Exercise Sheet 13

Prof. Kenny Paterson, F. Günther
M. Backendal, M. Filić

Discussion Questions (Authentication and Webpages).

(a) Whom are we authenticating in an entity authentication / key exchange protocol?

(b) Open a webpage of your choice in your browser. Find out if the connection to that webpage is using TLS and if so, which version and cipher suite. Who of you found the "most secure" connection?

Suggested focus. Attempt these problems
before class: Problem 1.
in class: Problems 2 and 3.

Suggested reading. Reading the following sections in the Boneh-Shoup book [1] might help with the problems on this exercise sheet: Section 8.10 (key derivation), Section 21.2 (key exchange, encryption-based), Section 21.10 (case study: TLS session setup)

Problem 1 (Sub-key derivation). In this problem, we will discuss a way to derive fresh and independent keys from an existing key. Let $\mathsf{F}\colon \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ be a secure PRF. From a given secret key $K \leftarrow\!\!\$\, \mathcal{K}$, we derive a new key $K' \in \mathcal{Y}$ as follows:

$$K' := \mathsf{F}(K, \mathsf{info}),$$

where $\mathsf{info} \in \mathcal{X}$ can be thought of as context shared by the entities who will subsequently use the key K'. As long as context values are distinct, the idea is that the resulting keys should be separated.

We will formalize this now, for the case of deriving two keys K^* and K' with distinct context info^* and info'. Our task is to now show that the derived keys K^*, K' provide some notion of "independent security", wherein (intuitively) even if an adversary gets access to K', it can't distinguish the other key K^* from a truly random key. More formally, consider the following security game for key independence w.r.t. a general key derivation function $\mathsf{KDF} : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$:

Game **KEY-indep**$(\mathcal{A}, \mathsf{KDF})$:

1 $K \leftarrow\!\!\$\, \mathcal{K}$
2 $b \leftarrow\!\!\$\, \{0,1\}$
3 $(\mathsf{info}', \mathsf{info}^*) \leftarrow\!\!\$\, \mathcal{A}()$ // $\mathsf{info}' \neq \mathsf{info}^*$
4 $K' \leftarrow \mathsf{KDF}(K, \mathsf{info}')$
5 $K_0^* \leftarrow \mathsf{KDF}(K, \mathsf{info}^*)$
6 $K_1^* \leftarrow\!\!\$\, \mathcal{Y}$
7 $b' \leftarrow\!\!\$\, \mathcal{A}(K', K_b^*)$
// K' is the "revealed" key, K_b^* is the real-or-random "challenge" key
8 Return $(b' = b)$

We define $\mathcal{A}$'s advantage in this game as

$$\mathbf{Adv}^{\mathbf{KEY\text{-}indep}}_{\mathsf{KDF}}(\mathcal{A}) = 2 \cdot \left| \Pr\left[\,\text{Game } \mathbf{KEY\text{-}indep}(\mathcal{A}, \mathsf{KDF}) \Rightarrow \mathsf{true}\,\right] - \frac{1}{2} \right| .$$

Given F is a secure PRF, show that F used as a KDF satisfies the notion of **KEY-indep**.

Problem 2 (Forward-secure key generation). Consider the following, simple approach[1] to derive a chain of random-looking keys K_i (for $i = 1, 2, 3, \ldots$) from a starting main key MK_0, using a function $\mathsf{F}\colon \mathcal{K} \times \{0,1\} \to \mathcal{K}$:

$$\begin{aligned} \mathrm{MK}_0 &\leftarrow\!\!\$\ \mathcal{K} \\ \mathrm{K}_i &\leftarrow \mathsf{F}(\mathrm{MK}_{i-1}, 0) \\ \mathrm{MK}_i &\leftarrow \mathsf{F}(\mathrm{MK}_{i-1}, 1) \end{aligned}$$

Following ideas from Problem 1, if F is a PRF, the derived keys K_i are uniformly random. In addition, we can show that this approach provides forward security in the following sense: even if MK_j is compromised, any K_i for $i \le j$ remains secure.

(a) Complete the following model for forward-secure key derivation: an adversary $\mathcal{A}$ obtaining q many derived keys (for a value q of its choice) as well as the final main key MK should not be able to distinguish the derived keys from random strings from an appropriate distribution.

Game $\mathbf{KEY\text{-}fs}(\mathcal{A}, \mathsf{F})$:

1 _____
2 $b \leftarrow\!\!\$\ \{0,1\}$
3 $\mathrm{MK}_0 \leftarrow\!\!\$$ _____
4 for $i := 1, \ldots, q$ do
5 if $b = 0$
6 then K_i_____
7 else K_i_____
8 MK_i_____
9 $b' \leftarrow\!\!\$\ \mathcal{A}(\mathrm{K}_1, \ldots, \mathrm{K}_q, \mathrm{MK}_q)$
10 Return $(b' = b)$

We define $\mathcal{A}$'s advantage in this game as

$$\mathbf{Adv}^{\mathbf{KEY\text{-}fs}}_{\mathsf{F}}(\mathcal{A}) = \_\_\_\_\_$$

[1] This mimicks the key updating mechanism in the TLS 1.3 record protocol (cf. Lecture 33-34) as well as Signal's symmetric ratcheting (cf. Lecture 35); a similar approach has been discussed for key generation in Lecture 31.

(b) Informally argue why the the above key derivation is secure in the sense of the **KEY-fs** game if F is a secure PRF.

(c) Show that the advantage $\mathbf{Adv}^{\textbf{KEY-fs}}_{\mathsf{F}}(\mathcal{A})$ of an adversary against the forward-secure key derivation above can be upper bounded by the advantage against the PRF security of F with a loss of $2q$:

$$\mathbf{Adv}^{\textbf{KEY-fs}}_{\mathsf{F}}(\mathcal{A}) \leq 2q \cdot \mathbf{Adv}^{\mathrm{PRF}}_{\mathsf{F}}(\mathcal{B})$$

Hint: For the factor q, think about how to apply PRF security step-by-step. For the factor 2, think of what is missing in the simulation after doing q steps.

Problem 3 (Key transport). Consider the following key transport protocol based on a public-key encryption scheme $\mathsf{PKE} = (\mathrm{KGen}, \mathrm{Enc}, \mathrm{Dec})$, illustrated in Figure 1. Alice (A) wishes to transport a key k to Bob (B). Let us assume that Alice possesses an authentic copy of Bob's public key. Bob begins by sending a random nonce r_B to Alice. Alice then picks a random nonce r_A and uses B's public key to encrypt a randomly generated session key $k \leftarrow\!\!\$\ \mathcal{K}$, her identity A, and the two nonces. She sends Bob the resulting ciphertext $c = \mathrm{Enc}(pk_B, (k, A, r_A, r_B))$, for some appropriate encoding of (k, A, r_A, r_B), as well as the nonce r_A. When Bob decrypts the obtained ciphertext without error, he checks if the obtained value r_B matches the sent value and if the decrypted nonce r_A matches the received one, and if so accepts that he is talking to Alice and uses the decrypted key $k \leftarrow\!\!\$\ \mathcal{K}$ for further communication.

Alice A (knows pk_B)		**Bob B** (knows sk_B, pk_B)
$r_A \leftarrow\!\!\$\ \mathcal{R}$	$\xleftarrow{r_B}$	$r_B \leftarrow\!\!\$\ \mathcal{R}$
$k \leftarrow\!\!\$\ \mathcal{K}$		
$c = \mathrm{Enc}(pk_B, (k, A, r_A, r_B))$	$\xrightarrow{r_A, c}$	$(k', A', r'_A, r'_B) \leftarrow \mathrm{Dec}(sk_B, c)$
		check $r_A = r'_A, r_B = r'_B$
accept key k		accept key k'

Figure 1: Key transport protocol based on PKE scheme PKE.

(a) Show that the session key k is secure against a passive key exchange adversary assuming PKE is IND-CPA secure. A passive key exchange adversary here merely gets to observe the exchange of messages between Alice and Bob in one session, and is then tasked with distinguishing the corresponding session key from an independent random key. More formally, consider the following security game with respect to the above key transport protocol based on PKE; here $\mathcal{I}$ is the identity space, $\mathcal{R}$ is the nonce space.

Game **KEY-passive**$(\mathcal{A}, \mathsf{PKE})$:

1 $b \leftarrow\!\!\$ \{0,1\}$

2 Fix $A, B \in \mathcal{I}$, with $A \neq B$ // Alice's and Bob's identities

3 $(pk_B, sk_B) \leftarrow\!\!\$ \mathrm{KGen}()$ // Bob's key-pair

4 $r_A \leftarrow\!\!\$ \mathcal{R}$ // Nonce sampled by Alice

5 $r_B \leftarrow\!\!\$ \mathcal{R}$ // Nonce sampled by Bob

6 $k_0 \leftarrow\!\!\$ \mathcal{K}$ // The "real" session key

7 $c \leftarrow\!\!\$ \mathrm{Enc}(pk_B, (k_0, A, r_A, r_B))$

8 $k_1 \leftarrow\!\!\$ \mathcal{K}$ // The "random" session key

9 $b' \leftarrow\!\!\$ \mathcal{A}((A, B, pk_B), (r_B, r_A, c), k_b)$
// Here (A, B, pk_B) is the public information and (r_B, r_A, c) is the communication transcript between Alice and Bob.

10 Return $(b' = b)$

We define $\mathcal{A}$'s advantage in this game as

$$\mathbf{Adv}^{\mathbf{KEY\text{-}passive}}_{\mathsf{PKE}}(\mathcal{A}) = 2 \cdot \left| \Pr\left[\,\text{Game } \mathbf{KEY\text{-}passive}(\mathcal{A}, \mathsf{PKE}) \Rightarrow \mathsf{true}\,\right] - \frac{1}{2} \right| .$$

Given that PKE is IND-CPA secure, show that the key-transport protocol based on PKE satisfies the notion of **KEY-passive** security.

(b) A crucial ingredient for the proof of Part (a) to work based on IND-CPA security is that we consider a passive key exchange adversary.

Discuss informally what would change if we considered a stronger security model where the adversary can be *active*: beyond seeing the messages r_B and (r_A, c) sent by Bob and Alice in the key transport protocol, the active adversary would be allowed to *change* these messages. The adversary would then be challenged on either the real key k that Alice generated or a random key, and would be allowed to see ("reveal") the key k' that Bob derives *if* it delivered a different $c' \neq c$ to Bob.

(c) Discuss why the above protocol does not provide (mutual) entity authentication by providing an attack.

(d) Propose a fix to the above protocol and argue informally why the fixed protocol achieves AKE security with mutual authentication. (You may introduce further cryptographic components/keys.)

Acknowledgements. This exercise sheet is in part inspired by (and adapted from) the book "A Graduate Course in Applied Cryptography" by Dan Boneh and Victor Shoup.

References

[1] D. Boneh and V. Shoup. *A Graduate Course in Applied Cryptography.* Online, version 0.6 edition, Jan. 2023.