Midterm #2

Started: Jul 21 at 11am

Quiz Instructions

Question 1

3 pts

Judge this protocol. Select all that apply.

Alice to Bob - "I'm Alice", $\{[R]_{Alice}\}_{Bob}$
Bob to Alice - $\{K_s\}_{Alice}$
Alice to Bob - $\{K_s\}_{Bob}$

Where R is the nonce, K_s is the session key.

{...} is encryption with specified PUBLIC key.

[...] is encryption with specified PRIVATE key.

- [x] Session key K is protected
- [ ] A Replay Attack is possible
- [x] Alice is authenticated
- [x] Bob is authenticated

Question 2

3 pts

Judge this protocol. Select all that apply.

Alice to Bob - "I'm Alice", R
Bob to Alice - $E(K_s,R+1, K)$
Alice to Bob - $\{K_s\}_{Bob}$

Where R is the nonce, K_s is the session key. K is a pre-shared symmetric key.

{...} is encryption with specified PUBLIC key.

[...] is encryption with specified PRIVATE key.

E(M, K) is encryption of message M using the cipher E and the symmetric key K.

- [x] Bob is authenticated
- [x] Session key K is protected
- [ ] A Replay Attack is possible
- [x] Alice is authenticated

Question 3

3 pts

Judge this protocol. Select all that apply.

Alice to Bob - "I'm Alice", R
Bob to Alice - $\{h(R+1)\}_{Alice}$
Alice to Bob - K_s, $\{R+2\}_{Bob}$

Where R is the nonce, K_s is the session key.

{...} is encryption with specified PUBLIC key.

[...] is encryption with specified PRIVATE key.

h(.) is a given hash function.

- [ ] Trudy can be mis-authenticated as Bob
- [x] A Replay Attack is possible
- [ ] The session key is protected.
- [ ] There is Muthual Authentication

- [x] Trudy can be mis-authenticated as Alice

Question 4 — 1 pts

Given this protocol:

```
Alice to Bob: "I'm Alice"
Bob to Alice: {R}Alice
Alice to Bob: {R+1}Bob
```

Where {...} is encryption with the specified PUBLIC key.

Is Alice authenticated?

- ○ No, Alice is not authenticated
- ◉ Yes, Alice is authenticated

Question 5 — 1 pts

Given this protocol:

```
Alice to Bob: "I'm Alice"
Bob to Alice: {R, Ks}Alice
Alice to Bob: {R+1}Bob
```

Where {...} is encryption with the specified PUBLIC key.

K_s is the Session Key.

Is the Session Key safe?

- ○ No, the Session Key is not safe
- ◉ Yes, the Session Key is safe

Question 6

1 pts

Given this protocol:

```
Alice to Bob: "I'm Alice"
Bob to Alice: "[R]Bob"
Alice to Bob: "[R]Alice"
```

Where [..] is the signature.

Is mutual authentication ensured?

- ○ No, Bob is not authenticated
- ◉ Yes, Alice and Bob are both authenticated
- ○ No, Alice is not Authenticated
- ○ No, neither of the two is authenticated

Question 7

2 pts

```
Alice to Bob - "I'm Alice", R
Bob to Alice - [R,Ks]Bob
Alice to Bob - [{R+1}Bob]Alice
```

Where R is the nonce, K_s is the session Key,

{...} is encryption with specified PUBLIC key.

[...] is encryption with specified PRIVATE key.

Which of these properties are ensured? (select all that apply)

- [ ] Session key K is protected
- [ ] Alice is authenticated
- [ ] Protection to Replay Attack
- [x] Bob is authenticated

Question 8

3 pts

Judge this protocol. Select all that apply.

Alice to Bob - "I'm Alice", $[\{T\}_{Bob}]_{Alice}$
Bob to Alice - $[\{K_s\}_{Alice}]_{Bob}$

Where T is the timestamp, K_s is the session Key.

{...} is encryption with specified PUBLIC key.

[...] is encryption with specified PRIVATE key.

- [ ] Alice is authenticated
- [x] Session key K is protected
- [x] Replay Attack is possible
- [x] Bob is authenticated

Question 9

1 pts

Imagine a possible Biometric System that relies on the human ability to jump and has a high Equal Error Rate.

Would it be suitable for Identification, Authentication or both?

- ○ Identification
- ○ Both
- ◉ Authentication

Question 10

1 pts

Please, imagine a possible Biometric System that relies on eating spaghetti (never with meatballs) and has a very low Equal Error Rate.

Would it be suitable for Identification, Authentication or both?

- ○ Authentication
- ○ Both
- ◉ Identification

Question 11

1 pts

These are the Equal Error Rates for four different kinds of Biometric Systems:

10^{-1}

10^{-21}

10^{-60}

10^{-19}

Can you select the one that belongs to the more reliable (especially in term of accuracy), considering both the Insult Rate and the Fraud Rate?

- ◉ 10^{-60}
- ○ 10^{-21}
- ○ 10^{-1}
- ○ 10^{-19}

Question 12

1 pts

Which of these three Access Control Matrices is affected by the Confused Deputy security problem?

A:

	Compiler	BILL DATA
Compiler	RW	WX
Atticus	RW	WX

B:

	Compiler	BILL DATA
Compiler	RW	RX
Ignatius J. Reilly	X	W

C:

	Compiler	BILL DATA
Compiler	R	R
Haplo	X	WX

- ○ Only C is affected
- ○ Only A is affected
- ○ Only A and B are affected
- ◉ Only B is affected

- ○ None of them is affected
- ○ Only A and C are affected
- ○ Only B and C are affected

Question 13

2 pts

Which type of firewall can stop the TCP ACK Scan attack? (Select all that apply)

- ☑ Stateful Packet Filter
- ☐ Application Proxy
- ☐ Stateless Packet Filter
- ☐ There is no way to stop this attack

Question 14

1 pts

Which transport layer protocol would be better to exchange a compressed file?

- ◉ TCP
- ○ UDP
- ○ HTML
- ○ IP

Question 15

1 pts

Which is the most common way to ensure that a protocol resists to a Denial of Service (DoS) attack?

Select all that apply.

- [ ] Guaranteeing mutual authentication
- [ ] Keeping the protocol stateful
- [x] Keeping the protocol stateless
- [ ] Guaranteeing protection of the session key

Quiz saved at 12:54pm

Submit Quiz