UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab 11: IPsec and Email security

Exercises from Lectures 19 and 20 (along with Lectures 17 and 18).

QUESTION 1

Explain why the lack of interaction in email delivery prevents the possibility to achieve forward secrecy for secure email.

Is there a way that forward secrecy could be approximated for email?

Hint: Email uses the *store-and-forward* principle.

QUESTION 2

In hybrid encryption, such as used in PGP, is it better to have the public key encryption or the symmetric key encryption to be the stronger of the two?

QUESTION 3

End-to-end security and link security are two ways of providing network security.

What are some of the advantages and disadvantages of each?

What protocols, or configurations, are available to provide each of these types of security in:

(a) email?

(b) IPsec?

QUESTION 4

Compare IPsec in host-to-gateway architecture with TLS.

Consider the following scenarios and discuss which would be the most suitable to provide security in each case:

(a) You have two applications on your server which you want to secure with independent keys and different security services.

cont/...

(b) You want to secure a server which has a number of applications and you may want to add new applications in the future without changing the security settings.

QUESTION 5

Three possible ways to combine encryption and MACs are:

- encrypt first and apply the MAC to the ciphertext;
- apply the MAC first and encrypt plaintext and MAC together;
- apply the MAC and encrypt the plaintext separately.

Which of these is used in TLS and which is used in the ESP protocol of IPsec?

Why is the third option not suitable in general?

Hint: Remember that the purpose of a MAC is only to provide authentication/integrity and not confidentiality.