

Quiz Summary

Section Filter ▾

Student analysis

Item analysis

Average score

83%

High score

100%

Low score

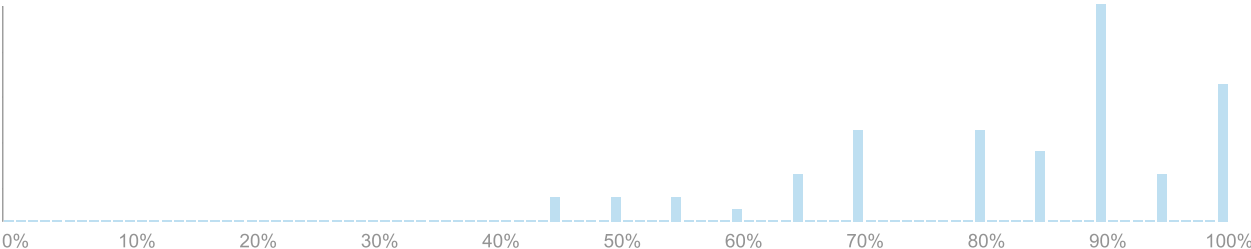
45%

Standard deviation

1.48

Average time

24:46



Question Breakdown

Attempts: 68 out of 68

Which of the following statements is CORRECT about STS (Station-to-station) protocol?

+0.35

Discrimination

Index ?

Leakage / compromise of Alice's long-term private key would allow an attacker to later obtain session key k.

2 respondents

3 %

Leakage / compromise of Bob's long-term private key would allow an

1 respondent

1 %

attacker to later obtain session key k.

Passive sniffing of messages

exchanged over network allows

4 respondents

6 %

attackers to obtain session key k.

STS is vulnerable against Man-in-the-

middle attack just like DH key

9 respondents

13 %

agreement protocol.

None of the above.

52 respondents

76 %



76%

answered

correctly

Attempts: 68 out of 68

Which of the following statements is CORRECT about KDC (Key distribution center)?

+0.22

Discrimination

Index (?)

KDC does not have to be online after permanent secret keys are established with all users in the system.

3 respondents

4 %

KDC uses asymmetric encryption schemes.

0 %

KDC must be highly secure and needs to be trusted by all users in the system..

60 respondents

88 %



In Kerberos authentication, User C('s workstation) needs to establish long-term shared key with Resource V in advance.

1 respondent

1 %

None of the above.

4 respondents

6 %

88%

answered

correctly

Attempts: 68 out of 68

Let us consider a scenario Alice is trying to submit a homework to CANVAS (<https://canvas.nus.edu.sg>) over HTTPS. The procedure to submit a homework is, after establishing TLS session, (1) login as "Alice" using her password, and then (2) select homework file and click "submit" on a web form. Eve is an eavesdropper, who can sniff whole communication incoming to or outgoing from CANVAS server. Which of the following information can be obtained by Eve? Check all that apply.

Which computer is connecting to CANVAS server

62 respondents

91 %

Content of the homework file

1 respondent

1 %

Approximate size of file uploaded

56 respondents

82 %

User ID used is "Alice".

20 respondents

29 %

Alice's login password

2 respondents

3 %

59%

answered
correctly

Attempts: 67 out of 68

+0.31

Which of the following statements is CORRECT about TLS?

Discrimination
Index (?)

TLS 1.2 handshake is vulnerable against Man-in-the-middle attack that manipulates random numbers etc. exchanged on the network.

4 respondents

6 %

Cipher suite is agreed between the server and client during the handshake.

62 respondents

91 %

Client certificate is always required.

0 %

TLS 1.3 increases the overhead of handshake, compared to TLS 1.2.

0 %

None of the above.

1 respondent

1 %

No Answer

1 respondent

1 %

91%

answered


correctly

Attempts: 68 out of 68

Which of the following statements is CORRECT about IPSec?

+0.46

Discrimination

Index 

In Transport mode, AH header provides authentication for both IP and TCP headers in the original packet.	2 respondents	3 %
Using Tunnel mode, we can protect both of the IP and TCP headers in the original packet.	57 respondents	84 %
ESP cannot provide authentication.	3 respondents	4 %
Transport mode of the IPSec works at the transport layer in the protocol stack.	4 respondents	6 %
None of the above.	2 respondents	3 %

84%

answered


correctly

Attempts: 68 out of 68

Which of the following digital certificates is the most trustworthy?

+0.52

Discrimination

Index 

Self-signed certificate		0 %
Domain validated certificate		0 %
Extended validation certificate	46 respondents	68 %
Compelled certificate	1 respondent	1 %
Certificate on Certificate Transparency log.	21 respondents	31 %

68%
answered
correctly

Attempts: 68 out of 68

In PKI, timely revocation of certificates is crucial. Which of the following mechanisms can reflect the up-to-date revocation status the most?

+0.33

Discrimination
Index (?)

Certificate Transparency	1 respondent	1 %
Short-lived certificate	4 respondents	6 %
OCSP	60 respondents	88 %
Convergence	1 respondent	1 %
Delta CRL	2 respondents	3 %

88%
answered
correctly

Attempts: 68 out of 68

Which of the following statements is WRONG about Perspective and Convergence?

+0.52

Discrimination

Index (?)

Both rely on online notary servers.	2 respondents	3 %
Increased overhead is a drawback of both schemes.		0 %
In both systems, notary servers can know which users are accessing which web sites.	57 respondents	84 %
If notary servers are seeing different certificate very recently for a certain HTTPS web site, it may be an indication of attack.	4 respondents	6 %
None of the above.	5 respondents	7 %

84%
answered
correctly

Attempts: 68 out of 68

Which of the following statements is CORRECT about Certificate Transparency?

+0.24

Discrimination

Index (?)


Certificate Transparency is a mechanism to enforce revocation of invalid digital certificates.		0 %
Certificate Transparency help us detect fraudulent domains that could be utilized for phishing.	61 respondents	90 %
Certificate Transparency requires online notary servers.	1 respondent	1 %
For consistency and availability, certificate log should be maintained by a single, trusted entity.		0 %
None of the above	6 respondents	9 %

90%
answered
correctly

Attempts: 68 out of 68

Which of the following is essential for Certificate Transparency to be effective?

+0.5

Discrimination
Index 

Clients (e.g., browsers) that do not accept certificates that are NOT on any certifica.te log	1 respondent	1 %
CAs or domain owners that continuously check certificate logs to detect fraudulent certificates.	3 respondents	4 %
Auditors that check if log servers are behaving correctly.	6 respondents	9 %
Timely revocation mechanism		0 %
All of the above	58 respondents	85 %

85%
answered
correctly