

Security Protocols and Application — Final Exam

Philippe Oechslin and Serge Vaudenay

27.6.2016

Family Name:

Given Name:

SCIPER:

- 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 Signal Protocol, the Improvement over OTR

Q.1 The words “axolotl” and “ratchet” both have double meanings. They have a meaning outside of computer science and they have a meaning in cryptography.

Answer the following questions.

- Give the two meanings of “axolotl”. How is it related to this exercise?
- Give the two meanings of “ratchet”. How is it related to this exercise?
- What does “OTR” mean?
- Name at least six objectives of Signal.

Q.2 In the Signal Protocol, when Alice wants to send a message to Bob for the first time, she first fetches Bob's long-term public key bG and one of his one-time public prekeys $x_{b,i}G$ from a central server (then, the server erases this prekey). All public keys are in Curve25519. Then, she selects her ephemeral public key $x_{a,eph}G$ and she sets $x_{b,eph}G = x_{b,i}G$. In other cases, when Alice wants to send a message to Bob, she already has a state containing $bG, x_{b,eph}G, x_{a,eph}G$. To send a message to Bob, Alice takes her long-term public key aG then computes offline

$$\text{secret} = ax_{b,eph}G || bx_{a,eph}G || x_{a,eph}x_{b,eph}G$$

Alice's message to Bob is then secured with secret. Together with her message, she advertises (sends) her ephemeral public key $x_{a,eph}G$ and identifies which of Bob's prekey was used as well. So, Bob will be able to build a state containing $aG, x_{a,eph}G, x_{b,eph}G$.

Answer the following questions.

- What is Curve25519?
- What are the secret keys and where do they belong to?
- When (and why) does Alice erase her ephemeral key?
- Why don't we use abG instead of these three values?

Q.3 The Signal Protocol uses the Double Ratchet Algorithm. The ratchet key is RK. When Alice sends her first message to Bob, the 3DH handshake is used to derive RK from secret. Then, for when Alice or Bob replies with a new message, RK is updated by

$$RK \parallel NHK \parallel CK \leftarrow \text{KDF}(\text{HMAC}(\text{RK}, x_{a,\text{eph}} x_{b,\text{eph}} G))$$

This way, a chain keys CK is derived. Then, a sequence of message keys MK are derived by iterative hashing on the chain key. A message is encrypted with MK.

In addition to making CK, RK is also used to derive a header key HK which is used to encrypt the ephemeral key $x_{a,\text{eph}}G$, the message number Ns within the ratchet, and the number PNs of sent messages in the previous ratchet. The NHK is the next value of HK in the next ratchet. So, Alice sends

$$\text{Enc}_{\text{HK}}(\text{Ns}, \text{PNs}, x_{a,\text{eph}}G) \parallel \text{Enc}_{\text{MK}}(\text{plaintext})$$

Encryption follows the encrypt-then-MAC principle using AES256 and HMAC-SHA256.

Answer the following questions.

- Explain why we call this algorithm “Double Ratchet” and why it is done like this.
- Why do we send Ns and PNs?
- Why don’t we use NHK right away instead of waiting for the next ratchet?
- Could the MAC of messages be used as a signature from Alice to prove that she did send a message to Bob?

2 Powerspy

Q.1 The powerspy attack is used to try to infer a phone's location without using the sensors supposed to provide location information.

Answer the following questions.

- Which sensors are usually used to provide location information to applications ?
- Why would an application not want to use these sensors ?

Q.2 The powerspy attack is able to deduce the location of the phone from its power consumption.

Answer the following questions.

- What makes the power consumption dependent on the location of the phone ?
- Given a single measurement of the (electric) current consumption of a phone, what can be said about its location ? Explain in a few words.
- Cite three goals concerning location that can be achieved by constantly monitoring the phone's current consumption.

Q.3 Suppose you want to use Powerspy to identify which route among a set of possible routes you have taken to come to the exam this morning.

Answer the following questions.

- What work did you have to do in advance of the exam to be able to carry out the attack today ?
- What preprocessing do yo have to apply to the measurements in order to facilitate the identification of the route ?
- Describe in a few sentences the algorithm that leads from the preprocessed measurements of this morning's power consumption to the identification of the route you took.

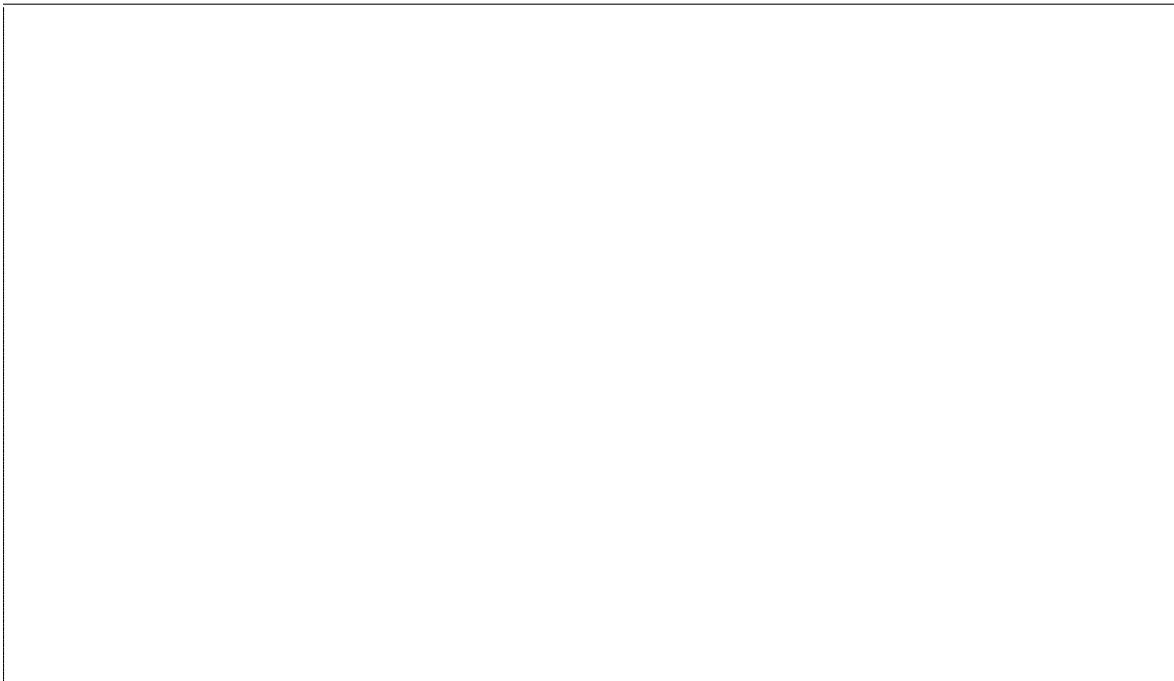
Q.4 Explain why the power consumption profile is different depending on the direction in which a route is taken.



Q.5 Different possibilities exist to prevent this attack.

Answer the following questions.

- What mechanism does an application use to know the current power consumption ?
- Why is adding noise to the available measurement of the power consumption not a satisfying solution ?
- What would be a simple and logical solution to prevent the attack ?



Q.6 Finally, can you find a useful and honest usage of the power consumption for the localisation of a phone ?

