Name, Firstname / *Nom, Prénom* : SALORD Florian

9,5/20

Software Security – *Sécurité Logicielle*
Quizz #1 – 10/10/2018

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / *Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.*
- No exchange (eraser, pen, responses …) is allowed between students / *Tout échange entre étudiants (gomme, stylo, réponses …) est interdit*
- You must switch off your mobile phone and store it into your bag / *Vous devez éteindre votre téléphone portable et le ranger dans votre sac*
- You have 12 minutes (except 3rd of time : 16 minutes) / *Vous avez 12 minutes (sauf tiers temps: 16 minutes)*
- Write your name, firstname, and group on every sheet / *Ecrivez nom, prénom et groupe sur chaque feuille*
- Selecting all **correct answers** will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. *Entourer toutes les **réponses correctes** à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.*
- **Selecting an incorrect answer will reduce the grade by 1 point.** ***Entourer une réponse incorrecte réduit la note de 1 point.***

Question 1 (3 points)

Which security mechanism(s) can directly implement the Integrity Service ? / *Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service d'Intégrité ?*

(a) Encryption / *le chiffrement*
(b) Privacy enforcement techniques / *les mécanismes de protection de la vie privée*
(c) Digital signature / *la signature numérique*
(d) Hash functions / *les fonctions de hachage*
(e) Logical access control / *le contrôle d'accès logique*

2

Question 2 (3 points)

Digital signature alone : / *La seule signature numérique :*

(a) can ensure the non-repudiation of origin / *peut assurer la non-répudiation d'origine*
(b) can ensure the non-repudiation of destination / *peut assurer la non-répudiation de destination*
(c) requires symmetric encryption / *nécessite le chiffrement symétrique*
(d) requires asymmetric encryption / *nécessite le chiffrement asymétrique*
(e) requires hash functions / *nécessite des fonctions de hachage*
(f) may optionally involve symmetric encryption / peut *s'appuyer optionnellement sur le chiffrement symétrique*
(g) may optionally involve asymmetric encryption / peut *s'appuyer optionnellement sur le chiffrement asymétrique*
(h) may optionally involve cryptographic hash functions / *peut s'appuyer optionnellement sur des fonctions de hachage cryptographique*

2

Question 3 (2 points)

Symmetric block ciphers rely on the following fundamental principles : / *Les chiffres symétriques par blocs s'appuient sur les principes fondamentaux suivants :*

(a) permutation / *des permutations*
(b) corruption / *des corruptions*
(c) substitution / *des substitutions*
(d) aggregation / *des agrégations*
(e) collusion / *des collusions*
(f) alteration / *des altérations*

0

Question 4 (4 points)

For block ciphers: / *Pour des chiffrements par blocs:*

(a) CBC mode offers a good protection / *le mode CBC offre une bonne protection*

2

Name, Firstname / *Nom, Prénom :* .....

(b) ECB mode offers a good protection / *le mode ECB offre une bonne protection*
(c) OFB mode offers a good protection / *le mode OFB offre une bonne protection*
(d) CTR mode offers a good protection / *le mode CTR offre une bonne protection*
(e) CBC mode requires padding / *le mode CBC nécessite du bourrage de données*
(f) OFB mode requires padding / *le mode OFB nécessite du bourrage de données*
(g) In chaining mode, no cleartext can be recovered if a single ciphertext block has been altered / *en cas de chaînage, aucun texte clair ne peut être récupéré si un seul bloc chiffré est altéré*

Question 5 (3 points)

Security: / *La sécurité:*
(a) often improves usability / *améliore souvent l'utilisabilité*
(b) may introduce new vulnerabilities / *peut introduire de nouvelles vulnérabilités*
(c) cannot rely on algorithms known to the public / ne peut s'appuyer sur des algorithmes connus publiquement
(d) should not assume any attacker model / *ne devrait supposer aucun modèle d'attaquant*
(e) may be compromised because of data leaks / *peut être compromise à cause de fuites d'informations*
(f) may be compromised because of faulty logic in software / *peut être compromise à cause de fautes logiques dans un logiciel*
(g) is a cost center for a company / *est un centre de coût pour une entreprise*

2,5

Question 6 (2 points)

Asymmetric cryptography : / *La cryptographie asymétrique:*
(a) consists in matching the strength of the selected cryptographic algorithms with the asymmetry of threats / *consiste à choisir la force des algorithmes cryptographiques retenue comme contremesure avec l'asymétrie des menaces*
(b) is an alternative name for the entropy of a cryptographic key / *est un terme alternatif pour l'entropie d'une clé cryptographique*
(c) is essential for electronic commerce / *est centrale dans le commerce électronique*
(d) requires a public key infrastructure / *nécessite une infrastructure de clé publique*
(e) requires two cryptographic keys instead of a single one / *nécessite deux clés cryptographiques au lieu d'une seule*
(e) requires a single cryptographic key and a cryptographic hash function / *ne nécessite qu'une seule clé cryptographique et une fonction de hachage cryptographique*
(f) is the selection of the cryptographic algorithm based on the attacker model, for instance weak cryptography for a weak attacker like a script kiddie / *est la sélection de l'algorithme cryptographique basée sur le modèle d'attaquant, par exemple un algorithme faible pour un attaquant faible tel qu'un « pirate du dimanche » (script kiddie)*

1

Question 7 (3 points)

A SQL injection / Une *injection SQL :*
(a) is a vulnerability referenced by OWASP / *est une vulnérabilité référencée par l'OWASP*
(b) aims at exploiting the vulnerabilities found in the implementation of a SQL database / *vise à exploiter les vulnérabilités d'implémentation d'une base de données SQL*
(c) is the term depicting the introduction of countermeasures into a Web application that relies on a SQL database / *est le terme décrivant l'introduction de contre-mesures dans une application Web qui s'appuie sur une base de données SQL*
(d) is a threat that has been known for tens of years / *est une menace connue depuis des dizaines d'années*
(e) is a recent threat arising due to Javascript / *est une menace récente à cause de Javascript*
(f) may occur in every Web application / *peut arriver à n'importe quelle application Web*

0