9.6 Network security

Name: _____ Class: _____ Date: _____ **Total: 24 marks**

KEY WORDS TLS • MAC

Objective

Pair each attack with its defense and order the handshake steps.

1 Key knowledge and worked examples

■ The pairings

Sniffing – encryption; alteration – MAC; impostor – certificates; replay – fresh randoms ✓. TLS: asymmetric once for the key, symmetric after ✓.

■ Worked example: the properties

Confidentiality (encryption), integrity (MAC), authentication (certificate chain) – drop one, fail differently ✓.

2 Practice

2.1 Which property does a MAC provide? [3]

2.2 Which mechanism defeats an impostor server? [3]

2.3 What do both Hellos contribute against replay? [3]

exercises.lol exercises.com.cn

3 Exam-style questions

3.1 Order these handshake steps and name each: offered suites and a random; chosen suite, a random and a certificate; premaster under the public key; both sides derive keys; both send Finished.

State what each side needs before it can derive the session keys (list the three values). State what a Finished message proves and what the first data byte uses. [8]

3.2 For each attack, name the defense and where it acts: passive sniffing on the wire; in-flight modification of a handshake message; a server impersonating the real one; replay of a captured whole handshake.

State what encrypting without authenticating gives you, in one line. State what HTTPS does and does not make honest. [7]