UNIVERSITY OF TWENTE.

Examination Secure Data Management

Module/course code: 192110940 (4TU students), 192110941 (Kerckhoffs students)
Date: 3 November 2017
Time: 3 hours 30 minutes *(+25% for students who may use extra time)*
Instructor: Willem Jonker

Instructions:

- **This is an open book examination. Allowed sources: your notes, the reader, the slides.**
- **No *communication* devices allowed.**
- **The examination consists of 4 open questions and 7 multiple choice questions.**
- **Weights are indicated per question.**
- **Success!**

1. **Authentication and Access Control (14 points)**
    a. What problems are there with using passwords as an authentication method. (2 points)
    b. What is the difference between a reference monitor and an access control manager? (3 points)
    c. Explain security requirements for Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Key-Policy Attribute Based Encryption (KPABE)? (3 points)
    d. Explain the role of Proxy in Proxy Re-encryption Schemes. Why RSA Proxy Re-encryption scheme is not secure? (3 points)
    e. Explain why CP-ABE is more powerful than a traditional public-key encryption (e.g. RSA)? (3 points)
2. **Blockchains (15 points)**
    a. Why is it important in Bitcoin that nobody has more than 50% of all the computational power of the system? What would be consequences if this happens? (4 points)
    b. How is double spending prevented in Bitcoin? (2 points)
    c. Where are your Bitcoins stored (if you have some)? (2 point)
    d. What is stored in your Bitcoin wallet? (2 points)
    e. Why could the DAO attack happen? Does that mean that Ethereum smart contracts are not secure (motivate your answer)? (5 points)
3. **Secure distributed data storage (11 points)**
    a. In a private data aggregation scheme why is it important that the (untrusted) aggregator cannot compute the aggregated value if there is at least one user who did not send data? (4 points)

b. In DECANTeR, when is an alert triggered, and why is it not triggered more easily or less easily? (7 points)

4. **Searchable Encryption (25 points)**
   a. When does forward index results in better search times than inverted index, and when is it the other way around? (4 points)

   With respect to the multi-user public key encryption with conjunctive keyword search scheme answer the following questions.
   b. What participants are in the scheme? Who stores what and how? (5 points)
   c. What cryptographic techniques are used in the scheme? (3 points)
   d. How can the data be queried? (2 points)
   e. What functionality does the scheme provide? (2 points)
   f. How secure is the scheme? Under which conditions? (6 points)
   g. What are the differences between the indistinguishability of ciphertext from ciphertext and the indistinguishability of multi-user ciphertext from random security games? (3 points)
5. **Which one is a group? (5 points)**
   a. $G = \{1, a, b, c\}$ where

$\odot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

   b. $(\mathbb{N}, +)$: natural numbers with addition as the operation
   c. $G = \{1, a\}$ where

$\odot$	1	a
1	1	a
a	a	a

   d. $(\mathbb{Z}, \cdot)$: integers with multiplication as the operation
6. **What is the main advantage of using elliptic curves instead of Galois fields for public key encryption? (5 points)**
   a. Elliptic curves enable very efficient polynomial evaluation which enables cryptographic schemes to have broader functionality than those that are not based on elliptic curves.
   b. Unlike for any other algebraic structure, in case of using elliptic curves the message space and the ciphertext place can be the same, making cryptographic schemes simpler.
   c. If the keys are chosen properly, elliptic curve encryption provides post-quantum security, making it suitable for long-term use.
   d. Given the public parameters and keys in an elliptic curve encryption scheme, computation of the private key(s) has much higher complexity than the encryption and the decryption operation. In case of schemes using Galois fields, the complexity of computing the private key is also higher but not as much higher.
7. **Which one of the following applications is the best fitted for blockchains? (5 points)**
   a. Decentralized notary: One interesting feature of the blockchain is its timestamp feature. The whole network essentially validates the state of wrapped piece of data at a certain particular time. As a trustless decentralized network, it essentially confirms

the existence of [something] at a stated time that is further provable in a court of law. Until now, only centralized notary services could serve this purpose.

b. Smart appliances: A smart appliance is a device that connects to the internet and gives you more information and control than before. For instance, a code connected to your appliance can be linked to the internet and alert you when your cookies are ready or if your laundry has stopped. These alerts keep your appliances in good condition, they save you money regarding energy efficiency and help you control your devices when away from home, among other benefits. Encrypting these appliances on the blockchain protects your ownership and enables transferability.
c. Blockchain healthcare: Personal health records could be encoded and stored on the blockchain with a private key which would grant access only to specific individuals. The same strategy could be used to ensure that research is conducted via HIPAA laws (in a secure and confidential way). Receipts of surgeries could be stored on a blockchain and automatically sent to insurance providers as proof-of-delivery. The ledger, too, could be used for general health care management, such as supervising drugs, regulation compliance, testing results, and managing healthcare supplies.
d. Digital passports: The blockchain protects your identity by encrypting it and securing it from spammers and marketing schemes. The first digital passport launched on Github in 2014 and could help owners identify themselves online and off. How does it work? You take a picture of yourself, stamp it with a public and private key, both of which are encoded to prove it is legitimate. The passport is stored on the ledger, given a Bitcoin address with a public IP, and confirmed by Blockchain users

8. Which is NOT a common cause for leaked or stolen data? (5 points)

a. No encryption used.
b. Non-compliance with security policies.
c. Not perfectly secure encryption schemes used.
d. Data exfiltration malwares.

9. What is the Blakeley Secret sharing scheme based on? (5 points)

a. Hyperplanes of n-dimensional space
b. Coefficients of a polynomial of degree n
c. N dimensional spheres
d. Prime factorization of natural numbers

10. What is Bloom Filter used for in the Secure Anonymous Database Search scheme? (5 points)

a. To find the most relevant matches.
b. To reduce search time.
c. To improve the security.
d. To broaden functionality.

11. We studied many schemes where there is an honest-but-curious party that can transform a ciphertext to another ciphertext (without being able to decrypt it) in such a way that it can be decrypted by a participant who do not have the secret key to decrypt the original ciphertext. Which is topic in which we did NOT use this party? (5 points)

a. Searchable encryption.
b. Proxy re-encryption.
c. Private data aggregation.
d. Mediated ciphertext-policy attribute-based encryption.