Exam Questions Applied Cryptology (Bart Preneel)

19 December 2014

1. Give two ways that NSA (probably) has used to get access to the data of the users of the Google services.
   Answer: 1) The PRISM program (request access to data stored in the cloud); 2) The MUSCULAR program (GCHQ intercepts the communication between the back-office servers of Google through Level 3 and shares the data with the NSA); 3) send a security letter to request the private SSL server key; 4) use spoofing (Quantum Insertion) to insert malware on the client device and then access the data at the client side.

2. Explain why the reuse of key stream in a stream cipher (or in the one time pad) is a serious problem.
   Answer: If one reuses the key stream, the difference between the ciphertexts is the difference between the plaintexts - this value is independent of the key stream. With statistical methods it is possible to derive a lot of information on the two plaintexts.

3. Consider the following ways to use the AES block cipher to protect data in a high speed communication protocol (10 Gbit/s); rank them in order of security, most secure first.

   A: CBC mode with as IV the packet number or frame counter

   B: CCM mode

   C: CBC mode combined with CBC-MAC computed on the plaintext

   D: CBC mode with a random and secret IV

   Answer:
   B > C > D > A.

4. EMV uses for entity authentication a challenge-response protocol based on digital signatures. Give three advantages of this protocol compared to passwords.
   Answer:
   1) Eavesdropping the channel gives no information that can be reused to later impersonate Alice; 2) The server (Bob) does not need any secret information to verify the response from Alice; 3) The secret of Alice is an RSA key that is definitely not easy to guess.

5. The following protocol has been proposed by ICAO to verify the authenticity of a passport A and a passport reader B.

   Alice A **Bob** B

   $$\xleftarrow{\qquad certB \qquad}$$

   $$\xrightarrow{\qquad \alpha^a \bmod p \;||\; r_A \qquad}$$

   $$\xleftarrow{\alpha^y \bmod p \;||\; \mathrm{Sig}_B(r_A||\alpha^y \bmod p)}$$

   Here one has the following definitions:

   - p a prime number
   - α a generator mod$p$
   - A the identity of Alice and B the identity of Bob
   - r_A a random string generated by Alice
   - a the private key of A
   - $\alpha^a \bmod p$ the public key of A

- y an integer chosen uniformly at random with $1 < y < p - 1$.
- $\mathrm{Sig}_X(.)$ signature with the private key S_X of X
- $certX$ a certificate of a third party on the public key of X

a) How can Alice and Bob agree on a session key?
Answer: Bob computes $k = (\alpha^a)^y \bmod p$ and Alice computes $k = (\alpha^y)^a \bmod p$. (Note that it would be even better to compute the hash value of $\alpha^{ay} \bmod p$.)

b) Does this protocol achieve entity authentication from Alice to Bob and from Bob to Alice? Motivate your answer.
Answer. The protocol does not provide entity authentication of Alice to Bob since Alice only sends her public key and a random number. The protocol provides entity authentication of Bob to Alice since Alice sends in step 2 a fresh challenge r_B and Bob returns in step 3 a signature on this challenge (computed with his private signing key).

c) Does this protocol achieve implicit key authentication from Alice to Bob, that is, does Bob know that Alice is the only party that can possibly obtain the session key? Similarly from Bob to Alice. Motivate your answer.
Answer. The protocol provides implicit key authentication of Alice to Bob *if Bob has an authenticated copy of Alice's public key, e.g., through a certificate.* In that case Bob knows that only Alice can find the session key. Without an authenticated copy of Alice's public key, the property does not hold.
The protocol provides implicit key authentication of Bob to Alice since from the signature in the third message Alice learns that Bob has generated $\alpha^y \bmod p$; from this Alice can deduce that Bob is the only other party who can compute the session key.

d) Does this protocol provide key confirmation from Alice to Bob and from Bob to Alice? Motivate your answer.
Answer. There is no key confirmation; Alice does not know that her message has arrived correctly and Bob does not know that his second message (third step) has arrived correctly. Moreover, even if those messages have arrived, the parties do not know from each other that they have performed the Diffie-Hellman key calculation correctly.

e) Does this protocol offer forward secrecy?
Answer. No. If Alice's long term secret key a leaks, an opponent who has stored all past interactions can deduce the session key for each of those interactions. If Bob's long term secret key leaks, there is no problem.

f) Does this protocol resist a known (session) key attack?
Answer. If someone would obtain a session key, it would not be possible to make the parties reuse the key. The reason is that an attacker could replay the value $\alpha^y \bmod p$ in the third message, but the signature cannot be replayed: it contains the fresh random number r_A just sent by Alice; this allows Alice to detect a replay.

6. Is it possible to build a secure electronic payment system without tamper resistance hardware for the user? Consider the case where the merchant is off-line and the case where the merchant is on-line.
Answer. If the merchant is off-line, nothing stops the user from doublespending his money so one cannot build a secure payment system. If the merchant is on-line, one can use e-cash to build a secure payment system; in this case the merchant can check online whether the e-cash has been spent before.