Security Protocols and Application — Final Exam

Philippe Oechslin and Serge Vaudenay

28.6.2017

- duration: 3h00
- no document allowed
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will not answer any technical question during the exam
- the answers to each exercise must be provided on separate sheets
- readability and style of writing will be part of the grade
- do not forget to put your name on every sheet!

1 Reconsidering generic Composition

Q.1 Explain the following acronyms: AE, MAC, MtE, IV.
Say why some ISO 19772 readers have a flat nose.

Q.2 Briefly explain what is the old Bellare-Namprempre result from 2000 and why it is not enough.

Q.3 We consider two keys K and L and two algorithms: one $\mathcal{E}_K(\mathsf{IV}, M)$ to encrypt a message M with IV (it produces ciphertexts of exact same length as M); one pseudorandom function $F_L()$ taking several inputs and producing a tag of fixed length. Consider the following constructions:

$$C = \mathcal{E}_K(F_L(N,A), M) \qquad T = F_L(N,A) \tag{1}$$

$$C = \mathcal{E}_K(F_L(N), M \| F_L(N,M)) \tag{2}$$

$$C = \mathcal{E}_K(F_L(N,M), M) \qquad T = F_L(N,C,A) \tag{3}$$

with nonce N, message M, and associated data A. For each construction, explain how to decrypt and why it is a bad construction.

Q.4 With the same notations as above, consider the SIV mode (A4)

$$C = \mathcal{E}_K(F_L(N,A,M), M) \quad T = F_L(N,A,M)$$

Give a forgery attack of probability of success $1-(1-2^{-n})^q$, where q is the number of queries and n is the output length of F_L. (Assume an adversary who can make chosen plaintext and chosen ciphertext queries.)
Compare this scheme with the following one (A2), in terms of functional and security properties:

$$C = \mathcal{E}_K(F_L(N,A), M) \quad T = F_L(N,A,M)$$

2 Automotive Remote Keyless Entries

Q.1 The most convenient car keys are the ones that you don't even need to take out of your pocket to open the car. They are called PKES or smart keys.

- Describe an attack to which this type of keys are vulnerable

– How can the owner of this type of keys prevent this attack.

Q.2 A typical rolling code contains the following elements:

$$\langle UID \parallel btn \parallel MAC_{keyUID}(btn, ctr)\rangle$$

– For each parameter, describe what it represents and explain why it is needed.

Q.3 Now assume your car has two different keys that use rolling codes of the format described above.

– Describe a method with which the car can accept messages from both keys and still not be vulnerable to a replay attack.

Q.4 The VW-1 scheme uses the following message structure: $\langle f(UID) \parallel g(ctr) \parallel btn\rangle$
Its security was mainly based on the fact that f and g were unknown. Once the functions are known, it is claimed that the car can be opened after a single message has been eavesdropped.
Assume that the f and g functions are a modern cryptographic hash function H like SHA-2. You have eavesdropped a message while your neighbor used his key to open his car.

– Explain how you can use the eavesdropped message $\langle H(UID) \parallel H(ctr) \parallel btn\rangle$ to create a new message that will enable you to open the car.
– What condition must be met for your attack to succeed ?

Q.5 The correlation attack on HiTag2 is based on the fact that partial guesses of the key can be classified according to a score. The function f takes 20 bits as inputs and outputs a single bit b.
The attacker guesses the first 8 inputs to the function f and calculates b for all possible combinations of the remaining 12 bits of input of the function.

– If the guess was wrong, how many times, in average, will the output b be correct for all possible values of the 12 remaining bits ?
– If the guess was right, how many times, in average, will the output b be correct for all possible values of the 12 remaining bits ?

Q.6 From the previous question we see that the difference in correlation scores between a correct guess and an incorrect guess is quite small. The authors say that the attack succeeds with as little as 4 captured messages.

– Using four messages, in how many different ways can a guess of 16 bits of the key be scored ? Explain briefly.
– Are all the scores of the same quality ? Explain briefly.

Q.7 HiTag2 uses keys of 48 bits. Such keys can be bruteforced with powerful computers.

0x0001	UID	btn	lctr	ks	0	chk

0 16 48 52 62 94 95 102

Fig. 1. message structure for Hitag2

Figure 1 shows the the different elements of a HiTag2 message and the number of bits of each element.

- How many messages do you need to eavesdrop in order to be able to run a bruteforce attack ?
- Describe your bruteforce attack.
- Give an estimate of the complexity of your attack