



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ
Τμήμα Πληροφορικής και Τηλεπικοινωνιών

Νικόλαος Κολοκοτρώνης
Καθηγητής

Διάρκεια εξέτασης
2,5 ώρες

Ασφάλεια Συστημάτων

ΕΞΕΤΑΣΤΙΚΗ ΦΕΒΡΟΥΑΡΙΟΥ 2025-26

Θέμα 1ο (2.0 μονάδες)

Ποιο είναι το τρίπτυχο της ασφάλειας; Να περιγράψετε (λεπτομερώς):

- (α) Πιθανά παραδείγματα/τρόπους ενσωμάτωσης σχετικών μηχανισμών ασφάλειας σε λειτουργικά συστήματα (π.χ. Linux και Windows), και
- (β) Μια επίθεση για καθένα παράδειγμα μηχανισμού ασφάλειας.

Θέμα 2ο (2.0 μονάδες)

Εξηγήστε τον τρόπο που λειτουργεί η πιστοποίηση χρηστών μέσω συνθηματικών. Με ποιο μηχανισμό προστατεύονται τα συνθηματικά χρηστών στο Unix; (θεωρήστε ως παράδειγμα την υλοποίηση της `crypt(3)` συνάρτησης) Να παρουσιάσετε αναλυτικά δυο τεχνικές τιθέσεων ανάκτησης συνθηματικών καθώς και μέτρα προστασίας.

Θέμα 3ο (3.0 μονάδες)

Να περιγράψετε τη δομή, τη λειτουργία, και τον τρόπο που συνδέονται μεταξύ τους:

Τα ψηφιακά πιστοποιητικά X.509 (εξηγήστε και τους αναγκαίους ελέγχους που πραγματοποιούνται για να εμπιστευτούμε ένα πιστοποιητικό X.509).

Το πρότυπο των λιστών ανακληθέντων πιστοποιητικών CRL (εξηγήστε και τα θέματα που ανακύπτουν ως προς τη διαχείριση καθώς και προτάσεις επίλυσης)

Το πρωτόκολλο OCSP λήψης της κατάστασης ενός ψηφιακού πιστοποιητικού X.509.

Θέμα 4ο (3.0 μονάδες)

Να πείξετε ότι δυο χρήστες θέλουν να διασφαλίσουν την επικοινωνία μέσω IPsec. Τότε:

α) Πρέπει να χρησιμοποιηθεί το IPsec (tunnel ή transport) και γιατί;

β) Προστατεύονται τα IPv4 πακέτα με IPsec AH στην ανωτέρω κατάσταση;

γ) Περιγράψτε το μηχανισμό του IPsec για προστασία σε replay attacks.

δ) Εξηγήστε το ρόλο των συσχετίσεων ασφάλειας (SAs) και πως πραγματοποιείται η επικοινωνία των εισερχόμενων και εξερχόμενων πακέτων.

ε) Να...