Brandenburg University of Technology
Cottbus-Senftenberg
Chair of IT Security

Exercise Class
"Introduction into Cyber Security"
Winter Term 2018/2019

Introduction into Cyber Security
– 7th Exercise Sheet –

Discussion on: 9th January 2019

Topics

This exercise deals with password agreement and hash functions. In the exercise itself we will discuss the second practical task on buffer overflow exploits as well. Please prepare your own questions.

Instructions

The exercise sheets are to be worked on by you in self-study. In the exercise classes, usually only the control / discussion of the solutions takes place. The following preparation is therefore obligatory:

1. Read the exercise sheet with the tasks carefully. In case you have questions, please resolve them in advance with the tutor or your fellow students.

2. Use the lecture slides to repeat the content of the current subject and check your knowledge.

Careful preparation and processing of the exercise sheets (in addition to attending the lecture) is an essential prerequisite for success in the final exam.

Task 1: Hashing

Consider the password hash function in the figure underneath.

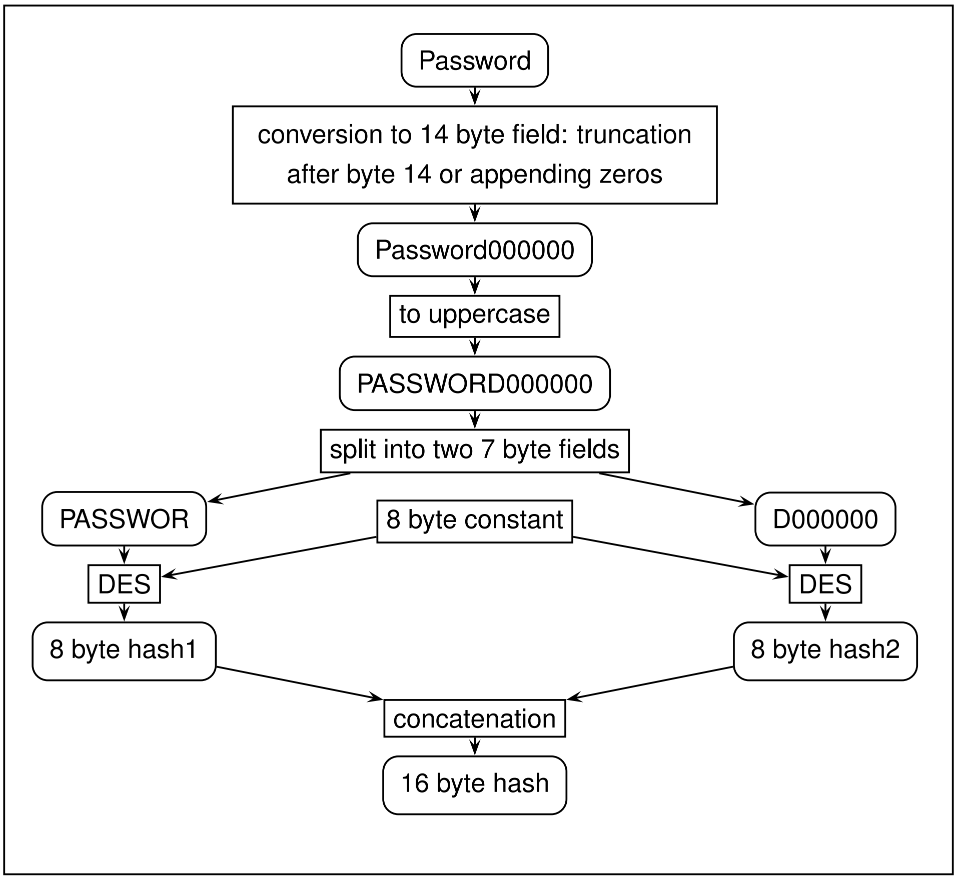

Figure 1: hash password function

Algorithms and constant are known publicly.

1. What would an attacker with access to a hash value do to recover the password?

2. Which design mistakes can you find in this password hash function?

Task 2: Password agreement

Consider the following key-exchange protocol:

1. Alice chooses $k, a \in \{0,1\}^n$ at random, and sends $s = k \oplus a$ to Bob.

2. Bob chooses $b \in \{0,1\}^n$ at random and sends $u = s \oplus b$ to Alice.

3. Alice computes $w = u \oplus a$ and sends w to Bob.

4. Alice uses k and Bob $w \oplus b$ as the secret key.

Now, answer the following questions.

1. Draw the protocol procedure.

2. Show that Alice and Bob share the same key.

3. Is this a secure key-exchange protocol?

4. If it is not secure, could you give some improvements for converting this key exchange into a secure one?

Task 3: IPsec

Describe in your own words why IP is unreliable and which of its shortcomings are addressed by IPsec. Then, answer the following questions:

1. Is it possible to use IPsec to prevent denial of service attacks?

2. On what OSI model layer does IPsec operate? Why exactly there, and not higher or lower?

3. Why does IPsec use MACs instead of digital signatures?

4. In which scenarios can tunnel and transport mode be used, respectively? Why are there two modes?

5. Why is it useful to check that the sequence number is not too old when processing incoming IPSec packets before proceeding with any further cryptographic checks?

6. Suppose that the current replay window spans from 120 to 530.

   a) If the next incoming authenticated packet has sequence number 340, what will the receiver do with the packet, and what will be the parameters of the window after that?

   b) If the next incoming authenticated packet has sequence number 598, what will the receiver do with the packet, and what will be the parameters of the window after that?

   c) If the next incoming authenticated packet has sequence number 110, what will the receiver do with the packet, and what will be the parameters of the window after that?

7. Why does AH (Authentication-Header) not work on a connection over NAT (network address translation) devices? How can IPsec be used anyways?

Task 4: Internet Key Exchange (IKE)

1. What are the most important changes from IKEv1 to IKEv2?

2. Think of some use cases in which you'd use the child SA creation in IKE.