Security on the Internet, summer 2007

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

12. Exercise sheet
Hand in solutions until Thursday, 5 July 2007.

Exercise 12.1 (Denial of Service). (3+3 points)

Read Steve Gibson, "The Strange Tale of the Denial of Service" at `http://www.grc.com/dos/grcdos.htm` (say, at least up to the FBI part).

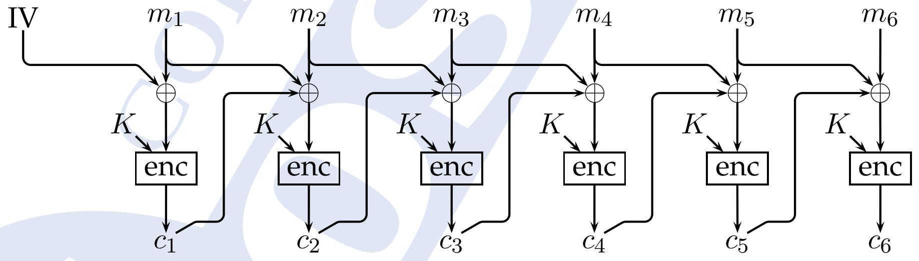
(i) Suppose your site only accepts IPsec packets. Consider the case that this attack is launched on your site and see whether you are better protected against it. $\boxed{2}$

(ii) Which modifications to IPsec would you suggest to increase its ability to withstand such an attack? $\boxed{1+1}$

(iii) Ask further questions. (Formulate at least two.) $\boxed{+2}$

Exercise 12.2 (Plaintext ciphertext block chaining, PCBC). (8+2 points)

The Kerberos designers unsuccessfully tried to do encryption and authentication in one go as follows:



At the end of the message they put a special recognizable piece of text. If and only if it decrypts properly the recipient decides that the message is ok.

(i) Describe the decryption. $\boxed{2}$

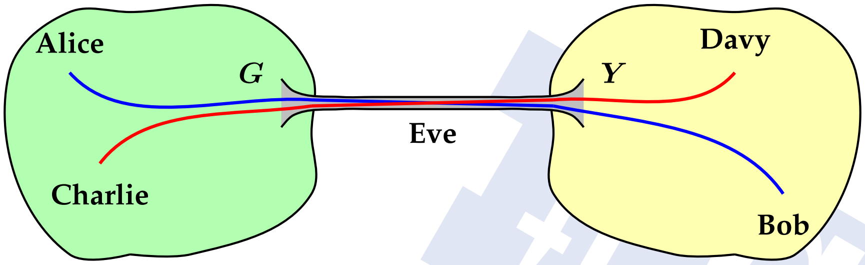
(ii) Which blocks are affected if an attacker or an error changes c_3? Explain. $\boxed{2}$

(iii) What happens if an attacker exchanges c_2 and c_3? $\boxed{2}$

(iv) What happens if an attacker exchanges c_2 and c_4? $\boxed{2}$

(v) Go beyond! $\boxed{+2}$

Exercise 12.3 (Splicing Attack). (6+2 points)



Suppose that the gateways G and Y link the green and the yellow LAN by an encrypted but not authenticated IPsec tunnel using a fixed SA. Assume that the encryption is done by some symmetric cipher in CBC mode. We want to show that Eve and her boss Davy can read all the traffic between Alice and Bob.

$\boxed{2}$ (i) How does the beginning of a packet from Charlie to Davy look like?

$\boxed{2}$ (ii) Replace the beginning of a packet from Alice to Bob or from Bob to Alice with the start of an eavesdropped packet from Charlie to Davy. What happens?

$\boxed{+2}$ (iii) How can Davy find out the part just after the replaced beginning? [Consider retransmitting. . .]

$\boxed{2}$ (iv) Draw conclusions. [Formulate a proposal, explain, argue.]

(v) Go beyond.

Exercise 12.4 (Advices). (0+12 points)

Comment on the following advices.

(i) Ensure perfect forward security.
(ii) Change keys periodically.
(iii) Use different keys in the two directions.
(iv) Use different keys for encryption versus integrity protection.
(v) Use different keys for different purposes.
(vi) Have both sides contribute to the master key. Do not let one side determine the key.
(vii) Use randomly chosen IVs.
(viii) Do not let encrypted data begin with a predictable value.
(ix) Compress data before encrypting it.
(x) Do not do encrpytion only.
(xi) Implement forward compatibility by allowing options and handling version numbers.
(xii) Negotiate parameters, and do it carefully.