Advanced cryptography: Cloud & More, winter 2013/14

MICHAEL NÜSKEN

5. Exercise sheet
Hand in solutions until Wednesday, 4 December 2013, 23:59

Exercise 5.1 (Realization of security recommendations). (8+4 points)

Pick one of the section 4, 5, 7, 8, 10, 11 or 13 of the BSI security recommendations (https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html) and compare the security statements of your favourite cloud provider against it. Discuss. 8+4

Example: Amazon provides a Whitepaper in the AWS Security Center (`http://aws.amazon.com/en/security/`).

Exercise 5.2 (Schoolbook RSA signatures). (8+4 points)

Consider the basic RSA signature scheme with

Algorithm. Verify.
Input: The user's public key (N, e), the message $m \in \mathbb{N}_{<N}$ and the signature $\sigma \in \mathbb{N}_{<N}$.
Output: Accept or reject.

1. If $m \equiv_N \sigma^e$ then
2. Return Accept
3. Else
4. Return Reject

and the key generation outputs a public key (N, e) and a private key (N, d) with the property that N is a product of two suitably large primes and $x^{ed} \equiv_N x$ for all $x \in \mathbb{N}_{<N}$.

(i) Is this scheme EUF-CMA secure? Prove your answer. 6

(ii) A key only attacker (KOA) is like a chosen message attacker without a signing or private key oracle. Is the scheme EUF-KOA secure? Prove. 2

(iii) For universal unforgeability (UUF) the attacker's task is to find a signature for a message m^* given to it. In other words: Other than in an existential forgery the attacker cannot choose $m*$. Is the scheme UUF-CMA secure? Prove your answer. +4