaced by the installlation of a preshared key.

Problem 8.12 IKEv1

Can a man-in-the-middle attacker modify the value SA contained in message m_2 of both IKEv1 Main Mode and Aggressive Mode? If he, e.g., modifies the encryption algorithm contained in SA in the Aggressive Mode, when will this change be noticed?

Solution

Yes. Since only $\vec{SA}$ is signed, he can modify SA. However, such a change may be detected if there is an algorithm mismatch. E.g., if he changed "AES" in SA ti "3DES", then the attaempt of the responder to decrypt c_5 (in Main Mode) with 3DES will fail, and the signature cannot be checked.

Problem 8.13 IKEv1

How does IKEv1 Phase 2 – Quick Mode, when used with DHKE enabled, fit into the definition of perfect forward secrecy (Definition 2.5)?

Solution

PFS is given if recorded sequence of encrypted messages cannot be decrypted later, even if the long-lived key of a participant is revealed later. In this contect the long-lived key (which is more approprietely described as medium-lived) is key k_0 user for key derivation.

Problem 8.14 IKEv2

Why is IKEv2 so much faster than IKEv1 - 2 RTT vs. 3 RTT?

Solution

Because Phase 2 is intertwined with Phase 1.

Problem 8.15 IKEv2

In Phase 1 (Figure 8.39), mac_i is always computed over the static value ID_I. Does this computation make sense? Or could we simply store mac_i in a static variable?

Solution

The value of mac_i is different in each execution of Phase 1, because the key k_{pi} is different. Therefore mac_i is not static.

Problem 8.16 IKEv2

Suppose that an active attacker wants to determine the initiator's identity in Phase 1 (Figure 8.39). How can he do that? Can he also determine the identity of a responder?

Solution

An active attacker acting as a responder can perform the IKE_SA_INIT phase, and the key derivation. He can then decrypt messasge c_3 and thus reveal the identity of the initiator.
This is not possible if the attacker acts as an initiator, because the responder will only send c_4 after successful verification of σ_i.

Problem 8.17 IKEv2

Suppose that Phase 2 (Figure 8.41) is always used without DHKE. Which of the five keys $(k_d, k_{ei}, k_{ai}, k_{er}, k_{ar})$ must an attacker, who has recorded all Phase 2 key exchanges, compromise to be able to compute all AH/ESP keys?

Solution

He must compromise keys k_d, k_{ei} and k_{er}. He needs k_{ei} and k_{er} to mdecrypt the nonces n'_I and n'_R, and k_d to derive the SA keys from these nonces.

Problem 8.18 NAT Detection

Can NAT detection also be used to determine two NAT gateways?

Solution

Yes, it can. In this case, both hash values in both NATD packets will be invalid after reception.

Problem 8.19 Dictionary attacks

Online dictionary attacks can check only one preshared key in each protocol execution. Please describe how an online dictionary attack against the responder works in Figure 8.44.

Solution

The attacker, acting as an initiator, guesses a PSK value psk'_{IR}. He executes the protocol according to its specification. If he receives message c_6, he knows that his guess was correct.

Problem 8.20 Bleichenbacher attacks

Suppose two hosts A and B have Bleichenbacher oracles. Sketch how an attacker could act as a man-in-the-middle between A and B, i.e., how he can decrypt and re-encrypt all ESP packets exchanged between A and B.

Solution

In the context of IPsec, "having a Bleichenbacher oracle" means that both hosts support IKEv1 with PKE authentication. Acting as a responder, the attacker can use the Bleichenbacher oracle in A to impersonate A to B, by decrypting the encrypted nonce in message m_3. Similarly, he can impersonate B to A. Once he impersonates both parties, he can switch into a role of man-in-the-middle, decrpyting all IP packets from A and re-encrypting them for B, and vice versa.
Since he is acting as a responder, this may take a while, since he has to wait for IKE requests from both parties.