Θέματα Ασφάλειας Τηλεπικοινωνιακών Συστημάτων

1. Αναφέρατε παραδείγματα Τηλεπικοινωνιακών Συστημάτων από:

α. Ενσύρματες Επικοινωνίες
β. Ασύρματες Επικοινωνίες
γ. Δορυφορικές Επικοινωνίες

2. Μεγάλο τμήμα των σύγχρονων τηλεπικοινωνιών χρησιμοποιούν το πρωτόκολλο TCP/IP. Πχ Ασύρματο Τηλέφωνο.

α. Σωστό
β. Λάθος

3. Έστω ένα τηλεπικοινωνιακό σύστημα που χειρίζεται Δημογραφικά δεδομένα. Αναπτύξτε τους λόγους για τους οποίους, αυτά αποτελούν πληροφορία με οικονομική αξία. Ως πληροφορία τα δημογραφικά δεδομένα έχουν διάρκεια ζωής/ισχύος?

4. Αναφέρατε τις πέντε απαιτήσεις Ασφάλειας ενός Πληροφοριακού Συστήματος.

5. Πως διασφαλίζεται η Ακεραιότητα (Integrity) της Πληροφορίας, που χειρίζεται ένα Πληροφοριακό Σύστημα.

6. Ένα Τηλεπικοινωνιακό Πληροφοριακό Σύστημα δέχεται επίθεση DDOS σε ένα κόμβο του, που εξυπηρετεί πελάτες. Καταστρατηγείται η Ασφάλεια των Πληροφοριών του. Υπό ποίαν έννοια?

7. Τι ακριβώς συνιστά η Κρυπτανάλυση?

8. Το ηλεκτρονικό ταχυδρομείο είναι παράδειγμα ασύγχρονης ή σύγχρονης επικοινωνίας? Τεκμηριώστε την απάντησή σας.

9. Έστω το παρακάτω κρυπτογραφικό σχήμα, για επικοινωνία μεταξύ της Alice και του Bob.

Η Alice και ο Bob έχουν δημόσια και ιδιωτικά κλειδιά τα οποία είναι ψηφιακά υπογεγραμμένα από μια ανεξάρτητη αρχή πιστοποίησης.

Η Alice θέλει να στείλει μια κλείδα 256bits για επικοινωνία συμμετρικής κρυπτογράφησης με τον κρυπταλγόριθμο AES με τον Bob. Κρυπτογραφεί την κλείδα με το ιδιωτικο της κλειδί και τη στέλνει στον Bob. Ο Bob λαμβάνει το κρυπτόγραμμα και αποκρυπτογραφεί την κλείδα με τη δημόσια κλείδα της Alice. Στη συνέχεια εγκαθιδρύει τη μυστική επικοινωνία με την Alice, εφόσον έχουν πια εγκαθιδρύσει και κλείδα συνόδου.

Να πούμε πως εδώ δεν απαιτείται έλεγχος ακεραιότητας. Περιγράψτε το πρόβλημα ασφαλείας που προκύπτει από την παραπάνω διαδικασία. Δώστε ένα παράδειγμα που να περιγράφει το πρόβλημα αυτό.

10. Αναφέρατε μια ομοιότητα και μια διαφορά μεταξύ ενός αλγορίθμου Ροής (Stream Cipher) κι ενός αλγορίθμου ομάδας (Block Cipher).

11. Πως τεκμηριώνεται η ασφάλεια των αλγορίθμων ομάδας? Αναπτύξτε σχετικά.

12. Αναφέρατε τρεις ιδιότητες μιας συνάρτησης ιδανικής για μονόδρομη κρυπτογράφηση.

13. Αναφέρατε ένα σχήμα που θα πιστοποιεί αξιόπιστα τον Παραλήπτη και τον Αποστολέα. Θεωρούμε ότι το διαβιβαζόμενο μήνυμα έχει μικρότερο μέγεθος από τις διαθέσιμες κλείδες.

14. Αναφέρατε τρία από τα προβλήματα κρυπτογράφησης Δημόσιου Ιδιωτικού κλειδιού.

15. (Ερωτήσεις όσον αφορά το διαδίκτυο)

16. Βιομετρικά δεδομένα (biometric data) είναι:

α. Διάφορα δεδομένα που αφορούν τα χαρακτηριστικά προσώπου που αποκτήθηκαν ή απεικονίζονται με διάφορους τρόπους.

β. Δεδομένα που προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με νομικά ή άλλα χαρακτηριστικά ή ιδιότητες.

γ. Δεδομένα που προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή άλλα χαρακτηριστικά ενός προσώπου.

17. Τα cookies θεωρούνται δεδομένα προσωπικού χαρακτήρα?

18. Θεωρούνται τα ΄μεταδεδομένα' των text documents, images, videos, spreadsheets, folders, software, κλπ δεδομένα προσωπικού χαρακτήρα?

19. Τα ηλεκτρονικά δίκτυα (υπολογιστών / επικοινωνιών) εταιριών απειλούνται από:

α. Εξωτερικούς εισβολείς μόνο
β. Εσωτερικούς εισβολείς μόνο
γ. Και από τους δυό ανωτέρω
δ. Δεν απειλούνται όταν έχουν παρθεί μέτρα.

20. Εξαφανίζουν οι πλήρεις δοκιμές στην πληροφορική όλα τα λάθη των εφαρμογών?

21. Γιατί μπορεί να χρησιμοποιείται η τεχνολογία honeynet(s)/honeyspot(s)?

α. Για να προσκαλεί χρήστες στα συστήματα της εταιρίας
β. για να διώχνει χρήστες από τα συστήματα της εταιρίας
γ. Για να παγιδεύει εισβολείς στα συστήματα της εταιρίας
δ. Για να επιτρέπει την επικοινωνία με την εταιρία.

22. Η τεχνολογία SSL (Secure Sockets Layer) χρησιμοποιείται για την κρυπτογράφηση:

α. Αρχείων σε servers
β. Passwords σε βάσεις δεδομένων
γ. Δεδομένων που μεταβιβάζονται μέσω δικτύων
δ. Δεδομένων σε βάσεις δεδομένων.

23. Τα bots είναι επικίνδυνα?

24. Τα μέτρα προστασίας για τα συστήματα πληροφορικής προστατεύουν:
(απαντήστε/τεκμηριώστε/αναπτύξτε και τις τρείς υποερωτήσεις)

α. Απόλυτα όλο το λογισμικό
β. Απόλυτα όλο το υλικό (hardware)
γ. Σχετικά όλα τα αγαθά της πληροφορικής.

25. Εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα προσώπου είναι:

α. Γενετικά δεδομένα
β. Βιομετρικά δεδομένα
γ. Ασφαλή κι ευαίσθητα δεδομένα προσωπικού χαρακτήρα

26. Ποιο από τα παρακάτω ΔΕΝ αποτελεί κύριο τμήμα ενός τηλεπικοινωνιακού συστήματος?

α. Τερματικό ή Η/Υ
β. Λογισμικό Δικτύου, ή Λειτουργικό Σύστημα
γ. Εξυπηρετητής Ονοματολογίας Δεδομένων (Domain Name Server - DNS)

27. Ποιο μπορεί να θεωρείται το πιο ευάλωτο τμήμα ενός τοπικού δικτύου (LAN), εξαιτίας των ασθενών χαρακτηριστικών ασφαλείας του?

α. Δρομολογητές (Routers)
β. Προσαρμογείς Δικτύου (Network Adapters - NICs)
γ. Κανάλι επικοινωνίας (Communications Channel)
δ. Προσωπικός Υπολογιστής (Personal Computer - PC)

28. Ποιος τύπος καλωδίωσης θεωρείται δύσκολος για επισύνδεση (υποκλοπή)?

α. Ασύρματος
β. Συνεστραμμένο ζεύγος (twisted pair wiring)
γ. Οπτική Ίνα
δ. Ομοαξονικό καλώδιο

29 Οι ..... επικοινωνίες βασίζονται περισσότερο σε συστήματα συγχρονισμού ρολογιού για να στείλουν και να λάβουν δεδομένα, παρά σε bits έναρξης και παύσης

α. Ασύγχρονες
β. Αναλογικές
δ. Σύγχρονες
ε. Ψηφιακές.

30. Τα bits πλειοψηφίας τυπικά χρησιμοποιούνται για:

α. Έλεγχο Σφαλμάτων
β. Συγχρονισμό ρολογιού
δ. Είσοδο και έξοδο δεδομένων
ε. Checksum

31. Ποια από τις παρακάτω επικοινωνίες είναι τυπικά ταχύτερη?

α. Ασύγχρονη
β. Σύγχρονη
δ. Χαλκός
ε. Ομοαξονική

32. Ποιο από τα παρακάτω ΔΕΝ είναι ένα από τα τρία στοιχεία που απαιτούνται όταν εφαρμόζουμε μια ασφαλή σύνδεση εξ' αποστάσεως?

α. Ακριβής Αυθεντικοποίηση χρήστη
β. Κατάλληλη φυσική ασφάλεια στην ιστοσελίδα
γ. Προστασία ενάντια στις υποκλοπές
δ. Περιορισμός των χρηστών στις αναγκαίες μόνο δικτυακές υπηρεσίες

33. Ποια είναι η καλύτερη μέθοδος άμυνας εναντίον στο network sniffing?

α. Χρήση Switch
β. Χρήση ενσύρματων δικτύων και απαγόρευση ασύρματων συνδέσεων

γ. Χρήση πύλης εισόδου (gateway)
δ. Κρυπτογράφηση

34. Οι ιοί θέλουν ένα αρχείο-οικοδεσπότη για να αντιγραφούν και να εξαπλωθούν στη συνέχεια.
α. Σωστό
β. Λάθος
Τεκμηριώστε την απάντησή σας

35. Τα σκουλήκια worms δύνανται να αναπαραχθούν από μόνα τους.
α. Σωστό
β. Λάθος
Τεκμηριώστε την απάντησή σας

36. Οι δούρειοι ίπποι αναπαράγονται από μόνοι τους.
α. Σωστό
β. Λάθος
Τεκμηριώστε την απάντησή σας

37. Ποιος από τους παρακάτω έχει σχεδιαστεί ώστε να παρέχει μονόδρομη κρυπτογράφηση?
α.SHA
β. AES
γ. RSA
δ. DES

38. Ποια από τις προϋποθέσεις ασφάλειας πληροφοριακών συστημάτων καταστρατηγείται σε μια επίθεση DDOS? Τεκμηριώστε την απάντησή σας.

39. Ο αλγόριθμος Diffie-Hellman βασίζεται σε ιδιωτική και δημόσια κλείδα για κρυπτογράφηση και αποκρυπτογράφηση.
α. Σωστό
β. Λάθος
Τεκμηριώστε την απάντησή σας.

40. Πως ονομάζεται η τεχνική του να κρύψει κανείς αν μυστικό μήνυμα μέσα σε ένα άλλο μήνυμα ή αρχείο?

41. Τι ακριβώς είναι το phishing?

42. Τι γνωρίζετε για τα rogues και τα scarewares?

43. Τι είναι Κοινωνική Μηχανική (Social Engineering)? Αναφέρατε δύο τεχνικές της.

44. Αναπτύξτε τι γνωρίζετε σχετικά με το pretexting ως τεχνική της Κοινωνικής Μηχανικής.

45. Σε τι συνίσταται και που χρησιμοποιείται ακριβώς το tailgagint στην Κοινωνική Μηχανική?

46. Πρόσφατα είχαμε το παράδειγμα της AEGEAN. Χρήστες του Facebook, και άλλων μέσων κοινωνικής δικτύωσης, λάμβαναν ενημέρωση για συμμετοχή σε διαγωνισμό με δώρο εισιτήρια. Κάποιοι εξ' αυτών εμφανίζονταν να κερδίζουν δωρεάν εισιτήρια για δημοφιλείς προορισμούς. Μπορούσαν να τυπώσουν μάλιστα τα εισιτήριά τους.
α. Σε τι ακριβώς συνίσταται το παραπάνω γεγονός?
β. Ποιες ήταν οι συνέπειες για την εταιρία? Τι βλάπτεται περισσότερο?

γ. Τι νομίζετε ότι κέρδιζαν εκείνοι που έκαναν την απάτη?

δ. Αναπτύξτε, τι θα κάνατε ως εκπρόσωπος της AEGEAN εάν σας ενημέρωναν για την απάτη αυτή. (πχ Τόσο ενέργειες, όσο και ένα επικοινωνιακό αντίμετρο).

47. Ξαφνικά βλέπετε μια ιστοσελίδα στο Facebook με τα προσωπικά σας στοιχεία, τη φωτογραφία σας, αλλά και φωτογραφίες της προσωπικής σας ζωής. Ο χρήστης της περσόνας που υποδύεται εσάς, μπαίνει και σχολιάζει σε διάφορα φόρα συζητήσεων συχνά με όχι τόσο κολακευτικό τρόπο για τον ίδιο. Δείχνει χωρίς να φοβάται ότι συμπαθεί ακραίες οργανώσεις και ακραίες ιδέες.

Οι όχι τόσο στενοί φίλοι σας, αρχίζουν να απομακρύνονται από εσάς. Στη συνέχεια ο προϊστάμενος στην εργασία σας, ματαιώνει την υποσχεθείσα ανάθεση σε εσάς μιας σημαντικής για την επαγγελματική σας εξέλιξη υπόθεσης.

Πως αναλύετε την ανωτέρω κατάσταση? Τι ενέργειες κάνετε?

48. Ένα site που επισκέπτεστε συχνά, διοργανώνει έναν διαγωνισμό με δώρο ένα ταξίδι στην Βιέννη για τα Χριστούγεννα. Εισέρχεστε στο χώρο και λαμβάνετε μέρος στον διαγωνισμό. Το site σας οδηγεί σε μια φόρμα συμπλήρωσης στοιχείων. Ζητάει:

α. Το ονοματεπώνυμό σας.
β. Το πατρώνυμο
γ. Ημερομηνία γέννησης
δ. Τηλέφωνο επικοινωνίας
ε. Αριθμό ταυτότητας
στ. ΑΦΜ
ζ. Email

Η φόρμα δεν περιέχει τίποτε άλλο παρά μόνο τα λογότυπα για την συμπλήρωση των στοιχείων. Προβαίνετε στην συμπλήρωση? Αιτιολογήστε την απάντησή σας.

49. Λαμβάνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, όπου ένας παλιός σας φίλος σας ενημερώνει για την παρουσία του και τη διάθεσή του για επανασύνδεση. Σας στέλνει μια φωτογραφία συνημμένη από παλιά.

α. Τι ενέργειες κάνετε?
β. Ανοίγετε τη φωτογραφία?
Αιτιολογήστε την απάντησή σας.

50. Ανακαλύπτετε ένα πρόσωπο από το παρελθόν σας και θέλετε επανασύνδεση μαζί του και για επαγγελματικούς και για προσωπικούς λόγους. Ο μόνος τρόπος να επικοινωνήσετε μαζί του είναι το ηλεκτρονικό του ταχυδρομείο (gmail).

α. Τι ενέργειες κάνετε?
β. Πως θα αποδείξετε σε αυτόν/ήν ότι δεν είστε ρομπότ ή ότι πράγματι είστε αυτός που είστε?
Αιτιολογήστε την απάντησή σας.