NTNU
The Norwegian University of
Science and Technology
Department of Telematics

TTM4100
Communication – Services and Networks

Assignments for "Security in Computer Networks"

SOLUTION

Only one answer or statement is correct for each question below.
Right answers or statements in **bold**, wrong answers or statements are ~~striked out~~.

1. General

1.a) *Message confidentiality* is the property that …

~~1.a.1 … the receiver can detect whether the message sent (whether encrypted or not) was altered in transit.~~
~~1.a.2 … the identity of the sender can be confirmed to be who or what they claim to be.~~
1.a.3 … the original plaintext message cannot be determined by an attacker who intercepts the ciphertext-encryption of the original plaintext message.
~~1.a.4 … the sender cannot deny having sent the message.~~

1.b) *Message integrity* is the property that …

1.b.1 … the receiver can detect whether the message sent (whether encrypted or not) was altered in transit.
~~1.b.2 … the identity of the sender can be confirmed to be who or what they claim to be.~~
~~1.b.3 … the original plaintext message can not be determined by an attacker who intercepts the ciphertext-encryption of the original plaintext message.~~
~~1.b.4 … the sender cannot deny having sent the message.~~

1c) Assume a group of N people (N > 2). To allow each member of the group to communicate confidentially with each of the other members of the group separately, how many **secret** keys are necessary in total when using *symmetric key cryptography*?

~~1.c.1 N~~
~~1.c.2. N(N-2)/2~~
~~1.c.3 N/2~~
1.c.4 N(N-1)/2
~~1.c.5 2N-1~~

1d) Same as 1c) above but using *public key cryptography* instead. How many **secret** keys are necessary now?

1.d.1 N
~~1.d.2. N(N-2)/2~~
~~1.d.3 N/2~~
~~1.d.4 N(N-1)/2~~
~~1.d.5 2N-1~~

2. Message integrity and Digital signatures

2.a) A *cryptographic hash function* …

***2.a.1* … has a property that states that it is computationally infeasible to find two messages which have the same hash function.**
~~*2.a.2* ... has identical properties with the CRC.~~

~~*2.a.3* … has a property that states that it is theoretically impossible to find two messages which have the same hash function.~~

2.b) A *message authentication code* (*MAC*) …

~~*2.b.1* … is not the result of a cryptographic hash function.~~
***2.b.2* … always uses a shared key to strengthen message integrity.**
~~*2.b.3* … does not need any shared information between sender and receiver.~~

2.c) A *digital signature* …

~~*2.c.1* … can be made by using the public key from a public key cryptographic algorithm to sign a message (or the hash of a message).~~
~~*2.c.2* … can be made by using the secret key from a symmetric key cryptographic algorithm to sign a message (or the hash of a message).~~
***2.c.3* … can be made by using the private key from a public key cryptographic algorithm to sign a message (or the hash of a message).**

3. Securing TCP connections: SSL

3.a) *Secure socket layer* (*SSL*) …

~~*3.a.1* … is used to implement communication security at the network layer.~~
***3.a.2* … enhance TCP with confidentiality, integrity, server authentication and client authentication.**
~~*3.a.3* … is implemented between the transport and network layers.~~

3.b) When using *Secure socket layer* (*SSL*) …

***3.b.1* … the two parties communicating agree on the specific cryptographic algorithms during the handshake phase.**
~~*3.b.2* … RSA with key length 256 is always used as the public key algorithm.~~
~~*3.b.3* … AES is always used as the symmetric key algorithm, but key length is negotiated.~~
~~*3.b.4* … RSA is always used as the public key algorithm, but key length is negotiated.~~

4. Operational Security: Firewalls

4.a) A *Traditional packet filter* firewall …

~~*4.a.1* … uses the same rules for datagrams leaving and entering the network.~~
***4.a.2* … uses different rules for datagrams leaving and entering the network.**
~~*4.a.3* … uses the same rules for all router interfaces.~~
~~*4.a.4* … cannot filter based on protocol type.~~

4.b) A *Stateful packet filter* firewall …

***4.b.1* … track ongoing TCP connections to decide whether to let received TCP packets into the network or not.**
~~*4.b.2* … make filtering decisions on each packet in isolation.~~
~~*4.b.3* … never allows any incoming TCP connections to be established.~~