Exam Data Security 2018

Show correct answers
Hide correct answers

Page 1

Security Protocols

Consider the following protocol in AnB notation:

```
Types:
 Agent A,B,s;
 Symmetric_key KAB;
 Function sk
Knowledge:
 A: A,B,s,sk(A,s);
 B: A,B,s,sk(B,s);
 s: A,B,s,sk(A,s),sk(B,s)
Actions:
 A->s: A,B
 s->A: {| KAB |}sk(A,s), {| KAB |}sk(B,s)
 A->B: A,{| KAB |}sk(B,s)
Goals:
A authenticates s on KAB,B
B authenticates s on KAB,A
KAB secret between A,B,s
```

Running this protocol with OFMC yields the following attack:

```
ATTACK TRACE:
i -> (s,1): x29,x401
(s,1) -> i: {|KAB(1)|}_(sk(x29,s)),{|KAB(1)|}_(sk(x401,s))
i -> (x401,1): x27,{|KAB(1)|}_(sk(x401,s)
```

Question 1

How does this attack relate to the AnB protocol? Mark which of the following statements are correct

- ☐ i claims to be x401
- ☐ x401 plays role A
- ☐ x401 plays role B

Question 2

Which of the specified goals is shown violated by the attack?

- ☐ A authenticates s on KAB,B
- ☐ B authenticates s on KAB,A
- ☐ KAB secret between A,B,s

Page 2

TLS

Consider the following simplified model of the TLS protocol where A does not have a certificate:

```
Types: Agent A,B,s;
       Number NA,NB,Sid,PA,PB,PMS;
       Function pk,hash,clientK,serverK,prf

Knowledge: A: A,pk(s),B,hash,clientK,serverK,prf;
       B: B,pk(B),pk(s),inv(pk(B)),
            {B,pk(B)}inv(pk(s)),hash,clientK,serverK,prf
Actions:
A->B: A,NA,Sid,PA
B->A: NB,Sid,PB,
      {B,pk(B)}inv(pk(s))
A->B: {PMS}pk(B),
      {hash(NB,B,PMS)}inv(pk(A)),
      {|hash(prf(PMS,NA,NB),A,B,NA,NB,Sid,PA,PB,PMS)|}
        clientK(NA,NB,prf(PMS,NA,NB))
B->A: {|hash(prf(PMS,NA,NB),A,B,NA,NB,Sid,PA,PB,PMS)|}
        serverK(NA,NB,prf(PMS,NA,NB)
```

Question 3

After this handshake, A and B can exchange messages symmetrically encrypted with clientK(...) and serverK(...), respectively. Which of the following properties hold:

- ☐ A can be sure that messages she sends can only be read by B.
  B can be sure that messages he sends can only be read by A.
- ☐ A can be sure that messages she sends can only be read by B.
  A can be sure that messages she receives can only come from B.
- ☐ A can be sure that messages she sends can only be read by B.
  B can be sure that messages he receives can only come from A.
- ☐ B can be sure that messages he sends can only be read by A.
  B can be sure that messages he receives can only come from A.

Page 3

Privacy

Consider a possible extension of Denmark's NemID solution, where every user with a CPR number who is over 18 years old can obtain a certificate of the following form:

{ over18, Timestamp, h(SP) }privkey

where "over18" is just a statement that this user is over 18, the Timestamp is the current time, "h(SP)" is a string provided by the user that is the hash of some service provider. The idea is that a user can now show this certificate to the service provider SP in order to prove that they are registered citizen in Denmark over 18 years old in a privacy friendly way.

Question 4

We assume that the intruder does not know any secret information like private keys, passwords, etc. that belong to an honest agent.

Which agents need to be honest in order for this solution to be secure?

- ☐ Just NemID needs to be honest
- ☐ NemID and the server S need both to be honest.
- ☐ All three participants NemID, SP, and the User need to be honest.
- ☐ This solution does not need anybody to be honest.

Question 5

Which privacy properties are achieved by this solution?

- ☐ The SP does not learn the name and date of birth of any honest user.
- ☐ NemID does not learn for which SP the certificate is issued.
- ☐ The SP does not learn the name and date of birth of any honest user.
  and NemID does not learn for which SP the certificate is issued.

Question 6

Which of the following attacks can be prevented by SP?

- ☐ The SP can prevent that the same certificate is used twice.
- ☐ The SP can prevent that a malicious user gives the certificate to a friend who is not a registered citizen or not yet 18 years old.
- ☐ The SP can prevent a malicious user from using a certificate.

Question 7

Is this correct: if a user interacts two times with the same SP and obtains a new certificate each time, then the SP cannot tell whether this is the same or a different user.

- ☐ Yes, the two instances are then unlinkable.
- ☐ No, the two instances are linkable.

Page 4

Buffer overflows

Question 8

There are many suggestions for avoiding buffer overflow attacks. Which of the following suggests alone is sufficient to prevent all buffer-overflow attacks?

- ☐ Write the program in Java (if we can assume there are no buffer overflows in the Java tools and libraries).
- ☐ If the programing language is C/C++: always use strncpy instead of strcpy.
- ☐ Check all places where input to the program is copied into a buffer: stop with an error, if the input is longer than the buffer size.

Page 5

Software Security

Question 9

Suppose there is a social media website where users can stay logged in using cookies. A malicious user makes a post on this website that contains some Javascript code that instructs the browser of a victim (who views the post) to transmit the victims cookie to a malicious website. What category of attack is this?

- ☐ Injection Attack
- ☐ Cross-Site Scripting Attack
- ☐ Cross-Site Request Forgery Attack

Page 6

Cryptology

Question 10

Encryption using AES-256 in CBC mode is …:

- ☐ Computationally secure
- ☐ Information theoretically secure
- ☐ Both
- ☐ None of the above

Question 11

Encryption using a one-time pad is …:

- ☐ Computationally secure
- ☐ Information theoretically secure
- ☐ Both
- ☐ None of the above

Question 12

Which security property does a successful block replay attack violate?

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☐ Privacy

Question 13

What statement best describes the concept of non-repudiation?

- ☐ Communication between two parties is secure
- ☐ A party cannot later deny sending a message
- ☐ An attacker cannot interfere with a message in transit
- ☐ An attacker cannot perform traffic analysis

Question 14

of the four general types of cryptanalysis requires the most powerful attacker?

- ☐ Cipher-text only attack
- ☐ Known plain-text attack
- ☐ Chosen plain-text attack
- ☐ Adaptive chosen-plaintext attack

Page 7

Secure Communication

Question 15

You have created a zero knowledge protocol, where the verifier randomly selects one of two challenges that the prover must satisfy. The prover must answer ***n*** challenges correctly in order to be verified.
You want to make it 4 times harder to be verified by guessing the answer to the challenges, so how many iterations of challenges should the new protocol include?

- ☐ n +2
- ☐ n + 4
- ☐ n * 2
- ☐ n * 4

Question 16

Alice and Bob use steganography to secure their communication by hiding it in the least significant bit of each pixel in a grayscale image; each pixel is encoded in a single byte. Their message is encoded in ASCII - a table of Decimal ASCII values is shown below.

Part of a hexadecimal dump of the image, which shows an old-fashioned TV tuned to a dead channel, is shown below, what does the part of the message say?

```
2A 39 42 44 55 5B 37 4f
4A 6D 78 4A 4B 4C 4D 77
50 32 33 6C 5A 4E 76 39
```

- ☐ Bob
- ☐ OMG
- ☐ WTF
- ☐ OK!

Question 17

The TCP handshake protocol starts by the initiator transmitting a **SYN** character (ASCII: 22) is encrypted using RSA. The following parameters are used for the RSA encryption and decryption: e = 7, d = 103 and n= 209. Which cipher-text corresponds to the encrypted SYN character?

- ☐ 27
- ☐ 33
- ☐ 90
- ☐ 154

Page 8

Network Security

Question 18

A system with 50 nodes implements secure communication based on symmetric cryptography using pre-shared keys. How many keys are required to allow each party to communicate with all other parties?

- ☐ 2500
- ☐ 2450
- ☐ 1225
- ☐ 1250

Question 19

Hop-by-hop encryption means that communication is encrypted “on the wire,” but decrypted and re-encrypted in all switches and routers. In which layer of the OSI reference model would you implement Hop-by-hop encryption?

- ☐ Layer 2 (data link layer)
- ☐ Layer 3 (network layer)
- ☐ Layer 4 (transport layer)
- ☐ Layer 7 (application layer)

Question 20

Which of the following advantages is **NOT** associated with Hop-by-hop encryption?

- ☐ Transparency to host
- ☐ Robustness against Denial of Service attacks
- ☐ Protection of packet meta data
- ☐ Fast encryption hardware can be used

Page 9

Authentication

Question 21

Some password authentication systems freezes the account after a number of unsuccessful authentication attempts. An attacker may take advantage of this mechanism by attempting to login as a particular user more than the allowed number of attempts. Which security goal is violated by this attack?

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☐ Privacy

Question 22

You are asked to evaluate the minimal security offered by four different authentication mechanisms based on either passwords or passphrases.
The first mechanism requires passwords that …: must contain at least 6 and at most 50 characters among at least three of the following four categories: lowercase letters ('a' to 'z'), uppercase letters ('A' to 'Z'), digits ('0' to '9') and the following special characters ('.', '-', '_', '+', '!', '?', '=').
The second mechanism requires passwords that …: must contain at least 5 and at most 50 characters with at least one character from each of the following four categories: lowercase letters ('a' to 'z'), uppercase letters ('A' to 'Z'), digits ('0' to '9') and the following special characters ('.', '-', _, '+', '!', '?', '=').
The third mechanism requires passphrases that …: must contain at least 5 ASCII printable characters (94 characters excluding “space”).
The fourth mechanism requires passphrases that …: must contain at least 3 randomly selected words from a 42,000 word vocabulary.
Which mechanism provides the strongest minimum security, i.e. the larges possible search space for brute force password cracking?

- ☐ Mechanism 1
- ☐ Mechanism 2
- ☐ Mechanism 3
- ☐ Mechanism 4

Question 23

An intelligent door-lock system for a smart home relies on an app on the user’s smartphone. The app uses the phone’s camera to perform facial recognition of the user and sends a message to unlock the door if a registered user is recognized. What authentication factors are used in this system?

- ☐ Something he possesses and something he is
- ☐ Something he possesses and something he knows
- ☐ Something he knows and something he is
- ☐ Something he knows and somewhere he is

Page 10

Access Control

Question 24

In the full implementation of the access control reference model from NIST, what component is or what components are responsible for the enforcement of access control policies?

- ☐ Policy Enforcement Point
- ☐ Policy Decision Point
- ☐ Policy Enforcement Point + Policy Decision Point
- ☐ Policy Enforcement Point + Policy Decision Point + Policy Information Point

Question 25

The access control matrix shown below encodes the access control policy of the company Foo International Ltd. The privileges encoded in the matrix relate to read (r), write (w) and amend (a) permissions to specific case files (numbered from 1-8 for your convenience).

The company desires to change to a system that uses the basic ($RBAC_0$) model of Role Based Access Control. What is the smallest number of roles that they need to define?

- ☐ 4
- ☐ 6
- ☐ 8
- ☐ 9

Question 26

Redo the question above assuming that Foo International Ltd desires to change to a system that uses the hierarchical ($RBAC_1$) model of Role Based Access Control. What is the smallest number of levels that they need to define in their role hierarchy (all roles that inherit from the same role are considered to be at the same level)?

- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5

Page 11

Security Administration

Question 27

The overall risk analysis of the ACME Company estimates an expected annual loss of 17 million kroner from identified security vulnerabilities. A survey of different security technologies identify four different technologies that mitigate one or more vulnerability, these are summarized below:
A Managed Security Service
costs 25 million kroner to implement, but will reduce the annual expected loss by 16 million kroner.
A Demilitarized Zone costs 10 million kroner to implement, but will reduce the annual expected loss by 12 million kroner.
A Security Operations Center costs 8 million kroner to implement, but will reduce the annual expected loss by 6 million kroner.
An Intrusion Detection System costs 6 million kroner to implement, but will reduce the annual expected loss by 5 million kroner.
The company wishes to optimize its investment in computer security, so it will only invest in the single technology that provides the best value for money.
Which technology do you recommend?

- ☐ Managed Security Service
- ☐ Demilitarized Zone
- ☐ Security Operations Center
- ☐ Intrusion Detection System

Question 28

Which security property does ransomware violate?

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☐ Privacy

Question 29

In the recent “Se & Hør” scandal in Denmark, a system administrator at Nets sold credit card information about celebrities. Which vulnerability best characterizes this situation?

- ☐ Weak assumptions
- ☐ Weak architecture
- ☐ Weak components
- ☐ Weak operation