ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

(ΘΕΜΕΛΙΩΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ) (2014-15)

ver. 1.2/20.09.2014

1. Ενδεικτική δομή και περιεχόμενο μαθήματος

Θέμα διάλεξης	Διάρκεια (x 45')	Διδακτικό μέσο	Βιβλιογραφία αναφοράς και συμπληρωματικό εκπαιδευτικό υλικό	
			Μονογραφίες, εγχειρίδια, άρθρα κλπ.	e-Υλικό (www.cis.aueb.gr)
Εννοιολογική Θεμελίωση: Βασικές έννοιες και ορισμοί. Σχέσεις και διαφοροποιήσεις. Ανάλυση και απεικόνιση μέσω διαγραμμάτων E-R.	2	Διάλεξη		AUEB_ISS_Terminology_v21.pdf
	1	Ντοκιμαντέρ		Ντοκιμαντέρ: *Security and Safety* (BBC, 2004)
Αποτίμηση Επικινδυνότητας: Στόχοι, δυνατότητες και περιορισμοί τεχνικών ανάλυσης και διαχείρισης επικινδυνότητας. Παραδείγματα τεχνικών (CRAMM, OCTAVE κλπ.).	2	Διάλεξη	Κάτσικα Σ., Γκρίτζαλη Δ., Γκρίτζαλη Σ., *Ασφάλεια Πληροφοριακών Συστημάτων*, σελ. 335-75, Εκδόσεις Νέων Τεχνολογιών (3η έκδοση), 2010. C. Pfleeger, *Security in Computing*, Prentice Hall (6th ed.), 2012.	AUEB_ISS_Risk_Analysis_v12.pdf
	2	Εργαστήριο		*CCTA Risk Analysis and Management Methodology* (CRAMM) (ver. 5.1)
Έλεγχος Προσπέλασης: Ταυτοποίηση, αυθεντικοποίηση, εξουσιοδότηση, χρήση μεθόδων CAPTCHA, αγνωστικά και πιθανοτικά πρωτόκολλα, βιομετρικές τεχνολογίες.	3	Διάλεξη	R. Anderson, *Security Engineering*, Wiley (2nd ed.), 2008. D. Gollmann, *Computer Security*, pp. 19-44, Wiley (3rd ed.), 2011.	AUEB_ISS_Access_Control_v11.pdf AUEB_ISS_540_Biometrics_General.pdf AUEB_ISS_570_Biometrics_Tech.pdf
Εισαγωγή στην Κρυπτολογία: Εννοιολογική θεμελίωση. Συμμετρική και Ασύμμετρη Κρυπτογραφία. Υποδομές Δημόσιου Κλειδιού (PKI). Ψηφιακές υπογραφές/πιστοποιητικά. Κρυπτανάλυση. Αξιοποίηση Κρυπτολογίας.	3	Διάλεξη	R. Anderson, *Security Engineering*, Wiley (2nd ed.) 2008. Γκρίτζαλη Σ., Κάτσικα Σ., Γκρίτζαλη Δ., *Ασφάλεια Δικτύων Υπολογιστών*, σελ. 69-141, Παπασωτηρίου (4η έκδοση), 2011. C. Pfleeger, *Security in Computing*, Prentice Hall (6th ed.), 2012.	AUEB_ISS_Cryptography_v1.pdf
	2	Εργαστήριο		1. Προετοιμασία και ενημέρωση φοιτητών για την εγκατάσταση των εργαλείων που θα χρησιμοποιηθούν στο εργαστήριο. 2. Εφαρμογή και αξιολόγηση κρυπτοσυστημάτων (με χρήση CryptTool)
	1	Ντοκιμαντέρ + case study		Ντοκιμαντέρ: *Codes* (History Channel, 2008)

Θέμα διάλεξης	Διάρκεια (x 45')	Διδακτικό μέσο	Βιβλιογραφία αναφοράς και συμπληρωματικό εκπαιδευτικό υλικό	
			Μονογραφίες, εγχειρίδια, άρθρα κλπ.	**e-Υλικό** (www.cis.aueb.gr)
Ιομορφικό Λογισμικό: Οριοθέτηση και ταξινόμηση. Δούρειοι ίπποι, αναπαραγωγοί (worms), προγράμματα ιοί. Αλγοριθμική προσέγγιση. Θεμελιώσεις: Cohen (Turing Machines), Adleman (αριθμητική Goedel), Kephart (κατευθυνόμενοι γράφοι). Πολιτικές, μέθοδοι και τεχνικές προληπτικής και κατασταλτικής αντιμετώπισης.	3	Διάλεξη	Adleman L., "An Abstract Theory of Computer Viruses", in Hoffman L. (Ed.), *Rogue Programmes*, Van Nostrand, pp. 307-323, 1990. Cohen F., "Computational aspects of computer viruses", *Computers and Security*, Vol. 8, No. 4, pp. 325-344, 1989. Kephart J., White S., "Directed graph epidemiological models of computer viruses", in *Proc. of the 1991 IEEE Symposium on Research in Security and Privacy*, pp. 343-359, 1991.	AUEB_ISS_Viral_Software_v11.pdf
	2	Εργαστήριο		Έλεγχος αρχείων για την παρουσία ιομορφικού κώδικα. Μελέτη περίπτωσης: Ανάλυση αναπαραγωγού (worm).
Ασφάλεια στο Διαδίκτυο, Hackers και Hacking: Θεωρία τεσσάρων ασυνεχειών. Μορφότυποι hackers. Ethics of Security. Hacking και Hacktivism. Ασφάλεια ασύρματων τοπικών δικτύων (WLAN). Λογισμικό αξιολόγησης και ελέγχου ασφάλειας (Openvas|Nessus, Metasploit, Nmap, Aircrack-ng κλπ.).	4	Διάλεξη	[1]Γκρίτζαλη Δ., *Αυτονομία και Πολιτική Ανυπακοή στον Κυβερνοχώρο*, σελ. 295-365, Παπασωτηρίου (2η ανατύπωση), 2011. Γκρίτζαλη Σ., Κάτσικα Σ., Γκρίτζαλη Δ., *Ασφάλεια Δικτύων Υπολογιστών*, Παπασωτηρίου (4η έκδοση),, 2011. Robins K., Webster F., *Η Εποχή του Τεχνοπολιτισμού*, Καστανιώτης, 2002.	AUEB_ISS_Hacking_v11.pdf
	7	Εργαστήριο		Εξειδικευμένο δημόσια διαθέσιμο λογισμικό ασφάλειας υπολογιστών, δικτύων και εφαρμογών Ιστού (nmap, nessus, metasploit, w3af, mutillidae).
Προστασία Προσωπικών Δεδομένων: Ιδιωτικότητα (privacy) και προστασία προσωπικών δεδομένων. Θεσμικό πλαίσιο (Ν. 2472/1997). Οπτική, ρόλος και ευθύνη των Πληροφορικών.	1	Διάλεξη	Κάτσικα Σ., Γκρίτζαλη Δ., Γκρίτζαλη Σ., *Ασφάλεια Πληροφοριακών Συστημάτων*, σελ. 443-518, Εκδόσεις Νέων Τεχνολογιών (3η έκδοση), 2010. Νόμος 2472/1997, *Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα*, ΦΕΚ 50Α', 10.04.1997 (και συμπληρώσεις του).	AUEB_ISS_Data_Protection_v11.pdf
	1	Μελέτη Περίπτωσης		ΜΠ-1: Βιομετρικές Τεχνολογίες ΜΠ-2: Ασφάλεια ΟΠΣ Νοσοκομείου
	1	Ντοκιμαντέρ + case study		Ντοκιμαντέρ: *DNA and personal data protection: Risks and promises* (BBC, 2010)

[1] Διανέμεται δωρεάν στους φοιτητές.

Θέμα διάλεξης	Διάρκεια (x 45')	Διδακτικό μέσο	Βιβλιογραφία αναφοράς και συμπληρωματικό εκπαιδευτικό υλικό	
			Μονογραφίες, εγχειρίδια, άρθρα κλπ.	**e-Υλικό** (www.cis.aueb.gr)
Ασφάλεια στο Απανταχού Υπολογίζειν: Ασφάλεια στο Cloud Computing. Internet of Things. Στρατηγικές ασφάλειας και ιδιωτικότητας στην Κοινωνία της Πληροφορίας και της Γνώσης. Εξειδικευμένα πεδία εφαρμογής ασφάλειας και προάσπισης ιδιωτικότητας (OSN, VoIP, κρίσιμες υποδομές κλπ.).	2	Διάλεξη	Γκρίτζαλη Δ., *Αυτονομία και Πολιτική Ανυπακοή στον Κυβερνοχώρο*, σελ. 85-199, Παπασωτηρίου (2η ανατύπωση), 2011. Γκρίτζαλης Δ. , Μήτρου Ν., Σκουλαρίδου Β., *Προστασία Κρισίμων Πληροφοριακών και Επικοινωνιακών Υποδομών της Δημόσιας Διοίκησης*, e-Goverment Forum, Σεπτέμβρης 2008. Gritzalis D., Theoharidou M., Dritsas S., Marias G., "Ambient Intelligence: The Promise, the Price, and the Social Disruption", *Review Report Series*, AUEB/REV-0106/v2.4, March 2006.	AUEB_ISS_Secure_WLAN_v12.pdf
	2	Ντοκιμαντέρ (+ case study) και Κινηματογραφική ταινία (+ συζήτηση)		Ντοκιμαντέρ: *Cyberterrorism* (History Channel, 2005) Κινηματογραφικές ταινίες: (α). *The China Syndrome* (1979) (β). *The Lives of Others* (2006)

2. Αντικείμενα εργαστηριακής εκπαίδευσης

Εργαστηριακές διαλέξεις	Διάρκεια (x 45')	Στόχος	Προσέγγιση και μέσα	
			Διδακτική προσέγγιση	**Εργαλεία λογισμικού/υλικού**
Αποτίμηση Επικινδυνότητας	2	CCTA Risk Analysis and Management Methodology (CRAMM)	Παρουσίαση	CRAMM
Προπαρασκευαστικό μάθημα: Οδηγίες εγκατάστασης λογισμικού	1	Ενημέρωση φοιτητών για την εγκατάσταση των ειδικών εργαλείων λογισμικού που θα χρησιμοποιηθούν στο εργαστήριο.	Παρουσίαση	-
Αναγνώριση και ανάλυση δικτύου	2	Ανεύρεση ενεργών κόμβων εσωτερικού δικτύου και αναγνώριση υπηρεσιών που προσφέρουν.	Επίδειξη-χρήση	Nmap
Αναγνώριση ευπαθειών υπολογιστικού συστήματος	1	Ανεύρεση και απαρίθμηση διαθέσιμων ευπαθειών σε υπολογιστικά συστήματα.	Επίδειξη-χρήση	Tenable Nessus
Ανάλυση ευπαθειών/τρωτοτήτων	2	Παρουσίαση τεχνικών παραβίασης ενός συστήματος με εκμετάλλευση γνωστών αδυναμιών.	Επίδειξη-χρήση	Metasploit Framework

Ασφάλεια εφαρμογών ιστού	2	Παρουσίαση τεχνικών παραβίασης σε εφαρμογές ιστού	Επίδειξη-χρήση	Mutillidae, w3af
Έλεγχος ιομορφικού κώδικα	2	Έλεγχος αρχείων για την παρουσία ιομορφικού κώδικα. Μελέτη περίπτωσης: Ανάλυση αναπαραγωγού (worm).	Παρουσίαση-ανάλυση	Virus scanners, manual analysis, Sandboxie, BSA
Κρυπτογραφικές τεχνικές	1	Παρουσίαση και ανάλυση κλασικών και σύγχρονων κρυπτογραφικών τεχνικών.	Επίδειξη-χρήση	Cryptool
Στεγανογραφία ήχου	1	Ανάλυση τεχνικών απόκρυψης μηνυμάτων μέσα σε ήχο.	Ανάλυση	-

3. Αξιολόγηση επίδοσης φοιτητών

2.1 Γραπτή (τελική και επαναληπτική) **εξέταση**	**Βαρύτητα**	**Σχόλια**
Πρέπει να απαντηθεί, μέσα σε σχετικά περιορισμένο χρόνο (~1.5 ώρα), ένας αριθμός θεμάτων, τα οποία περιλαμβάνουν (ενδεικτικά): (α). Ερωτήσεις κρίσης και σύνθεσης, (β). Ερωτήσεις σύγκρισης κα αξιολόγησης, (γ). Περιγραφή και ανάλυση τεχνολογιών, μεθόδων, τεχνικών κλπ.	**40%**	Για να θεωρηθεί επιτυχών ένας φοιτητής θα πρέπει να αξιολογηθεί και στη γραπτή εργασία και στο εργαστήριο και στην τελική εξέταση (σε κάθε μορφή αξιολόγησης, ξεχωριστά) με βαθμό ≥50%.
2.2 Γραπτή εργασία	**Βαρύτητα**	**Σχόλια**
Εκπόνηση γραπτής εργασίας (3-4.000 λέξεων). Θα υπάρξουν δύο *εναλλακτικά* θέματα. Το ένα θα έχει *πρακτικό-προγραμματιστικό* χαρακτήρα. Το δεύτερο θα αφορά *κριτική (βιβλιογραφική) επισκόπηση*. Η γραπτή εργασία αποσκοπεί στη συστηματική επεξεργασία και εμβάθυνση σε κάποιο θεωρητικό ή πρακτικό ζήτημα Ασφάλειας στις ΤΠΕ.	**30%**	Η εργασία είναι υποχρεωτική. Εκπονείται από ομάδες 2-3 φοιτητών, μέσα σε χρονικό διάστημα 3-4 βδομάδων. Ο βαθμός της εργασίας κατοχυρώνεται μόνο για τις 2 (κανονικές) εξεταστικές περιόδους της συγκεκριμένης χρονιάς.
2.3 Εργαστηριακές ασκήσεις	**Βαρύτητα**	**Σχόλια**
Επίλυση εξειδικευμένων ασκήσεων και απάντηση σε τεχνικές ερωτήσεις στο Εργαστήριο, συνήθως με χρήση εξειδικευμένου λογισμικού. Οι εργαστηριακές ασκήσεις αποσκοπούν στην εξοικείωση των φοιτητών με αμιγώς τεχνικά ζητήματα Ασφάλειας στις ΤΠΕ.	**30%**	Υποχρεωτικη εξέταση (στο Εργαστήριο) φοιτητών, ατομικά ή σε ομάδες. Ο βαθμός των ασκήσεων κατοχυρώνεται μόνο για τις 2 (κανονικές) εξεταστικές περιόδους της συγκεκριμένης χρονιάς.