Βιογραφικό Σημείωμα Παναγιώτη Ι. Κοτζανικολάου

Ι. Προσωπικά στοιχεία

- Επώνυμο: Κοτζανικολάου
- Όνομα: Παναγιώτης
- Ημερομηνία Γέννησης: 29 Οκτωβρίου 1974
- Διεύθυνση Κατοικίας: Δρίσκου 11-13, Γαλάτσι, 11 46, Αθήνα
- Τηλ. Επικοινωνίας: 210 414 2123 (γραφείου)
- Email: pkotzani@unipi.gr

ΙΙ. Σπουδές

- **Διδάκτορας Τμήματος Πληροφορικής Πανεπιστημίου Πειραιώς**

Νοέμβριος 1998 – Ιανουάριος 2003: Υποψήφιος Διδάκτορας Πανεπιστημίου Πειραιώς στο Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς.
Ημερομηνία Αναγόρευσης: Μάιος 2003.

- **Πτυχιούχος Τμήματος Πληροφορικής Πανεπιστημίου Πειραιώς**:

1993 - 1998: Φοίτηση στο Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς.
Ημερομηνία Αποφοίτησης: Σεπτέμβριος 1998.

ΞΕΝΕΣ ΓΛΩΣΣΕΣ

- **Αγγλική**: Proficiency in English, 1993.

ΙΙΙ. Επαγγελματική δραστηριότητα

ΙΙΙ.1 Επαγγελματικές θέσεις

1. Ιανουάριος 2019 – σήμερα: Μόνιμος Επίκουρος Καθηγητής του Τμήματος Πληροφορικής, της Σχολής Τεχνολογιών Πληροφορικής και Επικοινωνιών του Πανεπιστημίου Πειραιώς, στο γνωστικό αντικείμενο «Ασφάλεια και Ιδιωτικότητα σε Δίκτυα Νέας Γενιάς» (ΦΕΚ Διορισμού 1580/τ.Γ΄/31-12-2018)
2. Μάιος 2015 – Δεκέμβριος 2018: Επίκουρος Καθηγητής (με θητεία) του Τμήματος Πληροφορικής, της Σχολής Τεχνολογιών Πληροφορικής και Επικοινωνιών του Πανεπιστημίου Πειραιώς, στο γνωστικό αντικείμενο «Ασφάλεια και Ιδιωτικότητα σε Δίκτυα Νέας Γενιάς» (ΦΕΚ Διορισμού 443/τ.Γ΄/19-6-2015)
3. Ιούνιος 2010 – Μάιος 2015: Λέκτορας Τμήματος Πληροφορικής Πανεπιστημίου Πειραιώς στο γνωστικό αντικείμενο "Ασφάλεια και Ιδιωτικότητα σε Δίκτυα Νέας Γενιάς» (ΦΕΚ Διορισμού 466/τ.Γ΄/7-6-2010)
4. Ιανουάριος 2005 – Ιούνιος 2010: Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.). Ειδικό Επιστημονικό Προσωπικό στη Διεύθυνση Διασφάλισης του Απορρήτου στις Διαδικτυακές Επικοινωνίες. (*Αντικείμενο Εργασίας: Διασφάλιση του απορρήτου διαδικτυακών επικοινωνιών. Έλεγχος συμμόρφωσης των Παρόχων Πρόσβασης στο Διαδίκτυο (ISPs) με το Κανονιστικό Πλαίσιο. Έλεγχος και αυτοψίες στις εγκαταστάσεις των Παρόχων Πρόσβασης στο Διαδίκτυο. Διερεύνηση καταγγελιών.)*
5. Ιανουάριος 2002 – Φεβρουάριος 2003: Encode S.A. Σύμβουλος Ασφάλειας Πληροφοριακών Συστημάτων στην εταιρία παροχής συμβουλευτικών υπηρεσιών

Ενδεικτικά Έργα:

- *"Ανάπτυξη Προφίλ Κινδύνου για τη Σύνδεση στο Extranet"* για Ελληνικό τραπεζικό ίδρυμα.
- *"Ανάλυση Διαχείρισης Κρυπτογραφικών Κλειδιών και Έλεγχος Συμβατότητας με τις προδιαγραφές των ISO 8732 και Visa PIN Security Standards"* για τραπεζικό ίδρυμα της Σ. Αραβίας.
- *"Ανάλυση Πληροφοριακού Κινδύνου"* για Ελληνική ασφαλιστική εταιρία.
- *"Εκπαίδευση σε Θέματα Ψηφιακών Υπογραφών, Πιστοποιητικών και Υποδομών Δημόσιου Κλειδιού"* για Ελληνικό τραπεζικό ίδρυμα.
- *"Ανάπτυξη Πολιτικής Ασφάλειας"* για Ελληνική ασφαλιστική εταιρία.
- *"Ανάπτυξη Πολιτικής Ασφάλειας"* για Ελληνικό τραπεζικό ίδρυμα.
- *"Ανάπτυξη Σχεδίου Έκτακτης Ανάγκης και Συνέχειας Λειτουργίας"* για ασφαλιστική εταιρία.

ΙΙΙ.2 Διδακτική εμπειρία

1. Μάιος 2015- Δεκέμβριος 2018: Επίκ. Καθηγητής (με θητεία) στο Τμήμα Πληροφορικής, της Σχολής Πληροφορικής και Επικοινωνιών του Πανεπιστημίου Πειραιώς. Προπτυχιακά Μαθήματα: «Ασφάλεια Πληροφοριακών Συστημάτων» (7ο εξάμηνο), «Ασφάλεια Δικτύων» (8ο εξάμηνο), «Προγραμματισμός στο Διαδίκτυο και στον Παγκόσμιο Ιστό» (4ο εξάμηνο), «Λειτουργικά Συστήματα» (3ο εξάμηνο). Μεταπτυχιακά μαθήματα: "Ασφάλεια Δικτυακών Συστημάτων", "Ανάλυση Κρυπτογραφικών Πρωτοκόλλων", "Έλεγχος Εισβολών Δικτύων και Συστημάτων" (ΠΜΣ Προηγμένα Συστήματα Πληροφορικής), "Ασφάλεια Πληροφοριών" (ΠΜΣ Πληροφορική).
2. Ιούλιος 2010 – Μάιος 2015: Λέκτορας στο Τμήμα Πληροφορικής Πανεπιστημίου Πειραιώς. Μαθήματα: «Ασφάλεια Πληροφοριακών Συστημάτων» (7ο εξάμηνο), «Τεχνολογία και Πολιτικές Ασφάλειας» (7ο εξάμηνο), «Ασφάλεια Δικτύων» (8ο εξάμηνο), «Προγραμματισμός συστημάτων» (2ο εξάμηνο), «Δίκτυα Υπολογιστών» (4ο εξάμηνο), «Ασφάλεια Πληροφοριών», (ΜΠΣ – Πληροφορική), «Ασφάλεια Δικτύων και Πληροφοριακών Συστημάτων» (ΠΜΣ Προηγμένα συστήματα πληροφορικής).
3. Σεπτέμβριος 2007 – Φεβρουάριος 2008: Διδάσκων Π.Δ. 407 στη βαθμίδα του Λέκτορα στο Τμήμα Πληροφορικής Πανεπιστημίου Πειραιώς, για το μάθημα επιλογής 7ου εξαμήνου *«Τεχνολογία και Πολιτικές Ασφάλειας»*.
4. Σεπτέμβριος 2006 – Φεβρουάριος 2007: Διδάσκων Π.Δ. 407 στη βαθμίδα του Λέκτορα στο Τμήμα Πληροφορικής Πανεπιστημίου Πειραιώς, για το μάθημα επιλογής 7ου εξαμήνου *«Τεχνολογία και Πολιτικές Ασφάλειας»*.
5. Σεπτέμβριος 2005 – Φεβρουάριος 2006: Διδάσκων Π.Δ. 407 στη βαθμίδα του Λέκτορα στο Τμήμα Πληροφορικής Πανεπιστημίου Πειραιώς, για το μάθημα επιλογής 7ου εξαμήνου *«Τεχνολογία και Πολιτικές Ασφάλειας»*.
6. Φεβρουάριος 2005 – Ιούλιος 2005: Διδάσκων Π.Δ 407 στη βαθμίδα Λέκτορα στο Τμήμα Πληροφορικής Πανεπιστημίου Πειραιώς για το μάθημα *«Ασφάλεια Δικτύων και Πληροφοριακών Συστημάτων»*, του Μεταπτυχιακού Προγράμματος Σπουδών «Προηγμένα Συστήματα Πληροφορικής».
7. Οκτώβριος 2004 – Φεβρουάριος 2005: Διδάσκων Π.Δ. 407 στη βαθμίδα Λέκτορα στο Τμήμα Πληροφορικής Ιονίου Πανεπιστημίου, για το μάθημα 1ου εξαμήνου *«Εισαγωγή στον Προγραμματισμό»* και για το μάθημα *«Εισαγωγή στην Κοινωνία της Πληροφορίας»*.

ΙΙΙ.3 Συμμετοχή σε έργα Ε&ΤΑ

1. Φεβρουάριος 2019 – Αύγουστος 2022: **Τεχνικός Διευθυντής** του έργου CyberSec4Europe, το οποίο χρηματοδοτείται από την ΕΕ (Horizon2020).
2. Ιούλιος 2018 – Ιούλιος 2021: **Επιστημονικός Υπεύθυνος** του έργου «Ανάπτυξη Μεθοδολογιών και Ενσωματωμένων Λύσεων Ασφάλειας για Τεχνολογίες Internet of Things σε ηλεκτρονικές Υπηρεσίες Υγείας - ΜΕΛΙΤΥ» (κωδικός έργου Τ1ΕΔΚ-01958), Δράση Ερευνώ-Δημιουργώ-Καινοτομώ.

3. Ιανουάριος 2017-Ιούλιος 2017: **Επιστημονικός Υπεύθυνος** στο έργο *"Word of Mouth"* (Ιδιωτική χρηματοδότηση / Google DNI)

WoM is a prototype project funded by_Google DNI and the aim of the project is to develop a prototype mobile application that will allow the peer-to-peer spreading of Geo-location news, while at the same time protecting the location and other privacy characteristics of the users.

4. Ιούνιος 2015 – Μάιος 2018: Συμμετοχή στο έργο OPERANDO (Ευρωπαϊκό έργο / H2020)

The goal of the OPERANDO project is to specify, implement, field-test, validate and exploit an innovative privacy enforcement platform that will enable the Privacy as a Service (PaS) business paradigm and the market for online privacy services. The OPERANDO project will integrate and extend the state of the art to create a platform that will used by independent Privacy Service Providers (PSPs) to provide comprehensive user privacy enforcement in the form of a dedicated online service, called "Privacy Authority". The OPERANDO platform will support flexible and viable business models, including targeting of individual market segments such as public administration, social networks and Internet of Things.

5. Οκτώβριος 2015 – Μάιος 2016: **Τεχνικός Διευθυντής** στο έργο "ΟΛΙΚΥ: Ολιστική Προστασία Κρίσιμων Υποδομών: Ανθεκτικότητα και Προστασία Διασυνδέσεων" (Ιδιωτική χρηματοδότηση / ΔΙΑΝΕΟΣΙΣ)

Το έργο ΟΛΙΚΥ αποσκοπεί στην καταγραφή και αποτίμηση των εθνικών κρίσιμων υποδομών, καθώς και στη διατύπωση συγκεκριμένων και τεκμηριωμένων προτάσεων πολιτικής που αποβλέπουν στην ε-παρκή προστασία τους από κυβερνοεπιθέσεις. Οι πολιτικές που θα διατυπωθούν αποσκοπούν, ειδικότε-ρα, στην αύξηση της ανθεκτικότητας των κρίσιμων υποδομών σε επιθέσεις, καθώς και στην αποτίμηση των αλληλεξαρτήσεων τους, με σκοπό την ιεράρχηση της σημαντικότητας κάθε υποδομής.

6. Ιούλιος 2014 – Ιούνιος 2016: Συμμετοχή στο Ευρωπαϊκό έργο MEDUSA ως έμπειρος ερευνητής (Ευρωπαϊκό έργο / CIPS).

MEDUSA:Multi-ordEr Dependency approaches for managing cascading effects in ports' global sUpply chain and their integration in riSk Assesment frameworks". *MEDUSA will open new horizons in the area of port security, through produ*cing and sharing knowledge associated with the identification and assessment of cascading effects in the global ports' supply chain, with a view to predicting potential problems but also to minimize the consequences of diverge security incidents. MEDUSA is carried out by a multidisciplinary team, which brings together port stakeholders (Europhar), security experts (AIT), experts in multi-dependency algorithms (UPRC, UCY) and experts in ICT modelling and simulation tools (SiLO). F*unded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related risks Programme of the European Union.*

7. Ιανουάριος 2010 – 2013: Συμμετοχή στο έργο «S-PORT: Ένα ασφαλές, αυτοματοποιημένο, συνεργατικό περιβάλλον για την δημιουργία μεθοδολογιών Αποτίμησης Επικινδυνότητας, δημιουργίας Σχεδίου Επιχειρησιακής Συνέχειας και κέντρων Αποκατάστασης Καταστροφών για Πληροφοριακά Συστήματα Λιμένων», ως έμπειρος ερευνητής (εθνική χρηματοδότηση /ΣΥΝΕΡΓΑΣΙΑ).

Οι βασικοί στόχοι του «S-PORT» είναι: (1) Να ικανοποιήσει τις ανάγκες ασφάλειας των ΠΣ κρίσιμων υποδομών, όπως είναι οι εμπορικοί λιμένες, για την αδιάλειπτη παροχή υπηρεσιών, τη λήψη των κα-τάλληλων αντιμέτρων, την κατάστρωση στρατηγικών ασφάλειας και ανάκαμψης συστημάτων. (2) Να ενισχύσει τα μέσα και τις μεθόδους αξιολόγησης, σύγκρισης, ελέγχου, αναβάθμισης και εναρμόνισης των ΠΣ των εμπορικών λιμένων με τις βέλτιστες πρακτικές και τον κώδικα ISPS. Το σύστημα «S-PORT» αναμένεται να αποτελέσει το πρωτότυπο μιας νέας γενιάς καινοτόμων Πληροφοριακών Συστη-μάτων διαχείρισης ασφάλειας, το οποίο θα είναι ικανό να παρέχει τα απαραίτητα επίπεδα εμπιστοσύ-νης, αξιοπιστίας, διαδραστικότητας και διαλειτουργικότητας για τις κρίσιμες υποδομές των εμπορικών λιμένων. Το έργο χρηματοδοτείται από το πρόγραμμα ΣΥΝΕΡΓΑΣΙΑ της ΓΓΕΤ.

8. Σεπτέμβριος 2007 – Δεκέμβριος 2009: Μέλος της Ελλάδας στην επιτροπή European Security Research and Innovation Forum (ESRIF).

Η επιτροπή European Security Research and Innovation Forum (ESRIF) λειτουργεί υπό την επίβλεψη της Ευρωπαϊκής Επιτροπής (European Commission) και έχει ως βασικό σκοπό τον καθορισμό των μεσοπρόθεσμων και μακροπρόθεσμων αναγκών της Ευρωπαϊκής Ένωσης για έρευνα και ανάπτυξη σε όλες τις κατηγορίες που άπτονται σε ζητήματα Ασφάλειας. Στόχος του ESRIF είναι η σύνταξη πρότασης για τον Προγραμματισμό της Έρευνας σχετικά με την Ασφάλεια (Joint Security Research Agenda) στο τέλος του 2009.

9. Μάρτιος 2009 – Αύγουστος 2009: Συνεργάτης Ομάδας Ασφάλειας Πληροφοριακών Συστημάτων Οικονομικού Πανεπιστημίου Αθηνών στο έργο *«Στρατηγική Μελέτη Ασφάλειας των Πληροφοριακών Συστημάτων της Γενικής Γραμματείας Πληροφοριακών Συστημάτων» δεύτερη φάση.*

Η παρούσα στρατηγική μελέτη αποβλέπει στην προδιαγραφή της οργανωτικής υποδομής που είναι αναγκαία για την αποτελεσματική διαχείριση των ζητημάτων Ασφάλειας στις ΤΠΕ, της Γενικής Γραμματείας Πληροφοριακών Συστημάτων (ΓΓΠΣ) του Υπουργείου Οικονομίας και Οικονομικών. Το έργο αυτό περιλαμβάνει: (1) Προδιαγραφή οργανωτικής υποδομής ασφάλειας, (2) Επιμόρφωση προσωπικού της ΓΓΠΣ σε Ειδικά Θέματα Ασφάλειας στις ΤΠΕ, (3) Διασφάλιση ότι η προδιαγραφείσα οργανωτική υποδομή ασφάλειας της ΓΓΠΣ καλύπτει τις απαιτήσεις επεξεργασίας προσωπικών δεδομένων (Ν. 2472/ 97, Ν. 3471/ 03) και απορρήτου των επικοινωνιών (Ν. 2225/94, Ν. 3115/ 03, Π.Δ. 47/05) και (4) Πρότυπο σχέδιο της Πολιτικής Ασφάλειας και των Μέτρων Ασφάλειας των Ολοκληρωμένων Πληροφοριακών Συστημάτων της ΓΓΠΣ.

10. Ιούλιος 2008 – Σεπτέμβριος 2008: Μέλος της «Ομάδας Εργασίας για την Προστασία των Κρίσιμων Πληροφοριακών και Επικοινωνιακών Υποδομών της Δημόσιας Διοίκησης (CICIP)» της ομάδας e-government forum της *Κοινωνίας της Πληροφορίας Α.Ε.*.

Η Ομάδα Εργασίας για την Προστασία των Κρίσιμων Πληροφοριακών και Επικοινωνιακών Υποδομών της Δημόσιας Διοίκησης (CICIP), συστήθηκε από την Κοινωνία της Πληροφορίας Α.Ε. με σκοπό τη μελέτη των κρίσιμων πληροφοριακών και επικοινωνιακών υποδομών της Δημόσιας Διοίκησης. Για το σκοπό αυτό προτάθηκε σχέδιο για την ανάπτυξη και θέση σε λειτουργία σειράς οργανωτικών και διοικητικών σχημάτων, τα οποία αποβλέπουν στην αντιμετώπιση των απειλών που αφορούν της παραπάνω υποδομές της ελληνικής Δημόσιας Διοίκησης. Για τη σχεδίαση του σχήματος αυτού λήφθηκε υπόψη τόσο η σχετική διεθνής εμπειρία - η οποία περιγράφεται συνοπτικά και συστηματικά στο κείμενο - όσο και ορισμένες υπάρχουσες και αναπτυσσόμενες κρίσιμες υπηρεσίες ηλεκτρονικής διακυβέρνησης στην Ελλάδα (πχ. Σύζευξις, TaxisNET, Κέντρα Εξυπηρέτησης Πολιτών, Κέντρα Δεδομένων ΚτΠ Α.Ε κλπ.).

11. Φεβρουάριος 2007 – Μάιος 2007: Συνεργάτης Ομάδας Ασφάλειας Πληροφοριακών Συστημάτων Οικονομικού Πανεπιστημίου Αθηνών στο έργο *«Ασφάλεια διασύνδεσης φορέων Κοινωνικής Ασφάλισης με φορείς παροχής υγειονομικών υπηρεσιών και πραγματοποίησης ηλεκτρονικών συναλλαγών φορέων Κοινωνικής Ασφάλισης με Τράπεζες».*

Το κυρίως έργο, όπου εντάσσεται το παρόν, αφορά στην ανάπτυξη περιβάλλοντος διαλειτουργικότητας στη Γενική Γραμματεία Κοινωνικών Ασφαλίσεων (ΓΓΚΑ) και συγκεκριμένα: (α) Διασύνδεσης φορέων κοινωνικής ασφάλισης (ΦΚΑ) με φορείς παροχής υπηρεσιών υγείας (ΦΠΥΥ) για τον έλεγχο των δαπανών υγείας και (β) ανάπτυξης των ηλεκτρονικών συναλλαγών των ΦΚΑ με Τράπεζες. Η μελέτη ασφάλειας του έργου περιλαμβάνει τον εντοπισμό και αποτίμηση των απειλών και των αδυναμιών του Συστήματος, την περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας, την πρόταση Πολιτικής Ασφάλειας, καθώς και την αξιολόγηση της εφαρμογής των μέτρων ασφάλειας. Επίσης, την ανάπτυξη σχεδίου αντιμετώπισης και ανάκαμψης από καταστροφές του κέντρου διασύνδεσης των φορέων.

12. Απρίλιος 2007 – Οκτώβριος 2007: Συνεργάτης Ομάδας Ασφάλειας Πληροφοριακών Συστημάτων Οικονομικού Πανεπιστημίου Αθηνών στο έργο *«Στρατηγική Μελέτη Ασφάλειας των Πληροφοριακών Συστημάτων της Γενικής Γραμματείας Πληροφοριακών Συστημάτων»*.

Η παρούσα στρατηγική μελέτη αποβλέπει στην προδιαγραφή της οργανωτικής υποδομής που είναι αναγκαία για την αποτελεσματική διαχείριση των ζητημάτων Ασφάλειας στις ΤΠΕ, της Γενικής Γραμματείας Πληροφοριακών Συστημάτων (ΓΓΠΣ) του Υπουργείου Οικονομίας και Οικονομικών. Το έργο αυτό περιλαμβάνει: (1) Προδιαγραφή οργανωτικής υποδομής ασφάλειας, (2) Επιμόρφωση προσωπικού της ΓΓΠΣ σε Ειδικά Θέματα Ασφάλειας στις ΤΠΕ, (3) Διασφάλιση ότι η προδιαγραφείσα οργανωτική υποδομή ασφάλειας της ΓΓΠΣ καλύπτει τις απαιτήσεις επεξεργασίας προσωπικών δεδομένων (Ν. 2472/ 97, Ν. 3471/ 03) και απορρήτου των επικοινωνιών (Ν. 2225/94, Ν. 3115/ 03, Π.Δ. 47/05) και (4) Πρότυπο σχέδιο της Πολιτικής Ασφάλειας και των Μέτρων Ασφάλειας των Ολοκληρωμένων Πληροφοριακών Συστημάτων της ΓΓΠΣ.

13. Ιανουάριος 2004 – Δεκέμβριος 2004: Επιστημονικός Συνεργάτης Κέντρου Ερευνών Πανεπιστημίου Πειραιώς στο Πρόγραμμα E-Mayor.

Το πρόγραμμα e-mayor αφορά το σχεδιασμό και την υλοποίηση μιας ανοιχτής και ασφαλούς πλατφόρμας ηλεκτρονικής διακυβέρνησης για Ευρωπαϊκούς δημόσιους οργανισμούς μικρού και μεσαίου μεγέθους (όπως οι δήμοι) ώστε να υποστηρίξει: (1) ηλεκτρονικές υπηρεσίες σε πανευρωπαϊκό επίπεδο. (2) την ασφαλή επικοινωνία δήμων μεταξύ τους, καθώς και με τους πολίτες και τον επιχειρηματικό κόσμο, και (3) την ασφαλή τοπική και απομακρυσμένη πρόσβαση στα δεδομένα άλλων δήμων μόνο από εξουσιοδοτημένους χρήστες και δημόσιους υπαλλήλους. Το ασφαλές αυτό περιβάλλον θα περιλαμβάνει εφαρμογές εξειδικευμένες στις απαιτήσεις των δήμων και βασισμένες στην τεχνολογία XML, καθώς και στις Υπηρεσίες Διαδικτύου (Web Services), τις οποίες θα χρησιμοποιούν οι δήμοι για να επικοινωνήσουν με τους πολίτες, άλλους δήμους αλλά και επιχειρήσεις.

14. Ιούλιος 2000 – Απρίλιος 2001: Συμμετοχή στο πρόγραμμα ΠΕΝΕΔ *"Σχεδίαση και Ανάπτυξη Κατανεμημένης Πλατφόρμας Ελέγχου Υπηρεσιών με Τεχνολογία Κινητών Αντιπροσώπων και CORBA"*, (ΓΓΕΤ, 1999-2001).

Στόχος του προγράμματος είναι η ανάπτυξη μίας αρχιτεκτονικής ασφάλειας για κατανεμημένα ευφυή δίκτυα με τη χρήση Τρίτης Έμπιστης Οντότητας, των υπηρεσιών ασφάλειας της τεχνολογίας CORBA και κρυπτογραφικών μηχανισμών για κινητούς πράκτορες.

15. Νοέμβριος 1998 – Ιούνιος 2000: Συμμετοχή στο διαπανεπιστημιακό πρόγραμμα Ε.Π.Ε.Α.Ε.Κ. *"Ομόσπονδο Σύστημα Διαχείρισης Πανεπιστημιακού Εκπαιδευτικού Υλικού"*, (Προγράμματα Σπουδών – Συγγράμματα – 2ο Κοινοτικό Πλαίσιο Στήριξης).

Η συμμετοχή στο πρόγραμμα αφορούσε την εφαρμογή ψηφιακών υπογραφών για τον έλεγχο της ακεραιότητας του εκπαιδευτικού υλικού και την προστασία των πνευματικών δικαιωμάτων των δημιουργών εκπαιδευτικού υλικού, το οποίο είναι προσβάσιμο σε φοιτητές μέσω Διαδικτυακών υπηρεσιών.

III.4 Αξιολογήσεις, μελέτες, εμπειρογνωμοσύνες

1. Συμμετοχή στην επιτροπή αξιολόγησης της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) για το έργο Ανάπτυξη Ολοκληρωμένου Πληροφοριακού Συστήματος της ΑΔΑΕ το οποίο χρηματοδοτείται από την Κοινωνία της Πληροφορίας (Σεπτέμβριος 2007).

IV. Δημοσιευμένο έργο

IV.1 Επιμέλεια πρακτικών συνεδρίων και περιοδικών

Σε Διεθνή περιοδικά

1. **[Ed-1]** C. Alcaraz, M. Burmester, J. Cuellar, X. Huan, P. Kotzanikolaou and M. Psarakis, *"Guest Editorial: Special Issue on Secure Embedded IoT Devices for Resilient Critical Infrastructures"*, IEEE Internet of Things journal, Vol.6, Issue 5, pp.7988 – 7991, October 2019. **[IF: 9.515]**

Ελληνικές εκδόσεις

2. **[Ε-1]** Χ. Δουληγέρης, Π. Κοτζανικολάου, Ι. Γιαννάκος, *«Γενικές Αρχές Εθνικής Στρατηγικής για το Απόρρητο και την Ασφάλεια Δικτύων και Πληροφοριών».* Πρακτικά 2ης ετήσιας Ημερίδας της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), ISBN 978-960-98080-0-2, Ιανουάριος 2008.

IV.2 Μονογραφίες, αυτοτελείς μελέτες, εκπαιδευτικά βιβλία

3. **[Μ-1]** Π. Κοτζανικολάου, Δ. Πολέμη, *«Τεχνολογία και Πολιτικές Ασφάλειας»* - σημειώσεις μαθήματος για το μάθημα επιλογής 7ου εξαμήνου Τμήματος Πληροφορικής Πανεπιστημίου Πειραιώς, δεύτερη έκδοση, Οκτώβριος 2007.

IV.3 Διατριβές

4. **[Δ-1]** Π. Κοτζανικολάου, **«***Ασφαλή Συστήματα Κινητών Πρακτόρων»*, Διδακτορική Διατριβή, Τμήμα Πληροφορικής, Πανεπιστήμιο Πειραιώς, Ιανουάριος 2003

IV.4 Συγγραφή κεφαλαίων σε συλλογικούς τόμους

5. **[Β-12]** Stellios, I., Kotzanikolaou P., & Psarakis, M. (2019). "Advanced Persistent Threats and Zero-Day Exploits in Industrial Internet of Things" In *Security and Privacy Trends in the Industrial Internet of Things* (pp.47-68). Springer.

6. **[Β-11]** Petrakos, N., & Kotzanikolaou, P. (2019). Methodologies and Strategies for Critical Infrastructure Protection. In *Critical Infrastructure Security and Resilience* (pp. 17-33). Springer.

7. **[Β-10]** P. Kotzanikolaou (2016). Security and Privacy in Next Generation Networks and Services. In *Handbook of Research on Next Generation Mobile Communication Systems* (pp. 361-379). IGI Global.

8. **[Β-9]** P. Kotzanikolaou, M. Theoharidou, D. Gritzalis: *"Risk assessment of multi-order dependencies between critical information and communication infrastructures"*. Invited chapter, in *Critical Information Infrastructure Protection and Resilience in the ICT Sector* (Editors: Sandro Bologna & Paul Theron), IGI Global, pp.153-172, 2013.

9. **[Β-8]** Κ. Πατσάκης, Π. Κοτζανικολάου και Δ. Πολέμη: *«Μονόδρομες συναρτήσεις και Γεννήτορες ψευδοτυχαίων αριθμών».* Στο βιβλίο "Σύγχρονη κρυπτογραφία: Θεωρία και Εφαρμογές" (Επιστημονική Επιμέλεια: M. Burmester, Σ. Γκρίτζαλης, Σ. Κάτσικας, Β. Χρυσικόπουλος), σελ. 211-236, Εκδόσεις Παπασωτηρίου 2010.

10. **[Β-7]** Π. Κοτζανικολάου, Δ. Πολέμη και Χ. Δουληγέρης: « Διατήρηση Δεδομένων Επικοινωνίας και Διασφάλιση του Απορρήτου και της Ιδιωτικότητας». Στο βιβλίο "Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών" (Επιστημονική Επιμέλεια: Κ.Λαμπρινουδάκης, Λ.Μήτρου, Σ.Γκρίτζαλης, Σ.Κάτσικας), σελ. 73-91, Εκδόσεις Παπασωτηρίου, 2010.

11. **[Β-6]** C. Douligeris and P. Kotzanikolaou: *"Network Security"*. In Encyclopaedia of Life Support Systems, Telecommunication Systems and Technologies, Volume II, ISBN- 978-1-84826-000-9, EOLSS Publishers – UNESCO, pp. 250-267, 2007.

12. **[Β-5]** M. Burmester and P. Kotzanikolaou: *"Securing Networks against Extreme Attacks"*. In Volume of essays in honour of Professor Antonios C. Panayotopoulos, pp. 875–886, University of Piraeus, Greece, 2006.

13. **[Β-4]** C. Douligeris and P. Kotzanikolaou: *"Introduction to Network Security"***.** In "Network Security: Current Status and Future Directions", IEEE Press – Wiley Interscience, ISBN 978-0-471-70355-6, pp.1-12, April 2007.

14. **[Β-3]** P. Kotzanikolaou, C. Douligeris, R. Mavropodi and V. Chrissikopoulos: *"Mobile Agent Security"***.** In "Network Security: Current Status and Future Directions", IEEE Press – Wiley Interscience, ISBN 978-0-471-70355-6, pp.257-268, April 2007.

15. **[B-2]** M. Burmester, P. Kotzanikolaou and C. Douligeris: *"Security In Mobile Ad Hoc Networks"***.** Book chapter, in "Network Security: Current Status and Future Directions", IEEE Press – Wiley Interscience, ISBN 978-0-471-70355-6, pp.355-371, April 2007.

16. **[B-1]** P. Kotzanikolaou and C. Douligeris: *"Cryptography Primer: An Introduction to Cryptographic Principles and Algorithms"***.** In "Network Security: Current Status and Future Directions", IEEE Press – Wiley Interscience, ISBN 978-0-471-70355-6, pp.459-479, April 2007.

IV.5 Άρθρα σε επιστημονικά περιοδικά

Σε διεθνή περιοδικά

17. **[J-24]** M. Shahraeini and P. Kotzanikolaou, "A Dependency Analysis Model for Resilient Wide Area Measurement Systems in Smart Grid," *IEEE Selected Areas of Communications*, Special Issue on Communications and Data Analytics in Smart Grid, Accepted: October 2019, publication date: First Quarter 2020. **[IF: 9.302]**
18. **[J-23]** I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz and J. Lopez, "A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services," in *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453-3495, Forth quarter 2018. **[IF: 22.973]**
19. **[J-22]** Papastergiou, S., Polemi, N., & Kotzanikolaou, P. (2018) "Design and validation of the Medusa supply chain risk assessment methodology and system", *International Journal of Critical Infrastructures*, Inderscience, *14*(1), 1-39.
20. **[J-21]** Gkioulos, V., Wangen, G., Katsikas, S. K., Kavallieratos, G., & Kotzanikolaou, P. (2017). Security Awareness of the Digital Natives. *Information*, MDPI, *8*(2), 42.
21. **[J-20]** P. Kotzanikolaou, G. Chatzisofroniou, M. Burmester, "Broadcast Anonymous Routing (BAR): Scalable Real-Time Anonymous Communication", International Journal of Information Security, 6(3), pp 313–326, Springer, 2017. **[IF: 1.822]**
22. **[J-19]** G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, G. Lykou, D. Gritzalis, *"Time-based Critical Infrastructure Dependency Analysis for Large-Scale and Cross-Sectoral Failures", Elsevier* International Journal of Critical Infrastructure Protection 12(2016), 46-60. **[IF: 2.225]**
23. **[J-18]** P. Kotzanikolaou, C. Patsakis, E. Magkos, M. Korakakis, *"Lightweight Private Proximity Testing for Geospatial Social Networks"*, Elsevier Computer Communications 73 (2016) 263–270. **[IF: 2.766]**
24. **[J-17]** G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, D. Gritzalis, *"Risk Mitigation Strategies For Critical Infrastructures Based On Graph Centrality Analysis", Elsevier* International Journal of Critical Infrastructure Protection (IJIP) 10 (2015) 34–44, 2015. **[IF: 2.225]**
25. **[J-16]** P. Kotzanikolaou, M. Theoharidou, D. Gritzalis, "*Assessing n-order Dependencies Between Critical Infrastructures". Invited article (revised version of selected papers from CRITIS 2011)*, International Journal of Critical Infrastructures (IJCIS), Inderscience, Vol.9, Nos. 1/2, pp.93–110, 2013.
26. **[J-15]** E. Magkos, M. Avlonitis, P. Kotzanikolaou and M. Stefanidakis, *"Towards Early Warning Against Internet Worms Based on Critical-Sized Networks",* Security and Communication Networks, Wiley, Vol.6, pp.78-88, 2013. **[IF: 1.376]**
27. **[J-14]** A. Avramidis, P. Kotzanikolaou, C. Douligeris and M. Burmester, *"Chord-PKI: Providing Security and Privacy in P2P Networks with a Distributed PKI Architecture"*, Computer Networks, Vol.56, Issue 1, pp.378-398, Elsevier, January 2012. **[IF: 3.030]**
28. **[J-13]** M. Theoharidou, P. Kotzanikolaou and D. Gritzalis, *"Risk assessment methodology for interdependent critical infrastructures"*, International Journal of Risk Assessment and Management, Inderscience, Vol. 15, No.2/3, pp.128-148, 2011.

29. **[J-12]** E. Magkos and P. Kotzanikolaou, *"Achieving Privacy and Access Control in Pervasive Computing Environments"*, Journal of Security and Communication Networks, Wiley, DOI: 10.1002/sec.283, (Early View) February 2011, Vol.9(2), pp.94-105, 2016. **[IF: 1.376]**

30. **[J-11]** M. Theoharidou, P. Kotzanikolaou and D. Gritzalis,: *"A multi-layer Criticality Assessment methodology based on interdependencies"*, Computers & Security, Vol. 29, No.6, pp.643-658, Elsevier, 2010. **[IF: 3.062]**

31. **[J-10]** D.Zorbas, D. Glynos, P. Kotzanikolaou and C. Douligeris, *"Solving Coverage Problems in Wireless Sensor Networks Using Cover Sets"*, Ad Hoc Networks Vol.8 (2010), pp.400-415, Elsevier, 2010. **[IF: 3.490]**

32. **[J-9]** P. Kotzanikolaou, E. Magkos, D. Vergados and M. Stefanidakis *"Secure and Practical Key Establishment for Distributed Sensor Networks",* Journal of Security and Communication Networks, Vol.2, Issue 6, pp.595-610, Wiley 2009. **[IF: 1.376]**

33. **[J-8]** V. Stathopoulos, P. Kotzanikolaou, and E. Magkos, *"Secure Log Management for Privacy Assurance in Electronic Communications"*, Computers & Security, Vol.27, No.7-8, pp.298-308, Elsevier, 2008. **[IF: 3.062]**

34. **[J-7]** P. Kotzanikolaou, *"Data Retention and Privacy in Electronic Communications"*, IEEE Security & Privacy, Vol.6, No.5, pp. 18-24, September-October 2008. **[IF: 1.239]**

35. **[J-6]** P. Kotzanikolaou, D. Vergados, G. Stergiou and E. Magkos, *"Multi-Layer Key Establishment for Large Scale Sensor Networks"*, International Journal of Security and Networks (IJSN), Inderscience, Vol.3, No.1, pp. 1-9, January 2008.

36. **[J-5]** E. Magkos, P. Kotzanikolaou, and C. Douligeris: *"Towards Secure Online Elections – Models, Primitives and Open Issues"*, Electronic Government, Vol.4, No.3, pp.249-268, Inderscience, 2007.

37. **[J-4]** R. Mavropodi, P. Kotzanikolaou, and C. Douligeris: *"SecMR - A Secure Multipath Routing Protocol for Ad Hoc Networks"*, Ad Hoc Networks, Special Issue on Security Issues in Sensor and Ad Hoc Networks, Singhal and Misic (eds), Vol.5, No. 1, pp.87-99, Elsevier, January 2007. **[IF: 3.490]**

38. **[J-3]** P. Kotzanikolaou, R. Mavropodi, C. Douligeris, and V. Chrissikopoulos: *"Secure Distributed Intelligent Networks"***.** Elsevier Computer Communications, Special issue on Internet Security (B. Levine and C. Shields Eds), Vol.29, No.3, pp.325-336, February 2006. **[IF: 2.766]**

39. **[J-2]** D. Petropoulos and P. Kotzanikolaou: *"Some More Improvements on a Fair non-repudiation Protocol"*. Journal of Internet Technology, Vol.4 No.3, pp. 255-260, October 2003.

40. **[J-1]** P. Kotzanikolaou, M. Burmester, V. Chrissikopoulos and C. Douligeris: *"Role Based Access Control Policies in the Mobile Agent Paradigm"*. Informatik Forum Journal – Special Issue on Mobile Agent Technology. Vol.14, No.2, pp. 62-69, December 2002.

Σε Ελληνικά περιοδικά

41. **[Π-1]** Χ. Δουληγέρης και Π. Κοτζανικολάου: *"Το Απόρρητο στις Τηλεπικοινωνίες: Διασφάλιση και Αντιμετώπιση Παραβίασης"*, ΕΠΥ, Ενημερωτικό Δελτίο, Τεύχος 105, σελ. 30-31, Απρ. – Ιουν. 2006.

IV.6 Ανακοινώσεις σε συνέδρια με κριτές

1. **[C-36]** Geogre Chatzisophroniou and Panayiotis Kotzanikolaou, "Association Attacks in IEEE 802.11: Exploiting WiFi Usability Features". In Proc. Of the 9th International Workshop on Socio-Technical Aspects in SecuriTy – STAST2019 (*(ESORICS 2019 Workshops)*, Luxembourg, September 2019.

2. **[C-35]** Vagelis Malamas, Thomas Dasaklis, Panayiotis Kotzanikolaou, Mike Burmester and Sokratis Katsikas, *"A Forensics-by-design Management Framework for Medical Devices based on Blockchain"*. In Proc. Of the 1st IEEE SERVICES Workshop on Cyber Security & Resilience in the Internet of Things (CSRIoT 2019), Milan, Italy, July 2019.

3. **[C-34]** Stamatia Triandopoulou, Dimitris Papanikas and Panayiotis Kotzanikolaou, *"An Experimental Analysis of Current DDoS attacks Based on a Provider Edge Router Honeynet"*. In Proceedings of the 10th International Conference on Information, Intelligence, Systems and Applications (IISA2019), 15-17 July, Patras, Greece, IEEE.
4. **[C-33]** Georgios Makrodimitris, Panayiotis Kotzanikolaou, and Christos Douligeris. *"Preliminary design of a new approach to choose cyber exercise methodologies for critical infrastructures".* In *Proceedings of the 22nd Pan-Hellenic Conference on Informatics* (PCI '18), Karanikolas Nikitas and Mamalis Basilis (Eds.). ACM, New York, NY, USA, 40-45. November 2018.
5. **[C-32]** Zorbas D., Kotzanikolaou P., and Douligeris C. (2018) *"R-TSCH: Proactive Jamming Attack Protection for IEEE 802.15.4-TSCH Networks"*, in IEEE Symposium on Computers and Communications, Natal, Brazil, June 2018.
6. **[C-31]** Gritzalis, D., Stergiopoulos, G., Kotzanikolaou, P., Magkos, E., & Lykou, G. (2016). *"Critical Infrastructure Protection: A Holistic Methodology for Greece"*. In Conference on Security of Industrial-Control-and Cyber-Physical Systems (pp. 19-34). Springer.
7. **[C-30]** Stergiopoulos, G., Vasilellis, E., Lykou, G., Kotzanikolaou, P., & Gritzalis, D. (2016). *"Classification and Comparison of Critical Infrastructure Protection Tools"*. In Critical Infrastructure Protection X: 10th IFIP WG 11.10 International Conference, ICCIP 2016, Arlington, VA, USA, March 14-16, 2016, Revised Selected Papers 10 (pp. 239-255). Springer International Publishing.
8. **[C-29]** C. Patsakis, P. Kotzanikolaou and M. Bouroche, *"Private Proximity Testing on Steroids: An NTRU-based Protocol"*, Proceedings of the Security and Trust Management – STM2015 (ESORICS workshop), Vienna, September 2015, LNCS, Vol.9331, pp.172-184, Springer. (Lecture Notes in Computer Science)
9. **[C-28]** D. Polemi, P. Kotzanikolaou, *"Medusa: A Supply Chain Risk Assessment Methodology"*, Proceedings of the Cyber Security and Privacy (CSP Forum), Brussels 2015, Communications in Computer and Information Science Vol.530, pp.79-90, Springer.
10. **[C-27]** G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, D. Gritzalis, *"Using Centrality Measures in CI Dependency Risk Graphs for Efficient Risk Mitigation"*, Proceedings of the 9th Seventh Annual IFIP RI International, Arlington, USA, 16th–18th March 2015.
11. **[C-26]** E. Magkos, P. Kotzanikolaou, M. Magioladitis, S. Sioutas, and V.S. Verykios *"Towards Secure and Practical Location Privacy through Private Equality Testing"*, Proceedings of the Privacy in Statistical Databases (PSD2014), pp.312-235, LNCS Vol.8744, Springer, Ibiza, Spain, 17-19 September 2014. (Lecture Notes in Computer Science)
12. **[C-25]** D. Moustis and P. Kotzanikolaou, *"Evaluating security controls against HTTP-based DDoS attacks"*, Proceedings of the 2013 Fourth International Conference on Information, Intelligence, Systems and Applications (IISA 2013), pp.1-6, IEEE, July 10-12 2013, Piraeus, Greece.
13. **[C-24]** P. Kotzanikolaou, M. Theocharidou, and D. Gritzalis, *"Cascading Effects Of Common-Cause Failures On Critical Infrastructures",* Proceedings of the 7th Seventh Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection (CIP-2013), Springer, pp.171-182, George Washington University, Washington, DC, USA, March 18 - 20, 2013.
14. **[C-23]** P. Kotzanikolaou, E. Magkos, N. Petrakos, C. Douligeris and V. Chrissikopoulos, *"Fair Anonymous Authentication for Location Based Services",* Proceedings of DPM 2012 and SETOP 2012 *(ESORICS 2012 Workshops)*, LNCS Vol.7731, Springer, pp.1-14, Pisa, Italy, September 2012. (*Lecture Notes in Computer Science*)
15. **[C-22]** *Petrakos, N., Kotzanikolaou, P., & Douligeris, C., "Using Strand Space Model to Verify the Privacy Properties of a Fair Anonymous Authentication Scheme".* In Informatics (PCI), 2012 16th Panhellenic Conference on (pp. 105-110). IEEE, Piraeus, Greece, October 2012.

16. **[C-21]** P.Kotzanikolaou, M. Theocharidou, and D. Gritzalis, *"Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects"*, Proceedings of the 6th International Conference on Critical Information Infrastructures Protection (CRITIS2011), LNCS Vol. 6983, Springer, pp.104-115, Lucerne, Switzerland, September 2011. (*Lecture Notes in Computer Science*)
17. **[C-20]** T. Ntouskas, P. Kotzanikolaou and N. Polemi, *"Impact Assessment through Collaborative Asset Modeling: The STORM-RM approach",* Proceedings of the 1st International Symposium and 10th Balkan conference on Operational Research, (BALCOR2011), Thessaloniki, Greece. In *Optimization Theory, Decision Making, and Operations Research Applications,* Springer, pp.293-304, September 2011.
18. **[C-19]** E. Magkos, P. Kotzanikolaou, S. Sioutas and K. Oikonomou, *"A Distributed Privacy-Preserving Scheme for Location-Based Queries"*, Proceedings of the 4th International IEEE World of Wireless Mobile and Multimedia Networks (WoWMoM2010), Montreal, Canada, pp.1-6, June 2010.
19. **[C-18]** E. Magkos and P. Kotzanikolaou, *"Enhancing Privacy-Preserving Access Control for Pervasive Computing Environments"*, Proceedings of 2nd International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (MobiSec 2010), Springer, Catania, Italy, pp. 53-64, May 2010.
20. **[C-17]** P.Kotzanikolaou, S. Maniatis, E. Nikolouzou and V. Stathopoulos, *"Evaluating Common Privacy Vulnerabilities in Internet Service Providers",* Proceedings of the 3rd International Conference on e-Democracy, Greece, September 2009. In *Next Generation Society. Technological and Legal Issues,* Springer, pp. 161-170, 2010.
21. **[C-16]** M. Theocharidou, P. Kotzanikolaou and D. Gritzalis, *"Risk-Based Criticality Analysis",* Proceedings of the 3rd IFIP International Conference on Critical Infrastructure Protection (CIP-2009), C. Palmer and S. Shenoi (Eds.): Critical Infrastructure Protection III, IFIP AICT 311, Springer pp. 35–49, 2009.
22. **[C-15]** P. Kotzanikolaou and C. Douligeris: *"Privacy Threats of Data Retention in Internet Communications"*, Proceedings of the 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07), IEEE, pp.1-4, September 2007.
23. **[C-14]** A. Avramidis, P. Kotzanikolaou and C. Douligeris: *"Chord-PKI: Embedding a Public Key Infrastructure into the Chord Overlay Network",* Proceedings of the EUROPKI'2007, LNCS Vol.4582, Springer, pp.354-361, Mallorca, Spain, June 2007. (*Lecture Notes in Computer Science*)
24. **[C-13]** D. Zorbas, D. Glynos, P. Kotzanikolaou, C. Douligeris: *"B{GOP}: An Adaptive Algorithm for Coverage Problems in Wireless Sensor Networks"*, Proceedings of the 13th European Wireless Conference ", Paris, France, April 1 - 4, 2007
25. **[C-12]** V. Stathopoulos, P. Kotzanikolaou and E. Magkos: *"A Framework for Secure and Verifiable Logging in Public Communication Networks",* Proceedings of the 1st Critical Information Infrastructures Security (CRITIS'06), LNCS Vol. 4347, Springer, pp.273-284, Samos Island, Greece, Aug 2006. (*Lecture Notes in Computer Science*)
26. **[C-11]** E. Magkos, P. Kotzanikolaou, D. Vergados and M. Stefanidakis: "*An Asymmetric Key Establishment Protocol for Multiphase Self-Organized Sensor Networks"*, Proceedings of the 12th European Wireless Conference – "Enabling Technologies for Wireless Multimedia Communications", Athens, Greece, April 2 - 5, 2006.
27. **[C-10]** P. Kotzanikolaou, D. Vergados and G. Stergiou: *"Performance Analysis of a Hybrid Key Establishment Protocol"*, Proc. Of the 7th IEEE IMS'2005 conference, pp. 719-724, Irvine, California, USA, December 2005.
28. **[C-9]** P. Kotzanikolaou, E. Magkos, C. Douligeris and V. Chrissikopoulos: *"Hybrid Key Establishment for Multiphase Self-Organized Sensor Networks"*, Proceedings of 1st International IEEE Workshop on

Trust, Security and Privacy for Ubiquitous Computing (TSPUC'2005), IEEE, pp. 581-587, Taromina, Italy, June 2005.

29. **[C-8]** R. Mavropodi, P. Kotzanikolaou, and C. Douligeris: *"Performance Analysis of Secure Multipath Routing Protocols for Mobile Ad Hoc Networks"*, Proceedings of 3rd International Conference on Wired/Wireless Internet Communications (WWIC'2005), LNCS Vol. 3510, Springer, pp. 269-279, Xanthi, Greece, May 2005. (*Lecture Notes in Computer Science*)
30. **[C-7]** D. Glynos, P. Kotzanikolaou, and C. Douligeris: *"Preventing Impersonation Attacks in MANET with multi-factor authentication"*, Proceedings of 3rd International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WIOPT'2005), IEEE, pp. 59-64, Trentino, Italy, April 2005.
31. **[C-6]** P. Kotzanikolaou, R. Mavropodi, and C. Douligeris: *"Secure Multi-path Routing for Mobile Ad Hoc Networks",* Proceedings of 2nd Annual Conference on Wireless On-demand Network Systems and Services (WONS'2005), IEEE, pp. 89-96, St. Moritz, Switzerland, January 2005.
32. **[C-5]** M. Burmester, V. Chrissikopoulos, P. Kotzanikolaou and E. Magkos: *"Strong Forward Security".* Proceedings of IFIP/SEC 2001, Kluwer Academic Publishers, pp. 109–119, Paris, France, June 2001.
33. **[C-4]** E. Magkos, P. Kotzanikolaou, and V. Chrissikopoulos: *"An Asymmetric Traceabilty Scheme for Copyright Protection without Trust Assumptions".* Proceedings of EC-Web 2001, LNCS Vol. 2115, Springer, pp. 186–195, Munich, Germany, September 2001. (*Lecture Notes in Computer Science*)
34. **[C-3]** P. Kotzanikolaou, M. Burmester and V. Chrissikopoulos: *"Dynamic Multi-signatures for Secure Autonomous Agents".* Proceedings of DEXA 2001 Workshop, IEEE, pp. 582–586, Munich, Germany, September 2001.
35. **[C-2]** P. Kotzanikolaou, M. Burmester, and V. Chrissikopoulos: *"Secure Transactions with Mobile Agents in Hostile Environments".* Information Security and Privacy, ACISP 2000, LNCS Vol. 1841, Springer-Verlag pp. 289-297, Brisbane, Australia, 2000. (*Lecture Notes in Computer Science*)
36. **[C-1]** P. Kotzanikolaou, G. Katsirelos and V. Chrissikopoulos: *"Mobile Agents for Secure Electronic Transactions".* In Recent Advances in Signal Processing and Communications, World Scientific and Engineering Society Press pp. 363□368, Athens, Greece, 1999.

IV.7 Άλλες ανακοινώσεις και δημοσιεύσεις

1. Φεβρουάριος 2018: Προσκεκλημένος ομιλητής στο συνέδριο ICT security world 2018, για διάλεξη με θέμα "Διαδίκτυο των Πραγμάτων: Το σύγχρονο πεδίο απειλών" .

2. Οκτώβριος 2017, Προσκεκλημένος ομιλητής στο συνέδριο Conference on Informatics in Education (CIE2017). Τίτλος ομιλίας "Διαδίκτυο των Αντικειμένων (IoT): Το πεδίο των απειλών"

3. Ιούνιος 2017: Προσκεκλημένος ομιλητής στο συνέδριο ICT Security World 2017, για διάλεξη με θέμα "WORD-OF-MOUTH: Private Gossiping of Geolocation News".

4. Ιούλιος 2004: Προσκεκλημένος ομιλητής για διάλεξη με θέμα *«Ασφάλεια Κινητών Πρακτόρων και Κινητού Κώδικα»*, στο Τμήμα Πληροφορικής και Τηλεπικοινωνιών του Εθνικού Καποδιστριακού Πανεπιστημίου Αθηνών.

5. D. Petropoulos, and P. Kotzanikolaou: *"A Framework for Transaction Non-repudiation and Demonstrable Log Completeness".* Technical Report, Encode Security Labs, ESP-0402. September 2002.

6. Νοέμβριος 2002: Προσκεκλημένος ομιλητής για διάλεξη με θέμα: *"Security issues in distributed mobile agent applications"* στο Τμήμα Πληροφορικής του Πανεπιστημίου Florida State University των Ηνωμένων Πολιτειών.
7. D. Petropoulos, and P. Kotzanikolaou: *"Possible Weakness on 'F-Secure Antivirus' Virus Update Method Based on Unauthenticated HTTP Communication".* Technical Report, Encode Security Labs, ESA-0202. March 2002.
8. C. Douligeris, R. Mavropodi, and P. Kotzanikolaou: *"Agent-Based Security in Intelligent Multimedia Retrieval in Intelligent Networks".* INFORMS 2001, Performance Issues in High Speed Networks, November 2001.
9. Π. Κοτζανικολάου, Ρ. Μαυροπόδη, και Χ. Δουληγέρης: *«Ασφαλής Διαχείριση Ευφυών Δικτύων με τη χρήση Κινητών Πρακτόρων».* Ημερίδα για Ευφυείς Πράκτορες και Εικονική Πραγματικότητα, Οικονομικό Πανεπιστήμιο Αθηνών, Αθήνα, Ιούλιος 2001.
10. Π. Κοτζανικολάου: *«Προβλήματα Ασφάλειας σε Εφαρμογές Ηλεκτρονικών Δημοσιεύσεων»*. Διημερίδα για την Ηλεκτρονική Δημοσίευση, Ιόνιο Πανεπιστήμιο, Κέρκυρα, Ιούλιος 2001

V. Επιμελητής / Κριτής σε διεθνή επιστημονικά περιοδικά, μέλος επιτροπών συνεδρίων

V.1 Επιμελητής σε επιστημονικά περιοδικά

1. Οκτώβριος 2018 – Μάρτιος 2019: Guest Editor for the ***IEEE Internet of Things Journal*.** Special Issue on *"Secure Embedded IoT Devices for Resilient Critical Infrastructures"*. **(IF:5.86)**

V.2 Κριτής σε επιστημονικά περιοδικά

2. *IEEE Communication Surveys and Tutorials*
3. *IEEE Transactions on Information Forensics & Security*
4. *IEEE Transactions on Parallel and Distributed Systems*
5. *IEEE Security & Privacy*
6. *IEEE Internet of Things Journal*
7. *IEEE Sensors Journal*
8. *Journal of Communications and Networks, KICIS-IEEE*
9. *Computers & Security, Elsevier*
10. *Computers Networks, Elsevier*
11. *AdHoc Networks, Elsevier*
12. *The Journal of Systems and Software, Elsevier*
13. *International Journal of Information Security,* Springer
14. *Wireless Personal Communication, Springer*
15. *International Journal of Critical Infrastructure Protection, Elsevier*
16. *ACM Transactions on Embedded Computing Systems*
17. *Journal of Computer Security, IOS press*
18. *Security and Communication Networks, Wiley*
19. *Mobile Computing, Wiley*

V.3 Διεθνή συνέδρια

Πρόεδρος επιτροπών διεθνών συνεδρίων

1. *Πρόεδρος στην Τεχνική Επιτροπή* της Ειδικής Συνεδρίας ***" Trusted Computing for Critical Information Infrastructures – T(CI)^2"*** που πραγματοποιήθηκε στο πλαίσιο του Διεθνούς Επιστημονικού Συνεδρίου ***"4th IEEE International Conference on Information, Intelligence, Systems and Applications"*** **(IISA 2013),** Πειραιάς, 10-12 Ιουλίου 2013 (http://iisa2013.unipi.gr/tci)

Μέλος επιτροπών διεθνών συνεδρίων

1. *Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού Συνεδρίου* ***"14th International Conference on Critical Information Infrastructures Protection" (CRITIS2019),*** *23-25 September 2019, Likoping, Sweeden (https://critis2019.on.liu.se/)*
2. *Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού Συνεδρίου* ***"10th International Conference on Information, Intelligence, Systems and Applications (IISA2019)"***, 15-17 July, Patras, Greece (http://iisa2019.upatras.gr/)
3. *Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού Συνεδρίου* ***"ICS-CSR 2019: 6th International Symposium for ICS & SCADA Cyber Security Research"****, 10-12 September 2019, Athens, Greece* (http://www.ics-csr.com/)
4. *Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού Συνεδρίου* ***"eDemocracy 2019: 8th eDemocracy International Conference: Safeguarding Democracy and Human Rights in the Digital Age"****, 12-13 December 2019, Athens, Greece (http://www.edemocracy2019.eu/)*
5. *Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού Συνεδρίου* ***"IEEE Symposium on Computers and Communications" (ISCC2018),*** *25-28 June 2018, Natal, Brazil (http://iscc2018.ieee-iscc.org/)*
6. *Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού Συνεδρίου* ***"13th International Conference on Critical Information Infrastructures Protection" (CRITIS2018),*** *24-26 September 2018, Kaunas, Lithuania (http://www.lei.lt/critis2018/index.html)*
7. *Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού Συνεδρίου "****Workshop on Industrial Internet of Things Security" (WIIoTS)****, June 4-7 2018, Bilbao, Spain (https://www.nics.uma.es/news/workshop-industrial-internet-things-security-wiiots)*
8. *Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού Συνεδρίου* ***"7th International Conference on eDemocracy"****, 14-15 December 2017, Athens, Greece (http://www.edemocracy2017.eu/)*
9. *Μέλος στην Τεχνική Επιτροπή* του Διεθνούς Επιστημονικού Συνεδρίου ***"12th International Conference on Critical Information Infrastructures Protection"*** **(CRITIS2017),** October 8-th/13-th 2017, Lucca, Italy, (http://www.critis2017.org/)
10. *Μέλος στην Τεχνική Επιτροπή* του Διεθνούς Επιστημονικού Συνεδρίου ***"11th International Conference on Critical Information Infrastructures Protection"*** **(CRITIS2016),** October 10–12, 2016 - Paris, France (http://critis2016.org/)
11. *Μέλος στην Τεχνική Επιτροπή* του Διεθνούς Επιστημονικού Συνεδρίου ***"10th International Conference on Critical Information Infrastructures Protection"*** **(CRITIS2015),** Berlin, Germany, October 5–7, 2015 (https://www.critis2015.org)
12. Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού Συνεδρίου ***"13th International Conference on Cryptology and Network Security"*** **(CANS'14),** Herakleion, Greece, 22-24 October 2014 (http://www.ics.forth.gr/cans2014/committees.html)

13. Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού Συνεδρίου ***"19th IEEE Symposium on Computers and Communications"*** **(ISCC'14),** Madeira Portugal, 23-26 June 2014 (http://www.ieee-iscc.org/2014/Committees/tpc.html)
14. *Μέλος στην Τεχνική Επιτροπή* του Διεθνούς Επιστημονικού ***"8th International Conference on Critical Information Infrastructures Protection"*** **(CRITIS2013),** Amsterdam, Nederlands 16-18 September 2013 (http://www.critis2013.nl/)
15. *Μέλος στην Τεχνική Επιτροπή* του Διεθνούς Επιστημονικού Συνεδρίου ***"18th IEEE Symposium on Computers and Communications"*** **(ISCC'13),** Split, Croatia, , 7-10 July 2013 (http://www.ieee-iscc.org/TPC3.html)
16. Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού ***"12th IFIP Conference on e-Business, e-Services, e-Society – Collaborative, trusted and privacy aware e/m-services"*** **(I3E 2013),** Athens, Greece 25-26 April 2013 (http://athina.cs.unipi.gr/i3e2013/).
17. Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού ***"7th International Conference on Critical Information Infrastructures Protection"*** **(CRITIS2012),** Lillehammer, Norway, 17-18 September 2012.
18. Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού ***"6th International Conference on Critical Information Infrastructures Protection"*** **(CRITIS2011),** Lucerne, Switcherland, 7-9 September 2011.
19. Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού Συνεδρίου ***"16th IEEE Symposium on Computers and Communications"*** **(ISCC'11),** Corfu, Greece, 28 June-1 July 2011.
20. Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού Συνεδρίου ***Information Security Conference (ISC2010),*** Florida, USA., 25-28 October 2010.
21. Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού Συνεδρίου ***IEEE Workshop on Autonomic and Opportunistic Computing*** **(AOC2010),** Montreal, Canada, June 2010 (http://cnd.iit.cnr.it/aoc2010/technicalcommittee.html)
22. Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού Συνεδρίου ***PIMRC'2007 –"Security & Privacy on Electronic Communication Services Provisioning",*** Athens, Greece, September 2007 (http://www.pimrc2007.org/econf2/en/site.action?contentid=42&module=
23. Μέλος στην Τεχνική Επιτροπή του Διεθνούς Επιστημονικού Συνεδρίου ***Secure Mobile Ad-hoc Networks and Sensors*** **(Secure MADNES'2005)**, Singapore, 20-22 September 2005 (http://www.sait.fsu.edu/conferences/2005/madnes/cfp.shtml)

VI. Συμμετοχή σε επιτροπές, ομάδες εργασίας και θέσεις διοίκησης

1. Μάρτιος 2018 – σήμερα: Μέλος της Επιτροπής "Σπουδές-Εκπαίδευση" της Σχολής Τεχνολογιών Πληροφορικής και Επικοινωνιών του Πανεπιστημίου Πειραιώς.
2. Σεπτέμβριος 2017: Μέλος Επιτροπής για την επιλογή εκπαιδευτικού προσωπικού με τη σχέση εργασίας Ιδιωτικού Δικαίου Ορισμένου Χρόνου σύμφωνα με τις διατάξεις του ΠΔ407/80.
3. Ιούλιος 2016 - Δεκέμβριος 2016: Μέλος Επιτροπής Διενέργειας και Αξιολόγησης Ηλεκτρονικού Δημόσιου Διαγωνισμού του Πανεπιστημίου Πειραιώς (Αριθμ. Πρωτ.: 20164446/27-07-2016 Διακήρυξης)
4. Απρίλιος 2016: Μέλος Επιτροπής για την επιλογή εκαπιδευτικού προσωπικού με τη σχέση εργασίας Ιδιωτικού Δικαίου Ορισμένου Χρόνου σύμφωνα με τις διατάξεις του ΠΔ407/80.
5. Ιούνιος 2016: Πρόεδρος επιτροπής διενέργειας εκλογών Τμήματος Πληροφορικής Πανεπιστημίου Πειραιώς.

6. Μάιος 2014 – Ιανουάριος 2015: Μέλος της Επιτροπής «Πόροι, Υποδομές, Υπηρεσίες και Δυναμικό» της Σχολής Τεχνολογιών Πληροφορικής και Επικοινωνιών του Πανεπιστημίου Πειραιώς.
7. Ιούνιος 2014: Μέλος επιτροπής διενέργειας εκλογών Τμήματος Πληροφορικής Πανεπιστημίου Πειραιώς.
8. Οκτώβριος 2012 - Ιανουάριος 2014: Πρόεδρος της επιτροπής διενέργειας ανοικτού δημόσιου διαγωνισμού του Πανεπιστημίου Πειραιώς, για την προμήθεια εξυπηρετητών και λοιπού εξοπλισμού υποδομής πληροφοριών, για υπηρεσίες και εργαστήρια του Πανεπιστημίου Πειραιώς (Αρ. Διακ. 20125852/23-10-2012)
9. Φεβρουάριος 2012: Πρόεδρος της επιτροπής αξιολόγησης για την προμήθεια οπτικοακουστικού υλικού του Πανεπιστημίου Πειραιώς
10. Νοέμβριος 2011 (- Μάρτιος 2012): Μέλος της επιτροπής αξιολόγησης ανοικτού δημόσιου διαγωνισμού του Πανεπιστημίου Πειραιώς για την ανάθεση του έργου «Πληροφοριακό Σύστημα Δομής Απασχόλησης και Σταδιοδρομίας (Δ.Α.Σ.Τ.Α)» (Αρ. Διακ. 201111711/11-10-2011)
11. Οκτώβριος 2010: Μέλος της επιτροπής παραλαβής Hardware εξοπλισμού για το ΜΠΣ «Πληροφορική» του Τμήματος Πληροφορικής, Παν. Πειραιά
12. Οκτώβριος 2010: Μέλος της επιτροπής παραλαβής λοιπού εξοπλισμού για το ΜΠΣ «Προηγμένα Συστήματα Πληροφορικής» του Τμήματος Πληροφορικής, Παν. Πειραιά
13. Οκτώβριος 2010: Μέλος της επιτροπής παραλαβής Hardware εξοπλισμού για το ΜΠΣ «Πληροφορική» του Τμήματος Πληροφορικής, Παν. Πειραιά
14. Οκτώβριος 2010: Μέλος της επιτροπής παραλαβής λοιπού εξοπλισμού για το ΜΠΣ «Προηγμένα Συστήματα Πληροφορικής» του Τμήματος Πληροφορικής, Παν. Πειραιά
15. Οκτώβριος 2010: Μέλος της επιτροπής δημοσιότητας για τα ΜΠΣ «Πληροφορική» και «Προηγμένα Συστήματα Πληροφορικής». του Τμήματος Πληροφορικής, Παν. Πειραιά
16. Σεπτέμβριος 2010: Αναπληρωματικό Μέλος της επιτροπής Διενέργειας και Αξιολόγησης του δημόσιου ανοικτού διαγωνισμού για την προμήθεια εκπαιδευτικού πακέτου διδασκαλίας και λοιπού εξοπλισμού πληροφορικής για το Πανεπιστήμιο Πειραιώς.
17. Σεπτέμβριος 2007 – Δεκέμβριος 2009: Μέλος της Ελλάδας στην επιτροπή *European Security Research and Innovation Forum (ESRIF)*. Η επιτροπή ESRIF λειτουργεί υπό την επίβλεψη της Ευρωπαϊκής Επιτροπής (European Commission) και έχει ως βασικό σκοπό τον καθορισμό των μεσοπρόθεσμων και μακροπρόθεσμων αναγκών της Ευρωπαϊκής Ένωσης για έρευνα και ανάπτυξη σε όλες τις κατηγορίες που άπτονται σε ζητήματα Ασφάλειας. Στόχος του ESRIF είναι η σύνταξη πρότασης για τον Προγραμματισμό της Έρευνας σχετικά με την Ασφάλεια (Joint Security Research Agenda) στο τέλος του 2009.
18. Συμμετοχή ως τεχνικός σύμβουλος σε ομάδα εργασίας, με σκοπό την *εξέταση του νομικού πλαισίου για την ασφάλεια του ηλεκτρονικού εμπορίου μέσω Διαδικτύου στην Ελλάδα* (ΦΕΚ Β' 412/31-3-2005).

VII. Μέλος επιτροπών επίβλεψης/αξιολόγησης υποψηφίων διδακτόρων

1. Μέλος της επιτροπής αξιολόγησης της διδακτορικής διατριβής του κ. Κατσικογιάννη Γεωργίου με τίτλο «Προσαρμοστική Διαχείριση Ασφάλειας Βάσει Πολιτικών», Τμήμα Πληροφορικής, Πανεπιστήμιο Πειραιώς, Ιούνιος 2018.
2. Μέλος της επιτροπής αξιολόγησης της διδακτορικής διατριβής του κ. Αρούκατου Νικόλαου με τίτλο «Σύγχρονες Τεχνικές Στεγανογραφίας και Στεγανάλυσης», Τμήμα Πληροφορικής, Πανεπιστήμιο Πειραιώς, Μάρτιος 2016.
3. Μέλος της επιτροπής αξιολόγησης της διδακτορικής διατριβής του κ. Γεωργακάκη Εμμανουήλ με τίτλο «Αυθεντικοποίηση με Χρήση Οπτικής Πληροφορίας και Διαχείριση Πρόσβασης με Δυναμικές

παραμέτρους σε Πληροφοριακά Συστήματα», Τμήμα Πληροφορικής, Πανεπιστήμιο Πειραιώς, Φεβρουάριος 2016.

4. Μέλος της επιτροπής αξιολόγησης της διδακτορικής διατριβής του κ. Δέλλιου Κλεάνθη με τίτλο «Designing Secure, Interoperable & Sustainable Automobiles & Global Transportation Services & Systems», Τμήμα Πληροφορικής, Παν. Πειραιώς, Φεβρουάριος 2015.
5. Μέλος της επιτροπής αξιολόγησης της διδακτορικής διατριβής του κ. Καρκαζή Παναγιώτη με τίτλο «Design, Development and Implementation of Trusted and Energy-aware Routing Protocols in Wireless Sensor Networks», Τμήμα Ηλεκτρολόγων Μηχανιών και Μηχανικών Υπολογιστών, Πολυτεχνείο Κρήτης, Αύγουστος 2014.
6. Μέλος στην επιτροπή επίβλεψης της μεταδιδακτορικής έρευνας του διδάκτορα Παπαστεργίου Σπυρίδωνα, Ιανουάριος 2014.
7. Μέλος της επιτροπής αξιολόγησης της διδακτορικής διατριβής του κ. Μέρμηγκα Δημήτριου με τίτλο «Ποσοτικοποίηση της ασφάλειας συστημάτων πληροφορικής με τη χρήση στοχαστικών μεθόδων», Τμήμα Πληροφορικής, Παν. Πειραιώς, Οκτώβριος 2012.
8. Μέλος της επιτροπής αξιολόγησης της διδακτορικής διατριβής του κ. Γλυνού Δημητρίου με τίτλο «Αρχιτεκτονική, Διαχείριση και Ασφάλεια Προγραμματισμένων Δικτυακών Υποδομών», Τμήμα Πληροφορικής, Παν. Πειραιώς, Ιούλιος 2012.
9. Μέλος της επιτροπής αξιολόγησης της διδακτορικής διατριβής του κ. Χαρίλα Δημητρίου με τίτλο «Τεχνικές Βέλτιστης Διαχείρισης Πόρων σε Ασύρματα Δίκτυα Επόμενης Γενιάς για Διασφάλιση Ποιότητας Υπηρεσίας», Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, ΕΜΠ, Μάιος 2012.
10. Μέλος της επιτροπής αξιολόγησης της διδακτορικής διατριβής του κ. Φραγκάκη Μιχαήλ με τίτλο «Μοντέλα Ασφάλειας και Εμπιστοσύνης για Συστήματα Κινητών Πρακτόρων Λογισμικού», Τμήμα Πληροφορικής, Παν. Πειραιώς, Ιούνιος 2011.
11. Μέλος της επιτροπής αξιολόγησης της διδακτορικής διατριβής του κ. Ζορμπά Δημητρίου με τίτλο «Αλγόριθμοι επιμήκυνσης της διάρκειας ζωής των ασύρματων δικτύων αισθητήρων υπό τον περιορισμό της κάλυψης στόχων», Τμήμα Πληροφορικής, Παν. Πειραιώς, Απρίλιος 2011.

(Μεταπτυχιακές διατριβές)

1. Επιβλέπων καθηγητής της μεταπτυχιακής διατριβής της κ.Τριαντοπούλου Σταματίας με τίτλο: "An Experimental Analysis of Current DDoS Attacks Based on a Provider Edge Router Honeynet", Φεβρουάριος 2018.
2. Επιβλέπων καθηγητής της μεταπτυχιακής διατριβής του κ. Ανδριτάκη Δημήτριου με τίτλο "Ασφάλεια σε τεχνολογίες του Διαδικτύου των Πραγμάτων (IoT): Μελέτη περίπτωσης και δοκιμαστική υλοποίηση με τη χρήση Raspberry Pi και Arduino", Φεβρουάριος 2018.
3. Επιβλέπων καθηγητής της μεταπτυχιακής διατριβής του κ. Κατόπη Χρήστου με τιλος"Ασφάλεια Διαδικτυακών Εφαρμογών με Χρήση Προγραμματιστικού Πλαισίου Django", Μάρτιος 2017.
4. Επιβλέπων καθηγητής της μεταπτυχιακής διατριβής του κ. Παναγάκου Αλέξανδρου με τίτλο: "Ανάλυση επιθέσεων rootkit σε περιβάλλον Linux", Νοέμβριος 2016.
5. Ντίκος Χρήστος, «Μελέτη και προσομοίωση πολιτικών και αρχιτεκτονικών ασφάλειας δικτύου», Σεπτέμβριος 2014.
6. Επιβλέπων καθηγητής της μεταπτυχιακής διατριβής του κ. Κατσαντώνη Κωνσταντίνου με τίτλο «Μελέτη ευπαθειών διαδικτυακών εφαρμογών βασισμένων στο σύστημα διαχείρισης περιεχομένου Joomla», ΠΜΣ ΠΣΠ, Οκτώβριος 2013.

7. Επιβλέπων καθηγητής της μεταπτυχιακής διατριβής του κ. Μαντά Στυλιανού με τίτλο «Μελέτη Πρωτοκόλλων Ανταλλαγής και Εγκαθίδρυσης Κρυπτογραφικών Κλειδιών», ΠΜΣ ΠΛΗ, Οκτώβριος 2013.
8. Επιβλέπων καθηγητής της μεταπτυχιακής διατριβής της κ. Μαθιουδάκη Ελένης με τίτλο «Τεχνολογίες Προστασίας Απορρήτου και Ιδιωτικότητας στο Διαδίκτυο», ΠΜΣ ΠΛΗ, Οκτώβριος 2012.
9. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Καζάνα Σπυρίδωνος, με τίτλο " Θεωρία και πρακτική σύνοψης τυποποιημένων τριπλετών RDF", ΠΜΣ ΠΣΠ, Οκτώβριος 2014.
10. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Ασλάνης-Βασιλείου Ιωάννη, με τίτλο "Ανασκόπηση Λύσεων Υπολογιστικού Νέφους", ΠΜΣ ΠΣΠ, Μάιος 2014.
11. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Φωτιάδη Γεώργιου με τίτλο: «Ανάλυση Επιχειρηματικών Μοντέλων Η-Εμπορίου με Έμφαση στις Ηλεκτρονικές Αγορές», ΠΜΣ ΠΣΠ, Νοέμβριος 2013.
12. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής της κ. Πατρώνη Μαρίκας με τίτλο: «Μελέτη Honeypot συστημάτων με πειραματική εφαρμογή», ΠΜΣ ΠΣΠ, Οκτώβριος 2013.
13. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Κοτρονάρου Δημήτριου με τίτλο: «Ψηφιακή Ανάλυση – τεχνικές διείσδυσης», ΠΜΣ ΠΛΗ, Οκτώβριος 2013.
14. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής της κ. Μαλιάππη Μαριλένας με τίτλο: «Σχεδίαση και υλοποίηση συστημάτων προσανατολισμένων στις διαδικασίες: υλοποίηση πιλοτικού συστήματος και αξιολόγηση της επίδοσης του με χρήση προσομοίωσης», ΠΜΣ ΠΣΠ, Οκτώβριος 2013.
15. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Αρώνη Νικόλαου με τίτλο: «Σχεδίαση και υλοποίηση web εφαρμογής για μη κερδοσκοπική οργάνωση με χρήση Drupal 7», ΠΜΣ ΠΣΠ, Οκτώβριος 2013.
16. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Βουτσαδάκη Σταμάτιου με τίτλο: «Αρχές Λειτουργίας, έλεγχος και εφαρμογές του πρωτοκόλλου CAN», ΠΜΣ ΠΣΠ, Ιούνιος 2013.
17. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Καλογερόπουλου Ιωάννη με τίτλο: «Ανάλυση Επικινδυνότητας του Πληροφοριακού Συστήματος Ασφαλιστικής Εταιρίας Πιστώσεων με τη χρήση του Ebios», ΠΜΣ ΠΛΗ, Ιούνιος 2013.
18. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής της κ. Κύρκο Μαρινέλα με τίτλο: «Ανάπτυξη εφαρμογής για την επικοινωνία με τη διαδικτυακή υπηρεσία XML-RPC», ΠΜΣ ΠΛΗ, Μάιος 2013.
19. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Χριστοδούλου Απόστολου με τίτλο: «Ανάπτυξη διαδικτυακής εφαρμογής αντικειμενοστρεφούς αρχιτεκτονικής για επικοινωνία με γεωγραφικό πληροφοριακό σύστημα με τη χρήση τεχνικών χωρικής επεξεργασίας», ΠΜΣ ΠΛΗ, Μάιος 2013.
20. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Αδάμου Κωνσταντίνου με τίτλο: «StudiesInGreece: Έμπιστη, συνεργατική πλατφόρμα, για την παροχή η-υπηρεσιών σε ξένους φοιτητές», ΠΜΣ ΠΛΗ, Απρίλιος 2013.
21. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής της κ. Καραχάλιου Αλεξάνδρας με τίτλο: «Multiple Helpdesk System Ανάπτυξη δικτυακού πληροφοριακού συστήματος Εφαρμογή για Λειτουργίες Τμημάτων Αρωγής», ΠΜΣ ΠΣΠ, Απρίλιος 2013.
22. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής της κας. Λούκα Μαρίας με τίτλο: «Δυναμική διαμόρφωση κριτηρίων γεωπληροφοριακής αναζήτησης», ΠΜΣ ΠΛΗ, Μάρτιος 2013.
23. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής της κας. Ζογκού Μαρίας με τίτλο: «Cross Layer design for QoS in IEEE 802.11s wireless mesh networks», ΠΜΣ ΠΣΠ, Μάρτιος 2013.

24. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Παπαδάκη Χρυσοβαλάντη με τίτλο: «Ασύρματα Δίκτυα LTE», ΠΜΣ ΠΣΠ, Ιανουάριος 2013.
25. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Κωνσταντινίδη Δημήτριου-Παναγιώτη με τίτλο: «Οικονομικές επιπτώσεις από την εισαγωγή του Cloud Computing – Ανάπτυξη επιχειρησιακού σχεδίου ενός νέου οργανισμού για την παροχή υπηρεσιών υπολογιστικού νέφους », ΠΜΣ ΠΣΠ, Νοέμβριος 2012.
26. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Παρά Δημητρίου με τίτλο: «Ασφάλεια πληροφοριών σε περιβάλλοντα η-μάθησης – SWES: Μελέτη περίπτωσης η-εξετάσεων μέσω ιστού», ΠΜΣ ΠΣΠ, Οκτώβριος 2012.
27. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Θεοδοσίου Νικόλαου με τίτλο: «Παρουσίαση του Microsoft Sharepoint 2010 και υλοποίηση ενδοδικτυακής πύλης ενός μεγάλου οργανισμού για τη διαχείριση πληροφοριών», Σεπτέμβριος 2012.
28. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής της κ. Γρηγορίου Μαρίας με τίτλο: «Θέματα ιδιωτικότητας και προστασίας στο Web 2.0», Σεπτέμβριος 2012.
29. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Χαλκιόπουλου Αντώνιου με τίτλο: «Σύγχρονα και ασφαλή ωκεανογραφικά πληροφοριακά συστήματα – Σύστημα ΠΟΣΕΙΔΩΝ», Σεπτέμβριος 2012.
30. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Αριστείδη Στριγκλή του ΠΜΣ ΠΛΗ με θέμα «Αμφίδρομες υπηρεσίες video πάνω από το δίκτυο 3G», Ιούλιος 2012.
31. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Νικολάου Παπανικολάου του ΠΜΣ ΠΛΗ με θέμα: «Εφαρμογή καταχώρησης δεδομένων μέσω διαδικτυακής υπηρεσίας (με χρήση του πρωτοκόλλου XML-RPC)». Ιούλιος 2012
32. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Αποστολάτου Ιωάννη με τίτλο: «Όταν η Wikipedia συναντά την Google: Απευθύνοντας ερωτήματα με νόημα στην μηχανή αναζήτησης Google», Μάρτιος 2012.
33. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Γεωργακά Γεωργίου με τίτλο: «Ονόματα Χώρου: Νομική προστασία κατά την Ελληνική έννομη τάξη», Μάρτιος 2012.
34. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής της κ. Γεωργίου Σοφίας με τίτλο: «Ανάλυση και διαχείριση επικινδυνότητας στα Πληροφοριακά Συστήματα – Υλοποίηση μεθοδολογίας σε επιχειρησιακό περιβάλλον», Μάρτιος 2012.
35. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής της κ. Χατζηστάμου Μαρίας με τίτλο: «Συνεργατικό Πληροφοριακό Σύστημα Μεταφορών», Μάρτιος 2012.
36. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Θεσσαλονικεύς Γεώργιου με τίτλο «Υλοποίηση του ενσωματωμένου επεξεργαστή ανοικτού κώδικα Plasma στην πλατφόρμα ALTERA DE2-115», Μάρτιος 2012.
37. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Κρομμύδα Κυριάκου με τίτλο «Μελέτη και εκτέλεση ενός λειτουργικού συστήματος πραγματικού χρόνου στον ενσωματωμένο επεξεργαστή Plasma», Φεβρουάριος 2012.
38. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής της κας Παππά Βασιλικής με τίτλο: «Δημιουργία σχολικού δικτύου υπολογιστών μέσω πολιτικών του Ενεργού Καταλόγου της Microsoft», ΠΜΣ ΠΛΗ, Ιανουάριος 2012.
39. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Γιαννόπουλου Αντώνιου με τίτλο: «Μελέτη, σχεδιασμός και αξιολόγηση εργαστηρίου δικτυακής ασφάλειας», ΠΜΣ ΠΣΠ, Ιανουάριος 2012.

40. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Πέτρου Χρυσάνθη με τίτλο «SAP και υπηρεσίες ιστού», Οκτώβριος 2011.
41. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Ιωάννη Βενετικίδη με τίτλο «Συγκριτική μελέτη αρχιτεκτονικών και εργαλείων σχεδίασης προγραμματιζόμενων διατάξεων λογικής», Οκτώβριος 2011.
42. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Καλαϊτζή Ανδρέα με τίτλο «Ενορχήστρωση υπηρεσιών ιστού με τη γλώσσα εκτέλεσης επιχειρησιακών διαδικασιών BPEL», Σεπτέμβριος 2011.
43. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Ζαχαριάδη Νικόλαου με τίτλο «Δημιουργία Ιστοτόπου με τη χρήση και παραμετροποίηση εργαλειών διαχείρισης περιεχομένου», Ιούλιος 2011.
44. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Νικολακάκη Στυλιανού με τίτλο «Πληροφοριακή ασφάλεια - Συστήματα πληροφοριακής ασφάλειας», Ιούλιος 2011.
45. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Νικολακάκη Στυλιανού με τίτλο «Πληροφοριακή ασφάλεια - Συστήματα πληροφοριακής ασφάλειας», Ιούλιος 2011.
46. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Δέλλιου Αναστάσιου με τίτλο «Συστήματα Διαχείρισης Γνώσης», Μάιος 2011.
47. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Λάππα Ανασάσιου με τίτλο «Επίδοση Χρονοπρογραμματιστή σε WiMAX δίκτυα», Μάρτιος 2011.
48. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής της κας. Κιουφεντζή Δανάης με τίτλο «Χρονοπρογραμματισμός Εργατικού Δυναμικού και Βελτιστοποίηση Προγραμματισμού Ανάθεσης Εργασιών», Μάρτιος 2011.
49. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής της κας. Σταυρουλάκη Μαρίας με τίτλο «Μοντέλα Εμπιστοσύνης», Μάρτιος 2011.
50. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Ντούσκα Δημήτριου με τίτλο «Ενώσεις Ασφάλειας Πληροφοριακών Συστημάτων και Ψηφιακών Πειστηρίων», Ιανουάριος 2011.
51. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Άγγελου-Χρήστου Αναδιώτη (τίτλος εργασίας, «Το Κατανεμημένο Σύστημα Αρχείων EuterpeFS»), Ιανουάριος 2011.
52. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Μέφερη Κυριάκου (τίτλος εργασίας, «Ανάπτυξη Εφαρμογής Mobile Social Space»), Νοέμβριος 2010.
53. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής της κ. Παλαιολόγου Κωνσταντίνας (τίτλος εργασίας, «Επιπτώσεις Ηλεκτρομαγνητικής Ακτινοβολίας»), Νοέμβριος 2010.
54. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής του κ. Κλεάνθη Νόου (τίτλος εργασίας, «Πληροφοριακά Συστήματα Υπολογιστικού Νέφους – Ασφάλεια & Ιδιωτικότητα»), Οκτώβριος 2010.
55. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής της κας Καλλιάνη Ευαγγελίας (τίτλος εργασίας, «Μοντέλα ελέγχου πρόσβασης σε περιβάλλον Windows"), Οκτώβριος 2010.
56. Μέλος της επιτροπής αξιολόγησης της μεταπτυχιακής διατριβής της κας Ξέρα Αθανασίας (τίτλος εργασίας, «Μοντέλα ελέγχου πρόσβασης και υλοποίηση RBAC με ενσωμάτωση χρονικών περιορισμών σε περιβάλλον Windows"), Οκτώβριος 2010.

ΠΑΡΑΡΤΗΜΑΤΑ

Ι. Γνωστικές περιοχές ενδιαφέροντος και έρευνας

1. Ανωνυμία και ιδιωτικότητα στο διαδίκτυο (Anonymity and privacy over the Internet)
2. Προστασία Κρίσιμων Υποδομών (Critical Infrastructure Protection)
3. Ασφάλεια σε διάχυτα υπολογιστικά περιβάλλοντα (Security in Pervasive Computing Environment)
4. Ασφάλεια Εφοδιαστικής Αλυσίδας (Supply Chain Security)
5. Ασφάλεια στο Διαδίκτυο των Πραγμάτων (IoT Security)
6. Απόρρητο και ιδιωτικότητα σε τηλεπικοινωνιακά δίκτυα (Privacy Assurance in Telecommunications)
7. Ασφάλεια συστημάτων κινητού κώδικα και κινητού πράκτορα (mobile code / mobile agent security)
8. Ασφάλεια ευφυών δικτύων (Intelligent Network Security)
9. Ασφάλεια κινητών ad hoc ασύρματων δικτύων (Wireless Ad hoc Network Security)
10. Ασφάλεια δικτύων αισθητήρων (Sensor Network security)
11. Ψηφιακές υπογραφές και πολύ-υπογραφές (Digital Signatures and Multi-signatures)
12. Συστήματα διαμοίρασης και ανάκτησης κλειδιού (Key Escrow and Key Recovery)
13. Έλεγχος πρόσβασης βασισμένη σε ρόλους (Role Based Access Control)
14. Μεθοδολογίες ανάλυσης πληροφοριακού κινδύνου (Risk Analysis)
15. Πολιτικές και διαδικασίες ασφάλειας (Security Policies and Procedures)
16. Συστήματα ανταλλαγής και εγκαθίδρυσης κλειδιού (Key Exchange, Key Establishment)

ΙΙ. Αξιοποίηση επιστημονικού έργου από άλλους ερευνητές

Στατιστικά στοιχεία (Πηγή scholar.google.com):

- Σύνολο ετεροαναφορών : 1.705
- h-Index: 23
- h10-index: 38

ΙΙΙ. ΥΠΟΜΝΗΜΑ ΔΗΜΟΣΙΕΥΣΕΩΝ Π. ΚΟΤΖΑΝΙΚΟΛΑΟΥ

ΙΙΙ.1 Συνοπτική ανάλυση δημοσιεύσεων σε βιβλία

1. *Συνοπτική παρουσίαση της εργασίας* **[B-12]** *"Advanced Persistent Threats and Zero-Day Exploits in Industrial Internet of Things",* I.Stellios, P. Kotzanikolaou. And M. Psarakis

   Περίληψη: – Η μεταποιητική βιομηχανία, τα δίκτυα ηλεκτρικής ενέργειας, η αλυσίδα εφοδιασμού, η παραγωγή τροφίμων και οι μονάδες επεξεργασίας νερού έχουν εξαρτηθεί σε μεγάλο βαθμό από τα συστήματα Βιομηχανικού Αυτοματισμού και Ελέγχου (ΒΑΕ). Η ενσωμάτωση της τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ) διαδραμάτισε σημαντικό ρόλο στην εξέλιξη αυτών των συστημάτων. Νέες αναδυόμενες τάσεις και τεχνολογίες, όπως το Internet-of-Things (IoT), αλληλεπιδρούν με τα παραδοσιακά, απομονωμένα συστήματα ΒΑΕ. Τομείς όπως η κατασκευή, τα ηλεκτρικά δίκτυα, τα φαρμακευτικά προϊόντα και οι εγκαταστάσεις επεξεργασίας νερού ενσωματώνουν μέρος αυτών των «έξυπνων» τεχνολογιών προκειμένου να αυξηθεί η αποδοτικότητα και να μειωθεί το κόστος παραγωγής. Παρά τα πλεονεκτήματά της, η διασύνδεση μεταξύ έξυπνων συστημάτων και παραδοσιακών συστημάτων ΒΑΕ, δημιουργεί πολύπλοκες αλληλεξαρτήσεις, οι οποίες με τη σειρά τους καθιστούν επιτακτική την ανάγκη για εξειδικευμένα μέτρα ασφάλειας. Αυτή η ταχεία εξέλιξη επηρέασε πολύ το πεδίο απειλών. Προκειμένου να κατανοήσουμε αυτή τη ριζική αλλαγή, παρουσιάζουμε και αναλύουμε πρόσφατες και καλά τεκμηριωμένες επιθέσεις, οι οποίες στοχεύουν σε συστήματα Κρίσιμων Υποδομών. Συγκεκριμένα, εστιάζουμε σε εξελιγμένες επιθέσεις ενάντια σε διασυνδεδεμένες συσκευές αυτοματοποίησης και παρακολούθησης, συναφείς πλατφόρμες και συστήματα λογισμικού (π.χ. Προγραμματιζόμενοι Λογικοί Ελεγκτές - PLC, βιομηχανικά ρομπότ) που εγκαθίστανται σε βιομηχανικές εγκαταστάσεις και δίκτυα παραγωγής, μεταφοράς και διανομής έξυπνων δικτύων.

2. *Συνοπτική παρουσίαση της εργασίας* **[B-11]** *"Methodologies and Strategies for Critical Infrastructure Protection",* N. Petrakos and P. Kotzanikolaou.

   Περίληψη: – Η προστασία των υποδομών ζωτικής σημασίας σε εθνικό επίπεδο αποτελεί ένα σύνθετο έργο. Περιλαμβάνει διάφορα βήματα, όπως η καταγραφή, η ιεράρχηση προτεραιοτήτων και η προστασία των υποδομών και υπηρεσιών που είναι ζωτικής σημασίας για την ευημερία της κοινωνίας. Παρόλο που ορισμένοι τομείς, υποτομείς και υπηρεσίες φαίνεται να είναι πολύ σημαντικοί για όλες τις χώρες, άλλοι μπορεί να διαφέρουν ως προς τη σημασία τους βάσει των ειδικών οικονομικών, περιβαλλοντικών και κοινωνικών χαρακτηριστικών κάθε χώρας. Στο κεφάλαιο αυτό εξετάζουμε τις υφιστάμενες μεθοδολογίες και τις εθνικές στρατηγικές για την προστασία των κρίσιμων υποδομών. Εξετάζουμε μεθοδολογίες για τον εντοπισμό και την αξιολόγηση κρίσιμων τομέων και υπηρεσιών, που βασίζονται σε διαφορετικές προσεγγίσεις. Εξετάζουμε τις κοινές πρακτικές που εφαρμόστηκαν σε διάφορες χώρες για τον προσδιορισμό των υποδομών ζωτικής σημασίας και για τη θέσπιση εθνικών σχεδίων προστασίας. Τέλος, περιγράφουμε ένα σύνολο στόχων που βρίσκονται συνήθως σε διαφορετικές μεθοδολογίες και βέλτιστες πρακτικές για την προστασία κρίσιμης υποδομής.

3. *Συνοπτική παρουσίαση της εργασίας* **[B-10]** *"Security and Privacy in Next Generation Networks and Services",* P. Kotzanikolaou.

   Περίληψη: – Η ανάπτυξη δικτύων νέας γενιάς, όπως τα ασύρματα ευρυζωνικά δίκτυα και τα ασύρματα δίκτυα ad hoc, οδήγησε στη διάδοση νέων κινητών, διάχυτων και "απανταχού" υπηρεσιών, όπως τα κοινωνικά δίκτυα, οι υπηρεσίες βάσει τοποθεσίας ή οι υπηρεσίες cloud computing. Αυτά τα νέα παραδείγματα και υπηρεσίες δικτύων εγείρουν σοβαρές ανησυχίες για την προστασία της ιδιωτικότητας. Αυτό το κεφάλαιο εξετάζει τα θέματα ασφάλειας και ιδιωτικότητας στα δίκτυα νέας γενιάς. Αρχικά, παρουσιάζεται μια γενική κατηγοριοποίηση διαφόρων δημοφιλών δικτύων και υπηρεσιών. Στη συνέχεια εξετάζονται οι απειλές ασφάλειας και ιδιωτικής ζωής που εντοπίζονται για

κάθε κατηγορία, μαζί με μια σύντομη ανασκόπηση των σχετικών απαιτήσεων ασφαλείας και στρατηγικών μετριασμού που περιγράφονται στην πρόσφατη βιβλιογραφία.

4. *Συνοπτική παρουσίαση της εργασίας* **[B-9]** *"Risk assessment of multi-order dependencies between critical information and communication infrastructures",* P. Kotzanikolaou, M. Theoharidou, D. Gritzalis.

   Περίληψη: – Η αποτίμηση των κινδύνων ασφάλειας των πληροφοριακών και επικοινωνιακών υποδομών είναι μία δύσκολη προσπάθεια, εξαιτίας της πολυπλοκότητας ων Κρίσιμων Υποδομών (ΚΥ), αλλά και των μεταξύ τους αλληλεξαρτήσεων. Το κεφάλαιο αυτό παρουσιάζει ορισμένες βασικές αρχές της αποτίμησης κινδύνου για ΚΥ. Επιπλέον, περιγράφει μία πρόσφατη μεθοδολογία για ανάλυση κρισιμότητας (criticality assessment). Ο κύριος στόχος αυτής της μεθοδολογίας είναι η αποτίμηση του κινδύνου μίας υποδομής (ή ενός τομέα ΚΥ) , λαμβάνοντας υπόψη τις αλληλεξαρτήσεις μεταξύ διαφορετικών ΚΥ ή τομέων ΚΥ. Η μεθοδολογία που παρουσιάζεται είναι συμβατή με τα τρέχοντα πρότυπα και τις βέλτιστε πρακτικές της ασφάλειας πληροφοριακών συστημάτων. Το βασικό χαρακτηριστικό της μεθοδολογίας είναι η προσπάθεια που καταβάλει για να συσχετίσει τις τόσο τις οργανωτικές, όσο και τις κοινωνικές συνέπειες των πιθανών περιστατικών ασφάλειας, συσχέτιση η οποία συχνά παραβλέπεται από τις γνωστές μεθοδολογίες αποτίμησης πληροφοριακού κινδύνου.

5. *Συνοπτική παρουσίαση της εργασίας* **[B-8]***«Μονόδρομες συναρτήσεις και Γεννήτορες ψευδοτυχαίων αριθμών»,* Κ. Πατσάκης, Π. Κοτζανικολάου και Δ. Πολέμη.

   Περίληψη: – Σε αυτό το κεφάλαιο γίνεται μία αναλυτική περιγραφή των μονόδρομων συναρτήσεων και των εφαρμογών τους στη σύγχρονη κρυπτογραφία. Επειδή στην κρυπτογραφία είναι απαραίτητο να χρησιμοποιούνται όσο το δυνατόν πιο τυχαίοι αριθμοί, θα γίνει επίσης και μία παρουσίαση των ψευδοτυχαίων γεννητριών, συναρτήσεων και μεταθέσων. Σε αυτό το πλαίσιο θα παρουσιαστούν οι απαραίτητες ιδιότητες που θα πρέπει να έχουν οι μηχανισμοί αυτοί, προκειμένου να δημιουργούν ασφαλείς ψευδοτυχαίους αριθμούς.

6. Συνοπτική ανάλυση της εργασίας **[B-7]** *«Διατήρηση Δεδομένων Επικοινωνίας και Διασφάλιση του Απορρήτου και της Ιδιωτικότητας»*, Π. Κοτζανικολάου, Δ. Πολέμη και Χ. Δουληγέρης:

   Περίληψη: – Σε ολοένα και περισσότερες χώρες, οι πάροχοι δικτύων ηλεκτρονικών επικοινωνιών υποχρεούνται από την νομοθεσία να διατηρούν τα δεδομένα επικοινωνίας των συνδρομητών τους για συγκεκριμένο χρονικό διάστημα. Το είδος των συλλεγόμενων δεδομένων και ο τρόπος επεξεργασίας αυτών κατά τη διάρκεια της διατήρησής τους καθορίζεται μέσω Πολιτικών Ιδιωτικότητας που κοινοποιούνται από τους παρόχους. Οι Πολιτικές Ιδιωτικότητας θα πρέπει να είναι σύμφωνες με το ισχύον νομοθετικό πλαίσιο και να αναφέρουν ρητά τους όρους κάτω από τους οποίους πραγματοποιείται μια επικοινωνία. Βασικός σκοπός της διατήρησης των δεδομένων είναι η διευκόλυνση πιθανών ερευνών, σε μελλοντικό χρόνο, για τη διερεύνηση παράνομων δραστηριοτήτων. Το γεγονός αυτό έχει δημιουργήσει κοινωνικές ανησυχίες και ερωτήματα τεχνικής φύσεως, εφόσον τα διατηρούμενα δεδομένα περιλαμβάνουν ευαίσθητη πληροφορία. Πιθανή κατάχρηση των δεδομένων πέρα από τα όρια που έχουν καθοριστεί στις Πολιτικές Ιδιωτικότητας οδηγεί αναμφισβήτητα σε παραβίαση του απορρήτου και απώλεια της ιδιωτικότητας των συνδρομητών. Στο Κεφάλαιο αυτό εξετάζονται θέματα ιδιωτικότητας και απορρήτου που σχετίζονται με τη διατήρηση δεδομένων στις ηλεκτρονικές επικοινωνίες.

7. Συνοπτική ανάλυση της εργασίας **[B-6]** *"Network Security", Christos Douligeris and Panayiotis Kotzanikolaou.*

Περίληψη: – Η παγκόσμια ανάπτυξη διαφόρων τύπων δικτύων όπως είναι το Internet, τα δίκτυα τρίτης γενιάς, τα εταιρικά δίκτυα, τα ασύρματα δίκτυα WiFi ή τα προσωπικά δίκτυα Bluetooth για να αναφέρουμε μερικές περιπτώσεις, έχουν μετατρέψει τη δικτύωση σε καθημερινή εργασία. Όμως, οι κοινωνικές, οικονομικές, εμπορικές και ηθικές προεκτάσεις των διάφορων δικτυακών εφαρμογών, έχουν δημιουργήσει ανάγκες σχετικά με την ασφάλεια της χρήσης των δικτύων. Το άρθρο αυτό πραγματεύεται τα ζητήματα ασφάλειας των δικτύων. Αρχικά, παρουσιάζονται οι έννοιες σχετικά με την ασφάλεια πληροφοριών και δικτύων και αναλύονται οι στόχοι της ασφάλειας δικτύων. Επεξηγούνται οι έννοιες των απειλών, αδυναμιών και κινδύνων, ενώ περιγράφονται βασικές κατηγορίες απειλών και επιθέσεων ασφάλειας δικτύων. Η ασφάλεια των δικτύων επιτυγχάνεται μέσω υπηρεσιών ασφάλειας οι οποίες και παρουσιάζονται, μαζί με ευρέως χρησιμοποιούμενους μηχανισμούς ασφάλειας, οι οποίοι και υλοποιούν τις υπηρεσίες ασφάλειας. Τέλος, αναφέρονται οι διαφορές των απαιτήσεων ασφάλειας των ασύρματων δικτύων, σε αντίθεση με τις απαιτήσεις των σταθερών δικτύων.

8. Συνοπτική ανάλυση της εργασίας **[B-5]** *"Securing Networks against Extreme Attacks", Mike Burmester and Panayiotis Kotzanikolaou.*

   Περίληψη: – Το πρόβλημα της ασφάλειας επικοινωνιών έχει μελετηθεί εκτενώς στη διεθνή βιβλιογραφία και διάφορα μοντέλα ανάλυσης επιθέσεων έχουν προταθεί. Στο κλασικό μοντέλο Βυζαντινών επιθέσεων των Lamport, Shostac και Pease ο αντίπαλος έχει απεριόριστες δυνατότητες αλλά έχει περιορισμό στον αριθμό των κόμβων που μπορεί να επιτεθεί. Οι Hirt και Martin επέκτειναν αυτό το μοντέλο, διευρίνοντας τον τύπο των συνόλων των κόμβων. .Σε αυτή την εργασία εξετάζουμε ένα συγκεκριμένο μοντέλο επιθέσεων, το οποίο ορίζουμε ως «ακραίες επιθέσεις», στο οποίο ο αντίπαλος προσβάλει το σύστημα, δίχως κανένα υπολογισμό των συνεπειών ή των πιθανών οφελών του.Μία ακραία επίθεση μπορεί να θεωρηθεί ως μία εκτεταμένη Βυζαντινή επίθεση, στην οποία ο αντίπαλος επεκτείνει την ισχύ της επίθεσης, πραγματοποιώντας ταυτόχρονα μία ανεξάρτητη επίθεση (π.χ. μία φυσική επίθεση). Τέτοιες επιθέσεις επεκτείνουν το εύρος των Βυζαντινών σφαλμάτων. Για παράδειγμα, παρόλο που ένας κόμβος μπορεί να μην ανήκει στο σύνολο των κόμβων που έχουν προσβληθεί από τον αντίπαλο, δεν είνα σε κατάσταση κανονικής λειτουργίας λόγω μίας φυσικής επίθεσης. Η ασφάλεια των δικτύων έναντι τέτοιων επιθέσεων είναι δύσκολος στόχος, αλλά ιδιαίτερα σημαντικός για εφαρμογές κρίσιμων υποδομών, τραπεζικές και οικονομικές εφαρμογές, ή υπηρεσίες έκτακτης ανάγκης. Η προτεινόμενη λύση βασίζεται σε αναγνωρισμένα πρότυπα και κριτήρια ασφάλειας για έμπιστο υπολογισμό και ειδικότερα σε μεθόδους πλεονασμού (μέσω υψηλής διαθεσιμότητας) και ανεξαρτησίας (μέσω διάκρισης καθηκόντων).

9. Συνοπτική ανάλυση της εργασίας **[B-4]** *"Introduction to Network Security", Panayiotis Kotzanikolaou, and Christos Douligeris.*

   Περίληψη: – Το κεφάλαιο αυτό εισάγει βασικούς όρους σχετικά με την ασφάλεια δικτύων, ώστε να βοηθήσει τους αναγνώστε να έχουν μία κοινή θεώρηση των θεμάτων που αναπτύσσονται ειδικότερα στα επόμενα κεφάλαια. Ορίζει την ασφάλεια δικτύων από τεχνική και οικονομική θεώρηση και περιγράφει κοινές απειλές και επιθέσεις ασφάλειας στα διάφορα επίπεδα δικτύου. Τέλος, περιγράφει τις περιοχές της ασφάλειας δικτύων που καλύπτονται στο βιβλίο σε τέσσερις βασικές ενότητες: Σταθερών Δικτύων, Δικτυακών Υπηρεσιών, Ασύρματων Δικτύων και Υποδομών Ασφάλειας και Εμπιστοσύνης. Η χρήση κρυπτογραφίας, τα νομικά ζητήματα και τα πρότυπα ασφάλειας καλύπτονται σε ειδικά παραρτήματα για εύκολη αναφορά.

10. Συνοπτική ανάλυση της εργασίας **[B-3]** *"Mobile Agent Security", Panayiotis Kotzanikolaou, Rosa Mavropodi, Christos Douligeris and Vassilios Chrissikopoulos.*

    Περίληψη: – Τα παραδοσιακά κατανεμημένα συστήματα βασίζονταν σε στατικές διαδικασίες μεταξύ απομακρυσμένων διακομιστών, οι οποίοι επικοινωνούσαν με σύγχρονες ή ασύγχρονες κλήσεις (π.χ. Κλήσεις Απομακρυσμένων Διαδικασιών – RPC). Οι τεχνολογίες κινητού κώδικα επεκτείνουν τις αρχές

τις απομακρυσμένης εκτέλεσης, περιλαμβάνοντας περισσότερη προγραμματιστική συμπεριφορά σε ένα κινητό αντικείμενο. Οι τεχνολογίες κινητού πράκτορα επιτρέπουν σε ένα εκτελέσιμο κινητό πράκτορα ο οποίος εκτελείται σε ένα συγκεκριμένο διακομιστή, να διακόψει την εκτέλεση, να μεταφερθεί σε ένα απομακρυσμένο διακομιστή και να συνεχίσει εκεί την εκτέλεσή του. Οι κινητοί πράκτορες είναι ιδανικοί για να παρέχουν αποτελεσματική διαχείριση δικτύων σε κατανεμημένα περιβάλλοντα, όπως είναι τα Ευφυή Δίκτυα. Σε αυτό το κεφάλαιο εξετάζουμε τα ζητήματα ασφάλειας των κινητών πρακτόρων και περιγράφουμε αρχιτεκτονικές για ασφαλή διαχείριση Ευφυών Δικτύων χρησιμοποιώντας κινητούς πράκτορες.

11. Συνοπτική ανάλυση της εργασίας **[B-2]** *"Security In Mobile Ad Hoc Networks", Mike Burmester, Panayiotis Kotzanikolaou and Christos Douligeris.*

    Περίληψη: -. Στόχος μας σε αυτό το κεφάλαιο είναι να παρουσιάσουμε μία σύνοψη των λύσεων ασφάλειας για Κινητά Δίκτυα Ειδικού Σκοπού (Mobile Ad hoc Networks). Θα εστιάσουμε σε ζητήματα δρομολόγησης και ασφαλών συνδέσεων, ενώ θα εξετάσουμε ορισμένες νέες απειλές και τις πιθανές τους λύσεις. Θα εξετάσουμε ένα μεγάλο εύρος περιπτώσεων, από σχεδόν στατικά δίκτυα μέχρι εξαιρετικά δυναμικά (μεταβαλλόμενα) δίκτυα. Σε αντίθεση με τα παραδοσιακά δίκτυα τα οποία χρησιμοποιούν δικτυακά στοιχεία αποκλειστικά για σηματοδοσία, δρομολόγηση και διαχείριση δικτύου, στα Κινητά Δίκτυα Ειδικού Σκοπού αυτές οι διαδικασίες πραγματοποιούνται μέσα από δυναμική αλληλεπίδραση των κόμβων. Όμως, πολλές φορές δεν υπάρχει εκ των προτέρων εμπιστοσύνη ώστε να διασφαλίζεται η σωστή πραγματοποίηση αυτών των διαδικασιών. Η εμπιστοσύνη είναι το δεύτερο βασικό θέμα που θα εξετάσουμε. Επίσης, θα μελετήσουμε διάφορα μοντέλα ασφάλειας, από απλά απλούς κόμβους με περιορισμένες δυνατότητες και δυνατότητα τοπικής διαχείρισης εμπιστοσύνης, μέχρι στρατιωτικά μοντέλα όπου η εμπιστοσύνη διαχειρίζεται κεντρικά και οι κόμβοι έχουν αρκετές δυνατότητες για την εκτέλεση των απαιτούμενων κρυπτογραφικών μηχανισμών οι κόμβοι. Θα μελετήσουμε τις απαιτούμενες συνθήκες για ασφαλή επικοινωνία για διαφορετικές περιπτώσεις και θα συζητήσουμε πιθανές εφαρμογές.

12. Συνοπτική ανάλυση της εργασίας **[B-1]** *"Cryptography Primer: An Introduction to Cryptographic Principles and Algorithms", Panayiotis Kotzanikolaou and Christos Douligeris.*

    Περίληψη: - Το κεφάλαιο αυτό παρέχει στον αναγνώστη ένα βασικό υπόβαθρο στην εφαρμοσμένη κρυπτογραφία, με σκοπό να βοηθήσει στην κατανόηση των μηχανισμών ασφάλειας που παρουσιάζονται στα διάφορα κεφάλαια του βιβλίου και που χρησιμοποιούν κρυπτογραφικούς αλγόριθμους και πρωτόκολλα. Γίνεται μία εισαγωγή σε κρυπτογραφικές αρχές, μαζί με ευρέως χρησιμοποιούμενους αλγόριθμους και πρωτοκόλλα κρυπτογράφησης. Παρουσιάζονται συνοπτικά οι γεννήτριες παραγωγής τυχαίων ψηφίων, οι συναρτήσεις κατακερματισμού, τα συμμετρικά και ασύμμετρα κρυπτοσυστήματα, οι ψηφιακές υπογραφές και σε ζητήματα διαχείρισης κρυπτογραφικών κλειδιών.

III.2 Συνοπτική ανάλυση δημοσιεύσεων σε επιστημονικά περιοδικά

(Δημοσιευμένες Εργασίες – Σε διεθνή περιοδικά)

1. Συνοπτική ανάλυση της εργασίας **[J-23]** *"A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services"*, I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz and J. Lopez.

Περίληψη: – Καθώς η ανάπτυξη του Διαδικτύου των Πραγμάτων (IoT) είναι εκθετική, δεν αποτελεί έκπληξη το γεγονός ότι πολλές πρόσφατες κυβερνοεπιθέσεις βασίζονται σε IoT τεχνολογίες: αρχικά ο εισβολέας εκμεταλλεύεται κάποια ευάλωτη τεχνολογία IoT, ως το πρώτο βήμα προς την παραβίαση

ενός κρίσιμου συστήματος το οποίο συνδέεται, με κάποιο τρόπο, με το IoT σύστημα. Για ορισμένους τομείς, όπως η βιομηχανία, τα έξυπνα δίκτυα, οι μεταφορές και οι ιατρικές υπηρεσίες, η σημασία τέτοιων επιθέσεων είναι προφανής. Ωστόσο, σε άλλους τομείς όπου οι τεχνολογίες IoT βρίσκονται συνήθως κοντά στον τελικό χρήστη, όπως είναι τα έξυπνα σπίτια, οι επιθέσεις αυτές μπορούν να υποτιμηθούν, επειδή δεν εξετάζονται όλα τα πιθανά μονοπάτια επίθεσης. Σε αυτή την εργασία, αναλύονται πλήθος πραγματικών επιθέσεων που βασίζονται σε τεχνολογίες IoT και που έχουν πραγματοποιηθεί από το 2010 μέχρι σήμερα. Για κάθε τομέα, δίνουμε έμφαση στις πρόσφατες, επαληθευμένες επιθέσεις. Αναλύουμε μεθοδολογικά αντιπροσωπευτικές επιθέσεις που καταδεικνύουν άμεσα, έμμεσα, αλλά και αφανή μονοπάτια επίθεσης εναντίον κρίσιμων συστημάτων και υπηρεσιών. Ο στόχος μας είναι τριπλός: 1) να αξιολογηθούν οι επιθέσεις με μία προσέγγιση ανάλυσης κινδύνου, προκειμένου να αναδείξουν το σημερινό τοπίον απειλών 2) να εντοπισθούν κρυφά μονοπάτια επιθέσεων, τα οποία μπορεί να απειλούν κρίσιμες υποδομές και υπηρεσίες και 3) να εξεταστούν πιθανά μέτρα ελέγχου και στρατηγικές για την αντιμετώπιση τέτοιων επιθέσεων σε όλους τους υπό εξέταση τομείς εφαρμογής.

2. Συνοπτική ανάλυση της εργασίας **[J-22]** *"Design and validation of the Medusa supply chain risk assessment methodology and system", S.* Papastergiou, S. Polemi, N., & P. Kotzanikolaou.

Περίληψη: – Οι αλυσίδες εφοδιασμού – ΑΕ) (supply chains – SC) μπορούν να θεωρηθούν ως σύνθετα διασυνδεδεμένα συστήματα που διαδραματίζουν ζωτικό ρόλο στη μεταφορά και την παράδοση αγαθών και υπηρεσιών. Μία αλυσίδα εφοδιασμού συνήθως περιλαμβάνει διάφορες κρίσιμες υποδομές, κυρίως στον τομέα των μεταφορών, και εμφανίζει ενδο-τομεακές και διασυνοριακές εξαρτήσεις με διάφορες επιχειρηματικές οντότητες. Παρόλο που έχουν καταβληθεί προσπάθειες για την τυποποίηση των προσεγγίσεων της εκτίμησης κινδύνου της αλυσίδας εφοδιασμού (SCRA), υπάρχει έλλειψη στοχοθετημένων μεθοδολογιών. Σε προηγούμενη εργασία μας (Polemi and Kotzanikolaou 2015) έχουμε προτείνει μια προκαταρκτική εκδοχή της μεθοδολογίας SCRA Medusa, σύμφωνα με το πρότυπο ISO28001. Ο πρωταρχικός στόχος της μεθοδολογίας Medusa είναι να εκτιμήσει τους κινδύνους μιας ΑΕ που αυξάνεται από τις διασυνδέσεις και τις αλληλεξαρτήσεις μεταξύ της διάφορες οντότητες μέσα σε αυτό. Σε αυτή την εργασία, επεκτείνουμε σημαντικά την προηγούμενη εργασία μας προκειμένου να προσδιοριστούν όλες οι συγκεκριμένες λεπτομέρειες της μεθοδολογίας Medusa, όπως οι εκτιμήσεις των επιπέδων απειλής, συνέπειας, οι κλίμακες κινδύνου, οι κλιμακούμενοι κίνδυνοι, η δημιουργία μιας βασικής πολιτικής ασφαλείας ΑΕ και ο προσδιορισμός των ελέγχων ασφαλείας. Επιπλέον, επικυρώνουμε τη μεθοδολογία μας βάσει πραγματικών σεναρίων, τα οποία προέρχονται από τις πιλοτικές λειτουργίες του έργου Medusa και παρέχουμε λεπτομέρειες εφαρμογής του συνεργατικού συστήματος Medusa, το οποίο φιλοξενεί τη μεθοδολογία και προσφέρει υπηρεσίες SCRA στις εμπλεκόμενες οντότητες.

3. Συνοπτική ανάλυση της εργασίας **[J-21]** *"Security Awareness of the Digital Natives", V.* Gkioulos., G. Wangen, S. Katsikas, G. Kavallieratos, and P. Kotzanikolaou.

Περίληψη: – Οι νέες γενιές χρησιμοποιούν εκτεταμένα κινητές συσκευές, όπως smartphones, tablet και φορητούς υπολογιστές, ενώ μια πληθώρα κινδύνων ασφάλειας που συνδέονται με τέτοιες συσκευές προκαλούνται από ευπάθειες που σχετίζονται με τη συμπεριφορά των χρηστών. Επιπλέον, ο αριθμός των παραβιάσεων ασφαλείας μέσω φορητών συσκευών αυξάνεται εκθετικά. Έτσι, η ανάπτυξη κατάλληλων μεθόδων αντιμετώπισης κινδύνων απαιτεί τη διερεύνηση του τρόπου με τον οποίο οι ψηφιακοί γενιά (δηλαδή όλων όσων είναι γεννημένοι και εκτραφέντες στην ψηφιακή εποχή) χρησιμοποιούν τις κινητές συσκευές τους και το επίπεδο συνειδητοποίησης της ασφάλειας τους, προκειμένου να εντοπίσουν κοινά πρότυπα χρήσης με αρνητική επίπτωση ασφάλειας. Σε αυτό το άρθρο, παρουσιάζουμε τα αποτελέσματα μιας έρευνας που διεξήχθη σε έναν πολυεθνικό πληθυσμό δειγματοληψίας με διαφορετικό υπόβαθρο και επίπεδα ικανοτήτων όσον αφορά την ασφάλεια, για τον εντοπισμό αποκλίσεων στη συμπεριφορά των χρηστών λόγω περιφερειακών, εκπαιδευτικών και άλλων

παραγόντων. Τα αποτελέσματά μας υπογραμμίζουν σημαντικές επιρροές στη συμπεριφορά της ψηφιακής γενιάς, οι οποίες προκύπτουν από την εμπιστοσύνη των χρηστών, το εκπαιδευτικό υπόβαθρο και τις παραμέτρους που σχετίζονται με τη χρηστικότητα και την προσβασιμότητα. Τα αποτελέσματα αυτής της μελέτης δικαιολογούν την ανάγκη για περαιτέρω ανάλυση του θέματος, προκειμένου να προσδιοριστεί η επίδραση της σημασιολογίας, αλλά και η εδραίωση ευρέων και ανθεκτικών μοντέλων χρηστών.

4. Συνοπτική ανάλυση της εργασίας **[J-20]** "*Broadcast Anonymous Routing (BAR): Scalable Real-Time Anonymous Communication", P. Kotzanikolaou, G. Chatzisofroniou, M. Burmester*.

Περίληψη: – Σε αυτή την εργασία προτείνουμε το σύστημα BAR, ένα κλιμακωτό (scalable) ανώνυμο σύστημα επικοινωνίας μέσω Διαδικτύου που συνδυάζει τα χαρακτηριστικά των δικτύων εκπομπής (dc-net) με την πολυεπίπεδη κρυπτογράφηση των δικτύων μίξης (mix-net). Το κύριο πλεονέκτημα του BAR έναντι άλλων συστημάτων εκπομπής είναι η δυνατότητα ρύθμισης εύρους ζώνης: με τη χρήση επιλεκτικής μετάδοσης μπορεί να μειώσει σημαντικά το απαιτούμενο εύρος ζώνης για μικρή αύξηση της καθυστέρησης, χωρίς να επηρεάζεται η ανωνυμία. Σε αντίθεση με τα συστήματα mix-net, το BAR παρέχει προστασία από την έλλειψη αξιοπιστίας ενώ ταυτόχρονα ελαχιστοποιεί τη χρήση λειτουργιών δημόσιου κλειδιού. Το BAR παρέχει την ανωνυμία του αποστολέα, του παραλήπτη και της συνόδου με εμπιστευτική μυστικότητα. Αναλύουμε την αποτελεσματικότητα του BAR για διάφορες διαμορφώσεις ανωνυμίας χρησιμοποιώντας μια πρωτότυπη υλοποίηση.

5. Συνοπτική ανάλυση της εργασίας **[J-19]** "*Time-based Critical Infrastructure Dependency Analysis for Large-Scale and Cross-Sectoral Failures", G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, G. Lykou, D. Gritzalis*.

Περίληψη: – Η ανάλυση εξαρτήσεων των υποδομών ζωτικής σημασίας (Critical Infrastructure dependency analysis) είναι ένα πρόβλημα υπολογιστικής έντασης όταν πρόκειται για μεγάλης κλίμακας, διατομεακές, διαδοχικές (cascading) και κοινής αιτίας (common cause) αποτυχίες. Το πρόβλημα εντείνεται όταν πρόκειται για μια δυναμική ανάλυση του χρόνου εξάρτησης. Το παρόν έγγραφο επεκτείνει μια προηγούμενη μεθοδολογία ανάλυσης κινδύνου που βασίζεται σε γραφήματα για να αξιολογεί δυναμικά την εξέλιξη των αστοχιών κατά τη διάρκεια του χρόνου. Χρησιμοποιούνται διάφορα μοντέλα ανάπτυξης για την καταγραφή αργών, γραμμικών και ταχέως εξελισσόμενων αποτελεσμάτων, αλλά αντί να χρησιμοποιούν στατικές προβολές, η εξέλιξη κάθε εξάρτησης "αντικειμενοποιείται" από ένα ασαφές σύστημα το οποίο επίσης λαμβάνει υπόψη τα αποτελέσματα των κοντινών εξαρτήσεων. Για να επιτευχθεί αυτό, ο αντίκτυπος (και, ενδεχομένως, ο κίνδυνος) κάθε εξάρτησης ποσοτικοποιείται στον άξονα του χρόνου σε μια μορφή ασαφούς λογικής. Επιπλέον, η μεθοδολογία επεκτείνεται για να αναλύσει μείζονες αστοχίες που προκαλούνται από ταυτόχρονες καταρρεύσεις κοινής αιτίας. Χρησιμοποιείται ένα εργαλείο ανάλυσης εξάρτησης κρίσιμης υποδομής, το CIDA, το οποίο υλοποιεί τη μεθοδολογία εκτεταμένου κινδύνου. Το CIDA έχει σχεδιαστεί για να βοηθά τους υπεύθυνους για τη λήψη αποφάσεων να αναλύουν δυναμικά δυναμικά και σύνθετα μονοπάτια κινδύνου εξάρτησης με δύο τρόπους: (i) να εντοπίζουν δυνητικά υποτιμημένες εξαρτήσεις χαμηλού κινδύνου και να τις αναταξινομούν σε κατηγορία υψηλότερου κινδύνου πριν υλοποιηθούν, και (ii) προσομοίωση της αποτελεσματικότητας εναλλακτικών ελέγχων μετριασμού με διαφορετικούς χρόνους αντίδρασης. Έτσι, το εργαλείο CIDA μπορεί να χρησιμοποιηθεί για την αξιολόγηση εναλλακτικών στρατηγικών άμυνας για πολύπλοκα, μεγάλης κλίμακας και πολυτομεακά σενάρια εξάρτησης και για την αξιολόγηση της ανθεκτικότητας τους με οικονομικά αποδοτικό τρόπο.

6. Συνοπτική ανάλυση της εργασίας **[J-18]** "*Lightweight Private Proximity Testing for Geospatial Social Networks",* P. Kotzanikolaou, C. Patsakis, E. Magkos, M. Korakakis.

Περίληψη: – Η ευρεία υιοθέτηση των έξυπνων τηλεφώνων επέτρεψε στα Κοινωνικά Δίκτυα (Online Social Networks – OSN) να εκμεταλλευτούν τις δυνατότητες εφαρμογών σχετικά με την τοποθεσία, προσφέροντας στους χρήστες καλύτερη αλληλεπίδραση και περιεχόμενο σχετικό με την τοποθεσία του χρήστη. Παρόλο που τα χαρακτηριστικά αυτά είναι πολύ ελκυστικά, η δημοσίευση της τοποθεσίας των χρηστών σε έναν OSN τους εκθέτει σε κινδύνους για την προστασία της ιδιωτικής ζωής. Πρόσφατα, έχουν προταθεί διάφορα πρωτόκολλα για ιδιωτικές δοκιμές εγγύτητας (private proximity testing), όπου οι χρήστες είναι σε θέση να ελέγξουν εάν οι φίλοι τους σε απευθείας σύνδεση βρίσκονται κοντά, χωρίς να αποκαλύπτουν τις τοποθεσίες τους. Ωστόσο, το κόστος υπολογισμού των απαιτούμενων κρυπτογραφικών λειτουργιών που χρησιμοποιούνται σε τέτοια πρωτόκολλα δεν είναι πάντοτε αποτελεσματικό για κινητές συσκευές. Σε αυτό το άρθρο εισάγουμε ένα ελαφρύ και ασφαλές πρωτόκολλο ελέγχου της εγγύτητας, κατάλληλο για χρήστες σε απευθείας σύνδεση κινητές συσκευές. Δείχνουμε ότι το πρωτόκολλο μας είναι αποδεδειγμένα ασφαλές και βασίζεται στο γνωστό πρόβλημα της παραγοντοποίησης, και αναλύουμε την αποτελεσματικότητά του. Τα αποτελέσματά μας δείχνουν ότι η προσέγγισή μας ξεπερνά τα υπόλοιπα υπάρχοντα πρωτόκολλα, μειώνοντας σημαντικά το υπολογιστικό κόστος και καθιστώντας πρακτικό για συσκευές με περιορισμένους πόρους. Τέλος, αποδεικνύουμε τη δυνατότητα εφαρμογής της πρότασής μας σε μια πραγματική εφαρμογή που βασίζεται σε τοποθεσίες OSN για κινητά.

7. Συνοπτική ανάλυση της εργασίας **[J-17]** "*Risk Mitigation Strategies For Critical Infrastructures Based On Graph Centrality Analysis", G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, D. Gritzalis*.

Περίληψη: – Τα γραφήματα κινδύνου εξαρτήσεων έχουν προταθεί ως ένα εργαλείο για την ανάλυση των διαδοχικών αστοχιών (cascading failures) που οφείλονται στις αλυσίδες εξαρτήσεων κρίσιμης υποδομής. Ωστόσο, η ανάλυση της αλυσίδας εξάρτησης δεν είναι από μόνη της επαρκής για την ανάπτυξη μιας αποτελεσματικής στρατηγικής μετριασμού των κινδύνων - η οποία προσδιορίζει ποιες κρίσιμες υποδομές θα πρέπει να έχουν υψηλή προτεραιότητα για την εφαρμογή μέτρων ελέγχου ασφάλειας, προκειμένου να επιτευχθεί βέλτιστη μείωση του συνολικού κινδύνου. Η παρούσα εργασία επεκτείνει την προηγούμενη έρευνα ανάλυσης κινδύνου εξάρτησης για την εφαρμογή αποτελεσματικού μετριασμού του κινδύνου. Αυτό επιτυγχάνεται εξετάζοντας τη σχέση μεταξύ των διαδρομών κινδύνου εξάρτησης και των χαρακτηριστικών κεντρικής γραφής. Οι μετρήσεις κεντρικής γραφής εφαρμόζονται για τον σχεδιασμό και την αξιολόγηση της αποτελεσματικότητας εναλλακτικών στρατηγικών μετριασμού του κινδύνου. Οι πειραματικές αξιολογήσεις βασίζονται σε τυχαίες γραφικές παραστάσεις που προσομοιώνουν κοινά χαρακτηριστικά εξαρτήσεων κρίσιμης υποδομής όπως προσδιορίζονται από πρόσφατες εμπειρικές μελέτες. Τα πειραματικά αποτελέσματα χρησιμοποιούνται για τον καθορισμό ενός αλγορίθμου που δίνει προτεραιότητα στους κόμβους κρίσιμης υποδομής για την εφαρμογή ελέγχων προκειμένου να επιτευχθεί αποτελεσματικός μετριασμός του κινδύνου.

8. Συνοπτική ανάλυση της εργασίας **[J-16]** "*Assessing n-order Dependencies Between Critical Infrastructures",* P. Kotzanikolaou, M. Theoharidou, D. Gritzalis.

Περίληψη: – η προστασία Κρίσιμων Υποδομών (ΚΥ) είναι μία σύνθετη ενέργεια, επειδή περιλαμβάνει την αποτίμηση τόσο εσωτερικών όσο και εξωτερικών κινδύνων ασφάλειας. Στην πρόσφατη βιβλιογραφία έχουν προταθεί μεθοδολογίες για την αναγνώριση απειλών ασφάλειας σε επίπεδο υποδομής, ή ακόμα και σε επίπεδο διασύνδεσης πρώτου επιπέδου (δηλαδή κινδύνου ο οποίος προέρχεται από άμεσες εξαρτήσεις. Όμως, η ανάλυση των εξαρτήσεων πολλαπλών επιπέδων (δηλαδή η αποτίμηση των επιπτώσεων από διαδοχικά γεγονότα τα οποία προκαλούνται από ένα περιστατικό ασφάλειας) δεν έχει μελετηθεί επαρκώς. Σε αυτή την εργασία προτείνουμε μία μεθοδολογία για τον εντοπισμό και την αποτίμηση των εξαρτήσεων πολλαπλών επιπέδων. Συνδυάζουμε τις υφιστάμενες συνδέσεις πρώτου επιπέδου μές από γράφους εξαρτήσεων, με σκοπό να αποτιμήσουμε τις συνέπειες στις αντίστοιχες ΚΥ. Με αυτή τη μεθοδολογία είναι πιθανό να εντοπιστούν και να αποφευχθούν απειλές ασφάλειας με πολύ μεγάλο επίπεδο συνέπειας, οι οποίες απειλές θα ήταν πολύ δύσκολο να εντοπιστούν με την απλή μελέτη των εξαρτήσεων πρώτου επιπέδου.

9. Συνοπτική ανάλυση της εργασίας **[J-15]** *"Towards Early Warning Against Internet Worms Based on Critical-Sized Networks"*, E. Magkos, M. Avlonitis, P. Kotzanikolaou and M. Stefanidakis.

Περίληψη: –Σε αυτή την εργασία χρησιμοποιούμε ένα πρόσφατος στοχαστικό μοντέλο για τη μελέτη της εξάπλωσης ιών, στο οποίο τα τυχαία γεγονότα κατά την περίοδο της εξάπλωσης μοντελοποιούνται με τη χρήση διαφορικών στοχαστικών εξισώσεων. Μέσα σε αυτό το μοντέλο εισάγουμε την έννοια του κρίσιμου μεγέθους δικτύου, το οποίο είναι το ελάχιστο μέγεθος ενός δικτύου το οποίο μπορεί να μελετηθεί, ώστε να προβάλλει με μεγάλη βεβαιότητα τη συμπεριφορά του ιού σε πολύ μεγαλύτερα δίκτυα. Προτείνουμε μία μέθοδο για το θεωρητικό υπολογισμό του κρίσιμου μεγέθους δικτύου σε σχέση με κάποιον ιό. Στόχος μας είναι η εξισορρόπηση μεταξύ της ακρίβειας της πρόβλεψης της εξάπλωσης και της απόδοσης της μεθόδου. Επιπλέον χρησιμοποιούμε προσομοιώσεις ώστε να επαληθεύσουμε την ορθότητα της προτεινόμενης μεθόδου. Τέλος, με βάση την έννοια του κρίσιμου μεγέθους δικτύου, προτείνουμε ένα λογικό πλαίσιο για ένα κατανεμημένο σύστημα έγκαιρης προειδοποίησης της εξάπλωσης ταχέως εξαπλούμενων ιών.

10. Συνοπτική ανάλυση της εργασίας **[J-14]** *"Chord-PKI: Providing Security and Privacy in P2P Networks with a Distributed PKI Architecture"*, A. Avramidis, P. Kotzanikolaou, C. Douligeris and M. Burmester.

Περίληψη: – Πολλές εφαρμογές ομότιμων κόμβων (P2P applicationns) απαιτούν υπηρεσίες ασφάλειας όπως εμπιστευτικότητα, ανωνυμία, αυθεντικοποίηση και μη-αποποίηση. Τέτοιες υπηρεσίες ασφάλειας μπορούν να παρασχεθούν μέσω ιεραρχικών Υποδομών Δημόσιου Κλειδιού (ΥΔΚ). Όμως, τα δίκτυα ομότιμων κόμβων είναι συνήθως κατανεμημένα διαδικτυακά συστήματα μεγάλης κλίμακας και αποτελούνται από κόμβους με μη καθορισμένο επίπεδο εμπιστοσύνης. Συνεπώς, η υλοποίηση ιεραρχικών λύσεων ασφάλειας δεν είναι ρεαλιστική για τέτοια περιβάλλοντα. Σε αυτή την εργασία προτείνουμε το Chord-PKI, μία κατανεμημένη ΥΔΚ η οποία στηρίζεται στο ομότιμο δίκτυο Chord, με σκοπό την παροχή υπηρεσιών ασφάλειας. Η προτεινόμενη λύση διαμοιράζει τη λειτουργικότητα της ΥΔΚ μεταξύ των ίδιων των κόμβων τυο ομότιμου δικτύου χρησιμοποιώντας κρυπτογραφία κατωφλίου. Αναλύουμε την ασφάλεια της προτεινόμενης λύσης και με τη βοήθεια προσομοιώσεων αξιολογούμε την απόδοση της προτεινόμενης υποδομής για διάφορα σενάρια.

11. Συνοπτική ανάλυση της εργασίας **[J-13]** *"Risk assessment methodology for interdependent critical infrastructures"*, M. Theoharidou, P. Kotzanikolaou and D. Gritzalis.

Περίληψη: – Η αποτίμηση επικινδυνότητας των αλληλεξαρτώμενων Κρίσιμων Υποδομών (ΚΥ) είναι μία δύσκολη εργασία, λόγω της σύνθετης φύσης των ΚΥ. Σε αυτή την εργασία προτείνεται μία μεθοδολογία για την αποτίμηση κινδύνου μίας ΚΥ ή ενός τομέα ΚΥ, η οποία λαμβάνει υπόψη τις πιθανές αλληλεξαρτήσεις μεταξύ υποδομών και τομέων. Η προτεινόμενη μεθοδολογία είναι συμβατή με γνωστά πρότυπα ασφάλειας, όμως δίνει έμφαση στις κοινωνικές συνέπειες και όχι μόνο στις συνέπειες εντός της ίδιας της ΚΥ. Παράλληλα παρουσιάζονται αναλυτικά παραδείγματα μελέτης περίπτωσης.

12. Συνοπτική ανάλυση της εργασίας **[J-12]** *"Achieving Privacy and Access Control in Pervasive Computing Environments"*, E. Magkos and P. Kotzanikolaou.

Περίληψη: – Η παρούσα εργασία δίνει έμφαση στην εγγενή σχέση μεταξύ της προστασίας της ιδιωτικότητας και στον έλεγχο πρόσβασης σε περιβάλλοντα διάχυτου υπολογισμού (Pervasive

Computing Environments). Από τη μία πλευρά, οι πάροχοι υπηρεσιών απαιτούν την αυθεντικοποίηση των χρηστών για την πρόσβαση στις υπηρεσίες τους, ενώ από την άλλη πλευρά οι χρήστες έχουν ταυτόχρονα την απαίτηση οι συναλλαγές τους να είναι ανώνυμες. Όμως, σε ορισμένες περιπτώσεις είναι πιθανό να απαιτείται άρση της ανωνυμίας ορισμένων διαπιστευτηρίων (credentials) τα οποία έχουν χρησιμοποιηθεί με κακόβουλο τρόπο από ανώνυμους χρήστες. Αναλύουμε τις απαιτήσεις ασφάλειας και ιδιωτικότητας για τα περιβάλλοντα διάχυτου υπολογισμού, και δείχνουμε ότι τα υφιστάμενα σχήματα ελέγχου πρόσβασης με προστασία της ιδιωτικότητας δεν ικανοποιούν πλήρως αυτές τις απαιτήσεις. Στη συνέχεια προτείνουμε δύο προσεγγίσεις προς την κατεύθυνση του ελέγχου πρόσβασης με προστασία της ιδιωτικότητας. Ο στόχος μας είναι διττός: από τη μία πλευρά να ενισχύσουμε την ανωνυμία και ιδιωτικότητα των συναλλαγών έναντι εσωτερικών αντιπάλων. Από την άλλη πλευρά να ενισχύσουμε την ασφάλεια και την ινχηλασιμότητα κακώς χρησιμοποιούμενων ανώνυμων διαπιστευτηρίων. Τέλος παρουσιάζουμε μία συγκριτική μελέτη των προτεινόμενων σχημάτων σε σχέση με άλλα σχήματα προτεινόμενα στη βιβλιογραφία.

13. Συνοπτική ανάλυση της εργασίας **[J-11]** *"A multi-layer Criticality Assessment methodology based on interdependencies"*, M. Theoharidou, P. Kotzanikolaou and D. Gritzalis.

Περίληψη: – Σε αυτή την εργασία προτείνουμε μία ολιστική μεθοδολογία Ανάλυσης Κρισιμότητας υποδομών, κατάλληλης για την ανάπτυξη ενός σχεδίου Προστασίας Κρίσιμων Υποδομών σε εθνικό επίπεδο. Η προτεινόμενη μεθοδολογία στοχεύει στο συνδυασμό όλων των σχεδίων ασφάλειας και ανάλυσης κινδύνου που πιθανώς έχουν συντελεστεί σε επίπεδο κάθε ανεξάρτητης Υποδομής, με σκοπό να γίνει μία συνθετική ανάλυση κρισιμότητας σε επίπεδο τομέα (sector) η δια-τομεακό (intra-sector) επίπεδο. Για το σκοπό αυτό ορίζουμε τρία διαφορετικά επίπεδα ανάλυσης κινδύνου: το επίπεδο της ανεξάρτητης υποδομής, το επίπεδο ενός οικονομικού τομέα και το επίπεδο διασύνδεσης όλων των τομέων σε εθνικό επίπεδο. Με αυτό τον τρόπο, τα υφιστάμενα σχέδια ή πολιτικές ασφάλειας μπορούν να αξιοποιηθούν στο έπακρο ώστε να συντομεύσουν την ανάπτυξη ενός σχεδίου ασφάλειας για σύνθετες και αλληλοεξαρτώμενες Κρίσιμες Υποδομές (ΚΥ). Βασικό στοιχείο της μεθοδολογίας είναι ο τυπικός ορισμός των εξαρτήσεων μεταξύ διαφορετικών ΚΥ ή/και τομέων ΚΥ, με σκοπό την προβολή μακροσκοπικών αναλύσεων επικινδυνότητας με μεγάλο εύρος εφαρμογής. Οι υφιστάμενες μεθοδολογίες αποτίμησης επικινδυνότητας δεν είναι σχεδιασμένες ώστε να συνδυάζουν μακροσκοπικά, τα αποτελέσματα ανεξάρτητων μελετών ασφάλειας.

14. Συνοπτική ανάλυση της εργασίας **[J-10]**, *"Solving Coverage Problems in Wireless Sensor Networks Using Cover Sets"*, D.Zorbas, D. Glynos, P. Kotzanikolaou and C. Douligeris.

Περίληψη: – Για να επιτύχουμε αποδοτική, από πλευράς ενέργειας, παρακολούθηση στόχων από δίκτυα αισθητήρων, έχουν προταθεί διάφοροι αλγόριθμοι κάλυψης (coverage algorithms). Οι αλγόριθμοι αυτοί χωρίζουν τους κόμβους σε σύνολα κάλυψης, τέτοια ώστε κάθε σύνολο κάλυψης να μπορεί να παρακολουθήσει όλους τους στόχους. Η παραγωγή του μέγιστου αριθμού των υπαρχόντων συνόλων κάλυψης είναι NP-complete πρόβλημα, και για αυτό το λόγο έχουν προταθεί διάφοροι ευρεστικοί αλγόριθμοι οι οποίοι παράγουν υπο-βέλτιστες λύσεις. Σε αυτή την εργασία παρουσιάζουμε ένα νέο και αποδοτικό αλγόριθμο κάλυψης, ο οποίος μπορεί να παράγει τόσο ανεξάρτητα σύνολα όσο και επικαλυπτόμενα σύνολα, δηλαδή σύνολα με μη μηδενική τομή. Ο προτεινόμενος αλγόριθμος χρησιμοποιεί μία συνάρτηση κόστους η οποία λαμβάνει υπόψη την ακτίνα παρακολούθησης κάθε κόμβου, σε σχέση με τους στόχους με χαμηλή κάλυψη, αλλά και με την υπολειπόμενη ενέργεια κάθε κόμβου. Μέσω προσομοιώσεων, αποδεικνύεται ότι ο προτεινόμενος αλγόριθμος έχει καλύτερη επίδοση από άλλους ευρεστικούς αλγορίθμους, ενώ παράγει σύνολα κάλυψης πολύ κοντά στη θεωρητικά βέλτιστη λύση. Η μεγαλύτερη διαθεσιμότητα που παρέχουν τα παραγόμενα σύνολα κάλυψης και ο χαμηλός χρόνος εκτέλεσης του αλγορίθμου, τον καθιστούν μία καλή λύση για ένα μεγάλο εύρος από περιβάλλοντα ανάπτυξης δικτύων αισθητήρων.

15. Συνοπτική ανάλυση της εργασίας **[J-9],** *"Secure and Practical Key Establishment for Distributed Sensor Networks",* P. Kotzanikolaou, E. Magkos, D. Vergados and M. Stefanidakis.

Περίληψη: – Σε αυτή την εργασία εξετάζουμε της ασφάλεια των συστημάτων καταγραφής (logging security) των τηλεπικοινωνιακών παρόχων. Αρχικά γίνεται μία επισκόπηση των μοντέλων ασφάλειας για τα συστήματα καταγραφής συμβάντων. Στη συνέχεια επεκτείνουμε αυτά τα μοντέλα ασφάλειας ώστε να κατασκευάσουμε ένα μοντέλο ασφάλειας κατάλληλο για περιβάλλοντα τηλεπικοινωνιακών παρόχων, το οποίο λαμβάνει υπόψη εσωτερικές επιθέσεις τροποποίησης. Παρουσιάζουμε επίσης ένα πλαίσιο για την ασφαλή διαχείριση των αρχείων καταγραφής, καθώς και ένα σχέδιο υλοποίησης, το οποίο στοχεύει στην παροχή ιχνηλασιμότητας (traceability), εντός του εκτεταμένου μοντέλου ασφάλειας. Βασικό ρόλο στο μοντέλο αυτό έχει μία ανεξάρτητη ρυθμιστική Αρχή, η οποία είναι υπεύθυνη για τη διατήρηση των αποδείξεων ακεραιότητας των αρχείων καταγραφής.

16. Συνοπτική ανάλυση της εργασίας **[J-8]**, *"Secure and Practical Key Establishment for Distributed Sensor Networks",* Panayiotis Kotzanikolaou, Emmanouil Magkos, Dimitrios Vergados and Michalis Stefanidakis.

Περίληψη: – Η εγκαθίδρυση κλειδιού αποτελεί βασική τεχνική για την ασφάλεια της επικοινωνίας σε δικτυακό περιβάλλον, εφόσον μπορεί να εξασφαλίσει την εμπιστευτικότητα και την ακεραιότητα της επικοινωνίας μεταξύ των κόμβων. Όμως, η εγκαθίδρυση κλειδιού στα δίκτυα αισθητήρων αποτελεί δύσκολο στόχο, εξαιτίας των φυσικών περιορισμών που περιβάλλουν τους κόμβους αισθητήρων και λόγω της έκθεσής τους σε αρκετές απειλές. Τα υπάρχοντα πρωτόκολλα βασίζονται κυρίως σε συμμετρικές κρυπτογραφικές τεχνικές ώστε να είναι αρκετά αποδοτικά, αλλά αυτό τα καθιστά ευάλωτα σε διάφορες επιθέσεις πλαστοπροσωπίας από εσωτερικούς κόμβους. Σε αυτή την εργασία παρουσιάζονται δύο πρωτόκολλα εγκαθίδρυσης κλειδιού για κόμβους αισθητήρων, τα οποία είναι κατάλληλα για μη επιτηρούμενα, κατανεμημένα περιβάλλοντα. Το πρώτο πρωτόκολλο είναι υβριδικό και συνδυάζει ασύμμετρη κρυπτογραφία Ελλειπτικών Καμπύλων με συμμετρικές τεχνικές ανταλλαγής κλειδιού. Το δεύτερο πρωτόκολλο είναι πλήρως ασύμμετρο. Επιπλέον, μέσω προσομοιώσεων πραγματοποιείται μέτρηση της αποδοτικότητας των προτεινόμενων πρωτοκόλλων, σε σύγκριση με υπάρχοντα υβριδικά πρωτόκολλα. Τα αποτελέσματα δείχνουν ότι είναι εφικτή υπό προϋποθέσεις, η μερική χρήση ασύμμετρων κρυπτογραφικών τεχνικών για υψηλής επικινδυνότητας εφαρμογές δικτύων αισθητήρων, με στόχο την αντιμετώπιση των εσωτερικών απειλών πλαστοπροσωπίας.

17. Συνοπτική ανάλυση της εργασίας **[J-7]**, **"***Data Retention and Privacy in Electronic Communications",* Panayiotis Kotzanikolaou.

Περίληψη: – Σε πολλές χώρες, οι πάροχοι δικτύων ηλεκτρονικών επικοινωνιών είναι υπόχρεοι μέσω της νομοθεσίας να διατηρούν τα δεδομένα επικοινωνίας των συνδρομητών τους για συγκεκριμένο χρονικό διάστημα, με σκοπό τη διευκόλυνση ερευνών, σε μελλοντικό χρόνο, πιθανών παράνομων ενεργειών. Το γεγονός αυτό έχει δημιουργήσει κοινωνικές ανησυχίες και ερωτήματα τεχνικής φύσεως, εφόσον τα διατηρούμενα δεδομένα περιλαμβάνουν ευαίσθητη πληροφορία και μία πιθανή κατάχρηση των δεδομένων ενδέχεται να οδηγήσει σε παραβίαση του απορρήτου και απώλεια της ιδιωτικότητας των συνδρομητών. Σε αυτό το άρθρο εξετάζουμε τα θέματα ιδιωτικότητας και απορρήτου που σχετίζονται με τη διατήρηση δεδομένων στις ηλεκτρονικές επικοινωνίες. Επιπλέον περιγράφουμε ένα γενικό μοντέλο το οποίο συνδυάσει τεχνικά, διαδικαστικά και νομικά μέτρα με σκοπό την ασφαλή διατήρηση των δεδομένων επικοινωνίας και την ελαχιστοποίηση των απειλών κατά της ιδιωτικότητας των πολιτών. Οι βασικές αρχές ασφάλειας που θέτει το προτεινόμενο μοντέλο είναι ο διπλός έλεγχος (dual control) και η διάκριση καθηκόντων (separation of duties).

18. Συνοπτική ανάλυση της εργασίας **[J-6]**, *"Towards Secure Online Elections – Models, Primitives and Open Issues",* Emmanouil Magkos, Panayiotis Kotzanikolaou, and Christos Douligeris.

Περίληψη: – Η διεξαγωγή ηλεκτρονικών ψηφοφοριών αποτελεί μία εφικτή επιλογή για διάφορα περιβάλλοντα εκλογών, από περιπτώσεις κλειστών συνόλων μέχρι εθνικής εμβέλειας εκλογές. Η περίπτωση των ηλεκτρονικών ψηφοφοριών μέσω του διαδικτύου παρουσιάζει ιδιαίτερο ενδιαφέρον, εφόσον επιτρέπει την άμεση συμμετοχή σε ψηφοφορίες από οποιοδήποτε περιβάλλον το οποίο παρέχει πρόσβαση στο διαδίκτυο. Στην εργασία αυτή γίνεται μία ανασκόπηση των γενικών κρυπτογραφικών πρωτοκόλλων τα οποία έχουν προταθεί στη βιβλιογραφία για την ασφαλή διεξαγωγή ηλεκτρονικών ψηφοφοριών. Επίσης, παρέχει μία διεξοδική ανάλυση πρόσφατων πρωτοκόλλων ηλεκτρονικών ψηφοφοριών αναφορικά με την ασφάλεια και τη λειτουργικότητά τους, τα οποία (πρωτόκολλα) διευρύνουν τα γενικά μοντέλα ώστε να υποστηρίζουν ψηφοφορίες μέσω του διαδικτύου. Τέλος, τονίζονται διάφορα κρίσιμα ζητήματα ασφάλειας και υλοποίησης τα οποία θα πρέπει να αντιμετωπιστούν, πριν γίνει εφικτή η πραγματοποίηση διαδικτυακών ψηφοφοριών σε κρίσιμα περιβάλλοντα εκλογών.

19. Συνοπτική ανάλυση της εργασίας **[J-5]** *"SecMR - A Secure Multipath Routing Protocol for Ad Hoc Networks",* Rosa Mavropodi, Panayiotis Kotzanikolaou, and Christos Douligeris.

Περίληψη: – Τα πρωτόκολλα πολλαπλής δρομολόγησης για Κινητά Δίκτυα Ειδικού Σκοπού μειώνουν τις επιθέσεις ασφάλειας από συνεργαζόμενους κακόβουλους κόμβους, μέσω της μεγιστοποίησης του αριθμού των κόμβων που πρέπει να συμβιβάσει ένας αντίπαλος ώστε να ελέγξει την επικοινωνία. Σε αυτή την εργασία παρουσιάζονται διάφορες επιθέσεις οι οποίες καθιστούν ευπαθή τα πρωτόκολλα πολλαπλής δρομολόγησης σε επιθέσεις συνεργαζόμενων κακόβουλων κόμβων. Στη συνέχεια προτείνεται ένα νέο ασφαλές πρωτόκολλο δυναμικής δρομολόγησης, το πρωτόκολλο Secure Multipath Routing (SecMR) και αναλύονται οι ιδιότητες ασφάλειας που αυτό παρέχει. Τέλος, μέσω προσομοιώσεων γίνεται εκτίμηση της απόδοσης του πρωτοκόλλου σε σύγκριση με υπάρχονται πρωτόκολλα πολλαπλής δρομολόγησης.

20. Συνοπτική ανάλυση της εργασίας **[J-4]** *"Multi-Layer Key Establishment for Large Scale Sensor Networks", P. Kotzanikolaou, D. Vergados, G. Stergiou and E. Magkos.*

Περίληψη: – Η πρόσφατη έρευνα σχετικά με την εγκαθίδρυση κλειδιού (key establishment) σε κατανεμημένα δίκτυα αισθητήρων εστιάζει σε ελαφρά πρωτόκολλα τα οποία είναι υλοποιήσιμα σε κόμβους αισθητήρες, οι οποίοι εκ της φύσεώς τους έχουν περιορισμένες υπολογιστικές δυνατότητες. Αν και τα πλέον αποδοτικά πρωτόκολλα αυτής της κατηγορίας είναι αυτά που βασίζονται αποκλειστικά σε συμμετρική κρυπτογραφία, δεν μπορούν να προσφέρουν επαρκή προστασία από συγκεκριμένες επιθέσεις, όπως για παράδειγμα επιθέσεις πλαστοπροσωπίας (impersonation) ή επιθέσεις «πλαστής γενιάς» (fake generation). Για την αντιμετώπιση αυτών των προβλημάτων, έχουν προταθεί υβριδικά πρωτόκολλα εγκαθίδρυσης κλειδιού τα οποία κάνουν περιορισμένη χρήση κρυπτογραφίας δημόσιου κλειδιού, μέσω κρυπτοσυστημάτων ελλειπτικών καμπύλων (Elliptic Curve Cryptosystems). Δυστυχώς, αν και αυτά τα πρωτόκολλα έχουν βελτιστοποιηθεί ώστε να είναι εφικτή η εκτέλεσή τους από κόμβους αισθητήρων, παρόλα αυτά επηρεάζουν αρνητικά την απόδοση, ιδιαίτερα σε δίκτυα μεγάλου εύρους. Σε αυτή την εργασία, παρουσιάζεται ένα πρωτόκολλο πολλαπλών στρωμάτων (Multi-layer) για δίκτυα αισθητήρων, το οποίο συνδυάζει υβριδικές και συμμετρικές κρυπτογραφικές τεχνικές. Επιπλέον παρουσιάζεται μία ανάλυση απόδοσης του πρωτοκόλλου αυτού μέσω εξομοίωσης. Η ανάλυση αυτή αποδεικνύει μία γραμμική μείωση της απόδοσης, λόγω της βελτιστοποιημένης χρήσης της υβριδικής κρυπτογράφησης.

21. Συνοπτική ανάλυση της εργασίας **[J-3]** *"Secure Distributed Intelligent Networks", P. Kotzanikolaou, R. Mavropodi and C. Douligeris.*

Περίληψη: – Τα Ευφυή Δίκτυα (ΕΔ) διαχωρίζουν την διαδικασία ελέγχου και επεξεργασίας κλήσης από τη δρομολόγηση, οδηγώντας σε γρήγορες και ανεξάρτητες δικτύου υπηρεσίες, με μειωμένο κόστος

ανάπτυξης. Η ενοποίηση νέων τεχνολογιών όπως η τεχνολογία CORBA και η τεχνολογία κινητών πρακτόρων βελτιώνει την απόδοση των ΕΔ. Όμως, η χρήση κατανεμημένων τεχνολογιών αυξάνει τα προβλήματα ασφάλειας. Σε αυτή την εργασία παρουσιάζεται μια αρχιτεκτονική ασφάλειας ΕΔ χρησιμοποιώντας μηχανισμούς ασφαλείας όπως είναι υπηρεσίες ασφάλειας της CORBA, υπηρεσίες ασφάλειας της πλατφόρμας πρακτόρων Grasshopper και υπηρεσίες Τρίτης Έμπιστης Οντότητας. Επιπρόσθετα, υπολογίζεται μέσω προσομοίωσης το επιπλέον κόστος απόδοσης που επιβάλλεται από την χρήση των μηχανισμών ασφαλείας στο ΕΔ, σε εφαρμογές Αλληλεπιδραστικής Ανάκτησης Πολυμεσικών Δεδομένων. Τα αποτελέσματα της προσομοίωσης δείχνουν μια κλιμακωτή μείωση της απόδοσης στα διάφορα στοιχεία του δικτύου. Εντούτοις η αρχιτεκτονική ασφάλειας είναι αρκετά εύκαμπτη ώστε να επιτυγχάνεται μια αποδεκτή σχέση μεταξύ ασφάλειας και αποδοτικότητας. Με βάση τα αποτελέσματα της προσομοίωσης γίνεται φανερό ότι οι πολιτικές δικτύου και ασφάλειας μπορούν να διαμορφωθούν κατάλληλα, ώστε να επιτευχθεί η απαιτούμενη ισορροπία μεταξύ ασφάλειας και απόδοσης, σύμφωνα με τις ανάγκες εφαρμογής.

22. Συνοπτική ανάλυση της εργασίας **[J-2]** *"Some more improvements on a fair non-repudiation protocol", D. Petropoulos and P. Kotzanikolaou.*

Περίληψη: - Η εργασία αυτή εξετάζει το ισομερές πρωτόκολλο μη-αποποίησης ευθύνης (fair non-repudiation protocol) των Zhou και Gollmann, καθώς επίσης και την τροποποίηση αυτού του πρωτοκόλλου, όπως προτάθηκε από τους Kim *et al*. Περιγράφεται μία αδυναμία των δύο παραπάνω πρωτοκόλλων, η οποία μπορεί να ευνοήσει μία συγκεκριμένη επίθεση από κακόβουλους συμμετέχοντες και να οδηγήσει σε παρεμπόδιση της υπηρεσίας μη-αποποίησης ευθύνης ή ακόμα και σε άρνηση εξυπηρέτησης. Στη συνέχεια παρουσιάζεται μία τροποποίηση η οποία μπορεί να αντιμετωπίσει αυτή την απειλή. Επιπλέον, παρουσιάζεται μία παραλλαγή των πρωτοκόλλων η οποία προσφέρει σημασιολογική ασφάλεια (semantic security) στην εμπιστευτικότητα των μηνυμάτων, χωρίς να αυξάνει το κόστος διαχείρισης των κρυπτογραφικών κλειδιών.

23. Συνοπτική παρουσίαση της εργασίας **[J-1]** *"Role Based Access Control Policies in the Mobile Agent Paradigm", Panayiotis Kotzanikolaou, Mike Burmester, Vassilios Chrissikopoulos, and Christos Douligeris.*

Περίληψη: – Οι κινητοί πράκτορες είναι μία πρόσφατη τεχνολογία, η οποία έχει ευρεία εφαρμογή σε κατανεμημένες εφαρμογές. Αν και οι κινητοί πράκτορες επεκτείνουν τις παραδοσιακές μεθόδους δικτυακής επικοινωνίας, οδηγούν σε αύξηση των αδυναμιών ασφάλειας. Η Πολιτική Πρόσβασης Ρόλων (RBAC), έχει προταθεί στη βιβλιογραφία ως μία εναλλακτική λύση στα παραδοσιακά μοντέλα Υποχρεωτικού (MAC) και Διακριτικού (DAC) ελέγχου πρόσβασης. Η εργασία αυτή διερευνά τη σχέση μεταξύ των Πολιτικών Πρόσβασης Ρόλων και της τεχνολογίας κινητών πρακτόρων. Αρχικά εξετάζονται σχήματα ελέγχου πρόσβασης Ρόλων, τα οποία έχουν χρησιμοποιηθεί για τον έλεγχο πρόσβασης κινητών πρακτόρων. Στη συνέχεια, αναλύονται συστήματα τα οποία χρησιμοποιούν κινητούς πράκτορες ως υποστηρικτική τεχνολογία για την επιβολή Πολιτικών Πρόσβασης Ρόλων σε κατανεμημένες εφαρμογές. Τελικά, προτείνονται διάφοροι μηχανισμοί ασφάλειας οι οποίοι μπορούν να χρησιμοποιηθούν για να υλοποιήσουν Πολιτικές Πρόσβασης Ρόλων σε κατανεμημένα συστήματα και συζητούνται πιθανές επεκτάσεις και ανοικτά προβλήματα.

(Δημοσιευμένες Εργασίες – Σε Ελληνικά περιοδικά)

24. Συνοπτική ανάλυση της εργασίας **[Π-1]**, *"Το Απόρρητο στις Τηλεπικοινωνίες: Διασφάλιση και Αντιμετώπιση Παραβίασης"*, Χρήστος Δουληγέρης και Παναγιώτης Κοτζανικολάου.

Περίληψη: – Το ζήτημα της διασφάλισης του απορρήτου των τηλεπικοινωνιών έχει βρεθεί στο επίκεντρο της επικαιρότητας, ιδιαίτερα μετά την πρόσφατη αποκάλυψη της υπόθεσης των υποκλοπών στην κινητή τηλεφωνία. Σε αυτό το άρθρο εξετάζονται τα ευάλωτα σημεία των τηλεπικοινωνιακών δικτύων σε επιθέσεις υποκλοπής. Επιπλέον, παρουσιάζονται τα θεσμικά και τεχνικά μέτρα που έχει

λάβει η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) σχετικά με την προστασία της ιδιωτικότητας των τηλεπικοινωνιών μέσω της έκδοσης των σχετικών Κανονισμών Διασφάλισης Απορρήτου και των τακτικών ελέγχων από την ΑΔΑΕ στις εγκαταστάσεις και τα αρχεία των παρόχων, με σκοπό την επιβεβαίωση της ορθής εφαρμογής των μέτρων και των διαδικασιών ασφάλειας.

III.3. Συνοπτική ανάλυση δημοσιεύσεων σε επιστημονικά συνέδρια

1. Συνοπτική ανάλυση της εργασίας **[C-35]** *"A forensics-by-design management framework for medical devices based on blockchain", Malamas V., Dasaklis T., Kotzanikolaou P., Burmester M., Katsikas S.*

   Περίληψη: – The Internet of Medical Things (IoMT) provides ubiquitous healthcare services for patient monitoring and treatment. However, the interaction between doctors, patients, health-care personnel and device manufacturers, with different and often conflicting security and privacy objectives, make such services vulnerable and subject to exploitation. In addition, since parties may require different access levels and the IoMT devices involve different functionalities, access control can be challenging. In this paper, we propose a blockchain-enabled authorization framework for managing both IoMT devices and medical files by creating a distributed chain of custody and health data privacy scheme. The core idea is to build trust domains for the various stakeholders and IoMT devices, in such a way that fine-grain access is enabled by taking into account critical attributes of the IoMT ecosystem such as a) the different roles and capabilities of the IoMT devices and b) their interaction with the users/stakeholders. A private blockchain is used in combination with on-chain smart contracts to allow for a forensics-by-design management architecture with audit trails for integrity and provenance guarantees as well as health data privacy. The private blockchain ecosystem is authenticated by a proof-of-medical-stake consensus mechanism that is tailored for medical applications.

2. Συνοπτική ανάλυση της εργασίας **[C-34]** *" An Experimental Analysis of Current DDoS attacks Based on a Provider Edge Router Honeynet", Triandopoulou S., Papanikas D., and Kotzanikolaou P.*

   Περίληψη: – Η παρούσα εργασία παρουσιάζει μια πειραματική ανάλυση των σύγχρονων καταμενημένων επιθέσεων άρνησης υπηρεσίας (Distributed Denial of Service - DDoS). Η ανάλυσή μας βασίζεται σε πραγματικά δεδομένα που συλλέχθηκαν από ένα σύστημα honeynet το οποίοεγκαταστάθηκε σε ακραίο δρομολογητή ενός παρόχου υπηρεσιών διαδικτύου για περίοδο τεσσάρων μηνών. Στο εξεταζόμενο σενάριο, εντοπίζουμε και αναλύουμε κακόβουλες δραστηριότητες με βάση τα πακέτα που συλλέγονται και αναλύονται από εργαλεία ανάλυσης επιθέσεων, τα οποία βασίζονται σε εργαλεία ανάλυσης "υπογραφών επιθέσεων (signature-based). Η ανάλυσή μας δείχνει ότι οι επιθέσεις DDoS που βασίζονται στο Διαδίκτυο των Πραγμάτων είναι μία από τις πιο πρόσφατες και πιο αυξανόμενες τάσεις επίθεσης στην ασφάλεια δικτύων. Με βάση την ανάλυση των επιθέσεων, περιγράφουμε κάποιες τεχνικές μετριασμού που μπορούν να εφαρμοστούν στο δίκτυο των παρόχων για τον μετριασμό των συνεπειών τέτοιων επιθέσεων.

3. Συνοπτική ανάλυση της εργασίας **[C-33]** *"Preliminary design of a new approach to choose cyber exercise methodologies for critical infrastructures", Makrodimitris G., Kotzanikolaou P., Douligeris C.*

   Περίληψη: – Ως Κρίσιμες Υποδομές (ΚΥ) θεωρούνται οι υποδομές εκείνες των οποίων η απώλεια των επιμέρους συστημάτων και δικτύων θα είχε πολύ μεγάλη συνέπεια για την εθνική και οικονομική ασφάλεια. Ως εκ τούτου, η εκπαίδευση και η συνειδητοποίηση της ασφάλειας είναι ένας πολύ σημαντικός έλεγχος ασφάλειας για τις ΚΥ, των οποίων οι διαχειριστές θα πρέπει να εκπαιδεύονται συνεχώς για σχετικά ζητήματα, ώστε να είναι έτοιμοι να αντιμετωπίσουν καταστάσεις έκτακτης ανάγκης, όπως οι επιθέσεις στον κυβερνοχώρο. Για το λόγο αυτό, είναι απαραίτητη η συμμετοχή των στελεχών των ΚΥ σε ασκήσεις κυβερνοασφάλειας. Δεδομένου ότι αρκετές μεθοδολογίες ασκήσεων ασφάλειας στον κυβερνοχώρο έχουν αναπτυχθεί από διάφορους οργανισμούς,

ένα βασικό ερώτημα είναι ποια μεθοδολογία ασκήσεων κυβερνοασφάλειας είναι η πιο κατάλληλη για τις ΚΥ. Η παρούσα μελέτη συγκρίνει τις πιο γνωστές μεθοδολογίες ασκήσεων ασφάλειας στον κυβερνοχώρο και προτείνει μία νέα μέθοδο που θα μπορούσε να βοηθήσει τους διαχειριστές των ΚΥ στην επιλογή των καταλληλότερων μεθοδολογιών ασκήσεων κυβερνοασφάλειας, ανάλογα με τις εξελισσόμενες ανάγκες τους.

4. Συνοπτική ανάλυση της εργασίας **[C-32]** *"R-TSCH: Proactive Jamming Attack Protection for IEEE 802.15.4-TSCH Networks", Zorbas D., Kotzanikolaou P., and Douligeris C.*

Περίληψη: – Το Time Slotted Channel Hopping (TSCH) έχει προταθεί σε διάφορα ασύρματα πρωτόκολλα ως λύση για την καταπολέμηση εξωτερικών παρεμβολών, εξασθένισης διαδρομής και στατικών επιθέσεων εμπλοκής (static jamming attacks). Ωστόσο, δεδομένου ότι οι αλγόριθμοι TSCH δημιουργούν ένα ντετερμινιστικό και περιοδικό σχέδιο μετάβασης καναλιών, εξακολουθούν να υφίστανται επιθέσεις εμπλοκής. Η προληπτική τυχαιοποίηση της διαδικασίας δημιουργίας καναλιού θα μπορούσε να αποτελέσει μια καλή λύση κατά των επιθέσεων εμπλοκής, ωστόσο λόγω των αυστηρών χρονικών περιορισμών και ορίων, οι πρακτικές λύσεις πρέπει να είναι πολύ αποτελεσματικές. Σε αυτό το έγγραφο, προτείνουμε τον R-TSCH, έναν τυχαίο αλγόριθμο παραγωγής καναλιών ραδιοεκπομπής που μπορεί να χρησιμοποιηθεί για την προληπτική προστασία των ασύρματων κόμβων από επιθέσεις εμπλοκής. Με βάση μια κρυπτογραφική λειτουργία κατακερματισμού και ένα μυστικό κλειδί, το R-TSCH παράγει μια νέα ακολουθία ψευδοτυχαίων καναλιών, η οποία μοιάζει πραγματικά τυχαία σε οποιονδήποτε δεν έχει πρόσβαση στο κλειδί. Τα αποτελέσματά της προσομοίωσης δείχνουν ότι οι εφόσον οι στόχοι των επιθέσεων ενισχυθούν με τον προτεινόμενο μηχανισμό, μπορούν να επιτύχουν ποσοστό λήψης πακέτων άνω των 90% (PRR) παρουσία πολλαπλών επιθέσεων εμπλοκής.

5. Συνοπτική ανάλυση της εργασίας **[C-31]** *" Critical Infrastructure Protection: A Holistic Methodology for Greece", Gritzalis, D., Stergiopoulos, G., Kotzanikolaou, P., Magkos, E., & Lykou, G.*

Περίληψη: – Η προστασία των υποδομών ζωτικής σημασίας ή Κρίσιμων Υποδομών (ΚΥ) είναι, εξ ορισμού, υψίστης σημασίας για την ευημερία των πολιτών, λόγω των άμεσων απειλών και επίσης λόγω των εξαρτήσεων τους σε διεθνές και ευρωπαϊκό επίπεδο. Σήμερα, η Ελλάδα παραμένει μια από τις χώρες της Ευρωπαϊκής Ένωσης, η οποία δεν έχει σφαιρική στρατηγική για τη διαφύλαξη των εθνικών ΚΥ, ούτε οποιαδήποτε διαδικασία ανάπτυξης ενός ολοκληρωμένου σχεδίου, εκτός από ορισμένες πρωτοβουλίες της Γενικής Γραμματείας Ψηφιακής Πολιτικής. Στόχος του παρόντος εγγράφου είναι να συμβάλει: (i) στη δημιουργία καταλόγου όλων των εμπλεκόμενων φορέων (νομοθετικών, εποπτικών ή κανονιστικών) που εμπλέκονται στην προστασία των ΚΥ στην Ελλάδα, (ii) στον εντοπισμό των πιθανών εθνικών ΚΥ, καθώς και στις αλληλεξαρτήσεις τους iii) ανάπτυξη δομημένης αναγνώρισης βασισμένης στη μεθοδολογία εκτίμησης συνεπειών για τις εθνικές ΚΥ, η οποία λαμβάνει υπόψη τις διεθνώς εφαρμοζόμενες μεθοδολογίες αξιολόγησης ΚΥ και iv) παρέχει πιλοτική εφαρμογή της προτεινόμενης μεθοδολογίας.

6. Συνοπτική ανάλυση της εργασίας **[C-30]** *"Classification and Comparison of Critical Infrastructure Protection Tools", Stergiopoulos, G., Vasilellis, E., Lykou, G., Kotzanikolaou, P., & Gritzalis, D.*

Περίληψη: – Η μοντελοποίηση και ανάλυση των αλληλεξαρτήσεων κρίσιμης υποδομής είναι ένας τομέας έρευνας που έχει προσελκύσει σημαντικό ενδιαφέρον. Η αλληλεξάρτηση και οι αναλύσεις κινδύνου μπορούν να είναι υπολογιστικές εντατικές, αλλά μπορούν επίσης να αποφέρουν χρήσιμα αποτελέσματα που βελτιώνουν τις εκτιμήσεις κινδύνου και προσφέρουν εναλλακτικές λύσεις για τον μετριασμό του κινδύνου. Δυστυχώς, πολλά εργαλεία και μεθοδολογίες παραμένουν χωρίς υποστήριξη μετά την ολοκλήρωση των έργων που τα ανέπτυξαν. Αυτό το κεφάλαιο επιχειρεί να εντοπίσει και να ταξινομήσει πολλά υπάρχοντα εργαλεία και πλαίσια για να δημιουργήσει μια κοινή βάση για τον εντοπισμό απειλών και την αξιολόγηση των κινδύνων. Συγκρίνει επίσης τα χαρακτηριστικά και τις τεχνολογίες τους στη δημιουργία μιας ταξινόμησης. Εξετάζονται εννοιολογικές και ποιοτικές μελέτες

για τις αλληλεξαρτήσεις των υποδομών μαζί με τις προσεγγίσεις μοντελοποίησης και προσομοίωσης. Η σύγκριση βασίζεται σε δύο πτυχές: ο σκοπός που εξυπηρετεί κάθε εργαλείο και η προσέγγιση τεχνικής μοντελοποίησης. Αυτή η εργασία επιχειρεί να βοηθήσει την κοινότητα ασφαλείας του βιομηχανικού συστήματος ελέγχου ενεργώντας ως ενιαίο σημείο αναφοράς και εφιστώντας την προσοχή σε πιθανούς συνδυασμούς μοντελοποίησης για να επιτρέψει στους ερευνητές να εντοπίσουν και να κατασκευάσουν πολύπλοκες συνδυασμένες λύσεις που αποφέρουν καλύτερα αποτελέσματα. Η ανάλυση υποδεικνύει ότι η μελλοντική έρευνα θα πρέπει να αντιμετωπίσει τον μετριασμό του κινδύνου μέσω ποιοτικών και όχι ποσοτικών αναλύσεων. Οι συνεισφορές μπορούν να μεγιστοποιηθούν αναπτύσσοντας ολιστικά μετα-εργαλεία ή εστιάζοντας αποκλειστικά σε συγκεκριμένα προβλήματα.

7. Συνοπτική ανάλυση της εργασίας **[C-29]** *" Private Proximity Testing on Steroids: An NTRU-based Protocol", C. Patsakis, P. Kotzanikolaou and M. Bouroche*.

Περίληψη: – Σήμερα, τα περισσότερα κινητά τηλέφωνα έρχονται προ-εξοπλισμένα με δυνατότητες ανίχνευσης θέσης, επιτρέποντας στους προγραμματιστές να δημιουργούν μια μεγάλη ποικιλία εφαρμογών και υπηρεσιών θέσης. Ενώ η πληροφορία τοποθεσίας παρέχει καινοτόμα χαρακτηριστικά και λειτουργικότητα, ανοίγει την πόρτα σε πολλά προβλήματα ιδιωτικότητας. Σε πολλές περιπτώσεις, ωστόσο, οι χρήστες δεν χρειάζεται να μοιράζονται την πραγματική τους θέση, αλλά να καθορίζουν εάν βρίσκονται κοντά σε άλλους, κάτι που είναι σχεδόν ένα bit πληροφορίας. Τα ιδιωτικά πρωτόκολλα εγγύτητας επιτρέπουν αυτή τη λειτουργία χωρίς περαιτέρω διαρροή πληροφοριών. Σε αυτή την εργασία προτείνουμε ένα πρωτότυπο πρωτόκολλο το οποίο είναι πολύ πιο αποδοτικό από τις τρέχουσες λύσεις, και βασίζει την ασφάλειά του στην κρυπτογραφία βασισμένη σε πλέγματα (lattice-based cryptography).

8. Συνοπτική ανάλυση της εργασίας **[C-28]** *" Medusa: A Supply Chain Risk Assessment Methodology", D. Polemi, P. Kotzanikolaou*.

Περίληψη: – Παρόλο που έχουν καταβληθεί προσπάθειες για την προτυποποίηση της εκτίμησης κινδύνου για την ασφάλεια εφοδιασμού (ΑΕ), υπάρχει έλλειψη στοχοθετημένων μεθοδολογιών. Στο παρόν έγγραφο προτείνουμε τη μεθοδολογία Medusa, μια μεθοδολογία αξιολόγησης κινδύνου ΑΕ, σύμφωνα με το πρότυπο ISO28001. Η μεθοδολογία Medusa μπορεί να χρησιμοποιηθεί για να εκτιμηθεί ο συνολικός κίνδυνος ολόκληρης της αλυσίδας εφοδιασμού. Οι προκύπτουσες συνολικές τιμές κινδύνου χρησιμοποιούνται προκειμένου να δημιουργηθεί μια βασική πολιτική ασφαλείας ΑΕ, προσδιορίζοντας τους ελάχιστα αναγκαίους ελέγχους ασφάλειας για κάθε συμμετέχοντα στην ΑΕ. Επιπλέον, η Medusa αξιολογεί τον κίνδυνο κλιμακωτών σεναρίων απειλής σε μια ΑΕ. Αυτό δίνει τη δυνατότητα στους συμμετέχοντες να τελειοποιούν τις πολιτικές ασφαλείας σύμφωνα με τον επιχειρηματικό τους ρόλο καθώς και τις εξαρτήσεις τους.

9. Συνοπτική ανάλυση της εργασίας **[C-27]** *"Using Centrality Measures in CI Dependency Risk Graphs for Efficient Risk Mitigation", G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, D. Gritzalis*.

Περίληψη: – Ένας τρόπος για να μοντελοποιήσουμε διαδοχικές αστοχίες (cascading failures) κρίσιμων υποδομών είναι μέσω γραφημάτων κινδύνου εξάρτησης. Αυτές οι γραφικές παραστάσεις βοηθούν στην εκτίμηση του αναμενόμενου κινδύνου αλυσίδων εξάρτησης κρίσιμης υποδομής. Η έρευνα αυτή επεκτείνει μια υπάρχουσα μεθοδολογία ανάλυσης κινδύνου εξάρτησης από τη διαχείριση κινδύνου. Αναλύεται η σχέση μεταξύ των διαδρομών κινδύνου εξάρτησης και των μέτρων κεντρικής κατανομής των γραφικών παραστάσεων προκειμένου να εντοπιστούν κόμβοι που επηρεάζουν σημαντικά τον συνολικό κίνδυνο εξάρτησης. Εφαρμόζονται πειραματικά αποτελέσματα χρησιμοποιώντας τυχαία γραφήματα για την προσομοίωση κοινών χαρακτηριστικών εξάρτησης κρίσιμης υποδομής. Με βάση τα πειραματικά ευρήματα, προτείνεται ένας αλγόριθμος για τον αποτελεσματικό μετριασμό του κινδύνου. Ο αλγόριθμος μπορεί να χρησιμοποιηθεί για τον ορισμό προτεραιοτήτων στην επιλογή κόμβων για την εφαρμογή των ελέγχων ασφάλειας.

10. Συνοπτική ανάλυση της εργασίας **[C-26]** *"Towards Secure and Practical Location Privacy through Private Equality Testing", E. Magkos, P. Kotzanikolaou, M. Magioladitis, S. Sioutas, and V.S. Verykios.*

Περίληψη: – Σε αυτό το άρθρο, προτείνουμε ένα πρακτικό πρωτόκολλο ελέγχου ισότητας με προστασία ιδιωτικότητας (private equality testing protocol), το οποίο επιτρέπει σε δυο χρήστες να μάθουν αν μοιράζονται τα ίδια κρυπτογραφημένα δεδομένα εισόδου. Το πρωτόκολλό μας δεν απαιτεί καμία εμπιστοσύνη σε τρίτα μέρη και/ή άλλους χρήστες και είναι ειδικά κατάλληλο για δεδομένα χαμηλής ελάχιστης εντροπίας (δηλαδή δεδομένα που μπορούν να αναζητηθούν εξαντλητικά από έναν εισβολέα), όπως κρυπτογραφημένες τοποθεσίες χρηστών. Επιδεικνύουμε ότι το πρωτόγονο μας είναι ασφαλές και αποτελεσματικό: Για κάθε δοκιμή ισότητας απαιτούνται δύο εκθετικές πράξεις δημόσιου κλειδιού ανά χρήστη. Δίνουμε αποτελέσματα εφαρμογής, δείχνοντας ότι το πρωτόκολλό μας είναι πρακτικό σε ένα σενάριο πολλαπλών χρηστών. Τέλος, περιγράφουμε τον τρόπο με τον οποίο θα μπορούσαμε να χρησιμοποιήσουμε το μοντέλο μας ως δομικό στοιχείο για μια υπηρεσία κοινωνικών δικτύων, για την εύρεσης φίλων σε κοντινή τοποθεσία με προστασία της ιδιωτικότητας θέσης.

11. Συνοπτική ανάλυση της εργασίας **[C-25]** *"Evaluating security controls against HTTP-based DDoS attacks",* D. Moustis and P. Kotzanikolaou.

Περίληψη: – Οι Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσίας (DDoS) απαιτούν συνήθως έναν botmaster ο οποίος ελέγχει ένα μεγάλο αριθμό μολυσμένων συστημάτων (bot), με σκοπό την κατάρρευση μίας συγκεκριμένης υπηρεσίας-στόχου. Οι περισσότερο πρόσφατες επιθέσεις αυτού του τύπου στοχεύουν πλέον στο HTTP επίπεδο και όχι στο TCP επίπεδο όπως παλαιότερα και είναι πολύ αποτελεσματικές, ακόμη και με έναν σχετικά μικρό αριθμό από μολυσμένα συστήματα. Σε αυτή την εργασία μελετάμε τις επιθέσεις DDoS οι οποίες είναι αποτελεσματικές ακόμα και με λίγα μολυσμένα συστήματα Για τη μελέτη μας έχουμε υλοποιήσει ένα σύστημα Botnet σε δοκιμαστικό περιβάλλον. Προσομοιώνουμε τη συμπεριφορά των μολυσμένων συστημάτων τόσο σε Linux όσο και σε Windows συστήματα, τα οποία έχουν μολυνθεί από το Slowloris, ένα HTTP syn-flooder, ο οποίος στοχεύει σε ένα ευάλωτο εξυπηρετητή ιστού Apache. Εφαρμόζουμε διάφορα μέτρα ασφάλειας για να δοκιμάσουμε την αποτελεσματικότητά τους έναντι τέτοιων επιθέσεων. Τα αποτελέσματά μας δείχνουν ότι απαιτείται ένας κατάλληλα επιλεγμένος συνδυασμός μέτρων ασφάλειας για να μειωθεί η έκθεση του εξυπηρετητή σε τέτοιες επιθέσεις, χωρίς να επηρεάζεται η ποιότητα της παρεχόμενης υπηρεσίας.

12. Συνοπτική ανάλυση της εργασίας **[C-24]** *"Cascading Effects Of Common-Cause Failures On Critical Infrastructures",* P. Kotzanikolaou, M. Theocharidou, and D. Gritzalis.

Περίληψη: – Η αναγνώριση και η αντιμετώπιση των μεταβατικών περιστατικών ασφάλειας (cascading events) μεταξύ των διαφόρων υποδομών. Σε προηγούμενη έρευνά μας, έχουμε παρουσιάσει μία μέθοδο η οποία μπορεί να εφαρμοστεί για την αποτίμηση των αθροιστικών κινδύνων από μεταβατικά περιστατικά, εξαιτίας των διασύνδεσης πολλαπλών επιπέδων μεταξύ των υποδομών. Όμως, πρόσφατες εμπειρικές έρευνες έχουν δείξει ότι οι επιπτώσεις περιστατικών κοινής κατάστασης (common mode failure) οδηγούν συχνά σε πολύ υψηλές συνέπειες, οι οποίες είναι συγκρίσιμες ή και περισσότερο καταστροφικές από τις περιπτώσεις των μεταβατικών γεγονότων. Σε αυτή την εργασία προτείνουμε μία επέκταση του προηγούμενου μοντέλου μας με σκοπό να αποτιμήσουμε την επικινδυνότητα που προκύπτει σε σύνθετες καταστάσεις πολλαπλών μεταβατικών γεγονότων τα οποία όλα προέρχονται από ένα περιστατικό κοινής κατάστασης (ένα μεγάλο περιστατικό ασφάλειας το οποίο επηρεάζει ταυτόχρονα πολλές υποδομές. Επιπλέον παρουσιάζουμε ρεαλιστικά σενάρια τα οποία μπορούν αν χρησιμοποιηθούν ως σενάρια δοκιμής για την ανάλυση του προτεινόμενου μοντέλου.

13. Συνοπτική ανάλυση της εργασίας **[C-23]** *"Fair Anonymous Authentication for Location Based Services",* P. Kotzanikolaou, E. Magkos, N. Petrakos, C. Douligeris and V. Chrissikopoulos.

Περίληψη: – Σε αυτή την εργασία προτείνεται ένα αποδοτικό σχήμα ανώνυμης αυθεντικοποίησης το οποίο παρέχει μη ιχνηλασιμότητα (untraceability) και μη συνδεσιμότητα (unlinkability) για κινητές συσκευές κατά την πρόσβασή τους σε υπηρεσίες θέσης (Location-Based Services). Σε αυτό το σχήμα ακολουθείται η προσέγγιση κατά την οποία ο πάροχος δικτύου θεωρείται ως ένας έμπιστος εκδότης ανώνυμων διαπιστευτηρίων για τους χρήστες του. Όμως, το σχήμα αποτρέπει τόσο τη μεταφορά διαπιστευτηρίων (credential transferability) σε μη εξουσιοδοτημένους χρήστες, όσο και την παγιδευσιμότητα του χρήστη (user frameability) από τον πάροχο δικτύου και σε αντίθεση με άλλα σχήματα, χωρίς να απαιτείται η χρήση ενσωματωμένου ασφαλούς υλικού. Το σχήμα υποστηρίζει μία εξισορρόπηση μεταξύ της προσφερόμενης ανωνυμίας και της προστασίας από επιθέσεις κατάχρησης: Από τη μία πλευρά, ο πάροχος, ακόμα και σε συνεργασία με τους παρόχους υπηρεσιών, δεν μπορέι να παγιδεύσει έναν χρήστη, δημιουργώντας μία συναλλαγή η οποία να αποδίδεται λαθεμένα σε κάποιον χρήστη. Απότ ην άλλη πλευρά, σε περίπτωση κατάχρησης της ανωνυμίας, το σχήμα υποστηρίζει άρση της ανωνυμίας για αποδεδειγμένα κακόβουλους χρήστες. Το σχήμα στηρίζεται σε γνωστά κρυπτογραφικά εργαλεία όπως είναι οι αποδείξεις μηδενικής γνώσης, αποδείξεις ελέγχου ακεραιότητας και προκλήσεις/απαντήσεις. Η ασφάλεια του σχήματος αποδεικνύεται ότι στηρίζεται στην αδυναμία επίλυσης του προβλήματος διαιρετότητας Diffie-Hellman(Divisible Diffie-Hellman assumption).

14. Συνοπτική ανάλυση της εργασίας **[C-22]** *"Using Strand Space Model to Verify the Privacy Properties of a Fair Anonymous Authentication Scheme for Location Based Services",* N. Petrakos, P. Kotzanikolaou, C. Douligeris.

Περίληψη: – Το μοντέλο strand space έχει προταθεί ως ένα τυπικό μοντέλο για την επαλήθευση των στόχων ασφάλειας κρυπτογραφικών πρωτοκόλλων. Πολλά κρυπτογραφικά πρωτόκολλα στοχεύουν πλέον όχι μόνο στην ικανοποίηση ιδιοτήτων ασφάλειας αλλά και ιδιωτικότητας επικοινωνίας, όπως είναι η ανωνυμία. Σε αυτή την εργασία εφαρμόζεται το μοντέλο strand space με σκοπό την επαλήθευση των στόχων ασφάλειας και ιδιωτικότητας ενός πρόσφατου πρωτοκόλλου ανώνυμης αυθεντικοποίησης. Αποδεικνύεται ότι το μοντέλο strand space μπορεί να χρησιμοποιηθεί για την τυπική αναπαράσταση και έλεγχο ιδιοτήτων ιδιωτικότητας όπως είναι η μη-ιχνηλασιμότητα, η μη-συνδεσιμότητα, η μη-παγίδευση χρηστών και η μη-μεταφερσιμότητα των διαπιστευτηρίων πρόσβασης. Ως παράδειγμα πρωτοκόλλου χρησιμοποιούμε ένα πρόσφατο πρωτόκολλο το οποίο έχει προταθεί για την ανώνυμη αυθεντικοποίηση κινητών συσκευών για υπηρεσίες θέσης.

15. Συνοπτική ανάλυση της εργασίας **[C-21]** *"Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects",* P.Kotzanikolaou, M. Theocharidou, and D. Gritzalis.

Περίληψη: – Ένα από τα σημαντικότερα ζητήματα κατά την προστασία των Κρίσιμων Υποδομών είναι η αναγνώριση και η αποτίμηση των αλληλεξαρτήσεων. Σε αυτή την εργασία εξετάζουμε πιθανές μεταβατικές συνέπειες σε διάφορες υποδομές, οι οποίες μπορούν να προκληθούν από ένα περιστατικό ασφάλειας. Η μέθοδός μας παρέχει ένα τρόπο για την αναγνώριση των απειλών οι οποίες φαίνονται ασήμαντες εάν εξετάσουμε εξαρτήσεις πρώτου βαθμού μεταξύ υποδομών, αλλά θα μπορούσαν να προκαλέσουν σημαντικές συνέπειες εάν εξεταστούν από μία μακροσκοπική προσέγγιση οποία λαμβάνει υπόψη εξαρτήσεις πολλαπλού βαθμού. Βασιζόμενοι σε προηγούμενη εργασία μας, χρησιμοποιούμε γράφους εξαρτήσεων πρώτου βαθμού, με σκοπό να αποτιμήσουμε τις συνέπειες περιστατικών ασφάλειας σε διαδοχικές υποδομές με μακρινές εξαρτήσεις.

16. Συνοπτική ανάλυση της εργασίας **[C-20]** *"Impact Assessment through Collaborative Asset Modeling: The STORM-RM approach",* T. Ntouskas, P. Kotzanikolaou and N. Polemi.

Περίληψη: – Οι υπάρχουσες μεθοδολογίες ανάλυσης επικινδυνότητας βασίζονται κυρίως στην υλοποίηση από εξειδικευμένους αναλυτές και απαιτούν ένα μεγάλο αριθμό προσωπικών συνεντεύξεων μεταξύ των αναλυτών ασφάλειας και προσωπικού διαφόρων ειδικοτήτων του υπό μελέτη οργανισμού. Αυτή η ανάγκη αυξάνει τον απαιτούμενο χρόνο και το απαιτούμενο κόστος για μία ενδελεχή ανάλυση

επικινδυνότητας και πολλές φορές οδηγεί στην υλοποίηση μελετών με μικρότερο αριθμό συμμετεχόντων και κατά συνέπεια, μικρότερη συλλογή χρήσιμης πληροφορίας. Σε αυτή την εργασία επεκτείνουμε την πολύκριτηριακή μεθοδολογία ανάλυσης επικινδυνότητας STORM-RM. Πιο συγκεκριμένα, προτείνουμε συγκεκριμένα μοντέλα ανάλυσης χρηστών και αγαθών, η οποία στηρίζεται στην πολυκριτηριακή μεθοδολογία λήψης αποφάσεων AHP, με σκοπό την αναγνώριση των αγαθών του υπό μελέτη οργανισμού και τον υπολογισμό των πιθανών συνεπειών ασφάλειας.

17. Συνοπτική ανάλυση της εργασίας **[C-19]** *"A Distributed Privacy-Preserving Scheme for Location-Based Queries"*, E. Magkos, P. Kotzanikolaou, S. Sioutas and K. Oikonomou.

Περίληψη: – Σε αυτή την εργασία εξετάζουμε την ιστορική ιδιωτικότητα (historical privacy) σε Υπηρεσίες Προσανατολισμένες στη Θέση (Location Based Service – LBS), στις οποίες οι χρήστες υποβάλλουν την ακριβή θέση τους στον πάροχο της υπηρεσίας. Προτείνεται ένα κατανεμημένο σύστημα το οποίο επιτυγχάνει έλεγχο πρόσβασης αλλά προστατεύει ταυτόχρονα την ιδιωτικότητα των χρηστών σε σποραδικά ή συνεχή ερωτήματα προς υπηρεσίες θέσης. Η προτεινόμενη λύση χρησιμοποιεί μία υβριδική αρχιτεκτονική δικτύου στην οποία οι χρήστες: (α) μπορούν να επικοινωνούν με τον πάροχο μέσω ενός δικτύου (π.χ. ενός παρόχου κινητής τηλεφωνίας) και (β) μπορούν επιπλέον να δημιουργούν τα δικά τους ασύρματα ad-hoc δίκτυα με άλλους κοντινούς κόμβους έτσι ώστε να προστατέψουν την ανωνυμία τους από επίθεσης ανάλυσης κίνησης. Για την προστασία της ιστορικής ανωνυμίας χρησιμοποιούμε πολλαπλά ψευδώνυμα τα οποία αλλάζουν σε τακτά χρονικά διαστήματα. Για την επίτευξη της μη-ανιχνευσιμότητας τα μηνύματα δεν στέλνονται απευθείας στον πάροχο δικτύου αλλά μέσω του ad hoc δικτύου του χρήστη, το οποίο λειτουργεί ως δίκτυο μόχλευσης (mix network) και επανακρυπτογραφεί κάθε μήνυμα πριν αυτό σταλεί στον πάροχο υπηρεσιών θέσης. Ως πιθανή επέκταση προτείνεται η συγχώνευση ανεξάρτητων ερωτημάτων πριν την αποστολή τους στον πάροχο υπηρεσιών θέσης. Αυτή η προσέγγιση είναι κατάλληλη σε εφαρμογές στις οποίες μπορούν να χρησιμοποιηθούν συγχωνευμένα δεδομένα θέσης (π.χ. παρακολούθηση και έλεγχος κίνησης).

18. Συνοπτική ανάλυση της εργασίας **[C-18]** *"Enhancing Privacy-Preserving Access Control for Pervasive Computing Environments"*, E. Magkos and P. Kotzanikolaou.

Περίληψη: – Η αυξανόμενη χρήση διάχυτου υπολογιστικού περιβάλλοντος (Pervasive Computing Environment) για την ανταλλαγή πληροφοριών, δημιουργεί ανησυχίες ως προς την ασφάλεια και την ιδιωτικότητα. Από τη μία πλευρά οι πάροχοι υπηρεσιών απαιτούν την αυθεντικοποίηση και εξουσιοδότηση των χρηστών πριν την παροχή των υπηρεσιών τους. Από την άλλη πλευρά οι χρήστες επιθυμούν την προστασία των συναλλαγών τους από επιθέσεις αναζήτησης και σύνδεσης μεταξύ των διαφορετικών συναλλαγών τους. Σε αυτή την εργασία παρουσιάζονται βασικές απαιτήσεις ασφάλειας και ιδιωτικότητας για τον έλεγχο πρόσβασης σε διάχυτα υπολογιστικά περιβάλλοντα. Επιπλέον, αποδεικνύεται ότι διάφορα πρόσφατα συστήματα ελέγχου πρόσβασης για αυτά τα περιβάλλοντα, δεν καταφέρνουν να ικανοποιήσουν όλες τις παραπάνω απαιτήσεις. Τέλος, παρουσιάζεται μία γενική προσέγγιση για την επίτευξη επιθυμητών επιπέδων ιδιωτικότητας έναντι επιθέσεων προερχόμενων από κακόβουλους εσωτερικούς χρήστες, δίνοντας έμφαση στην ισορροπία ανταγωνιστικών απαιτήσεων όπως είναι ο έλεγχος πρόσβασης και ο καταλογισμός ευθύνης.

19. Συνοπτική ανάλυση της εργασίας **[C-17]** *"Evaluating Common Privacy Vulnerabilities in Internet Service Providers"*, P.Kotzanikolaou, S. Maniatis, E. Nikolouzou and V. Stathopoulos.

Περίληψη: – Η ιδιωτικότητα στις ηλεκτρονικές επικοινωνίες έχει λάβει σημαντική προσοχή τόσο σε επίπεδο έρευνας, όσο και σε επίπεδο βιομηχανίας. Αυτή η τάση οφείλεται τόσο στις απαιτήσεις των χρηστών για προστασία της ιδιωτικότητας των επικοινωνιών τους, όσο και στις νομικές και ρυθμιστικές απαιτήσεις σε εθνικό και διεθνές επίπεδο. Η ιδιωτικότητα στις διαδικτυακές επικοινωνίες βασίζεται σε μεγάλο βαθμό στο επίπεδο ασφάλειας των Παρόχων Διαδικτυακών Επικοινωνιών (ISP), αλλά και στο

επίπεδο ενημέρωσης των τελικών χρηστών για θέματα ασφάλειας και ιδιωτικότητας των επικοινωνιών τους. Σε αυτή την εργασία εξετάζεται ο ρόλος των Παρόχων Διαδικτυακών Επικοινωνιών για την προστασία της ιδιωτικότητας. Με βάση τα αποτελέσματα πραγματικών ελέγχων ασφάλειας που έχουν πραγματοποιηθεί σε Παρόχους εθνικής κλίμακας, παρουσιάζουμε απειλές ασφάλειας που σχετίζονται με την προστασία του απορρήτου των επικοινωνιών, αλλά και αδυναμίες που εμφανίζονται πολύ συχνά λόγω αστοχιών στην υλοποίηση των πολιτικών ασφάλειας. Τέλος παρουσιάζονται συγκεκριμένα μέτρα ασφάλειας τα οποία μπορούν να υλοποιηθούν σε επίπεδο Παρόχου, με σκοπό την καλύτερη υλοποίηση των πολιτικών ασφάλειας και την πληρέστερη προστασία της επικοινωνίας των τελικών χρηστών.

20. Συνοπτική ανάλυση της εργασίας **[C-16]** *"Risk-Based Criticality Analysis",* M. Theocharidou, P. Kotzanikolaou and D. Gritzalis.

Περίληψη: – Η προστασία των Κρίσιμων Υποδομών (ΚΥ) απαιτεί την αποτίμηση της κρισιμότητας των υποδομών και τον καθορισμό προτεραιοτήτων για τα αγαθά που απαρτίζουν τις ΚΥ. Όμως η ανάλυση κρισιμότητας – σε αντίθεση με την ανάλυση επικινδυνότητας – δεν έχει μελετηθεί επαρκώς και δεν έχει προτυποποιηθεί. Σε αυτή την εργασία εξετάζεται η σχέση μεταξύ της επικινδυνότητας και της κρισιμότητας. Αναλύονται οι ομοιότητες και οι διαφορές τους ως προς το εύρος, τους στόχους, τις συνέπειες, τις απειλές και τις αδυναμίες. Επιπλέον, προτείνεται μία γενική μεθοδολογία ανάλυσης κρισιμότητας η οποία στηρίζεται στις βασικές αρχές της ανάλυσης επικινδυνότητας. Παρουσιάζονται επίσης ορισμένα κριτήρια συνεπειών (impact criteria) τα οποία μπορούν να χρησιμοποιηθούν για την αποτίμηση της κρισιμότητας των υποδομών. Έμφαση δίνεται σε τύπους συνεπειών οι οποίοι είναι προσανατολισμένοι σε εξωτερικές (ευρύτερες κοινωνικές συνέπειες ή συνέπειες για ολόκληρο ένα ολόκληρο τομέα υποδομών), σε αντίθεση με τις παραδοσιακές μεθοδολογίες αποτίμησης επικινδυνότητας οι οποίες δίνουν έμφαση σε συνέπειες εσωτερικές / προσανατολισμένες προς τον ίδιο τον υπό μελέτη οργανισμό ή υποδομή.

21. Συνοπτική ανάλυση της εργασίας **[C-15]** *"Privacy Threats of Data Retention in Internet Communications",* Panayiotis Kotzanikolaou and Christos Douligeris.

Περίληψη: – Ο όρος Διατήρηση Δεδομένων επικοινωνίας (data retention) αναφέρεται στη νομική υποχρέωση των Παρόχων Πρόσβασης στο Διαδίκτυο (ISPs) για την διατήρηση των δεδομένων επικοινωνίας των συνδρομητών τους για κάποια ορισμένη περίοδο, με σκοπό την εξυπηρέτηση νόμιμων ερευνών και τη διερεύνηση πιθανών εγκλημάτων. Η διατήρηση δεδομένων επικοινωνίας αυξάνει τους κινδύνους ασφάλειας ιδιαίτερα έναντι του απορρήτου και της προστασίας της ιδιωτικότητας των συνδρομητών. Σε αυτή την εργασία εξετάζουμε τους κινδύνους αυτούς και προτείνουμε πιθανούς μηχανισμούς ασφάλειας οι οποίοι ενδέχεται να μειώσουν αυτούς τους κινδύνους εναντίον της ιδιωτικότητας και του απορρήτου των επικοινωνιών των συνδρομητών.

22. Συνοπτική ανάλυση της εργασίας **[C-14]** *"Chord-PKI: Embedding a Public Key Infrastructure into the Chord Overlay Network",* Agapios Avramidis, *Panayiotis Kotzanikolaou and Christos Douligeris.*

Περίληψη: – Στόχος αυτής της εργασίας είναι η υποστήριξη υπηρεσιών ασφάλειας όπως είναι η αυθεντικοποίηση, η εμπιστευτικότητα και ο καταλογισμός ευθύνης σε δίκτυα ομότιμων κόμβων. Προτείνεται μία κατανεμημένη αρχιτεκτονική Υποδομής Δημόσιου Κλειδιού, κατάλληλη για ομότιμα δίκτυα, και πιο συγκεκριμένα για το δίκτυο Chord. Η προτεινόμενη λύση ενσωματώνει την Υποδομή Δημόσιου Κλειδιού στην αρχιτεκτονική του Chord. Γίνεται χρήση γνωστών κρυπτογραφικών τεχνικών όπως είναι η κρυπτογραφία κατωφλίου και η προληπτική ανανέωση κλειδιού.

23. Συνοπτική ανάλυση της εργασίας **[C-13]** *"B{GOP}: An Adaptive Algorithm for Coverage Problems in Wireless Sensor Networks",* Dimitrios Zorbas, Dimitrios Glynos, *Panayiotis Kotzanikolaou and Christos Douligeris.*

Περίληψη: – Η εργασία αυτή ασχολείται με την επίτευξη υψηλής διαθεσιμότητας σε δίκτυα αισθητήρων. Η κάλυψη περιοχών από δίκτυα αισθητήρων για μέγιστα χρονικά διαστήματα, απαιτεί τη διαίρεση των κόμβων σε υποσύνολα κάλυψης ώστε κάθε υποσύνολο να καλύπτει το σύνολο των στόχων της κάλυψης. Η δημιουργία του μέγιστου πλήθους τέτοιων υποσυνόλων κάλυψης έχει αποδειχθεί ότι είναι πρόβλημα NP-complete και συνεπώς, οι προτεινόμενες λύσεις είναι υπο-βέλτιστες. Σε αυτή την εργασία προτείνεται ένας κεντροποιημένος αλγόριθμος για την αποδοτικό υπολογισμό ανεξάρτητων συνόλων πλήρους κάλυψης. Τα αποτελέσματα της προσομοίωσης δείχνουν βελτίωση σε σχέση με τις υπάρχουσες μεθόδους, με αποτελέσματα που τείνουν προς τη βέλτιστη λύση. Με αυτό τον τρόπο η διαθεσιμότητα του δικτύου κάλυψης προσεγγίζει το μέγιστο δυνατό χρόνο κάλυψης.

24. Συνοπτική ανάλυση της εργασίας **[C-12]** *"A Framework for Secure and Verifiable Logging in Public Communication Networks"*, Vassilios Stathopoulos, *Panayiotis Kotzanikolaou and Emmanouil Magkos.*

Περίληψη: – Η εργασία αυτή ασχολείται με την ασφάλεια και την αξιοπιστία των αρχείων καταγραφής των παρόχων ηλεκτρονικών επικοινωνιών. Γίνεται ανασκόπιση των μοντέλων ασφάλειας των συστημάτων καταγραφής γεγονότων και στη συνέχεια προτείνεται ένα εκτεταμένο μοντέλο ασφάλειας το οποίο είναι κατάλληλο για το περιβάλλον των παρόχων ηλεκτρονικών επικοινωνιών. Επιπλέον, προτείνεται ένα πλαίσιο για την ασφάλεια των συστημάτων καταγραφής όπως και παραδείγματα σχεδιασμού υλοποίησης του προτεινόμενου πλαισίου. Βασικό ρόλο σε αυτό το μοντέλο έχει μία ανεξάρτητη Ρυθμιστική Αρχή η οποία έχει το ρόλο έμπιστης οντότητας και έχει τη βασική ευθύνη να επαληθεύει την ακεραιότητα των αρχείων καταγραφής.

25. Συνοπτική ανάλυση της εργασίας **[C-11]** *"An Asymmetric Key Establishment Protocol for Multiphase Self-Organized Sensor Networks", E. Magkos, P. Kotzanikolaou, D. Vergados and M. Stefanidakis*

Περίληψη: – Σε αυτή την εργασία παρουσιάζεται ένα ασύμμετρο πρωτόκολλο εγκαθίδρυσης κλειδιού για κατανεμημένα δίκτυα αισθητήρων (DSNs). Το πρωτόκολλο υποστηρίζει ανάπτυξη των κόμβων στο δίκτυο σε πολλαπλές φάσεις, μέσω ομαδοποιήσεων των κόμβων σε σύνολα τα οποία είναι γνωστά ως «γενιές» κόμβων. Μετά την ανάπτυξη των κόμβων της πρώτης γενιάς, οι γειτονικοί κόμβοι εγκαθιδρύουν μεταξύ τους κλειδιά ανά ζεύγη, έτσι ώστε να είναι δυνατή η μεταξύ τους ασφαλής επικοινωνία μεταξύ γειτονικών κόμβων. Στη συνέχεια, κάθε επερχόμενη γενιά κόμβων ξεκινά μία νέα φάση εγκαθίδρυσης κλειδιού, ώστε να είναι δυνατό να επικοινωνήσουν οι νέοι κόμβοι μεταξύ τους, αλλά και με τους κόμβους των προηγούμενων γενεών. Το πρωτόκολλο αυτό επεκτείνει το υβριδικό πρωτόκολλο των Kotzanikolaou et al. Μετατρέποντας το σχήμα αυτό από υβριδικό σε πλήρως ασύμμετρο, επιλύεται μία αδυναμία ασφάλειας του υβριδικού πρωτοκόλλου, χωρίς να αυξάνεται το απαιτούμενο κόστος υπολογισμού και επικοινωνίας.

26. Συνοπτική ανάλυση της εργασίας **[C-10]** *"Performance Analysis of a Hybrid Key Establishment Protocol for Wireless Sensor Networks", P. Kotzanikolaou, D. Vergados, and G. Stergiou*

Περίληψη: – Τα Κατανεμημένα Δίκτυα Αισθητήρων γίνονται ολοένα και πιο δημοφιλή, λόγω της δυνητικής χρήσης τους σε διάφορες εφαρμογές. Όμως, οι περιορισμοί που προκύπτουν από τη φύση των κόμβων αισθητήρων, όπως είναι οι περιορισμοί σε ενέργεια, μνήμη και υπολογιστική δύναμη, απαιτούν την ανάπτυξη νέων τεχνικών δικτύωσης. Τα Κατανεμημένα Δίκτυα Αισθητήρων είναι γενικά περισσότερο ευπαθή σε επιθέσεις ασφάλειας από ότι άλλες τεχνολογίες ενσύρματης ή ασύρματης δικτύωσης. Διάφορα πρωτόκολλα εγκαθίδρυσης κλειδιών έχουν προταθεί για την διασφάλιση τέτοιων δικτύων, τα οποία μπορούν να περιλάβουν περιπτώσεις ανάπτυξης του δικτύου σε πολλαπλές φάσεις. Σε αυτή την εργασία αναλύουμε την απόδοση ενός υβριδικού πρωτοκόλλου εγκαθίδρυσης κλειδιών, όπως προτάθηκε από τους Kotzanikolaou et al.

27. Συνοπτική ανάλυση της εργασίας **[C-9]** *"Hybrid Key Establishment for Multiphase Self-Organized Sensor Networks", Panayiotis Kotzanikolaou, Emmanouil Magkos, Christos Douligeris and Vassilios Chrissikopoulos.*

Περίληψη: - Η πρόσφατη έρευνα σε πρωτόκολλα εγκαθίδρυσης κλειδιών για δίκτυα αισθητήρων έχει αποδείξει ότι είναι δυνατό να χρησιμοποιηθεί περιορισμένη Κρυπτογράφηση Ελλειπτικών Καμπύλων, μέσω υβριδικών πρωτοκόλλων. Σε αυτή την εργασία, παρουσιάζεται ένα υβριδικό πρωτόκολλο εγκαθίδρυσης κλειδιών για ομοιόμορφα αυτό-οργανωμένα δίκτυα αισθητήρων. Το προτεινόμενο πρωτόκολλο συνδυάζει το πρωτόκολλο εγκαθίδρυσης κλειδιών Ελλειπτικής Καμπύλης Diffie-Hellmann, με τη χρήση έμμεσων πιστοποιητικών (implicit certificates) και συμμετρικών κρυπτογραφικών τεχνικών. Το πρωτόκολλο μπορεί να εφαρμοστεί σε ομοιόμορφα δίκτυα τα οποία αποτελούνται εξολοκλήρου από κόμβους περιορισμένων δυνατοτήτων. Επιπλέον, λόγω της ασύμμετρης φύσης του, το πρωτόκολλο μπορεί να αντιμετωπίσει ένα μεγάλο εύρος ενεργών και παθητικών επιθέσεων ασφάλειας, όπως είναι επιθέσεις κατά της εμπιστευτικότητας, ακεραιότητας και αυθεντικότητας της επικοινωνίας. Το πρωτόκολλο είναι αποδοτικό και εφαρμόσιμο σε συσκευές χαμηλών δυνατοτήτων, όσον αφορά τις δυνατότητες αποθήκευσης, επικοινωνίας και υπολογισμού. Το κόστος για κάθε κόμβο περιορίζεται σε έναν πολλαπλασιασμό σε ελλειπτική καμπύλη με τυχαίο σημείο, και σε έναν πολλαπλασιασμό με σταθερό σημείο.

*28.*Συνοπτική ανάλυση της εργασίας **[C-8]** *"Performance Analysis of Secure Multipath Routing Protocol for Mobile Ad Hoc Networks", Rosa Mavropodi, Panayiotis Kotzanikolaou, and Christos Douligeris.*

Περίληψη: - Τα πρωτόκολλα πολλαπλής δρομολόγησης για Κινητά Δίκτυα Ειδικού Σκοπού Mobile Ad Hoc Networks), προτάθηκαν στη διεθνή βιβλιογραφία, στοχεύοντας αρχικά στην εξυπηρέτηση αναγκών Ποιότητας Υπηρεσίας (Quality of Service), εφόσον δεν απαιτούν την επανεκκίνηση της αναζήτησης διαδρομής δρομολόγησης μετά από κάθε διακοπή διασύνδεσης. Η πρόσφατη έρευνα έχει αποδείξει ότι τα πρωτόκολλα πολλαπλής δρομολόγησης παρέχουν αυξημένη αντίσταση σε επιθέσεις κακόβουλων συνεργαζόμενων κόμβων. Προς αυτή την κατεύθυνση, διάφορα πρωτόκολλα πολλαπλής δρομολόγησης προτείνονται στη βιβλιογραφία, τα οποία παρέχουν αυτή την αυξημένη προστασία σε κρίσιμες εφαρμογές Κινητών Δικτύων Ειδικού Σκοπού. Παρόλα αυτά, οι ενσωματωμένοι μηχανισμοί ασφάλειας που χρησιμοποιούν, αυξάνουν το κόστος της διαδικασίας δρομολόγησης. Σε αυτή την εργασία, γίνεται μία σύγκριση της απόδοσης των υφισταμένων πρωτοκόλλων για ασφαλή πολλαπλή δρομολόγηση σε Κινητά Δίκτυα Ειδικού Σκοπού, μέσω προσομοιώσεων σε διάφορα σενάρια κίνησης.

29. Συνοπτική ανάλυση της εργασίας **[C-7]** *"Preventing Impersonation Attacks in MANET with multi-factor authentication", Dimitrios Glynos, Panayiotis Kotzanikolaou, and Christos Douligeris.*

Περίληψη: - Τα υπάρχοντα σχήματα αυθεντικοποίησης για Κινητά Δίκτυα Ειδικού Σκοπού δεν μπορούν να προστατέψουν πλήρως τους κόμβους από επιθέσεις πλαστοπροσωπίας. Αν και τα σχήματα αυτά συνδέουν κρυπτογραφικά μία οντότητα με μία ισχυριζόμενη ταυτότητα, η πραγματική οντότητα δεν συνδέεται ποτέ με τα φυσικά χαρακτηριστικά του κόμβου. Παρόλα αυτά, ο σύνδεσμος αυτός μεταξύ του κόμβου και της οντότητας υπονοείται εμμέσως. Αυτό το χαρακτηριστικό μπορεί εύκολα να χρησιμοποιηθεί κακόβουλα στα Κινητά Δίκτυα Ειδικού Σκοπού, εξαιτίας του τρόπου μετάδοσης του χρησιμοποιούμενου μέσου πρόσβασης. Σε αυτή την εργασία προτείνεται ένα πλαίσιο αυθεντικοποίησης πολλαπλών παραγόντων, το οποίο επεκτείνει τον κρυπτογραφικό σύνδεσμο, συνδέοντας μία οντότητα με τα φυσικά χαρακτηριστικά του κόμβου. Αυτό επιτυγχάνεται χρησιμοποιώντας δύο διακριτούς παράγοντες αυθεντικοποίησης: α) πιστοποιημένα κρυπτογραφικά κλειδιά και β) πιστοποιημένα φυσικά χαρακτηριστικά του κόμβου. Αν και το προτεινόμενο πλαίσιο απαιτεί επιπλέον ικανότητες αναγνώρισης χαρακτηριστικών από τους κόμβους, παρέχει ένα επιπλέον επίπεδο βεβαιότητας για την αυθεντικοποίηση κόμβων για ιδιαίτερα κρίσιμες εφαρμογές.

30. Συνοπτική ανάλυση της εργασίας **[C-6]** *"Secure Multi-path Routing for Mobile Ad Hoc Networks", Panayiotis Kotzanikolaou, Rosa Mavropodi and Christos Douligeris.*

Περίληψη: - Τα πρωτόκολλα πολλαπλής δρομολόγησης για Κινητά Δίκτυα Ειδικού Σκοπού μειώνουν τις επιθέσεις ασφάλειας από συνεργαζόμενους κακόβουλους κόμβους, μέσω της μεγιστοποίησης του αριθμού των κόμβων που πρέπει να συμβιβάσει ένας αντίπαλος ώστε να ελέγξει την επικοινωνία. Σε αυτή την εργασία παρουσιάζονται διάφορες επιθέσεις οι οποίες καθιστούν τα πρωτόκολλα πολλαπλής δρομολόγησης περισσότερο ευπαθή από ότι αναμένεται, σε επιθέσεις συνεργαζόμενων κακόβουλων κόμβων. Στη συνέχεια προτείνεται ένα νέο ασφαλές πρωτόκολλο δυναμικής δρομολόγησης, το πρωτόκολλο Secure Multipath Routing (SecMR) και αναλύονται οι ιδιότητες ασφάλειας που αυτό παρέχει. Το SecMR μπορεί εύκολα να ενσωματωθεί σε μία ευρεία γκάμα πρωτοκόλλων δυναμικής δρομολόγησης όπως είναι το DSR και το AODV.

31. Συνοπτική ανάλυση της εργασίας **[C-5]** *"Strong Forward Security", Mike Burmester, Vassilios Chrissikopoulos, Panayiotis Kotzanikolaou and Emmanouil Magkos.*

Περίληψη: - Η χρονική ασφάλεια έχει προταθεί ως μέθοδος ελαχιστοποίησης των συνεπειών από τη μη-εξουσιοδοτημένη αποκάλυψη ενός μυστικού κλειδιού. Σε αυτή την εργασία αναλύεται αυτή η μέθοδος και εξετάζεται μία αδυναμία της, η οποία οφείλεται στο γεγονός ότι η αποκάλυψη του μυστικού κλειδιού μπορεί να μην εντοπιστεί έγκαιρα. Όλα τα κρυπτοσυστήματα χρονικής ασφάλειας που έχουν προταθεί μέχρι τώρα είναι ευπαθή κατά την περίοδο ανάμεσα στην αποκάλυψη κλειδιού και στον εντοπισμό της αποκάλυψης. Στη συνέχεια, παρουσιάζεται η έννοια της *ισχυρής χρονικής ασφάλειας* η οποία στοχεύει στην προστασία των κρυπτογραφικών στοιχείων, όχι μόνο για τις περιόδους πριν την αποκάλυψη του κλειδιού αλλά και μετά από αυτήν. Τέλος, παρουσιάζονται δυο εφαρμογές με αυτή την πρωτότυπη ιδιότητα: μία βασική λύση εφαρμόσιμη σε οποιοδήποτε κρυπτοσύστημα δημόσιου κλειδιού και ένα σχήμα διαμοίρασης κλειδιού (key escrow system) βασισμένο στο κρυπτοσύστημα ElGamal.

32. Συνοπτική ανάλυση της εργασίας **[C-4]** *"An Asymmetric Traceability Scheme for Copyright Protection without Trust Assumptions", Emmanouil Magkos, Panayiotis Kotzanikolaou, and Vassilios Chrissikopoulos.*

Περίληψη: - Τα σχήματα ανίχνευσης «προδοτών» έχουν προταθεί ως ένα μέτρο προστασίας των πνευματικών δικαιωμάτων για εφαρμογές ευρείας μετάδοσης πληροφορίας. Στην περίπτωση ασύμμετρης ανίχνευσης «προδοτών» δεν είναι δυνατό ένας αθώος χρήστης να κατηγορηθεί άδικα ως «προδότης», από ένα κακόβουλο κέντρο μετάδοσης πληροφορίας. Σε αυτή την εργασία παρουσιάζεται ένα ασύμμετρο σχήμα ανίχνευσης «προδοτών», το οποίο βασίζεται στο πλέον αποδοτικό σχήμα των Kurosawa και Desmedt. Στο προτεινόμενο σχήμα δεν γίνονται υποθέσεις εμπιστοσύνης για το κέντρο μετάδοσης. Επιπλέον, επιτυγχάνεται ανωνυμία των τίμιων χρηστών. Γίνεται χρήση καλά διαδεδομένων κρυπτογραφικών τεχνικών, όπως είναι η επιλήσμονη μεταφορά (oblivious transfer), τα παίγνια ορισμένου χρόνου (time lock puzzles) και οι τυφλές υπογραφές (blind signatures). Τελικά, προτείνεται μία τεχνική αποκοπής και επιλογής για την επιβεβαίωση της ορθότητας των κλειδιών αποκρυπτογράφησης.

33. Συνοπτική ανάλυση της εργασίας **[C-3]** *"Dynamic Multi-signatures for Secure Autonomous Agents", Panayiotis Kotzanikolaou, Mike Burmester and Vassilios Chrissikopoulos.*

Περίληψη: - Ένα βασικό πρόβλημα για την ασφάλεια των κινητών πρακτόρων είναι η μειονεκτική θέση τους σε σχέση με το περιβάλλον εκτέλεσης. Το πρόβλημα αυτό γίνεται ακόμα εντονότερο όταν ένας πράκτορας εκτελείται αυτόνομα σε πολλαπλά διαδοχικά περιβάλλοντα εκτέλεσης. Οι λύσεις που προτείνονται στη διεθνή βιβλιογραφία για ασφαλείς αυτόνομους πράκτορες είναι περισσότερο θεωρητικού ενδιαφέροντος εφόσον είναι μη πρακτικές για πραγματικές εφαρμογές. Σε αυτή την εργασία παρουσιάζεται ένα κρυπτογραφικό πρωτόκολλο για ασφαλείς αυτόνομους πράκτορες το οποίο βασίζεται

σε δυναμικές πολλαπλές υπογραφές με ευελιξία μηνύματος. Το προτεινόμενο σχήμα είναι πρακτικό και δεν παραβιάζει τα πλεονεκτήματα της τεχνολογίας των κινητών πρακτόρων.

34. Συνοπτική ανάλυση της εργασίας **[C-2]** *"Secure Transactions with Mobile Agents in Hostile Environments", Panayiotis Kotzanikolaou, Mike Burmester and Vassilios Chrissikopoulos*.

Περίληψη: - Ένα μεγάλο πρόβλημα των κινητών πρακτόρων είναι η διαφαινόμενη αδυναμία τους να υπογράφουν με ασφάλειας συναλλαγές, κατά τη διάρκεια της εκτέλεσής τους σε μη έμπιστα περιβάλλοντα. Σε αυτή την εργασία παρουσιάζεται ένα πλαίσιο για την προστασία της κακόβουλης χρήσης της δυνατότητας υπογραφής των κινητών πρακτόρων από το περιβάλλον εκτέλεσης, χωρίς να επηρεάζεται η δυνατότητα μετανάστευσης και η αυτονομία των πρακτόρων. Η προτεινόμενη λύση χρησιμοποιεί κρυπτογραφημένες συναρτήσεις για να σχεδιάσει συστήματα μη αποσπώμενης υπογραφής (undetachable signature). Παρουσιάζεται μία RSA υλοποίηση μη αποσπώμενης υπογραφής, η οποία απαντά θετικά στο ανοικτό πρόβλημα των Sander και Tschudin για την δυνατότητα υλοποίησης τέτοιων υπογραφών.

35. Συνοπτική ανάλυση της εργασίας **[C-1]** *"Mobile Agents for Secure Electronic Transactions", Panayiotis Kotzanikolaou, George Katsirelos and Vassilios Chrissikopoulos*

Περίληψη: - Οι κινητοί πράκτορες χρησιμοποιούνται σε εφαρμογές ηλεκτρονικού εμπορίου για την αναζήτηση προϊόντων, τη διαπραγμάτευση της αγοράς και σε ηλεκτρονικές δημοπρασίες. Στην εργασία αυτή, περιγράφεται ένα πολυ-πρακτορικό σύστημα για την ασφαλή αναζήτηση και αγορά προϊόντων και τη διεκπεραίωση ηλεκτρονικών αγορών. Το σύστημα αυτό στηρίζεται σε μία αρχιτεκτονική κύριου – εξαρτημένων πρακτόρων και συνδυάζει ένα στατικό με πολλούς κινητούς πράκτορες για τη συναλλαγή ενός χρήστη με διάφορα ηλεκτρονικά καταστήματα. Η εξουσιοδότηση των πρακτόρων πραγματοποιείται με τη χρήση τεκμηρίων πρόσβασης.