Exam Security 2IS05 TU/e technische universiteit eindhoven **April 18th 2012**

No additional materials/equipment may be used during the exam.
Exam result = total points / 10 (Max. punts per question indicated.)

1. (16p) Indicate to what degree you agree with the following statements (for each give a short motivation in which each part of the statement is clarified and evaluated).

(a) The Bell-LaPadula access control model prevents that data with a `high' label can be read by a user with only a `low' clearance.
(b) With Kerberos a user can, by logging in once, get access to all systems where the user has an account.
(c) A biometric reading is never exactly right. The `equal error rate' of a biometric gives the ideal error margin that may be present in a measurement.
(d) If an encryption is IND-CPA secure it is not susceptible to an effective side-channel attack.
(e) In an asymmetric cryptosystem the keys are larger than in a symmetric system but still it requires less secure storage in the end.
(f) If large messages are sent using Output Feedback mode then there is no error propagation if an incorrect block arrives but if a block is missed then the rest of the message is not decrypted correctly anymore.
(g) With Direct Anonymous Attestation users can proof procession of an attribute without revealing their identity.
(h) A Cross Site Scripting (XSS) attack can be prevented by executing all scripts in a sandbox.

2. (24p) Recall that RSA uses a public modulus N, a public key E and a secret key D such that $a^{E*D} = a \bmod N$. Only Alice knows private key D_A belonging to public key E_A and modulus N_A

(a) What methods (multiple) are there for Bob to make sure that public key E_A is really the public key of Alice?
(b) Consider a large message M (M is several times larger than N). How can
    (i) Bob send message M to Alice so only she can read it?
    (ii) Alice sign message M so others can check the signature?
(c) The following MUL(multiply) – SQR(square) implementation of RSA exponentiation contains a countermeasure. What countermeasure is that, what attack does it protect against and how?

```
r = 1;
for ( i = 0; i < bitlength( k ); i++ ) {
        r = SQR( r, M );
        if ( bit( k, i ) == 1 )     r = MUL( r, m, M );
        else                        s = MUL( r, m, M );
}
```

Pseudo code RSA exponentiation

(d) What is easier to attack using a Differential Power Analysis (DPA) attack in this implementation; the four least significant bits of the key or the four most significant bits of the key? Motivate your answer and describe how the attack to retrieve these 4 bits would work.

3. (20p) A transport company has a fleet of vehicles. To manage and maintain its fleet it wants to collect live data from each vehicle's onboard systems (e.g. location, status, driving style, amount of breaking, speed, etc.). The location and speed will also be made available to the company BobBob which uses this information for its route planner products.
Do a basic security analysis for this scenario:
- Who are the stakeholders, their interests and which trade-offs between these interests exist.
- Who are potential attackers, their goals and possible attacks.
- Which security mechanisms could be applied and what is their influence on possible attacks but also on the interests of the stakeholders.

4. (15p) The birthdate is a commonly used `secret' for choosing a pincode.
(a) What is the entropy of the combinations dd-mm (day and month) and mm-yy (month and 2 digits year), assuming no specific information about the pin owner is known?
(b) What happens to the entropy of the two combinations in (a) if it is known that the pin owner is a student?
(c) Even the entropy of a randomly chosen 4 digit pincode is much lower than what is typically required for the key of a cryptographic algorithm. Why then is it considered good enough for protecting pin payments?

1. $A \rightarrow S$: A,B
2. $S \rightarrow A$: $\{K_{AB}, \{A, K_{AB}\}K_{BS}\}K_{AS}$
3. $A \rightarrow B$: $\{A, K_{AB}\}K_{BS}$
4. $B \rightarrow A$: $\{B\}K_{AB}$

Mutual authentication and session key exchange protocol with A and B agent identities, S a trusted server, K_{AB} a fresh session key and K_{AS} and K_{BS} keys shared between A and S and B and S respectively. { M }K is the encryption of message M with key K.

5. (25p) In the Dolev-Yao model the attacker has complete control over the network.
(a) Consider a user (Alice) trying to access a website (Bob.com) and an attacker (Mallory) on the same local network as Alice. Give three different attacks which each allow Mallory to achieve at least one of the following:
(i) Mallory sends a message that seems to come from Alice.
(ii) Mallory sees what messages Alice sends to Bob.
(iii) Mallory prevents a message of Alice from reaching Bob?
The protocol above aims at mutual authentication of agents A and B and at giving them a new session key, gegenerated by trusted party S.
(b) Which message is intended to achieve authentication of A and which authentication of B?
(c) After the protocol is A sure she is taking to B and that (besides A and S) only B can have the session key? If so: give argumentation. If not: give an attack and a repaired protocol with argumentation why that does work.
(d) After the protocol is B sure she is taking to A and that (besides B and S) only A can have the session key? If so: give argumentation. If not: give an attack and a repaired protocol with argumentation why that does work.