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

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.

True; blp assigns a confidentiality level to each resource (piece of data) e.g. secret, and a clearance level to each subject e.g. `public' and allows only read access to those resources at or below one's clearance level.

(b) With Kerberos a user can, by logging in once, get access to all systems where the user has an account.

False; though Kerberos does offer single sign on it does this for all systems which trust the authentication server used, not 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.

False. Thought the first sentence is basically true, the ERR is just one possible choice of the tradeoff, there is no general `ideal' choice – it depends on the application.

(d) If an encryption is IND-CPA secure it is not susceptible to an effective side-channel attack.

False. The IND-CPA only puts requirements on the functional behaviour (i.e. only considering input and output thus without the side channels).

(e) In an asymmetric cryptosystem the keys are larger than in a symmetric system but still it requires less secure storage in the end.

True(iss). Though somewhat dependent on the exact application and assumptions and what exactly is meant by `secure' storage – typically asymmetric keys are larger but we only need to store private keys confidential manner (+ protect integrity). We do need the public keys of others but they only need integrity protection (which we could do with our secret key).

(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.

True; OFB works like a stream cipher so bit errors only effect the current block but missing a block will mean each following block with get decrypted (xored) with the `wrong' key.

(g) With Direct Anonymous Attestation users can proof procession of an attribute without revealing their identity.

True; in DAA a user can give a zero-knowledge proof of having a certain certificate (which states the given attribute for the user).

(h) A Cross Site Scripting (XSS) attack can be prevented by executing all scripts in a sandbox.

False; the problem is that the XSS script seems to come from a `trusted site' – thus will have access to the info/resources meant for this trusted site (including info a user may enter). This is not solved by running it 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?

Name at least two of these three categories; - alternate, secure, channel (including in person exchange), - Certificate Authority, - Web of trust

(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?

Use block mode; either directly or encrypt a `session key' and use symmetric cipher with the session key.

(ii) Alice sign message M so others can check the signature?

[Standard as we sign the hash the size of message is not important (hash value is smaller than N)] Signature = Hash of the message to the power D (i.e. decrypted with RSA). Others can check be raising signature to power E (encrypting it) and checking it is same as hash of message.

(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?
Timing attacks(partial points for mentioning timing or Power analysis attack); execution time depends on the (nr 1s in the) key. If combined with power analysis (SPA) then can likely even read each bit of the key from the power trace. Defense ensures execution time and (form of the) power trace do not have this dependency on the key (partial points for `removes key dependency') (at the cost of added execution time – approx. double the time needed).

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

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.
Intermediate value r is the most natural point to attack. Predicting the value of r in the earlier rounds as it depends on less bits of the key (the most significant ones). Attacking less significant bits requires first finding the more significant bits of the key.
Attack could be one bit at a time (first round attack bit1, after that use found value for the first bit and attack second bit in round 2. Could also do in a single attack in the 4th round; guess all 4 bits at the time and validate the guess using computation of r in round 4.
DPA attack; set of random inputs, measure power traces for each input , try all possible value for the relevant key bits (2 or 16 possibilities) group traces hi/lo by #1s in predicted value of r. Take difference of averages of the two groups. (alternative to hi/lo groups: look at correlation #1s predicted value and power used.)

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(3p), their interests(3p) and which trade-offs(2p) between these interests exist.
- Who are potential attackers(3p), their goals(2p) and possible attacks(2p).
- Which security mechanisms(3p) could be applied and what is their influence on possible attacks but also on the interests of the stakeholders(2p).

Stakeholders; name at least 3. Required: Transport Company(TC), BobBob(BB), driver
Optional: TC customer, BB customer, data collector (e.g. telco operator), government, ...
Interests: give at least 1-2 realistic requirements of each stakeholder. (E.g. correct data of as many drivers as possible for Bob Bob, Privacy for Driver)

Trade-offs: give at least two relevant, realistic conflicting interests (e.g. potential conflict with the two given interests above).
Attackers: At least 3, including 1 insider (one of the stake holders), 1 outsider (e.g. Transport competitor, BobBob competitor)
Goals: for insider; the conflicting goal, goals for outsiders (e.g. decrease quality BobBob service, etc.)
Attacks: Should achieve one of the goals, should indicate how; be more than `achieve goal x' (enough details to assign and evaluate a specific security mechanism). E.g. tamper with the communication between the cars and BobBob, changing the speed of the cars (so BobBob does not see a traffic jam.)
Mechanisms: at least three relevant mechanisms.
E.g. signing messages send by the car..
Influence mechanisms: For each mechanism. At least 1 interesting trade-off (i.e. decreases another interest).
E.g. Protects against changes but may threaten privacy driver.

4. (15p) The birthdate is a commonly used `secret' for choosing a pincode.

(a) What is the entropy of the combinations
(i) dd-mm (day and month) and
(ii) mm-yy (month and 2 digits year),
assuming no specific information about the pin owner is known?
*log2 of 365.25 (log2 of 365 of 366 or even of 12*31 acceptable) and log2 of 12*100 (actual values or formulas with logs and sums which result in the same are acceptable).*

(b) What happens to the entropy of the two combinations in (a) if it is known that the pin owner is a student?
*No change for (i) and (ii) drops to about log2 of 12*6; the age range of students is approximately 6 years. (Basically any valid argument that says second drops a lot is acceptable).*

(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?
Pin payments are security critical – yet a user cannot remember long codes so some trade-off is needed.
Different setting; crypto assumes you have access to a cipher text meaning you can try as many keys to decrypt it as you want. With pin there is also the need to have the card (what you have authentication) and the number of tries is typically limited (e.g. after 3 wrong tries card block and no more tries are possible).

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.
e.g. IP spoof
(ii) Mallory sees what messages Alice sends to Bob.
e.g. simple eaves dropping if on same hub, or ARP poisoning so Alice thinks Mallory is the gate way. attack DNS; change IP of Bob.com to something controlled by Alice.
(iii) Mallory prevents a message of Alice from reaching Bob?
e.g. (D)Dos Bob so bob does not receive any message. Same man in middle attacks as in ii. (Need to name 3 different attacks-no double points for same attack in two categories.)

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?
Message 3: A, message 4: B (These are the only options); the others are messages from/to S so cannot authenticate Alice or Bob (can give info that will be used but do not achieve the authentication.).
(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.

Attack:
A ->I(S): A,B
B->S: A,I
S→A: $\{K_{AB}, \{I, K_{AB}\}K_{IS}\}K_{AS}$
A->I(B)->$\{I, K_{AB}\}K_{IS}$
(I now has session key Kab)

Fix: Add B in message from S to A, e.g. $\{K_{AB},B,\{A, K_{AB}\}K_{BS}\}K_{AS}$
(Note using {A,B}KAS in message 1 is not sufficient; attacker could store {A,I}KAS from earlier run where Alice does want to talk to I.)
Argument ok:
Now A knows only B will be able to get K_{AB} from message 3. So upon receiving msg 4 knows B is involved and trying to communicate with her (As A included in message to Bob).
(Note that the message from S may be very old and not actually the response to the message A,B that we sent in this run; still the attacker cannot gain anything important by doing this – need to add a nounce or timestamp if want to prevent this.)

(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.

When B receives 3: he knows, must have come from S, and S will only release Kab in the form of message 2 so A is the only one who can have Kab. (Note that we are not sure that A is really trying to talk to B – for that an added step would be needed; e.g. a step in which A sends anything (other than B) encrypted with Kab to B. When B receives this he knows A received message 4 and thus knows she is talking to B. (For the fixed protocol of part c this is not needed: there message 2 already ensures A knows she is talking to B).
Note that we also do not know when Kab was created-that could be a long time ago.