ΑΝΑΛΥΤΙΚΟ ΒΙΟΓΡΑΦΙΚΟ ΣΗΜΕΙΩΜΑ

ΕΜΜΑΝΟΥΗΛ Β. ΜΑΓΚΟΣ

ΝΟΕΜΒΡΙΟΣ 2016

ΒΙΟΓΡΑΦΙΚΟ ΣΗΜΕΙΩΜΑ

ΜΑΓΚΟΥ ΕΜΜΑΝΟΥΗΛ

Επίκ. Καθηγητή Τμήματος Πληροφορικής, Ιονίου Πανεπιστημίου

Γνωστικό αντικείμενο: Κρυπτογραφία και Ασφάλεια Υπολογιστικών Συστημάτων

ΠΡΟΣΩΠΙΚΑ ΣΤΟΙΧΕΙΑ

Έτος γέννησης: 1975

Εθνικότητα: Ελληνική

Οικογενειακή Κατάσταση: Έγγαμος

Email: emagos@ionio.gr; emagkos@gmail.com

URL: http://di.ionio.gr/~emagos

ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ

Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Εργαστήριο Δικτύων, Πολυμέσων και Ασφάλειας Συστημάτων (NMSLab)

Πλατεία Τσιριγώτη 7, Κέρκυρα, 49100,

Τηλ: 26610 87704, 6973749311

FAX: 26610 87766

ΣΠΟΥΔΕΣ

Διδακτορικό Δίπλωμα **1999-2003**

Πανεπιστήμιο Πειραιώς, Τμήμα Πληροφορικής

Τίτλος Διατριβής: «Ασφαλή Ηλεκτρονικά Συστήματα Συναλλαγών στο Διαδίκτυο»

Βασικό Πτυχίο **1993-1997**

Πανεπιστήμιο Πειραιώς, Τμήμα Πληροφορικής

ΓΛΩΣΣΕΣ

Αγγλικά (Πλήρης επάρκεια, University of Cambridge – Proficiency in English)

Γαλλικά (Πλήρης επάρκεια, Université de Paris – Sorbonne II)

ΔΙΔΑΚΤΙΚΗ ΕΜΠΕΙΡΙΑ

Επίκ. Καθηγητής (μόνιμος) **2015-Σήμερα**

Επίκ. Καθηγητής (επί θητεία) **2011-Σήμερα**

Λέκτορας (επί θητεία) **2007-2011**

Διδάσκων Π.Δ. 407/80 **2005-2007**

Ιόνιο Πανεπιστήμιο, Τμήμα Πληροφορικής

Μαθήματα (Προπτυχιακό): "Ασφάλεια Η/Υ & Προστασία Δεδομένων" (4^{ο} Εξάμηνο), Κρυπτογραφία (3^{ο} Εξάμηνο), "Ασφάλεια Πληροφοριακών Συστημάτων" (8^{ο} Εξάμηνο), "Πολιτικές και Τεχνολογίες Ιδιωτικότητας" (5^{ο} Εξάμηνο), "Κοινωνικά και Νομικά Θέματα των ΤΠΕ" (7^{ο} Εξάμηνο)

Μαθήματα (Μεταπτυχιακό): "Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτων", "Ειδικά θέματα ασφάλειας και ιδιωτικότητας στο Διαδίκτυο", "Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων"

Διδάσκων Π.Δ. 407/80 **2003-2007**

Ιόνιο Πανεπιστήμιο, Τμήμα Αρχειονομίας-Βιβλιοθηκονομίας

Μαθήματα (Προπτυχιακό): "Δίκτυα Υπολογιστών" (5^{ο} Εξάμηνο), "Ηλεκτρονικό Επιχειρείν" (6^{ο} Εξάμηνο), "Ανάκτηση Πληροφορίας" (7^{ο} Εξάμηνο)

Μαθήματα (Μεταπτυχιακό): "Από τις Υπηρεσίες Πληροφόρησης στο Ηλεκτρονικό Επιχειρείν", "Συστήματα Επικοινωνίας και Δίκτυα"

Καθηγητής Β/θμιας Εκπαίδευσης **2001-2007**

20^{ο} Γυμνάσιο Αθηνών (2001-2002) - Αναπληρωτής

3^{ο} ΤΕΕ Κέρκυρας (2002-2007) – Διορισμός μέσω ΑΣΕΠ

Μαθήματα: Βασικές Αρχές Πληροφορικής, Δίκτυα Η/Υ, Προγραμματισμός, Υπηρεσίες Διαδικτύου, Πολυμέσα, Κοινωνία της Πληροφορίας, Χρήση Η/Υ, Εφαρμογές Η/Υ

ΕΠΙΒΛΕΨΗ ΔΙΔΑΚΤΟΡΙΚΩΝ ΕΡΓΑΣΙΩΝ

2013-: Μ. Μαγιολαδίτης. Ασφάλεια και Ιδιωτικότητα Κατανεμημένων Πληροφοριακών Συστημάτων. Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο, σε εξέλιξη.

ΜΕΛΟΣ ΕΠΙΤΡΟΠΗΣ ΔΙΔΑΚΤΟΡΙΚΩΝ ΔΙΑΤΡΙΒΩΝ

2009: Συμμετοχή σε επταμελή (εξεταστική) επιτροπή αξιολόγησης, Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου. Υποψήφια: Ευθυμία Αϊβαλόγλου, «Ασφάλεια & Ιδιωτικότητα σε Ασύρματα Δίκτυα Αισθητήρων».

2016: Συμμετοχή σε επταμελή (εξεταστική) επιτροπή αξιολόγησης, Σχολή Θετικών Επιστημών και Τεχνολογίας, Ελληνικό Ανοικτό Πανεπιστήμιο. Υποψήφιος: Δημήτρης

Καραπιπέρης, «A Service-Oriented and Privacy-Aware Framework for Performing Efficiently Record Linkage Tasks»

ΕΠΙΒΛΕΨΗ ΔΙΠΛΩΜΑΤΙΚΩΝ ΔΙΑΤΡΙΒΩΝ (Τελευταία 5 χρόνια)

2016: Σ. Ψωφίδης: Ηλεκτρονικά Εργαλεία Ενίσχυσης της Ιδιωτικότητας στο Διαδίκτυο. Ελληνικό Ανοικτό Πανεπιστήμιο (ΕΑΠ - ΠΛΣ).

2015: Μ. Τσελεπίδου. Διερεύνηση και αξιολόγηση σύγχρονων τεχνικών και εργαλείων για τη διενέργεια Ασφαλών & Ιδιωτικών Ηλεκτρονικών Εκλογών μέσω Διαδικτύου (ΗΕΔ). Ελληνικό Ανοικτό Πανεπιστήμιο (ΕΑΠ - ΠΛΣ).

2014: Κ. Πεχλιβάνης. Μελέτη Ασφάλειας Πληροφοριακού Συστήματος Νοσοκομείου Κέρκυρας. Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο.

2014: Δ. Φρόνιμος, Εξειδικευμένα Θέματα Ηλεκτρονικής Εγκληματολογίας-Ανάλυση Κακόβουλου Λογισμικού. Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο.

2013: Α. Δημέγγελης**.** Διερεύνηση τεχνικών ψηφιακής ανάλυσης πολυμεσικού περιεχομένου με εφαρμογή στην ψηφιακή εγκληματολογία. Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο.

2012: Σ. Πολενάκης, Μελέτη Εξάπλωσης Κακόβουλου Λογισμικού Νέας Γενιάς. Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο.

ΟΡΓΑΝΩΣΗ ΔΙΕΘΝΩΝ ΕΠΙΣΤΗΜΟΝΙΚΩΝ ΣΥΝΕΔΡΙΩΝ & ΕΚΔΗΛΩΣΕΩΝ

2015: IIS 2015, Corfu, Greece, July 06-08, 2015. Διοργάνωση Special Session "SPFG: Security and Privacy in Future Generation Services".

2013: Eurocrypt 2013, Athens, Greece, May 26-30, 2013, Μέλος Οργανωτικής Επιτροπής.

2011: IPICS 2011 Summer School (Intensive Program on Information Communication Security), 22-31 Aug 2011, Corfu Greece. General Chair, Επιστημονικός Υπεύθυνος.

2010: PSD 2010 - Privacy in Statistical Databases, 22-24 Sep. 2010, Corfu, Greece Προεδρεύων (General Chair).

2009: PCI 2009 - 13th Panhellenic Conference on Informatics, 10-12 Sep. 2009, Corfu, Greece Μέλος Οργανωτικής Επιτροπής.

ΜΕΛΟΣ ΕΠΙΤΡΟΠΩΝ ΠΕΡΙΟΔΙΚΩΝ

Κριτής (εξωτερικός αξιολογητής) σε διεθνή επιστημονικά περιοδικά

- IEEE Transactions on Vehicular Technology
- International Journal of Information Security
- Data & Knowledge Engineering (Elsevier)
- Computer Standards & Interfaces (Elsevier)
- Computer Networks (Elsevier)
- Security and Communication Networks (Wiley)

- Journal in Computer Virology (Springer Paris)
- The Computer Journal (Oxford Journals)

ΜΕΛΟΣ ΤΕΧΝΙΚΩΝ ΕΠΙΤΡΟΠΩΝ ΣΕ ΔΙΕΘΝΗ ΕΠΙΣΤΗΜΟΝΙΚΑ ΣΥΝΕΔΡΙΑ

2016: Algorithms-SI-2016

2015: IISA 2015

2013: PRISMS 2013, HAICTA 2013, IISA 2013

2012: MobiSec 2012, PSD 2012, WISTP 2012

2011: ISC 2011, ISCC 2011

2010: ISC 2010, PSD 2010, PSDML 2010, AOC 2010

2009: PCI 2009, AOC 2009

ΣΥΜΜΕΤΟΧΗ ΣΕ ΕΡΕΥΝΗΤΙΚΑ ΚΑΙ ΑΝΑΠΤΥΞΙΑΚΑ ΕΡΓΑ

- **ΟΛΙΚΥ** **2015-2016**
  Ολιστική Προστασία Κρίσιμων Υποδομών: Ανθεκτικότητα και Προστασία Διασυνδέσεων. ΔιαΝΕΟσις - Οργανισμός Έρευνας και Ανάλυσης.
  Ρόλος: Βασικός Ερευνητής
- **TRAMOOC** **2015-2017**
  TraMOOC, Translation for Massive Open Online Courses.
  Ρόλος: Σχεδιασμός και Υλοποίηση Πολιτικής Ιδιωτικότητας
- **ADRIATinn** **2014-2015**
  An Adriatic Network for Advancing Research Development & Innovation towards the Creation of New Policies for Sustainable Competiveness & Technological Capacity of SMEs
  Ρόλος: Σύμβουλος τεχνικής υποστήριξης
- **PACINNO** **2013-2014**
  Πλατφόρμα δια-Ακαδημαϊκής Συνεργασίας στην Καινοτομία
  Ρόλος: Σύμβουλος τεχνικής υποστήριξης
- **SMART BUILT** **2012-2013**
  Δομική Ανάλυση Ιστορικών Κτηρίων
  Ρόλος: Σύμβουλος τεχνικής υποστήριξης
- **PELAGOS. INTERREG III (Ελλάδα – Ιταλία).** **2007-2009**
  Εξέλιξη και ενίσχυση των συστημάτων ασφαλείας, επιτήρησης και ελέγχου στους λιμένες Μπάρι-Κέρκυρα.
  Ρόλος: Σύμβουλος Τεχνικής Υποστήριξης
- **SWEB, IST-2006-2.6.5** **2006-2009**

Secure interoperable cross border m-services contributing towards a trustful European cooperation with the non-EU member Western Balkan countries
Ρόλος: Σύμβουλος Τεχνικής Υποστήριξης Δήμου Αγ. Γεωργίου, Κέρκυρα (υπεργολαβια)

- **ELLECTRA-WeB, IST-045153** **2007-2008**
  Electronic Public Procurement Application Framework in the Western Balkan Region.
  Ρόλος: Σύμβουλος Τεχνικής Υποστήριξης (υπεργολαβία)
- **Διαδραστικό Περιβάλλον Νέου Φρουρίου Κέρκυρας** **2005-2006**
  Επιχειρησιακό Πρόγραμμα Ιονίων Νήσων, Μέτρο 1.5 «Κοινοπραξίες Έρευνας και Τεχνολογικής Ανάπτυξης σε τομείς Εθνικής Προτεραιότητας».
  Ρόλος: Σύμβουλος Τεχνικής Υποστήριξης
- **Ανάπτυξη Μητροπολιτικών Δικτύων Οπτικών Ινών** **2004-2005**
  Περιφέρεια Ιονίων Νήσων
  Ρόλος: Σύμβουλος Τεχνικής Υποστήριξης
- **Επιχειρησιακό Πρόγραμμα Έρευνας και Τεχνολογίας (ΕΠΕΤ ΙΙ), ΓΓΕΤ** **1999-2001**
  Κρυπτογραφικές τεχνικές σε χρηματοοικονομικά συστήματα συναλλαγών μέσω Internet (97 ΕΛ-83).
  Ρόλος: Βασικός Ερευνητής.

ΠΡΟΣΚΕΚΛΗΜΕΝΕΣ ΟΜΙΛΙΕΣ

2016: "*Προστασία Εθνικών Κρίσιμων Υποδομών: Μεθοδολογία Προσδιορισμού και Αξιολόγησης*". Παρουσίαση των αποτελεσμάτων της έρευνας «Η Προστασία Των Κρίσιμων Υποδομών Της Ελλάδας». Κλειστή Συνάντηση Εργασίας για την Προστασία των Κρίσιμων Υποδομών, Τρίτη 28 Ιουνίου 2016, Αίγλη Ζαππείου - Αίθουσα ΟΛΥΜΠΙΑ

2016: "*Προστασία Κρίσιμων Υποδομών: Πολιτικές και Σχέδια Δράσης Ανά τον Κόσμο"*. 2ο Ετήσιο Συνέδριο ICT SECURITY WORLD, Τετάρτη 25 Μαΐου 2016, Ξενοδοχείο Novotel, Αθήνα.

2015: "*Παιδιά και Ασφαλές Διαδίκτυο: Μια Πολύπλευρη Θεώρηση*". Προσκεκλημένη Ομιλία. Σύλλογος Γονέων και Κηδεμόνων 12ου Δημοτικού Σχολείου Κέρκυρας. 20 Μαρτίου, 2015.

2014: "*Ασφάλεια και Ιδιωτικότητα στην Κοινωνική Δικτύωση".* Ενημερωτική Ημερίδα,, Σύστημα εκπαιδευτικής – ερευνητικής, λειτουργικής και κοινωνικής δικτύωσης Ιονίου Πανεπιστημίου , 16/01/2014.

2013: "*Ανήλικοι σε ένα Ασφαλές Διαδίκτυο: Ενέργειες και Τεχνολογίες για τον Περιορισμό των Κινδύνων".* Δημόσια Κεντρική Βιβλιοθήκη Κέρκυρας, Εκδήλωση Ασφάλειας στο Διαδίκτυο, 18/10/2013.

2011: "*Applied Cryptography for Privacy & Security*". 6 April 2011, Universitat Rovira i Virgili Department of Computer Engineering and Maths. ERASMUS Teaching Staff Mobility, Academic Year 2010/11.

2008: "*Κρυπτογραφικές Τεχνικές για την Προστασία της Ιδιωτικότητας σε Κατανεμημένα Συστήματα Εξόρυξης Δεδομένων*". Πανεπιστήμιο Αιγαίου, Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, Διημερίδα με θέμα «Ασφάλεια και Προστασία της Ιδιωτικότητας στην Κοινωνία της Πληροφορίας», Καρλόβασι Σάμου, 23 Νοεμβρίου 2008.

2008: "*Security Issues and Challenges in a Mobile World*". 2nd International Conference on Methodologies, Technologies and Tools enabling e-Government (MeTTeG'08), Corfu, Greece 25 - 26 September 2008.

2007: "*Εφαρμογές Κρυπτογραφίας*". Ιόνιο Πανεπιστήμιο, Τμήμα Αρχειονομίας/ Βιβλιοθηκονομίας. Ημερίδα με θέμα «Εφαρμογές των Μαθηματικών», Ιόνιος Ακαδημία, 5 Δεκεμβρίου 2007.

ΜΕΛΟΣ ΕΠΙΤΡΟΠΩΝ - ΣΥΛΛΟΓΩΝ

2015-2016: Πρόεδρος του Δ.Σ. της Ένωσης Διδασκόντων Ιονίου Πανεπιστημίου (ΕΔΙΠ) - μέλους της ΠΟΣΔΕΠ

ΠΕΡΙΟΧΕΣ ΕΡΕΥΝΗΤΙΚΟΥ ΕΝΔΙΑΦΕΡΟΝΤΟΣ

- Κρυπτογραφικές Τεχνικές στην Ασφάλεια Υπολογιστών, Δικτύων και Π.Σ.
- Ασφάλεια και Ιδιωτικότητα στο Διαδίκτυο.
- Ασφάλεια και Ιδιωτικότητα σε Κατανεμημένες Εφαρμογές.

ΑΞΙΟΠΟΙΗΣΗ ΕΠΙΣΤΗΜΟΝΙΚΟΥ ΕΡΓΟΥ – ΑΝΑΦΟΡΕΣ ΣΤΟ ΕΡΓΟ (Πηγή: Scholar Google)

Αριθμός Αναφορών: 574 (ημ.πρόσβ. 03/04/2017)

h-index: 13

i10-index: 16

Αναφορές ανά Εργασία: https://scholar.google.gr/citations?user=qy_LFbsAAAAJ&hl=el

Αναγορές Ανά Εργασία			
Α/Α	**Άρθρο**	**Έτος Συγγραφής**	**Αναφορές**
1	Σ34	2001	101
2	Β5	2007	79
3	Σ21	2008	49
4	Π10	2009	28
5	Σ35	2002	27
6	Π4	2012	26

7	Σ23	2006	25
8	Σ25	2005	21
9	Σ28	2003	19
10	Π8	2011	19
11	Π13	2007	15
12	Π15	2009	14
13	Π16	2007	13
14	Π17	2003	13
15	Π11	2009	11
16	Σ27	2003	11
17	Σ15	2010	9
18	Σ33	2001	8
19	Σ10	2012	8
20	Σ9	2013	6
21	Π14	2008	6
22	Π3	2013	6
23	Π1	2016	6
24	Π6	2012	5
25	Π9	2010	4
26	Σ24	2006	4
27	Σ36	2000	4
28	Σ2	2014	3
29	Σ17	2009	3
30	Π5	2012	3
31	Π19	2002	3
32	Π12	2009	3
33	Σ5	2014	2

34	Σ11	2012	2
35	Σ14	2010	2
36	Σ16	2009	2
37	Σ22	2008	2
38	Σ31	2002	2
39	Σ7	2014	1
40	Σ6	2014	1
41	Π7	2011	1
42	Σ30	2003	1

ΑΡΘΡΑ ΣΕ ΔΙΕΘΝΗ ΕΠΙΣΤΗΜΟΝΙΚΑ ΠΕΡΙΟΔΙΚΑ (19)

[Π1] P. Kotzanikolaou, C. Patsakis, E. Magkos, M. Korakakis. Lightweight private proximity testing for geospatial social networks. In Computer Communications, Elsevier, Vol. 73, Part B, 1 January 2016, pp. 263–270.

[Π2] G. Koufoudakis, N. Skiadopoulos, E. Magkos, K. Oikonomou. “Synchronization Issues in an Innovative Wireless Sensor Network Architecture Monitoring Ambient Vibrations in Historical Buildings”. In: Key Engineering Materials, v. 628, Trans Tech Publication, 2014

[Π3] E. Magkos, M. Avlonitis, P. Kotzanikolaou, M. Stefanidakis. "Towards Early Warning Against Internet Worms Based on Critical-Sized Networks". In: Security and Communication Networks, Vol 6(1), pp. 78-88, Wiley Interscience, 2013.

[Π4] M. Burmester, E. Magkos, V. Chrissikopoulos. "Modeling Security in Cyber-Physical Systems". In: International Journal of Critical Infrastructure Protection, Elsevier, In Press, Available online 17 August 2012.

[Π5] K. Vlachopoulos, E. Magkos and V. Chrissikopoulos. "A Model for Hybrid Evidence Investigation". In: International Journal of Digital Crime and Forensics (IJDCF), IGI Global, To be published, 2012.

[Π6] M. Burmester, E. Magkos, V. Chrissikopoulos. "Secure and Privacy-Preserving, Timed Vehicular Communications". International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC), Vol. 10 (4), pp. 219-229, Inderscience Publishers, 2012.

[Π7] S., Sioutas, E., Magkos, I., Karydis, V., Verykios: “Uncertainty for Privacy and 2-Dimensional Range Query Distortion”, Journal of Computing Science and Engineering, vol. 5 (3), pp. 210-222, 2011

[Π8] E. Magkos. "Cryptographic Approaches for Privacy Preservation in Location-Based Services: A Survey". International Journal of Information Technologies and the Systems Approach (IJITSA), Vol. 4 (2), pp. 48-69, IGI Global, 2011.

[Π9] E. Magkos, P. Kotzanikolaou. “Achieving Privacy and Access Control in Pervasive Computing Environments”. International Journal of Security and Communication Networks (SCN), Special Issue on "Physical Layer Security in Mobile Devices and Networks", Wiley (accepted for publication– October 2010)

[Π10] E. Magkos, M. Maragoudakis, V. Chrissikopoulos, S. Gritzalis. "Accurate and Large-Scale Privacy-Preserving Data Mining using the Election Paradigm". In: Data & Knowledge Engineering 68(2009), pp. 1124-1236, Elsevier, 2009.

[Π11] P. Kotzanikolaou, D. Vergados, G. Stergiou and E. Magkos. "Multi-Layer Key Establishment for Large Scale Sensor Networks". In: International Journal of Security and Networks (IJSN), Vol. 3(1), pp. 1-9, Inderscience Publishers, 2009.

[Π12] M. Avlonitis, E. Magkos, M. Stefanidakis, and V. Chrissikopoulos. "Treating Scalability and Modeling Human Countermeasures Against Local Preference Worms via Gradient models". In: Journal in Computer Virology, Springer Paris, Vol. 5 (4), pp. 357-371, 2009.

[Π13] P. Kotzanikolaou, E. Magkos, D. Vergados and M. Stefanidakis. "Secure and Practical Key Establishment for Distributed Sensor Networks". In: Security and Communication Networks, Wiley, Volume 2, Issue 6, pp 595 – 610, 2009.

[Π14] V. Stathopoulos, P. Kotzanikolaou, and E. Magkos, "Secure Log Management for Privacy Assurance in Electronic Communications", In: Computers & Security, Elsevier, Volume 27 (7-8), pp. 298-308, 2008, available at doi:10.1016/j.cose.2008.07.010.

[Π15] E. Magkos, P. Kotzanikolaou, C. Douligeris. “Towards Secure Online Elections: Models, Primitives and Open Issues”, In: Electronic Government, an International Journal, Inderscience Publishers, Volume 4 - Issue 3, pp. 249-268, 2007.

[Π16] M. Avlonitis, E. Magkos, M. Stefanidakis, and V. Chrissikopoulos. A Spatial Stochastic Model for Worm Propagation: Scale Effects. In: Journal of Computer Virology, Vol. 3(2), Springer Paris, pp. 87-92, 2007.

[Π17] M. Burmester, E. Magkos, V. Chrissikopoulos: “Uncoercible e-bidding Games”. In Electronic Commerce Research Journal, Vol. 4, Special Issue on Security Aspects in E-Commerce, Kluwer Academic Publishers, pp. 113-125, 2003.

[Π18] Ε. Μάγκος. Ένα Υβριδικό Μοντέλο Ανάκτησης Κλειδιού. In Cyprus Computer Society Journal, Issue 3. pp. 35-40, 2003.

[Π19] E. Magkos, and V. Chrissikopoulos. Equitably Fair Internet Voting. In Journal of Internet Technology, Vol. 3(3), Special Issue on Network Security, pp. 187-193, 2002.

ΑΡΘΡΑ ΣΕ ΔΙΕΘΝΗ ΕΠΙΣΤΗΜΟΝΙΚΑ ΣΥΝΕΔΡΙΑ (36)

[Σ1] D. Gritzalis, G. Stergiopoulos, P. Kotzanikolaou, E. Magkos, G. Lykou. Critical Infrastructure Protection: A Holistic Roadmap for Greece. In: 2nd Workshop On The

Security Of Industrial Control Systems & Cyber-Physical Systems (CyberICPS 2016) - In Conjunction With ESORICS 2016.

[Σ2] P. Grammenos, N.A. Syreggela, E. Magkos, and A. Tsohou. Internet Addiction of Young Greek Adults: Psychological Aspects and Information Privacy. In: GENEDIS 2016 - Genetics, Health Aging and Mental Wellness in the new digital era. October 20 – 23, 2016, Sparta, Greece.

[Σ3] E. Karavaras, E. Magkos, A. Tsohou. Low User Awareness Against Social Malware: An Empirical Study and Design of a Security Awareness Application. In 13th European Mediterranean & Middle Eastern Conference on Information Systems (EMCIS 2016).

[Σ4] E. Magkos, P. Kotzanikolaou, M. Magioladitis, S. Sioutas, and V. S. Verykios. “Towards Secure and Practical Location Privacy, through Private Equality Testing”. In: Privacy in Statistical Databases - PSD 2014, 17-19 Sep. 2014, Eivissa, Spain. Lecture Notes in Computer Science LNCS v. 8744, Springer-Verlag, 2014.

[Σ5] M. Korakakis, E. Magkos, P. Mylonas. “Automated CAPTCHA Solving: An Empirical Comparison of Selected Techniques”. In: SMAP 2014, 9th International Workshop on Semantic and Social Media Adaptation and Personalization, November 6-7th, 2014, Corfu, Greece. IEEE Computer Society's Conference Publishing Services (CPS), 2014.

[Σ6] E. Magkos, E. Kleisiari, P. Chanias, V. Giannakouris-Salalidis. “Parental Control and Children’s Internet Safety: The Good, the Bad and the Ugly”. In: 6th International Conference on Information Law and Ethics (ICIL 2014), "Lifting Barriers to Empower the Future of Information Law and Ethics", Thessaloniki, May 30-31, 2014.

[Σ7] D. Fronimos, E. Magkos, V. Chrissikopoulos. “Evaluating Low Interaction Honeypots and On their Use against Advanced Persistent Threats”. In 18th Panhellenic Conference on Informatics - PCI 2014, 2-4 October, Athens, Greece, 2014.

[Σ8] G. Koufoudakis, N. Skiadopoulos, E. Magkos, K. Oikonomou. “Synchronization Issues in an Innovative Wireless Sensor Network Architecture Monitoring Ambient Vibrations in Historical Buildings”. In: S.M.ART. BUIL.T. International Conference, March 27-29, Bari Italy, 2014.

[Σ9] M. Burmester, E. Magkos, V. Chrissikopoulos. "T-ABAC: An Attribute-Based Access Control Model for Real-Time Availability in Highly Dynamic Systems". In: 18th IEEE Symposium on Computers and Communications, July 7-10, 2013, Split Croatia, IEEE

[Σ10] P. Kotzanikolaou, E. Magkos, N.Petrakos, C.Douligeris, V. Chrissikopoulos. "Fair Anonymous Authentication for Location Based Services". In: Data Privacy Management, 7th International Workshop (DPM 2012), Pisa, Italy, September 13-14. Lecture Notes in Computer Science (LNCS), Springer-Verlag, to be published, 2012.

[Σ11] K. Vlachopoulos, E. Magkos and V. Chrissikopoulos. "A Model for Hybrid Evidence Investigation". In: 7th International Annual Workshop on Digital Forensics & Incident Analysis (WDFIA 2012), Hersonissos, Crete, 6-8 June, 2012.

[Σ12] M. Burmester, E. Magkos, V. Chrissikopoulos. "Modeling Security in Cyber-Physical Systems". In: Sixth Annual IFIP Working Group 11.10 International Conference on

Critical Infrastructure Protection, National Defense University Fort McNair, Washington, DC, USA, March 19 - 21, 2012.

[Σ13] S. Sioutas, E. Magkos, I. Karydis, and V.S. Verykios. "Uncertainty for Anonymity and 2-Dimensional Range Query Distortion". In: Privacy in Statistical Databases - PSD 2010, 22-24 Sep. 2010, Corfu, Greece. Lecture Notes in Computer Science LNCS v. 6344, Springer-Verlag, pp. 85-96, 2010.

[Σ14] E. Magkos, P. Kotzanikolaou. "Enhancing Privacy-Preserving Access Control for Pervasive Computing Environments". In: The Second International ICST Conference on Security and Privacy in Mobile Information and Communication Systems - MOBISEC 2010, May 27-28, Catania, Sicily. LNICST, Springer, to be published, 2010

[Σ15] E. Magkos, P. Kotzanikolaou, S. Sloutas, K. Oikonomou. "A Distributed Privacy-Preserving Scheme for Location-Based Queries". In: The Fourth IEEE WoWMoM Workshop on Autonomic and Opportunistic Communications - AOC 2010, 14-17 June, Montreal QC Canada. IEEE Computer Society, pp. 1-6, 2010

[Σ16] M. Avlonitis, E. Magkos, M. Stefanidakis and V. Chrissikopoulos. "A Novel Stochastic Approach for Modeling Random Scanning Worms". In: 13th Panhellenic Conference on Informatics - PCI 2009, 10-12 September, Corfu, Greece. IEEE Computer Society, pp. 176-179, 2009.

[Σ17] K. L. Kermanidis and E. Magkos. "Empirical Paraphrasing of Modern Greek Text in Two Phases; An Application to Steganography". In: A. Gelbukh (Ed.): CICLing 2009, LNCS 5449, pp. 535–546, Springer-Verlag Berlin, 2009.

[Σ18] A. Pateli, A. Floros, K. Oikonomou, E. Magkos. "Corfunet: A Mesh Network Providing Wireless Services At Metropolitan Level". In: IADIS Wireless Applications and Computing (WAC 2008), July 21-24, Amsterdam, 2008.

[Σ19] E. Magkos, V. Chrissikopoulos. "Towards Efficient Cryptography for Privacy Preserving Data Mining in Distributed Systems". In: 4th International Conference on Web Information Systems and Technologies (WEBIST 2008), May 4-7 2008, Madeira, Portugal. INSTICC Press, pp. 301-304, 2008.

[Σ20] M. Avlonitis, E. Magkos, M. Stefanidakis, and V. Chrissikopoulos. "Exploring Scalability and Fast Spreading of Local Preference Worms via Gradient Models". In: 17th EICAR Annual Conference, 3-6 May 2008, Laval, France, 2008.

[Σ21] M. Burmester, E. Magkos, V. Chrissikopoulos. "Strengthening Privacy Protection in VANETs". IEEE 1st International Workshop on Security and Privacy in Wireless and Mobile Computing, Networking and Communications SecPri_WiMob 08, pp. 508-513, 2008.

[Σ22] E. Magkos, M. Maragoudakis, V. Chrissikopoulos, and S. Gridzalis. "Accuracy in Privacy-Preserving Data Mining Using the Paradigm of Cryptographic Elections". In: Privacy in Statistical Databases (PSD '08), 24-26 Sep. 2008, Istanbul. Lecture Notes in Computer Science (LNCS), Vol. 5262/2008, Springer-Verlag, pp. 284-297, 2008.

[Σ23] V. Stathopoulos, P. Kotzanikolaou, and E. Magkos. “A Framework for Secure and Verifiable Logging in Public Communication Networks”. In: Critical Information

Infrastructures Security, First International Workshop, CRITIS 2006, Samos, Greece, August 31 - September 1, 2006, Lecture Notes in Computer Science, Vol. 4347, Springer, pp. 273-284, 2006.

[Σ24] E. Magkos, P. Kotzanikolaou, M. Stefanidakis. "An Asymmetric Key Establishment Protocol for Multiphase Self-Organized Sensor Networks". In: 12th European Wireless Conference (EW 2006) "Enabling Technologies for Wireless Multimedia Communications", April 2 - 5, 2006, Athens Greece.

[Σ25] P. Kotzanikolaou, E. Magkos, C. Douligeris, V. Chrissikopoulos V., "Hybrid Key Establishment for Multiphase Self-Organized Sensor Networks". 1st International Workshop on Trust, Security and Privacy for Ubiquitous Computing (TSPUK 2005), June 13, 2005, Taormina, Sicily, Italy. In: Proc. of 6th WoWMoM 2005, IEEE, pp. 581-587, 2005.

[Σ26] Ε. Μάγκος, Β. Χρυσικόπουλος, Ν. Αλεξανδρής, Μ. Πούλος. "Ηλεκτρονική Ψηφοφορία μέσω Internet: Ουτοπία ή Πραγματικότητα;" Ηλεκτρονική Δημοκρατία – Κοινωνία της Πληροφορίας και τα Δικαιώματα του Πολίτη, 1ο Εθνικό Συνέδριο με Διεθνή Συμμετοχή, 25 - 26 Σεπτεμβρίου 2003, Κτίριο ΕΒΕΑ. Proceedings. Εκδόσεις Σάκουλας, pp. 525-540, 2003.

[Σ27] M. Poulos, A. Evangelou, E. Magkos, S. Papavlasopoulos. "Fingerprint Verification Based on Image Processing Segmentation Using An Onion Algorithm of Computational Geometry". In: 6th International Workshop on Mathematical Methods in Scattering Theory and Biomedical Engineering, 18-21 September 2003, Tsepelovo, Greece. WOLRD SCIENTIFIC publications, pp. 550-559, 2003.

[Σ28] M. Poulos, E. Magkos, V. Chrissikopoulos, and N. Alexandris. "Secure Fingerprint Verification Based on Image Processing Segmentation using Computational Geometry Algorithms". In: SPPRA '2003 – IASTED International Conference on Signal Processing, Pattern Recognition, and Applications. June 30 – July 2, Rhodes, Greece, ACTA Press, pp. 308-312, 2003.

[Σ29] E. Magkos, V., Chrissikopoulos, N. Alexandris, and M. Poulos. "Secure Key Recovery for Archived and Communicated Data in the Corporate Intranet". In: 7th WSEAS International Conference on Circuits, Systems, Communications and Computers. July 7-10, Corfu, Greece, pp. 191-195, 2003.

[Σ30] M. Poulos, N. Alexandris, V.S. Belessiotis, E. Magkos. "Comparison between Computational Geometry and Coherence Methods applied to the EEG for Medical Diagnostic Purposes". In: Proceedings of the 7th International Multicoference on Circuits, Systems, Communications and Computers, Corfu Island Greece, July 7-10, pp. 247-252, 2003.

[Σ31] E. Magkos, V. Chrissikopoulos, N. Alexandris. "A Common Security Model for Conducting e-Auctions and e-Elections". 6th International Conference on Communications. In Recent Advances in Computers, Computing and Communications, WSEAS, pp. 463-467, 2002.

[Σ32] E. Magkos, V. Chrissikopoulos, N. Alexandris. “Software-based Receipt-Freeness in On-line Elections”. In: IFIP TC11 WG11.4 1st Annual Working Conference on Network Security, November 26-27, 2001, Leuven, Belgium. In Advances in Network And Distributed Systems Security, Kluwer Academic Publishers, pp. 33-43, 2001.

[Σ33] E. Magkos, P. Kotzanikolaou, V. Chrissikopoulos. «An Asymmetric Traceability Scheme for Copyright Protection without Trust Assumptions». In: 2nd International Conference on Electronic Commerce and Web technologies EC-WEB 2001, Munich, Germany, September 4-6, LNCS Vol. 2115, Springer-Verlag, pp. 186-195, 2001.

[Σ34] E. Magkos, M. Burmester, and V. Chrissikopoulos. “Receipt-Freeness in Large-scale Elections without Untappable Channels”. In: 1st IFIP Conference on E-Commerce/Business/Government, Kluwer Academic Publishers, pp. 683-693, 2001.

[Σ35] M. Burmester, V. Chrissikopoulos, P. Kotzanikolaou, and E. Magkos. “Strong Forward Security”. In: IFIP-SEC '01 Conference, Kluwer Academic Publishers, pp. 109-119, 2001.

[Σ36] E. Magkos, M. Burmester, V. Chrissikopoulos. “An Equitably Fair On-line Auction Scheme”. In 1st International Conference on Electronic Commerce and Web technologies - EC-WEB 2000, LNCS Vol. 1875, Springer-Verlag, Berlin, pp. 72-84, 2000.

ΒΙΒΛΙΑ – ΔΙΔΑΚΤΙΚΟ ΥΛΙΚΟ (1)

[Δ1] Ε. Μάγκος. "Κρυπτογραφία και Ασφάλεια Δικτύων". 2016

Ανάπτυξη Διδακτικού Υλικού, Ελληνικό Ανοικτό Πανεπιστήμιο (ΕΑΠ), Μεταπτυχιακή Εξειδίκευση στα Πληροφοριακά Συστήματα (ΠΛΣ) - Ενότητα ΠΛΣ 62/Γ - Κρυπτογραφία και Ασφάλεια Δικτύων.

1η Κυκλοφορία: Σεπτέμβριος 2016

ΚΕΦΑΛΑΙΑ ΣΕ ΒΙΒΛΙΑ ΚΑΙ ΣΥΛΛΟΓΙΚΟΥΣ ΤΟΜΟΥΣ (5)

[Β1] E. Magkos, M. Burmester, V. Chrissikopoulos. "Αυθεντικοποιημένη Εδραίωση Κλειδιού". Συλλογικός Τόμος με τίτλο: "Σύγχρονη Κρυπτογραφία: Θεωρία και Εφαρμογές". M. Burmester, Σ. Γκρίτζαλης, Σ. Κάτσικας, Β. Χρυσικόπουλος (Eds). Εκδόσεις Παπασωτηρίου, Μάρτιος 2011.

[Β2] E. Magkos, M. Maragoudakis, V. Chrissikopoulos. "Προστασία Ιδιωτικότητας σε Κατανεμημένα Συστήματα Εξόρυξης Δεδομένων". Συλλογικός Τόμος με τίτλο: "Προστασία της Ιδιωτικότητας στις Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα". Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, Σ. Κάτσικας (Eds). Παπασωτηρίου, 2009.

[Β3] C. Lambrinoudakis, E. Magkos, V. Chrissikopoulos. "Electronic Voting Systems". (Chapter) In: J. Lopez, S. Furnell, A. Patel, S. Katsikas, (Ed.), "Securing Information and Communication Systems: Principles, Technologies and Applications". Artech House Publishers, Computer Security Series, pp. 307-323, 2008.

[B4] N. Alexandris, V. Chrissikopoulos and E. Magkos. “The role of Cryptography in Large-Scale Internet Elections”. Volume of essays in honour of Professor Antonios C. Panayotopoulos pp. 93–110, 2006.

[B5] M. Burmester, E. Magkos. “Towards Secure and Practical e-Elections in the New Era”. In: Advances in Information Security - Secure Electronic Voting, Kluwer Academic Publishers pp. 63-76, 2003.

ΜΕΛΕΤΕΣ (3)

[M1] Δ. Γκρίτζαλης, Π. Κοτζανικολάου, Μ. Μάγκος, Γ. Στεργιόπουλος, Γ. Λύκου. Ολιστική Προστασία Κρίσιμων Υποδομών - Μέρος Α': Καταγραφή Εθνικών Κρίσιμων Υποδομών Και Διασυνδέσεων). ΔιαΝΕΟσις - Οργανισμός Έρευνας και Ανάλυσης, 2016. http://www.dianeosis.org/wp-content/uploads/2016/06/infrastucture_paradoteo1_Version_020616_6.pdf

[M2] Δ. Γκρίτζαλης, Π. Κοτζανικολάου, Μ. Μάγκος, Γ. Στεργιόπουλος, Γ. Λύκου. Ολιστική Προστασία Κρίσιμων Υποδομών - Μέρος Β’: Αξιολόγηση Υποψήφιων Εθνικών Κρίσιμων Υποδομών. ΔιαΝΕΟσις - Οργανισμός Έρευνας και Ανάλυσης, 2016. http://www.dianeosis.org/wp-content/uploads/2016/06/infrastucture_paradoteo2_Version_020616_3.pdf

[M3] Δ. Γκρίτζαλης, Π. Κοτζανικολάου, Μ. Μάγκος, Γ. Στεργιόπουλος, Γ. Λύκου. Ολιστική Προστασία Κρίσιμων Υποδομών - Μέρος Γ': Πρόταση Ολιστικής Πολιτικής Προστασίας Και Ανθεκτικότητας Κρίσιμων Υποδομών. ΔιαΝΕΟσις - Οργανισμός Έρευνας και Ανάλυσης, 2016. http://www.dianeosis.org/wp-content/uploads/2016/06/infrastucture_paradoteo3_version_020616_2.pdf

ΕΠΙΜΕΛΕΙΑ ΠΡΑΚΤΙΚΩΝ / ΣΥΛΛΟΓΙΚΩΝ ΤΟΜΩΝ (1)

[E1] J. Domingo-Ferrer, E. Magkos (ed.). Proceedings of the 2010 International Conference on Privacy in Statistical Databases (PSD 2010), Lecture Notes in Computer Science (LNCS 6344) Springer Verlag, Berlin, Heidelberg, 2010, ISBN: 978-3-642-15837-7.

ΑΝΑΛΥΤΙΚΟ ΥΠΟΜΝΗΜΑ – ΠΕΡΙΛΗΨΗ ΔΗΜΟΣΙΕΥΣΕΩΝ

[Π1] P. Kotzanikolaou, C. Patsakis, E. Magkos, M. Korakakis. Lightweight private proximity testing for geospatial social networks. In Computer Communications, Vol. 73, Part B, 1 January 2016, pp. 263–270.

Our paper introduces a novel lightweight protocol for private proximity testing.The proposed protocol clearly outperforms current state of the art.We formally prove that the protocol is secure in the semi-honest model.We present experimental results in Python and C++ and compare it with its peers.We demonstrate an Android application that uses are protocol and proves its efficacy. The wide adoption of smart phones has enabled Online Social Networks (OSNs) to exploit the location awareness capabilities offering users better interaction and context aware content. While these features are very attractive, the publication of users' location in an OSN exposes them to privacy hazards. Recently, various protocols have been proposed for private proximity testing,

where users are able to check if their online friends are near, without disclosing their locations. However, the computation cost of the required cryptographic operations utilized in such protocols is not always efficient for mobile devices. In this paper we introduce a lightweight and secure proximity testing protocol, suitable for online mobile users. We show that our protocol is provably secure under the well-known factoring problem and we analyze its efficiency. Our results show that our approach outperforms other existing protocols, by significantly reducing the computational cost and making it practical for devices with limited resources. Finally, we demonstrate the applicability of our proposal in an actual OSN location-based, mobile application.

[Π2] G. Koufoudakis, N. Skiadopoulos, E. Magkos, K. Oikonomou. “Synchronization Issues in an Innovative Wireless Sensor Network Architecture Monitoring Ambient Vibrations in Historical Buildings”. In: Key Engineering Materials, v. 628, Trans Tech Publication, 2014

The problem of bridging the gap between the traditional wired monitoring systems and the wireless ones, was the objective of an innovative network architecture that elegantly combined benefits from both approaches. The monitoring focus is on historical buildings in which installing wires maybe range from difficult (e.g., fragile constructions) to impossible (e.g., prohibitive legislation). However, this innovative approach is vulnerable with respect to synchronization issues. In particular, all data sensed by different sensors need to have the correct universal time stamp. Since under this approach there is no central entity to take a synchronization role, in this paper the use of a local NTP server is proposed and as it is shown here using experimental results, this approach suffices for the particular monitoring needs. Thus, the claim that the innovative system can efficiently support the required monitoring of ambient vibrations in historical buildings.

[Π3] E. Magkos, M. Avlonitis, P. Kotzanikolaou, M. Stefanidakis. "Towards Early Warning Against Internet Worms Based on Critical-Sized Networks". In: Security and Communication Networks, Vol 6(1), pp. 78-88, Wiley Interscience, 2013.

In this paper we build on a recent worm propagation stochastic model [1], in which random effects during worm spreading were modeled by means of a stochastic differential equation. Based on this model, we introduce the notion of the critical size of a network, which is the least size of a network that needs to be monitored, in order to correctly project the behavior of a worm in substantially larger networks. We provide a method for the theoretical estimation of the critical size of a network in respect to a worm with specific characteristics. Our motivation is the requirement in real systems to balance the needs for accuracy (i.e. monitoring a network of a sufficient size in order to reduce false alarms) and performance (i.e. monitoring a small-scale network to reduce complexity). In addition, we run simulation experiments in order to experimentally validate our arguments. Finally, based on the notion of critical-sized networks, we propose a logical framework for a distributed early warning system against unknown and fast-spreading worms. In the proposed framework, propagation parameters of an early- detected worm are estimated in real time, by studying a critical-sized network. In this way, security is enhanced as estimations generated by a critical-sized network may help large-scale networks to respond faster to new worm threats.

[Π4] M. Burmester, E. Magkos, V. Chrissikopoulos. "Modeling Security in Cyber-Physical Systems". In: International Journal of Critical Infrastructure Protection, Elsevier, In Press, Available online 17 August 2012.

This paper describes a framework for modeling the security of a cyber–physical system in which the behavior of the adversary is controlled by a threat model that captures – in a unified manner – the cyber aspects (with discrete values) and the physical aspects (with continuous values) of the cyber–physical system. In particular, the framework addresses combined (dependent) vector attacks and synchronization/localization issues. The framework identifies the cyber–physical features that must be protected according to theprevailing security policy. Also, the framework can be used for formal proofs of thesecurity of cyber–physical systems.

[Π5] K. Vlachopoulos, E. Magkos and V. Chrissikopoulos. "A Model for Hybrid Evidence Investigation". In: International Journal of Digital Crime and Forensics (IJDCF), IGI Global, To be published, 2012.

With the advent of Information and Communication Technologies, the means of committing a crime and the crime itself are constantly evolved. In addition, the boundaries between traditional crime and cybercrime are vague: a crime may not have a defined traditional or digital form since digital and physical evidence may coexist in a crime scene. Furthermore, various items found in a crime scene may worth be examined as both physical and digital evidence, which we consider as hybrid evidence. In this paper, a model for investigating such crime scenes with hybrid evidence is proposed. Our model unifies the procedures related to digital and physical evidence collection and examination, taking into consideration the unique characteristics of each form of evidence. Our model can also be implemented in cases where only digital or physical evidence exist in a crime scene.

[Π6] M. Burmester, E. Magkos, V. Chrissikopoulos. "Secure and Privacy-Preserving, Timed Vehicular Communications". International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC), Vol. 10 (4), pp. 219-229, Inderscience Publishers, 2012.

We consider the problem of privacy (anonymity) and security in vehicular (V2V) communication, in particular securing routine safety messages. Traditional public key mechanisms are not appropriate for such applications because of the large number of safety messages that have to be transmitted by each vehicle, typically one message every 100-300 ms. We first show that a recently proposed V2V communication scheme, the TSVC, based on the Time Efficient Stream Loss-tolerant Authentication (TESLA) scheme, is subject to an impersonation attack in which the adversary can distribute misleading safety information to vehicles, and propose a modification that secures it against such attacks. We then address general concerns regarding the inappropriateness of TESLA for vehicular applications (caused by the delayed authentication and buffer overflows), and propose a V2V communication scheme based on a variant of TESLA, TESLA0, for which there is no delay and packets are self-authenticating. This is appropriate for applications in which vehicles are in close proximity. Finally we combine both schemes to get a hybrid communication scheme that addresses in a flexible way the mobility requirements of V2V communications. Current research in location-based

services (LBSs) highlights the importance of cryptographic primitives in privacy preservation for LBSs, and presents solutions that attempt to support the (apparently) mutually exclusive requirements for access control and context privacy (i.e., identity and/or location), while at the same time adopting more conservative assumptions in order to reduce or completely remove the need for trust on system entities (e.g., the LBS provider, the network operator, or other peer nodes). This paper surveys the current state of knowledge concerning the use of cryptographic primitives for privacy-preservation in LBS applications.

[Π7] S., Sioutas, E., Magkos, I., Karydis, V., Verykios: "Uncertainty for Privacy and 2-Dimensional Range Query Distortion", Journal of Computing Science and Engineering, vol. 5 (3), pp. 210-222, 2011

In this work, we study the problem of privacy-preserving data publishing in moving objects databases. In particular, the trajectory of a mobile user on the plane is no longer a polyline in a two-dimensional space, instead it is a two-dimensional surface of fixed width 2A_{min}, where A_{min} defines the semidiameter of the minimum spatial circular extent that must replace the real location of the mobile user on the XY-plane, in the anonymized (kNN) request. Since a malicious attacker can observe that during the time, many of the neighbours ids change except for a small number of users, the desired anonimity is not achieved and the whole system becomes vulnerable to attackers. Thus, we reinforce the privacy model by clustering the mobile users according to their motion patterns in (u, θ) plane, where u and θ define the velocity measure and the motion direction (angle) respectively. In this case the anonymized (kNN) request lookups neighbours, who belong to the same cluster with the mobile requester in (u, θ) space: So, we know that the trajectory of the k-anonymous mobile user is within this surface, but we do not know exactly where. We transform the surface's boundary poly-lines to dual points and we focus on the information distortion introduced by this space translation. We develop a set of effiient spatio-temporal access methods and we experimentally measure the impact of information distortion by comparing the performance results of the same spatio-temporal range queries executed on the original database and on the anonymized one.

[Π8] E. Magkos. "Cryptographic Approaches for Privacy Preservation in Location-Based Services: A Survey". International Journal of Information Technologies and the Systems Approach (IJITSA), Vol. 4 (2), pp. 48-69, IGI Global, 2011.

Current research in location-based services (LBSs) highlights the importance of cryptographic primitives in privacy preservation for LBSs, and presents solutions that attempt to support the (apparently) mutually exclusive requirements for access control and context privacy (i.e., identity and/or location), while at the same time adopting more conservative assumptions in order to reduce or completely remove the need for trust on system entities (e.g., the LBS provider, the network operator, or other peer nodes). This paper surveys the current state of knowledge concerning the use of cryptographic primitives for privacy-preservation in LBS applications.

[Π9] E. Magkos, P. Kotzanikolaou. "Achieving Privacy and Access Control in Pervasive Computing Environments". International Journal of Security and Communication

Networks (SCN), Special Issue on "Physical Layer Security in Mobile Devices and Networks", Wiley (accepted for publication– October 2010)

Η εργασία επικεντρώνεται στο εγγενές αντιστάθμισμα μεταξύ ιδιωτικότητας και ελέγχου πρόσβασης σε Διάχυτα Υπολογιστικά Περιβάλλοντα (ΔΥΕ). Εκ πρώτης, οι Πάροχοι απαιτούν αυθεντικοποίηση χρήστη και εξουσιοδότηση πριν την παροχή μιας υπηρεσίας, ενώ από την άλλη οι χρήστες απαιτούν ανωνυμία, συγκεκριμένα μη ανιχνευσιμότητα (untraceability) και μη συνδεσιμότητα (unlinkability) για τις συναλλαγές τους. Υπάρχουν επίσης περιπτώσεις όπου η ταυτότητα που αντιστοιχεί σε ένα συγκεκριμένο διαπιστευτήριο πρέπει να ανιχνευθεί, προκειμένου να αποδοθεί ευθύνη για κάποια πράξη. Σε αυτή την εργασία αναλύουμε τις απαιτήσεις ασφάλειας και ιδιωτικότητας για τον έλεγχο πρόσβασης σε ΔΥΕ και εξηγούμε γιατί η σχετική βιβλιογραφία δεν ικανοποιεί πλήρως τις απαιτήσεις αυτές. Στη συνέχεια περιγράφουμε δυο καινούριες προσεγγίσεις για την επίτευξη των στόχων της ασφάλειας και ιδιωτικότητας. Ο στόχος μας είναι διττός: (α) αφενός να ενισχύσουμε την ιδιωτικότητα (μη ανιχνευσιμότητα και μη συνδεσιμότητα) έναντι κακόβουλων εσωτερικών εχθρών του συστήματος, και (β) να ενισχύσουμε την ασφάλεια επιτυγχάνοντας υπό προϋποθέσεις ανιχνευσιμότητα των διαπιστευτηρίων των χρηστών, και, ει δυνατόν, μη αποποίηση ευθύνης για τη συμμετοχή ενός χρήστη σε μια συναλλαγή. Τέλος, αναλύουμε και συγκρίνουμε τα προτεινόμενα σχήματα, από τη σκοπιά της ασφάλειας και πρακτικότητας, με τη σχετική βιβλιογραφία.

[Π10] E. Magkos, M. Maragoudakis, V. Chrissikopoulos, S. Gritzalis. "Accurate and Large-Scale Privacy-Preserving Data Mining using the Election Paradigm". In: Data & Knowledge Engineering 68(2009), pp. 1124-1236, Elsevier, 2009.

Η άνθηση των τεχνολογιών ΤΠΕ σε συνδυασμό με την ωρίμανση των τεχνολογιών εξόρυξης δεδομένων εγείρουν ζητήματα σχετικά με την επεξεργασία και χρήση ευαίσθητων πληροφοριών, ιδίως σε κατανεμημένα περιβάλλοντα όπου οι συμμετέχοντες μπορεί να είναι μη έμπιστες οντότητες. Σε αυτήν την εργασία περιγράφουμε σχεδιαστικές απαιτήσεις καθώς και απαιτήσεις ασφάλειας και ιδιωτικότητας σε κατανεμημένα συστήματα εξόρυξης μεγάλης κλίμακας. Τοποθετούμαστε υπέρ της υιοθέτησης του ομομορφικού κρυπτογραφικού μοντέλου για τη διενέργεια ηλεκτρονικών εκλογών, και συγκεκριμένα ορισμένων επεκτάσεων αυτού του μοντέλου για την υποστήριξη πολλαπλών υποψηφίων και μεγάλου πλήθους ψηφοφόρων. Στη συνέχεια περιγράφουμε ορισμένες αδυναμίες και επιθέσεις κατά του σχήματος που προτάθηκε στην [1], το οποίο αποτελεί το πρώτο σχήμα που υλοποιεί το ομομορφικο μοντέλο σε κατανεμημένα συστήματα εξόρυξης. Τέλος, δείχνουμε πώς η προσέγγιση μας μπορεί να χρησιμοποιηθεί σε ταξινομήσεις τύπου random forest, επί οριζόντια κατατμημένων δεδομένων.

[Π11] P. Kotzanikolaou, D. Vergados, G. Stergiou and E. Magkos. "Multi-Layer Key Establishment for Large Scale Sensor Networks". In: International Journal of Security and Networks (IJSN), Vol. 3(1), pp. 1-9, Inderscience Publishers, 2009.

Η διεθνής βιβλιογραφία στην έρευνα για τεχνικές εδραίωσης κλειδιού σε αποκεντρωμένα δίκτυα αισθητήρων (DSNs), εστιάζει στην ανάγκη περιγραφής αποδοτικών πρωτοκόλλων, λόγω των περιορισμένων δυνατοτήτων των αισθητήρων.

Παρότι τα πλέον αποδοτικά σχήματα χρησιμοποιούν συμμετρικές τεχνικές, τα σχήματα αυτά δεν προσφέρουν επαρκή προστασία έναντι επιθέσεων πλαστοπροσωπίας. Σε αυτό το πλαίσιο, ορισμένα υβριδικά πρωτόκολλα κάνουν περιορισμένη χρήση τεχνικών δημόσιου κλειδιού που βασίζονται στην κρυπτογραφία Ελλειπτικής Καμπύλης (ECC). Σε αυτήν την εργασία προτείνεται ένα υβριδικό πρωτόκολλο εδραίωσης κλειδιού για DSNs, το οποίο βελτιώνει την απόδοση του δικτύου συγκριτικά με τη σχετική βιβλιογραφία. Στο δίκτυο υπό θεώρηση, οι κόμβοι οργανώνονται κατά γεωγραφικές περιοχές – γειτονιές; επίσης, σε κάθε γειτονιά υπάρχει ένας κόμβος με ενισχυμένες δυνατότητες – ο ενισχυμένος κόμβος. Η εδραίωση κλειδιού λαμβάνει χώρα σε τρεις φάσεις: (α) Εδραίωση κλειδιού εντός της γειτονιάς, (β) Εδραίωση κλειδιού μεταξύ των ενισχυμένων κόμβων, και (γ) Εδραίωση κλειδιού με κόμβους εκτός γειτονιάς.

[Π12] M. Avlonitis, E. Magkos, M. Stefanidakis, and V. Chrissikopoulos. "Treating Scalability and Modeling Human Countermeasures Against Local Preference Worms via Gradient models". In: Journal in Computer Virology, Springer Paris, Vol. 5 (4), pp. 357-371, 2009.

Στην εργασία αυτή αναδεικνύονται οι προκλήσεις που σχετίζονται με την ανάγκη, για λόγους κόστους και αποδοτικότητας, της παρακολούθησης δικτύων μικρής κλίμακας χωρίς ωστόσο να πλήττεται η ακρίβεια ενός συστήματος πρόβλεψης εξάπλωσης ταχέως εξαπλούμενου κακόβουλου λογισμικού (ΤΕΜΛ). Προβλέψεις βασιζόμενες σε δεδομένα μικρής κλίμακας είναι πιθανόν επισφαλείς κυρίως λόγω της ετερογένειας των δικτύων αλλά και της ανομοιόμορφης συμπεριφοράς ενός ΤΕΜΛ. Ωστόσο, το κόστος και η πολυπλοκότητα της παρακολούθησης ενός πολύ μεγάλου δικτύου δεν μπορούν να παραβλεφθούν. Στην εργασία αυτή παρουσιάζονται ζητήματα κλίμακας που αφορούν την εξάπλωση σκουληκιών είτε με στρατηγικές τυχαίας ανίχνευσης (random scanning) ή με στρατηγικές τοπικής προτίμησης (local preference). Επίσης επεκτείνουμε τη μεθοδολογία που προτάθηκε στην [Π8] και προτείνουμε ένα στοχαστικό μοντέλο το οποίο λαμβάνει υπόψη όλες τις δυναμικές αλληλεπιδράσεις κατά την εξάπλωση ΤΕΜΛ. Τα θεωρητικά αποτελέσματα επικυρώνονται από αποτελέσματα προσομοίωσης.

[Π13] P. Kotzanikolaou, E. Magkos, D. Vergados and M. Stefanidakis. "Secure and Practical Key Establishment for Distributed Sensor Networks". In: Security and Communication Networks, Wiley, Volume 2, Issue 6, pp 595 – 610, 2009.

Στη σχετική βιβλιογραφία πρωτοκόλλων εδραίωσης κλειδιού σε δίκτυα αισθητήρων, τα πρωτόκολλα που βασίζονται σε συμμετρικές κρυπτογραφικές τεχνικές είναι πολύ αποδοτικά, ωστόσο παρουσιάζουν αδυναμίες έναντι εσωτερικών εχθρών καθώς και ενεργητικών εχθρών που εξαπολύουν επιθέσεις πλαστοπροσωπίας. Από τη άλλη, τα ασύμμετρα πρωτόκολλα είναι ανθεκτικά έναντι αυτών των επιθέσεων, ωστόσο συχνά δεν είναι αποδοτικά, ιδιαιτέρως σε δίκτυα αισθητήρων όπου οι απαιτήσεις για απόδοση είναι αυξημένες. Στην εργασία προτείνονται δύο πρωτόκολλα εδραίωσης κλειδιού για αποκεντρωμένα δίκτυα αισθητήρων (DSNs). Το πρώτο πρωτόκολλο είναι υβριδικό και συνδυάζει ασύμμετρες (Ελλειπτική Καμπύλη) και συμμετρικές τεχνικές. Το δεύτερο πρωτόκολλο είναι πλήρως ασύμμετρο, ωστόσο ιδιαιτέρως αποδοτικό. Η ασφάλεια των προτεινόμενων πρωτοκόλλων αναλύεται, καθώς και η απόδοση τους,

μέσω προσομοίωσης. Επίσης δίνεται μια συγκριτική ανάλυση των προτεινόμενων πρωτοκόλλων με τη σχετική βιβλιογραφία.

[Π14] V. Stathopoulos, P. Kotzanikolaou, and E. Magkos, "Secure Log Management for Privacy Assurance in Electronic Communications", In: Computers & Security, Elsevier, Volume 27 (7-8), pp. 298-308, 2008, available at doi:10.1016/j.cose.2008.07.010.

Η εργασία αυτή επικεντρώνεται στην ασφαλή καταγραφή γεγονότων σε εθνικούς τηλεπικοινωνιακούς παρόχους. Δίδεται μια επισκόπηση των υπαρχόντων μοντέλων απειλών, και προτείνεται ένα καινούριο μοντέλο απειλών, ειδικά προσαρμοσμένο στο περιβάλλον των ISPs. Επίσης προτείνεται ένα πλαίσιο λειτουργίας για την ασφαλή καταγραφή σε τηλεπικοινωνιακά δίκτυα, έναντι των απειλών που περιγράφονται. Σημαντικό ρόλο στο προτεινόμενο πλαίσιο λειτουργίας διαδραματίζει μια Ανεξάρτητη Ρυθμιστική Αρχή, υπεύθυνη για την επαλήθευση της ακεραιότητας των αρχείων καταγραφής.

[Π15] E. Magkos, P. Kotzanikolaou, C. Douligeris. “Towards Secure Online Elections: Models, Primitives and Open Issues”, In: Electronic Government, an International Journal, Inderscience Publishers, Volume 4 - Issue 3, pp. 249-268, 2007.

Μεσοπρόθεσμα, συστήματα ηλεκτρονικής ψηφοφορίας αναμένεται να χρησιμοποιηθούν σε τοπικές ή/και εθνικές εκλογές. Σε μία ηλεκτρονική ψηφοφορία μέσω Internet, οι πολίτες υποβάλλουν τις ψήφους τους μέσω Web κάνοντας χρήση λογισμικού πλοήγησης. Η εργασία αυτή παρουσιάζει μια επισκόπηση των κρυπτογραφικών μοντέλων που έχουν προταθεί στη διεθνή βιβλιογραφία για τη διενέργεια ασφαλών και ιδιωτικών συστημάτων ηλεκτρονικών ψηφοφοριών. Επίσης περιγράφει ανοικτά προβλήματα και προκλήσεις που πρέπει να επιλυθούν πριν τα συστήματα ηλεκτρονικής ψηφοφορίας χρησιμοποιηθούν σε κρίσιμες εκλογές μεγάλης κλίμακας.

[Π16] M. Avlonitis, E. Magkos, M. Stefanidakis, and V. Chrissikopoulos. A Spatial Stochastic Model for Worm Propagation: Scale Effects. In: Journal of Computer Virology, Vol. 3(2), Springer Paris, pp. 87-92, 2007.

Τα κλασσικά επιδημιολογικά μοντέλα επιχειρούν να περιγράψουν την εξάπλωση σκουληκιών με στρατηγικές τυχαίας ανίχνευσης, είτε θεωρώντας το Internet ως ένα ομοιογενές δίκτυο, είτε επιλέγοντας τη (μη αποδοτική) μελέτη δικτύων πολύ μεγάλης κλίμακας για την εξαγωγή ασφαλών συμπερασμάτων. Στην εργασία αυτή προτείνεται ένα στοχαστικό μοντέλο για την περιγραφή της εξάπλωσης ενός σκουληκιού τυχαίας στρατηγικής σε ένα υποδίκτυο «κατάλληλα μικρής» (critical) κλίμακας. Το μοντέλο μπορεί να λαμβάνει υπόψη τις δυναμικές αλληλεπιδράσεις μεταξύ γειτονικών υποδικτύων καθώς και την ανομοιογένεια των δικτύων. Επίσης, προτείνεται η ιδέα της παρακολούθησης της συμπεριφοράς ενός ΤΕΜΛ σε δίκτυα μικρής κλίμακας με σκοπό την πρόβλεψη της εξάπλωσης του ΤΕΜΛ σε μεγαλύτερα δίκτυα (π.χ. το Διαδίκτυο).

[Π17] M. Burmester, E. Magkos, V. Chrissikopoulos: “Uncoercible e-bidding Games”. In Electronic Commerce Research Journal, Vol. 4, Special Issue on Security Aspects in E-Commerce, Kluwer Academic Publishers, pp. 113-125, 2003.

Στην εργασία προτείνεται ένα πρωτόκολλο ηλεκτρονικής δημοπρασίας μέσω Internet, το οποίο εκπληρώνει όλες τις απαιτήσεις ασφάλειας και επιπλέον παρέχει οικουμενική επαληθευσιμότητα: ένας εξωτερικός παρατηρητής μπορεί να βεβαιωθεί ότι τα αποτελέσματα της δημοπρασίας είναι έγκυρα. Αυτό επεκτείνει την ασφάλεια σε πρωτόκολλα δημοπρασιών που έχουν προταθεί έως σήμερα, τα οποία παρέχουν μόνο ατομική επαληθευσιμότητα. Παράλληλα το πρωτόκολλο παρέχει Προστασία από Καταναγκασμό (Uncoercibility) για όλους τους χρήστες που συμμετέχουν σε μια ηλεκτρονική δημοπρασία Πρώτης ή Δεύτερης Τιμής. Δηλαδή, κανείς χρήστης, ακόμα και αν το επιθυμεί, δε μπορεί να αποδείξει σε κάποιον τρίτο την τιμή της προσφοράς που υπέβαλε στο σύστημα.

[Π18] E. Magkos. "Ένα Υβριδικό Μοντέλο Ανάκτησης Κλειδιού". Cyprus Computer Society Journal "Pliroforiki", Issue 3. pp. 35-40, 2003.

Στην εργασία καταγράφονται οι πλέον δημοφιλείς μέθοδοι ανάκτησης κλειδιού (key recovery) για την αποκρυπτογράφηση συνομιλιών που ανταλλάσσονται μέσω του Διαδικτύου ή στο περιβάλλον των επιχειρήσεων. Επίσης περιγράφονται οι πιθανές επιθέσεις στην ασφάλεια των συστημάτων ανάκτησης κλειδιού. Για την αντιμετώπιση αυτών των επιθέσεων προτείνεται ένα υβριδικό μοντέλο στο οποίο ενσωματώνονται δύο διαφορετικές προσεγγίσεις ώστε να επιτευχθεί ασφάλεια, χωρίς παραβίαση της ιδιωτικότητας των πολιτών. Σύμφωνα με την Παραδοσιακή Προσέγγιση, τα κλειδιά αποκρυπτογράφησης μακράς διαρκείας (που χρήζουν αυξημένης προστασίας) είναι υποθηκευμένα σε μια Αρχή Υποθήκευσης Κλειδιού η οποία για προστασία της ιδιωτικότητας των πολιτών υλοποιείται ως ένα σύνολο από πολλές ανεξάρτητες έμπιστες οντότητες. Αντιθέτως τα κλειδιά περιορισμένης διαρκείας (κλειδιά συνόδου) μπορούν να ανακτηθούν από μια Αρχή Ανάκτησης Κλειδιού. Η αρχιτεκτονική αυτή δεν συνιστά μεγάλη πολυπλοκότητα καθώς τα κλειδιά μακράς διαρκείας ανακτώνται μόνον όταν ανιχνευτεί επίθεση διπλής κρυπτογράφησης (double encryption) στο σύστημα.

[Π19] E. Magkos, and V. Chrissikopoulos. "Equitably Fair Internet Voting". In Journal of Internet Technology, Vol. 3(3), Special Issue on Network Security, pp. 187-193, 2002.

Στην εργασία αυτή προτείνονται κρυπτογραφικοί μηχανισμοί για την αντιμετώπιση του προβλήματος των απεχόντων ψηφοφόρων σε ηλεκτρονικές ψηφοφορίες με κεντρική διαχείριση. Στις ψηφοφορίες αυτής της κατηγορίας, οι εκλογικές αρχές έχουν τη δυνατότητα να υποβάλλουν πλαστές ψήφους για λογαριασμό όσων εξουσιοδοτημένων ψηφοφόρων αποφασίζουν να απέχουν από την ψηφοφορία. Το σύστημα που προτείνεται είναι «δίκαιο»: κάθε ψηφοφόρος έχει το δικαίωμα να απέχει από τη ψηφοφορία, ωστόσο όλοι οι εγγεγραμμένοι ψηφοφόροι που τελικά υποβάλουν την κρυπτογραφημένη ψήφο τους καλούνται να την επιβεβαιώσουν ηλεκτρονικά, διατηρώντας παράλληλα την ανωνυμία τους. Το σύστημα που προτείνεται ικανοποιεί τις περισσότερες απαιτήσεις ασφάλειας των ηλεκτρονικών ψηφοφοριών και μπορεί να χρησιμοποιηθεί για ηλεκτρονικές ψηφοφορίες καθώς και σε δημοσκοπήσεις στο Web.

[Σ1] P. Grammenos, N.A. Syreggela, E. Magkos, and A. Tsohou. Internet Addiction of Young Greek Adults: Psychological Aspects and Information Privacy.

The main goal of this study is to examine the Internet addiction status of Greek young adults, aged from 18 to 25, using Young's Internet Addiction Test (IAT) and self-administered questionnaires. In addition this paper assesses the psychological traits of addicted persons per addiction category, using the big five factor model tool to study the user's personality and analyze the components that lead a person to become Internet addicted.Our results show that the majority of people per addiction level, that are addicted, are women. Except the moderate addiction level.Furthermore, we found an association between addicted people and the five factors from the Big Five Factor Model; i.e., extraversion, agreeableness, conscientiousness, neuroticism, openness to experience. Moreover, this paper discussesinformation privacy and security issues related to Internet Addiction.

[Σ2] D. Gritzalis, G. Stergiopoulos, P. Kotzanikolaou, E. Magkos, G. Lykou. Critical Infrastructure Protection: A Holistic Roadmap for Greece.

The protection of Critical Infrastructures (CIs) is, by definition, of high importance for the welfare of citizens of each country; especially nowadays, both because of direct threats (dictated by the current international political situation) and also due to emerging interactions or dependencies developed between national CIs at international and European levels. Today, Greece remains one of the few countries of the European Union, which (besides the formal trans-position of the 114/2008/EC Directive into domestic legislation) has no comprehensive strategy to safeguard national CIs, nor any process of developing such an integrated plan, except for some initiatives taken from the General Secretariat of Digital Policy. This paper aims to contribute: (i) The creation of an inventory of all stakeholders, i.e. actors who have some form of power (legislative, supervisory or regulatory) to protect CIs in Greece., (ii) the identification and indicative cataloguing of potential national CIs, as well as their interdependencies, (iii) the development of a structured identification methodology of national CIs, that takes into account internationally applied CI assessment methodologies and (iv) provide a pilot implementation of the proposed methodology to a list of candidate national CI fields in order to rank their criticality.

[Σ3] E. Magkos, P. Kotzanikolaou, M. Magioladitis, S. Sioutas, and V. S. Verykios. "Towards Secure and Practical Location Privacy, through Private Equality Testing". In: Privacy in Statistical Databases - PSD 2014, 17-19 Sep. 2014, Eivissa, Spain. Lecture Notes in Computer Science LNCS v. 8744, Springer-Verlag, 2014.

We propose a practical, privacy-preserving equality testing protocol which allows two users to learn if they share the same encrypted input data. Our protocol assumes no trust on third parties and/or other peers, and it is suited for low-min entropy data i.e., which can be exhaustively searched by an attacker), such as encrypted users locations. Our primitive is secure and efficient: Two public-key exponentiations are required, per each user, for each equality testing. Finally, we describe how we could use our primitive as a building block for a proximity testing buddy-finder service for social networks.

[Σ4] M. Korakakis, E. Magkos, P. Mylonas. "Automated CAPTCHA Solving: An Empirical Comparison of Selected Techniques". In: SMAP 2014, 9th International Workshop on

Semantic and Social Media Adaptation and Personalization, November 6-7th, 2014, Corfu, Greece. IEEE Computer Society's Conference Publishing Services (CPS), 2014.

CAPTCHAs exploit the gap in the ability between a human and a machine to understand the semantics of specific multimedia content, with vast applications in computer security. In this paper we compare two techniques in automated CAPTCHA solving for text-based CAPTCHA schemes, i.e., classification based on the Vector Space Model (VSM) versus a popular Optical Character Recognition (OCR) engine. For each technique, we build a CAPTCHA solver and give it specific sets of text-based challenges to break. From our results we draw conclusions whether it is efficient to create a CAPTCHA solver by applying parts of the VSM theory and implementing a Vector Space Image Recognizer (VSIR).

[Σ5] E. Magkos, E. Kleisiari, P. Chanias, V. Giannakouris-Salalidis. “Parental Control and Children’s Internet Safety: The Good, the Bad and the Ugly”. In: 6th International Conference on Information Law and Ethics (ICIL 2014), "Lifting Barriers to Empower the Future of Information Law and Ethics", Thessaloniki, May 30-31, 2014.

In this paper we assess the threats and risks that children are exposed to as a by-product of their Internet experience. We assess good and bad strategies and practices for increasing children’s online safety, from a technological, legal and ethical point of view, and explore some of the challenges that law, ethos, technology must overcome towards Internet safety for children. For example we pose the question whether a parent could ever become, intentionally or not, a threat source for a child’s privacy loss. At the technical field, we run an experiment that demonstrates why parental control software has a long road ahead in meeting some minimum goals for filtering effectiveness

[Σ6] D. Fronimos, E. Magkos, V. Chrissikopoulos. “Evaluating Low Interaction Honeypots and On their Use against Advanced Persistent Threats”. In 18th Panhellenic Conference on Informatics - PCI 2014, 2-4 October, Athens, Greece, 2014.

In this paper we evaluate several Low Interaction Honeypots (LIHs) according to several usability and performance criteria. Furthermore we argue on the utilization of LIHs that could indicate early signs of jeopardy from Advanced Persistent Threats (APT).

[Σ7] G. Koufoudakis, N. Skiadopoulos, E. Magkos, K. Oikonomou. “Synchronization Issues in an Innovative Wireless Sensor Network Architecture Monitoring Ambient Vibrations in Historical Buildings”. In: S.M.ART. BUIL.T. International Conference, March 27-29, Bari Italy, 2014.

We propose a practical, privacy-preserving equality testing protocol which allows two users to learn if they share the same encrypted input data. Our protocol assumes no trust on third parties and/or other peers, and it is suited for low-min entropy data (\textit{i.e.}, which can be exhaustively searched by an attacker), such as encrypted users locations. Our primitive is secure and efficient: Two public-key exponentiations are required, per each user, for each equality testing. Finally, we describe how we could use our primitive as a building block for a proximity testing buddy-finder service for social networks.

[Σ8] M. Burmester, E. Magkos, V. Chrissikopoulos. "T-ABAC: An Attribute-Based Access Control Model for Real-Time Availability in Highly Dynamic Systems". In: 18th IEEE Symposium on Computers and Communications, July 7-10, 2013, Split Croatia, IEEE

In highly dynamic systems resources may have to be accessed in real-time, within the strict time limits of underlying physical processes, with availability becoming critical. Current access control models such as RBAC and ABAC do not address real-time availability in a scalable way for such scenarios. In this paper we propose a real-time attribute-based access control model that extends the functionality of ABAC by using real-time attributes that reflect the requirements of critical applications. We describe two applications of our model: (a) a substation automation system, and (b) a medical cyber-physical system.

[Σ9] P. Kotzanikolaou, E. Magkos, N.Petrakos, C.Douligeris, V. Chrissikopoulos. "Fair Anonymous Authentication for Location Based Services". In: Data Privacy Management, 7th International Workshop (DPM 2012), Pisa, Italy, September 13-14. Lecture Notes in Computer Science (LNCS), Springer-Verlag, to be published, 2012.

We propose an efficient anonymous authentication scheme that provides untraceability and unlinkability of mobile devices, while accessing Location-Based Services. Following other recent approaches for mobile anonymity, in our scheme the network operator acts as an anonymous credential issuer for its users. However, our scheme supports credential non-transferability, without requiring embedded hardware security features. In addition it supports fairness characteristics. On one hand, it reduces the trust assumptions for the issuer by supporting non-frameability: the issuer, even in collaboration with the LBS provider, cannot simulate a transaction that opens back to an honest user. On the other hand, it supports anonymity revocation for illegally used credentials. Our scheme uses standard primitives such as zero-knowledge proofs, MACs and challenge/responses. We provide formal security proofs based on the intractability of the Divisible Diffie-Hellman assumption.

[Σ10] K. Vlachopoulos, E. Magkos and V. Chrissikopoulos. "A Model for Hybrid Evidence Investigation". In: 7th International Annual Workshop on Digital Forensics & Incident Analysis (WDFIA 2012), Hersonissos, Crete, 6-8 June, 2012.

With the advent of Information and Communication Technologies, the means of committing a crime and the crime itself are constantly evolved. In addition, the boundaries between traditional crime and cybercrime are vague: a crime may not have a defined traditional or digital form since digital and physical evidence may coexist in a crime scene. Furthermore, various items found in a crime scene may worth be examined as both physical and digital evidence, which we consider as hybrid evidence. In this paper, a model for investigating such crime scenes with hybrid evidence is proposed. Our model unifies the procedures related to digital and physical evidence collection and examination, taking into consideration the unique characteristics of each form of evidence. Our model can also be implemented in cases where only digital or physical evidence exist in a crime scene.

[Σ11] M. Burmester, E. Magkos, V. Chrissikopoulos. "Modeling Security in Cyber-Physical Systems". In: Sixth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, National Defense University Fort McNair, Washington, DC, USA, March 19 - 21, 2012.

We propose a framework for modeling the security of cyber-physical systems in which the behavior of the adversary is controlled by a threat model that captures both the cyber aspects (with discrete values) as well as the physical aspects (with continuous values) of such systems in a unified way. In particular, it addresses combined (dependent) vector attacks, and synchronization/localization issues. The framework identifies the cyber-physical features specified by the se- curity policies that need to be protected, and can be used for proving formally the security of cyber-physical systems.

[Σ12] S. Sioutas, E. Magkos, I. Karydis, and V.S. Verykios. "Uncertainty for Anonymity and 2-Dimensional Range Query Distortion". In: Privacy in Statistical Databases - PSD 2010, 22-24 Sep. 2010, Corfu, Greece. Lecture Notes in Computer Science LNCS v. 6344, Springer-Verlag, pp. 85-96, 2010.

Εδώ εστιάζουμε στη διατήρηση της ανωνυμίας σε δεδομένα βάσεων κινούμενων αντικειμένων (Moving Objects Databases). Συγκεκριμένα, μελετάμε τροχιές κινούμενων αντικειμένων οι οποίες δεν είναι πλέον 2-διάστατες τεθλασμένες γραμμές αλλά επιφάνειες (λωρίδες) που τις περικλείουν. Γνωρίζουμε ότι η τροχιά του κινούμενου χρήστη είναι μέσα στην επιφάνεια, αλλά δεν γνωρίζουμε ποια ακριβώς είναι. Μετατρέπουμε τις εξισώσεις των γραμμών των άκρων της επιφάνειας σε dual points και εξετάζουμε τη διαστρέβλωση της πληροφορίας (information distortion) που προκαλεί το παραπάνω space translation, δηλαδή αυτό που παράγει τις ψευδό-τροχιές που περικλείουν την πραγματική τροχιά. Υλοποιούμε ένα πλήθος αποδοτικών χώρο-χρονικών δομών δεδομένων που διατηρούν δυναμικά τα παραπάνω dual points των ψευδό-τροχιών και μετράμε πειραματικά τον αντίκτυπο που έχει η εν λόγω διαστρέβλωση της πληροφορίας συγκρίνοντας την απόδοση των spatio-temporal range queries όταν αυτά εκτελούνται στην αυθεντική βάση δεδομένων που αποθηκεύει τις πραγματικές τροχιές και όταν αυτά εκτελούνται στην ανώνυμη βάση δεδομένων που αποθηκεύει τις ψευδό-τροχιές.

[Σ13] E. Magkos, P. Kotzanikolaou. "Enhancing Privacy-Preserving Access Control for Pervasive Computing Environments". In: The Second International ICST Conference on Security and Privacy in Mobile Information and Communication Systems - MOBISEC 2010, May 27-28, Catania, Sicily. LNICST, Springer, to be published, 2010

Η διενέργεια συναλλαγών μεταξύ χρηστών και Παρόχων Υπηρεσιών σε Διάχυτα Υπολογιστικά Περιβάλλοντα (ΔΥΕ), εγείρει ζητήματα ασφάλειας και ιδιωτικότητας. Από τη μία, οι Πάροχοι απαιτούν αυθεντικοποίηση χρήστη και εξουσιοδότηση πριν την παροχή μιας υπηρεσίας, ενώ από την άλλη οι χρήστες απαιτούν ανωνυμία, συγκεκριμένα μη ανιχνευσιμότητα (untraceability) και μη συνδεσιμότητα (unlinkability) για τις συναλλαγές τους. Σε αυτή την εργασία συζητούμε τις απαιτήσεις ασφάλειας και ιδιωτικότητας για τον έλεγχο πρόσβασης σε ΔΥΕ και καταδεικνύουμε τις αδυναμίες ασφάλειας του πρόσφατου σχήματος που προτάθηκε από τους Ren και Lou. Στη συνέχεια περιγράφουμε μια καινούρια προσέγγιση για την επίτευξη των στόχων

ασφάλειας και ιδιωτικότητας έναντι εσωτερικών ή/και εξωτερικών εχθρών του συστήματος.

[Σ14] E. Magkos, P. Kotzanikolaou, S. SIoutas, K. Oikonomou. "A Distributed Privacy-Preserving Scheme for Location-Based Queries". In: The Fourth IEEE WoWMoM Workshop on Autonomic and Opportunistic Communications - AOC 2010, 14-17 June, Montreal QC Canada. IEEE Computer Society, pp. 1-6, 2010

Η εργασία πραγματεύεται ζητήματα ασφάλειας και ιστορικής ιδωτικότητας (historical privacy) σε εφαρμογές βασισμένες σε υπηρεσίες θέσης (LBS), όπου οι χρήστες υποβάλλουν την ακριβή θέση τους σε έναν Πάροχο LBS. Προτείνεται ένα κατανεμημένο σχήμα που εδραιώνει έλεγχο πρόσβασης και παράλληλα προστατεύει την ιδιωτικότητα ενός χρήστη τόσο σε σποραδικά όσο και σε συνεχή ερωτήματα τύπου LBS. Η προτεινόμενη λύση κάνει χρήση μιας υβριδικής δικτυακής αρχιτεκτονικής στην οποία οι χρήστες έχουν τη δυνατότητα: (α) να επικοινωνούν με έναν Πάροχο LBS διαμέσου ενός τηλεπικοινωνιακού παρόχου (OP), και (β) να δημιουργούν άμεσες συνδέσεις (ad-hoc) μεταξύ τους προκειμένου να εδραιώσουν ιδιωτικότητα έναντι ενός παθητικού εχθρού που εξαπολύει επιθέσεις ανάλυσης κίνησης. Το μοντέλο απειλών μας περιλαμβάνει τον Πάροχο OP, τον Πάροχο LBS καθώς και άλλους χρήστες-κόμβους του συστήματος.

[Σ15] M. Avlonitis, E. Magkos, M. Stefanidakis and V. Chrissikopoulos. "A Novel Stochastic Approach for Modeling Random Scanning Worms". In: 13th Panhellenic Conference on Informatics - PCI 2009, 10-12 September, Corfu, Greece. IEEE Computer Society, pp. 176-179, 2009.

Ένα κακόβουλο λογισμικό τύπου Σκουλήκι αναπτύσσεται με διαφορετικούς ρυθμούς σε διαφορετικές περιοχές, κυρίως λόγω των εγγενών ανομοιογενειών των υπολογιστικών δικτύων στα οποία αναπτύσσεται. Στην εργασία αυτή μελετάται το κατά πόσο τα στοχαστικά ή τα ντετερμινιστικά μοντέλα είναι ικανά να περιγράψουν το φαινόμενο εξάπλωσης σκουληκιών. Επίσης προτείνεται ένα στοχαστικό μοντέλο για τη μελέτη της εξάπλωσης σκουληκιών με στρατηγικές τυχαίας ανίχνευσης (random scanning), στο οποίο οι δυναμικές αλληλεπιδράσεις λόγω της ανομοιογένειας της υποδομής συνυπολογίζονται στη δυναμική της εξάπλωσης του κακόβουλου λογισμικού. Η θεωρία που παρουσιάζεται επικυρώνεται από αποτελέσματα προσομοίωσης.

[Σ16] K. L. Kermanidis and E. Magkos. "Empirical Paraphrasing of Modern Greek Text in Two Phases; An Application to Steganography". In: A. Gelbukh (Ed.): CICLing 2009, LNCS 5449, pp. 535–546, Springer-Verlag Berlin, 2009.

Η εργασία πραγματεύεται την εφαρμογή τεχνικών παράφρασης στην στεγανογραφία, χρησιμοποιώντας τα νεο-ελληνικά ως το φορέα των μηνυμάτων που ανταλλάσσονται (stego medium).

[Σ17] A. Pateli, A. Floros, K. Oikonomou, E. Magkos. "Corfunet: A Mesh Network Providing Wireless Services At Metropolitan Level". In: IADIS Wireless Applications and Computing (WAC 2008), July 21-24, Amsterdam, 2008.

Η Εργασία αυτή περιγράφει τις τεχνολογικές και εμπορικές προκλήσεις που αναδεικνύονται στα πλαίσια της προσπάθειας που καταβάλλεται για την υλοποίηση του CorfuNet, ενός ασύρματου μητροπολιτικού δικτύου στην πόλη της Κέρκυρας. Η

ανάπτυξη του δικτύου θα βασίζεται σε τεχνικές ασύρματων δικτύων πλέγματος (wireless mesh), όπως πολυ-κάναλη λειτουργία, δρομολόγηση πολλαπλών βημάτων (multi-hop) και ταυτόχρονη σύνδεση με σταθερό δίκτυο υποδομής, ώστε να αρθούν οι περιορισμοί από τις επικρατούσες τεχνολογίες ασύρματης δικτύωσης σε μητροπολιτικό επίπεδο. Το οραματιζόμενο δίκτυο θα παρέχει πλήθος υπηρεσιών, απευθυνόμενων σε πολίτες, τουρίστες και επιχειρήσεις στην Κέρκυρα.

[Σ18] E. Magkos, V. Chrissikopoulos. "Towards Efficient Cryptography for Privacy Preserving Data Mining in Distributed Systems". In: 4th International Conference on Web Information Systems and Technologies (WEBIST 2008), May 4-7 2008, Madeira, Portugal. INSTICC Press, pp. 301-304, 2008.

Είναι κοινώς αποδεκτό ότι η προστασία της ανωνυμίας των πληροφοριών και της ιδιωτικότητας των χρηστών που συναλλάσσονται στο Διαδίκτυο θα οδηγούσε σε μεγαλύτερη προθυμία παροχής χρήσιμων προσωπικών πληροφοριών σε συστήματα εξόρυξης δεδομένων. Η σύγχρονη βιβλιογραφία καταδεικνύει την ανάγκη περιγραφής μηχανισμών για την επίτευξη ακρίβειας και ιδιωτικότητας σε κατανεμημένα συστήματα εξόρυξης δεδομένων, όπου όλα τα εμπλεκόμενα μέρη είναι μη έμπιστα. Στην εργασία αυτή συζητούμε πώς η πολύτιμη γνώση και τα αποτελέσματα της έρευνας για ασφαλείς και ιδιωτικές ηλεκτρονικές ψηφοφορίες μέσω Internet μπορούν να αξιοποιηθούν στην έρευνα για ιδιωτικά συστήματα εξόρυξης δεδομένων.

[Σ19] M. Avlonitis, E. Magkos, M. Stefanidakis, and V. Chrissikopoulos. "Exploring Scalability and Fast Spreading of Local Preference Worms via Gradient Models". In: 17th EICAR Annual Conference, 3-6 May 2008, Laval, France, 2008.

Η περιγραφή της συμπεριφοράς ενός ταχέως εξαπλούμενου σκουληκιού (worm) με ρεαλιστικό τρόπο είναι δύσκολη, κυρίως λόγω των πολύπλοκων αλληλεπιδράσεων μεταξύ των δικτυωμένων κόμβων. Αυτή η εργασία επεκτείνει ένα πρόσφατα προτεινόμενο μοντέλο εξάπλωσης (Π8), με σκοπό τη μελέτη εξάπλωσης Σκουληκιών με στρατηγική τοπικής προτίμησης (local preference). Συγκεκριμένα, περιγράφονται στοχαστικές διαφορικές εξισώσεις στις οποίες όλες οι δυναμικές αλληλεπιδράσεις είτε λόγω της ανομοιογένειας της υποδομής, είτε λόγω της στρατηγικής εξάπλωσης του Σκουληκιού είτε τέλος λόγω των τυχαίων δράσεων των χρηστών (στρατηγικές επιδιόρθωσης-patch, πολιτικές firewalls, απομάκρυνση κόμβων από το δίκτυο κλπ), συνυπολογίζονται στη δυναμική της εξάπλωσης του σκουληκιού με την εισαγωγή κατάλληλων αντίστοιχων ντετερμινιστικών ή/και στοχαστικών όρων στο κλασσικό επιδημιολογικό μοντέλο. Η θεωρία που παρουσιάζεται στην εργασία επικυρώνεται από αποτελέσματα προσομοίωσης.

[Σ20] Burmester, E. Magkos, V. Chrissikopoulos. "Strengthening Privacy Protection in VANETs". IEEE 1st International Workshop on Security and Privacy in Wireless and Mobile Computing, Networking and Communications SecPri_WiMob 08, pp. 508-513, 2008.

Στο όχι τόσο μακρινό μέλλον, τα οχήματα αναμένεται να επικοινωνούν με διερχόμενα οχήματα καθώς και με μία σταθερή υποδομή, διαθέσιμη στο οδικό δίκτυο, με σκοπό την βελτίωση της οδηγικής εμπειρίας, την άμβλυνση των κυκλοφοριακών προβλημάτων

και την αύξηση του αισθήματος ασφάλειας κατά τη μετακίνηση. Η προοπτική υλοποίησης οχηματικών δικτύων άμεσης σύνδεσης (VANETs) εγείρει ζητήματα και προκλήσεις ασφάλειας και ιδιωτικότητας. Συγκεκριμένα μελετάται το αντιστάθμισμα μεταξύ της ιδιωτικότητας των οδηγών και της ευθύνης οδηγού (π.χ. σε περίπτωση πρόκλησης ατυχήματος). Μία άλλη πρόκληση είναι η εδραίωση ιδιωτικότητας τοποθεσίας έναντι οικουμενικών παθητικών εχθρών που υποκλέπτουν κάθε επικοινωνία στο δίκτυο. Στην εργασία αυτή προτείνονται κρυπτογραφικοί μηχανισμοί που ισορροπούν το αντιστάθμισμα μεταξύ ιδιωτικότητας και ασφάλειας σε VANETs. Επίσης συζητούνται στρατηγικές για την επίτευξη ιδιωτικότητας τοποθεσίας.

[Σ21] E. Magkos, M. Maragoudakis, V. Chrissikopoulos, and S. Gridzalis. "Accuracy in Privacy-Preserving Data Mining Using the Paradigm of Cryptographic Elections". In: Privacy in Statistical Databases (PSD '08), 24-26 Sep. 2008, Istanbul. Lecture Notes in Computer Science (LNCS), Vol. 5262/2008, Springer-Verlag, pp. 284-297, 2008.

Οι τεχνολογίες εξόρυξης δεδομένων εγείρουν ζητήματα σχετικά με την επεξεργασία και χρήση ευαίσθητων πληροφοριών, ιδίως σε κατανεμημένα περιβάλλοντα όπου οι συμμετέχοντες μπορεί να είναι μη έμπιστες οντότητες. Σε αυτήν την εργασία τοποθετούμαστε υπέρ της χρήσης ευρέως γνωστών κρυπτογραφικών τεχνικών, που έχουν προταθεί στα πλαίσια της έρευνας για ασφαλή και ιδιωτικά συστήματα ηλεκτρονικών εκλογών. Η προσέγγιση μας υιοθετεί το κλασσικό ομομορφικό μοντέλο για ηλεκτρονικές εκλογές, και συγκεκριμένα ορισμένες επεκτάσεις αυτού του μοντέλου για την υποστήριξη εκλογών πολλαπλών υποψηφίων. Στη συνέχεια περιγράφουμε ορισμένες αδυναμίες, από τη σκοπιά της ασφάλειας, του σχήματος που προτάθηκε στην [1], το οποίο αποτελεί το πρώτο σχήμα που υλοποιεί το ομομορφικο μοντέλο σε κατανεμημένα συστήματα εξόρυξης.

[Σ22] V. Stathopoulos, P. Kotzanikolaou, and E. Magkos. “A Framework for Secure and Verifiable Logging in Public Communication Networks”. In: 1st International Workshop, CRITIS 2006, Samos, Greece, August 31 - September 1, 2006, Lecture Notes in Computer Science, Vol. 4347, Springer, pp. 273-284, 2006.

Η εργασία αυτή επικεντρώνεται σε συστήματα ασφαλούς καταγραφής και ελέγχου για δικτυακούς και τηλεπικοινωνιακούς παρόχους. Γίνεται μια επισκόπηση των υπαρχόντων μοντέλων απειλών, και προτείνεται ένα καινούριο μοντέλο απειλών, ειδικά προσαρμοσμένο στο περιβάλλον των ISPs. Επίσης προτείνεται ένα πλαίσιο λειτουργίας για την ασφαλή καταγραφή σε τηλεπικοινωνιακά δίκτυα, έναντι των απειλών που περιγράφονται. Σημαντικό ρόλο στο προτεινόμενο πλαίσιο λειτουργίας διαδραματίζει μια ανεξάρτητη ρυθμιστική αρχή, υπεύθυνη για την επαλήθευση της ακεραιότητας των αρχείων καταγραφής.

[Σ23] E. Magkos, P. Kotzanikolaou, M. Stefanidakis. “An Asymmetric Key Establishment Protocol for Multiphase Self-Organized Sensor Networks”. In: 12th European Wireless Conference (EW 2006) “Enabling Technologies for Wireless Multimedia Communications”, April 2 - 5, 2006, Athens Greece.

Στην εργασία αυτή προτείνεται ένα ασύμμετρο πρωτόκολλο εδραίωσης κλειδιού για αποκεντρωμένα δίκτυα αισθητήρων (DSNs). Το πρωτόκολλο είναι πολλαπλών φάσεων,

δηλαδή υποστηρίζει εισαγωγή κόμβων στο δίκτυο σε διαφορετικές χρονικές περιόδους, όπου κάθε ομάδα που εισέρχεται σε συγκεκριμένη χρονική περίοδο απαρτίζει μια γενιά κόμβων. Μετά την αρχικοποίηση τους, οι κόμβοι της πρώτης γενιάς συμμετέχουν σε ένα πρωτόκολλο εδραίωσης κλειδιού ώστε να επικοινωνούν στη συνέχεια με μυστικότητα και αυθεντικότητα. Έπειτα, κάθε νέο-εισερχόμενη γενιά αρχικοποιεί μια φάση εδραίωσης κλειδιού, ώστε οι καινούριοι κόμβοι να επικοινωνούν με ασφάλεια τόσο μεταξύ τους, όσο και με κόμβους παλαιότερων γενιών. Το πρωτόκολλο επεκτείνει το υβριδικό πρωτόκολλο των Kotzanikolaou et al [Σ13]. Συγκεκριμένα, μετατρέποντας το σχήμα της [Σ13] σε πλήρως ασύμμετρο, το πρωτόκολλο διορθώνει μια ευπάθεια ασφάλειας του σχήματος της [Σ13], χωρίς να απαιτούνται περισσότεροι πόροι σε επεξεργασία και επικοινωνία.

[Σ24] Kotzanikolaou P., Magkos E., Douligeris C., Chrissikopoulos V., “Hybrid Key Establishment for Multiphase Self-Organized Sensor Networks”. First International Workshop on Trust, Security and Privacy for Ubiquitous Computing (TSPUK 2005), June 13, 2005, Taormina, Sicily, Italy. In: Proc. of 6th IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, (WoWMoM 2005) IEEE, pp. 581-587, 2005.

Στην εργασία προτείνεται ένα υβριδικό πρωτόκολλο για την ανταλλαγή κρυπτογραφικών κλειδιών σε ασύρματα ad-hoc δίκτυα αισθητήρων. Το πρωτόκολλο χρησιμοποιεί ασύμμετρες κρυπτογραφικές μεθόδους βασισμένες σε Ελλειπτικές Καμπύλες για την ταυτοποίηση των κόμβων και την αντιμετώπιση επιθέσεων πλαστοπροσωπίας. Επίσης, προτείνονται συμμετρικές τεχνικές για την ανταλλαγή ορισμένης τυχαιότητας (randomness) που θα χρησιμοποιεί στην κατασκευή των κλειδιών συνόδου σύμφωνα με το πρωτόκολλο των Diffie-Hellman. Το προτεινόμενο πρωτόκολλο είναι ασφαλές και αποδοτικό σε κατανεμημένα περιβάλλοντα ad-hoc όπου η θέση των κόμβων δεν είναι γνωστή εκ των προτέρων και ως εκ τούτου η ασφάλεια του συστήματος δε μπορεί να βασίζεται σε ήδη προ-εγκατεστημένα κλειδιά ή στην ύπαρξη μιας Αρχής Διαμοίρασης Κλειδιών (τύπου Kerberos).

[Σ25] Μάγκος Ε., Χρυσικόπουλος, Β., Αλεξανδρής, Ν., Πούλος, Μ.: "Ηλεκτρονική Ψηφοφορία μέσω Internet: Ουτοπία ή Πραγματικότητα;". Ηλεκτρονική Δημοκρατία – Κοινωνία της Πληροφορίας και τα Δικαιώματα του Πολίτη, 1ο Εθνικό Συνέδριο με Διεθνή Συμμετοχή, 25 - 26 Σεπτεμβρίου 2003, Κτίριο ΕΒΕΑ. Proceedings: To be published, 2003.

Η καθιέρωση της ηλεκτρονικής ψηφοφορίας, και συγκεκριμένα της ψηφοφορίας μέσω Internet, ως εναλλακτικού τρόπου υποβολής της ψήφου αναμένεται να αυξήσει την συμμετοχή των πολιτών στις εκλογές και να αυτοματοποιήσει τις διαδικασίες της υποβολής και της καταμέτρησης των ψήφων, μειώνοντας μακροπρόθεσμα το κόστος διεξαγωγής των εκλογών. Ωστόσο, για να ολοκληρωθεί η μετάβαση σε συστήματα εξ’ αποστάσεως ψηφοφορίας μέσω Internet, πρέπει πρωτίστως να επιλυθούν ζητήματα ασφάλειας και λειτουργικότητας, τα οποία συχνά αγνοούνται από τους σχεδιαστές συστημάτων. Στην εργασία αυτή καθορίζουμε απαιτήσεις ασφάλειας και πρακτικότητας, συζητούμε προϋποθέσεις και περιγράφουμε κρυπτογραφικά μοντέλα ασφάλειας για την υλοποίηση ηλεκτρονικών εκλογών μεγάλης κλίμακας μέσω Internet.

Επίσης, αναφέρουμε τις προοπτικές που διαγράφονται για την υιοθέτηση συστημάτων ηλεκτρονικής ψηφοφορίας στα σύγχρονα δημοκρατικά καθεστώτα.

[Σ26] Poulos, M., Evangelou, A., Magkos, E., Papavlasopoulos, S.: "Fingerprint Verification Based on Image Processing Segmentation Using An Onion Algorithm of Computational Geometry". In: 6th International Workshop on Mathematical Methods in Scattering Theory and Biomedical Engineering, 18-21 September 2003, Tsepelovo, Greece. WOLRD SCIENTIFIC publications, pp. 550-559, 2003.

Στην εργασία προτείνεται μια τεχνική επεξεργασίας ψηφιακής εικόνας με χρήση τεχνικών "onion algorithm" υπολογιστικής γεωμετρίας. Αυτή η μέθοδος μπορεί να χαρακτηριστεί ως μια εναλλακτική μέθοδος για την εξαγωγή των χαρακτηριστικών σημείων του δαχτυλικού αποτυπώματος σε συστήματα επαλήθευσης ταυτότητας. Ο προτεινόμενος αλγόριθμος συγκρίνεται με το δημοφιλή αλγόριθμο επαλήθευσης ταυτότητας που προτάθηκε από τον Ratha. Επιπλέον η εφαρμογή του αλγορίθμου σε μετρήσεις εμφάνισε ιδιαιτέρως χαμηλά ποσοστά λανθασμένης αποδοχής-απόρριψης (FAR-FRR) της τάξεως του 0.1%

[Σ27] Poulos, M., Magkos, E., Chrissikopoulos, V., and Alexandris, N.: "Secure Fingerprint Verification Based on Image Processing Segmentation using Computational Geometry Algorithms". In: SPPRA '2003 – IASTED International Conference on Signal Processing, Pattern Recognition, and Applications. June 30 – July 2, Rhodes, Greece, ACTA Press, pp. 308-312, 2003.

Στην εργασία προτείνεται ένα ηλεκτρονικό σύστημα επαλήθευσης ταυτότητας με τη χρήση δακτυλικών αποτυπωμάτων. Πιο συγκεκριμένα, προτείνεται η χρήση τεχνικών υπολογιστικής γεωμετρίας (computational geometry) κατά την εξαγωγή των χαρακτηριστικών του δαχτυλικού αποτυπώματος στη διαδικασία της εγγραφής του χρήστη στο σύστημα. Στη συγκεκριμένη τεχνική, εξάγεται ένα «χαρακτηριστικό πολύγωνο» για κάθε χρήστη, του οποίου η θέση είναι μοναδική για κάθε δείγμα. Κατά αυτόν τον τρόπο, τα ποσοστά λανθασμένης αποδοχής (false acceptance) και λανθασμένης απόρριψης (false rejection) περιορίζονται στο ελάχιστο.

[Σ28] Magkos, E., Chrissikopoulos, V., Alexandris, N., and Poulos, M.: "Secure Key Recovery for Archived and Communicated Data in the Corporate Intranet". In: 7th WSEAS International Conference on Circuits, Systems, Communications and Computers. July 7-10, Corfu, Greece, pp. 191-195, 2003.

Στην εργασία θεωρούνται τα συστήματα ανάκτησης κλειδιού στο εταιρικό περιβάλλον, δηλαδή συστήματα στα οποία δίνεται η δυνατότητα ανάκτησης ηλεκτρονικών εγγράφων και εταιρικών δεδομένων σε περίπτωση απώλειας των κρυπτογραφικών κλειδιών που χρησιμοποιήθηκαν κατά την ασφαλή αποθήκευση ή διακίνηση τους. Συζητούνται επιθέσεις από κακόβουλους χρήστες ενάντια σε αυτά τα συστήματα, και περιγράφεται ένα σύστημα για την προστασία των αρχειοθετημένων δεδομένων καθώς και των δεδομένων που διακινούνται στο εταιρικό ενδοδίκτυο. Το μοντέλο που προτείνεται είναι «δίκαιο» υπό την έννοια ότι προστατεύεται η ιδιωτικότητα των υπαλλήλων, αλλά παράλληλα επιτυγχάνεται η έγκαιρη ανάκτηση των δεδομένων όταν τα κλειδιά που χρησιμοποιήθηκαν για την κρυπτογράφηση τους δεν είναι διαθέσιμα

[Σ29] M. Poulos, N. Alexandris, V.S. Belessiotis, E. Magkos. "Comparison between Computational Geometry and Coherence Methods applied to the EEG for Medical Diagnostic Purposes". In: Proceedings of the 7th International Multicoference on Circuits, Systems, Communications and Computers, Corfu Island Greece, July 7-10, pp. 247-252, 2003.

The examination of differences in intra-hemispheric coherence and a novel method based on computational geometric algorithms between the left and right hemispheres of the same EEG. The Coherence and Computational geometry methods are computed from the same EEG segment and especially in the alpha and beta activities. The Results of the application of Coherence and Computational geometry methods showed that beta activity differed dramatically in the occipital intra-hemisphere. In conclusion, Computational Geometry method showed that it can give an accurate solution for EEG medical diagnostic purposes, especially in those patient cases which present severe asymmetric brain damage.

[Σ30] Magkos, E., Chrissikopoulos, V., Alexandris, N.: "A Common Security Model for Conducting e-Auctions and e-Elections". In: 6th WSEAS International Conference on Communications. In N. Mastorakis, V. Mladenov: Recent Advances in Computers, Computing and Communications, WSEAS, pp. 463-467, 2002.

Στην εργασία περιγράφεται ένα μοντέλο ηλεκτρονικών συναλλαγών στο οποίο α) κάθε χρήστης επιλέγει μια προσφορά από ένα σύνολο προσφορών, β) ο χρήστης χρησιμοποιεί το Διαδίκτυο για να υποβάλλει την προσφορά του στην Αρχή του συστήματος, γ) η Αρχή αξιολογεί την προσφορά ως επιτυχή ή ανεπιτυχή, βάση ενός συνόλου κανόνων, και δ) τα αποτελέσματα ανακοινώνονται στους χρήστες μέσω του Διαδικτύου. Το παραπάνω μοντέλο συστημάτων ηλεκτρονικών συναλλαγών περιλαμβάνει μια ποικιλία εφαρμογών σε διαφορετικά περιβάλλοντα. Έτσι, για παράδειγμα, ένα ηλεκτρονικό σύστημα συναλλαγών που βασίζεται στο ανωτέρω μοντέλο μπορεί να είναι: Α) ένα σύστημα ηλεκτρονικής ψηφοφορίας ή Β) ένα σύστημα ηλεκτρονικής δημοπρασίας. Στην εργασία περιγράφονται οι ομοιότητες μεταξύ των δύο συστημάτων από τη σκοπιά της ασφάλειας και στη συνέχεια προτείνεται ένα μοντέλο ασφάλειας ο οποίο μπορεί να εφαρμοστεί και στις δύο περιπτώσεις.

[Σ31] Magkos, E., Chrissikopoulos, V., Alexandris, N.: "Software-based Receipt-Freeness in On-line Elections". In: IFIP TC11 WG11.4 1st Annual Working Conference on Network Security, November 26-27, 2001, Leuven, Belgium. In Advances in Network And Distributed Systems Security, Kluwer Academic Publishers, pp. 33-43, 2001.

Στην εργασία καταδεικνύονται τα προβλήματα που παρουσιάζονται κατά την υλοποίηση πρόσφατων κρυπτογραφικών πρωτοκόλλων ηλεκτρονικής ψηφοφορίας. Τα πρωτόκολλα αυτά επιτυγχάνουν προστασία από καταναγκασμό καθώς και οικουμενική επαληθευσιμότητα, επικαλούμενα την ύπαρξη «φυσικά» προστατευμένων καναλιών (physically untappable channels) από την Αρχή προς τον ψηφοφόρο ή/και αντίστροφα. Τα κανάλια αυτά είναι φυσικά κανάλια μονής/διπλής κατεύθυνσης, τα οποία χρησιμοποιούν η Αρχή και ο ψηφοφόρος για να ανταλλάξουν μηνύματα με απόλυτη μυστικότητα. Ωστόσο οι φυσικές αυτές υποθέσεις είναι μη πρακτικές, ειδικά για εκλογές μεγάλης κλίμακας που διενεργούνται μέσω Διαδικτύου. Προς αυτήν την

κατεύθυνση προτείνεται ένα πρωτόκολλο ηλεκτρονικής ψηφοφορίας μέσω Internet χωρίς να απαιτείται η «φυσική» ασφάλεια του καναλιού επικοινωνίας μεταξύ του ψηφοφόρου και της Αρχής. Προκειμένου να επιτευχθεί η προστασία από καταναγκασμό προτείνεται η χρήση των Γρίφων Συγκεκριμένου Χρόνου Επίλυσης (Time-Lock Puzzles) κατά την κρυπτογράφηση των ψήφων ώστε να καθίστανται εξαιρετικά δύσκολες οι επιθέσεις μαζικού καταναγκασμού των ψηφοφόρων.

[Σ32] Magkos, E., Kotzanikolaou, P., Chrissikopoulos, V.: "An Asymmetric Traceability Scheme for Copyright Protection without Trust Assumptions". In: 2nd International Conference on Electronic Commerce and Web technologies EC-WEB 2001, Munich, Germany, September 4-6, LNCS Vol. 2115, Springer-Verlag, pp. 186-195, 2001.

Στην εργασία περιγράφονται και προτείνονται τρόποι αντιμετώπισης της παράνομης αναδιανομής ηλεκτρονικής πληροφορίας από εξουσιοδοτημένους χρήστες («προδότες» - traitors). Γίνεται θεώρηση, με κριτήρια ασφάλειας και πρακτικότητας, των σχημάτων ανίχνευσης «προδοτών» (traitor tracing) που έχουν προταθεί στη διεθνή βιβλιογραφία για την προστασία των πνευματικών δικαιωμάτων σε εφαρμογές αναμετάδοσης κρυπτογραφημένου υλικού. Στη συνέχεια προτείνεται ένα ασύμμετρο σχήμα ανίχνευσης «προδοτών» χωρίς τρίτη έμπιστη οντότητα, όπου ο π του υλικού δε γνωρίζει εκ των προτέρων το αποτύπωμα που περιέχει ο αποκωδικοποιητής ενός εξουσιοδοτημένου χρήστη, αλλά μπορεί να ανιχνεύσει την ταυτότητα ενός «προδότη» που διαθέτει το αποτύπωμα του στην κατασκευή ενός πειρατικού αποκωδικοποιητή. Στο σχήμα επίσης ενσωματώνονται επιπλέον έλεγχοι ορθότητας ώστε ο παροχέας να μη μπορεί να συμπεριφερθεί κακόβουλα και να ενοχοποιήσει άδικα έναν χρήστη του συστήματος..

[Σ33] Magkos, E., Burmester, M., and Chrissikopoulos V.: "Receipt-Freeness in Large-scale Elections without Untappable Channels". In: 1st IFIP Conference on E-Commerce/Business/Government, Kluwer Academic Publishers, pp. 683-693, 2001.

Στην εργασία αναλύονται οι ιδιαίτερες παράμετροι του προβλήματος του καταναγκασμού στα συστήματα ηλεκτρονικής ψηφοφορίας, καθορίζονται οι ελάχιστες απαιτήσεις ασφάλειας που πρέπει να τηρούνται και προτείνεται ένα πρωτόκολλο το οποίο επιτυγχάνει Προστασία από Καταναγκασμό με τη χρήση μιας Έξυπνης Κάρτας (smart card) που συνεισφέρει κάποια τυχαιότητα στην κρυπτογράφηση της ψήφου, με τρόπο που δεν αφήνει περιθώρια κακόβουλων ενεργειών στον χρήστη ή στην κάρτα. Η προσέγγιση παρουσιάζει ιδιαίτερο ενδιαφέρον, καθώς είναι ιδανική για ηλεκτρονικές ψηφοφορίες μέσω Internet, όπου το κανάλι επικοινωνίας είναι ευάλωτο σε ωτακουστές.

[Σ34] Burmester, M., Chrissikopoulos, V., Kotzanikolaou, P., and Magkos, E.: "Strong Forward Security". In: IFIP-SEC '01 Conference, Kluwer Academic Publishers, pp. 109-119, 2001.

Στην εργασία αυτή εισάγεται η έννοια της ισχυρής χρονικής ασφάλειας (strong forward security) ως μια μέθοδος για την ελαχιστοποίηση των συνεπειών της εξουσιοδοτημένης (π.χ. στην περίπτωση της νόμιμης ανάκτησης κλειδιού από Αρχές Επιβολής Νόμου) ή μη εξουσιοδοτημένης (π.χ. υποκλοπή-υπεξαίρεση κλειδιών) αποκάλυψης ενός ιδιωτικού

κλειδιού, στα πλαίσια ενός κρυπτογραφικού συστήματος δημοσίου κλειδιού. Σύμφωνα με τη μέθοδο αυτή, η οποία μπορεί να αξιοποιηθεί και για την προστασία ιδιωτικών κλειδιών ψηφιακής υπογραφής, το ζεύγος ιδιωτικού/δημόσιου κλειδιού ενός χρήστη ανανεώνεται ανά τακτά χρονικά διαστήματα. Ο μηχανισμός ανανέωσης επεκτείνει την παραδοσιακή έννοια της χρονικής ασφάλειας καθώς εξασφαλίζει ότι η αποκάλυψη του ιδιωτικού κλειδιού ενός χρήστη κατά τη διάρκεια μιας συγκεκριμένης περιόδου, δε θα υπονομεύσει την ιδιωτικότητα του χρήστη κατά τις περιόδους που προηγήθηκαν (χρονική ασφάλεια) αλλά και κατά τις περιόδους που έπονται της αποκάλυψης (ισχυρή χρονική ασφάλεια). Ο μηχανισμός ανανέωσης που προτείνεται δεν απαιτεί φυσικές (out-of-band) μεθόδους αυθεντικοποίησης, αλλά επιτυγχάνεται αυθεντικοποιώντας το ανανεωμένο ιδιωτικό κλειδί με το προηγούμενο ιδιωτικό κλειδί, και υποβάλλοντας το αντίστοιχο δημόσιο κλειδί σε μια Αρχή Πιστοποίησης (Certification Authority – CA).

[Σ35] E. Magkos, M. Burmester, V. Chrissikopoulos. “An Equitably Fair On-line Auction Scheme”. In 1st International Conference on Electronic Commerce and Web technologies - EC-WEB 2000, LNCS Vol. 1875, Springer-Verlag, pp. 72-84, 2000.

Στην εργασία καταδεικνύονται τα ζητήματα ασφάλειας που τίθενται κατά τη σχεδίαση και υλοποίηση συστημάτων ηλεκτρονικών δημοπρασιών, αναφέρονται τα βασικά κρυπτογραφικά μοντέλα που απαντώνται στη διεθνή βιβλιογραφία και περιγράφεται ένα «δίκαιο» πρωτόκολλο ηλεκτρονικής δημοπρασίας για καταλογισμό ευθύνης στους χρήστες που υποβάλλουν προσφορά αλλά στη συνέχεια αποφασίζουν να την αποσύρουν. Η μέθοδος που προτείνεται είναι «δίκαιη» (equitably fair) για τους χρήστες και τους δημοπράτες. Αυτό σημαίνει πως το σύστημα προστατεύει την ανωνυμία των χρηστών και την μυστικότητα των προσφορών τους, εδραιώνοντας παράλληλα καταλογισμό ευθύνης για κάθε έγκυρη προσφορά που υποβάλλεται.

[Δ1] Ε. Μάγκος. "Κρυπτογραφία και Ασφάλεια Δικτύων". 2015

Στόχοι του διδακτικού τόμου είναι:

- Η κατανόηση των αντιπροσωπευτικότερων κλασσικών τεχνικών κρυπτογραφίας και κρυπτανάλυσης, οι οποίες θεωρούνται πρόγονοι των μοντέρνων συμμετρικών κρυπτογραφικών αλγορίθμων.
- Η κατανόηση και θεμελίωση της έννοιας της απόλυτης ασφάλειας, που αποτελεί το μέγιστο επίπεδο ασφάλειας που μπορεί να χαρακτηρίζει κάθε κρυπτογραφικό αλγόριθμο
- Η κατανόηση των μαθηματικών εννοιών που θα αποτελέσουν τα θεμέλια για την περιγραφή των κρυπτογραφικών τεχνικών κρυπτογράφησης και ψηφιακής υπογραφής,
- Η κατανόηση των αρχών λειτουργίας, της δομής και της ασφάλειας των μοντέρνων συμμετρικών αλγορίθμων για την προστασία της εμπιστευτικότητας και της ακεραιότητας/αυθεντικότητας των μηνυμάτων που ανταλλάσσονται σε ένα δίκτυο επικοινωνίας παρουσία παθητικών και ενεργητικών εχθρών
- Η εξοικείωση με τους μηχανισμούς δημόσιου κλειδιού (ΔΚ) που χρησιμοποιούνται για την προστασία της εμπιστευτικότητας, ακεραιότητας και αυθεντικότητας των

μηνυμάτων που ανταλλάσσονται μεταξύ απομακρυσμένων οντοτήτων σε μη ασφαλή δίκτυα.

- Η επισκόπηση των εννοιών και ζητημάτων που σχετίζονται με τα πιστοποιητικά ΔΚ, τη διαχείριση τους καθώς και τις υποδομές ΔΚ για την αυθεντικότητα των δημόσιων κλειδιών των χρηστών σε ένα σύστημα επικοινωνίας.
- Η επισήμανση των αδυναμιών των συμβατικών τεχνικών ταυτοποίησης με κωδικούς πρόσβασης, καθώς και η διόρθωση ορισμένων από αυτές τις αδυναμίες με κρυπτογραφικό τρόπο. Επίσης, η κατανόηση των κρυπογραφικών τεχνικών ταυτοποίησης απομακρυσμένης οντότητας για τον έλεγχο λογικής πρόσβασης στην ασφάλεια υπολογιστικών συστημάτων και δικτύων.
- Η κατανόηση των πλέον δημοφιλών κρυπτογραφικών τεχνικών αυθεντικοποιημένης εδραίωσης ενός συμμετρικού κλειδιού συνόδου για την προστασία της εμπιστευτικότητας και της αυθεντικοτητας ενός καναλιού επικοινωνίας.

[B1] E. Magkos, M. Maragoudakis, V. Chrissikopoulos. "Προστασία Ιδιωτικότητας σε Κατανεμημένα Συστήματα Εξόρυξης Δεδομένων". Συλλογικός Τόμος με τίτλο: "Προστασία της Ιδιωτικότητας στις Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα". Παπασωτηρίου, 2009.

Στο παρόν κεφάλαιο γίνεται βιβλιογραφική επισκόπηση στο ερευνητικό πεδίο που αφορά στην προστασία της ιδιωτικότητας σε κατανεμημένα συστήματα εξόρυξης δεδομένων. Δίνουμε έμφαση σε περιβάλλοντα όπου τα συμβαλλόμενα μέρη αφενός δεν εμπιστεύονται ο ένας τον άλλο (π.χ. ανταγωνιζόμενες επιχειρήσεις, χρήστες στο Web κλπ), αφετέρου δεν εμπιστεύονται (πλήρως) κάποια Τρίτη οντότητα για την ανάλυση των δεδομένων τους. Στο πρώτο μέρος του κεφαλαίου γίνεται μια εισαγωγή στις γενικές ιδέες που διέπουν την προστασία της Ιδιωτικότητας σε πλήρως κατανεμημένα περιβάλλοντα εξόρυξης δεδομένων. Στο δεύτερο μέρος του κεφαλαίου εξετάζονται, μέσω της σχετικής βιβλιογραφίας, τεχνικές και μηχανισμοί από τους ερευνητικούς χώρους της Κρυπτογραφίας και Ασφάλειας Πληροφοριών για την προστασία της ιδιωτικότητας σε συστήματα εξόρυξης δεδομένων, δίνοντας έμφαση σε μοντέλα ταξινόμησης και εξαγωγής κανόνων συσχέτισης. Στο τελευταίο μέρος του κεφαλαίου περιγράφονται ορισμένες εφαρμογές των τεχνικών που εξετάστηκαν για την εξαγωγή στατιστικής γνώσης από κατανεμημένες βάσεις δεδομένων σε συστήματα μεγάλης κλίμακας.

[B2] E. Magkos, M. Burmester, V. Chrissikopoulos. "Αυθεντικοποιημένη Εδραίωση Κλειδιού". Συλλογικός Τόμος με τίτλο: "Σύγχρονη Κρυπτογραφία: Θεωρία και Εφαρμογές". M. Burmester, Σ. Γκρίτζαλης, Σ. Κάτσικας, Β. Χρυσικόπουλος (Eds). Εκδόσεις Παπασωτηρίου, 2009.

Στο κεφάλαιο παρουσιάζονται και αναλύονται οι κατηγορίες πρωτοκόλλων εδραίωσης κλειδιού, ιστορικών και σύγχρονων, καθώς και οι εφαρμογές τους στην ασφάλεια δικτύων. Συγκεκριμένα, μελετώνται οι απαιτήσεις ασφάλειας και πρακτικότητας στους αλγόριθμους εδραίωσης, παρουσιάζονται και αναλύονται, από τη σκοπιά της

ασφάλειας, πρωτόκολλα διανομής, μεταφοράς και συμφωνίας κλειδιού, με χρήση συμμετρικών τεχνικών ή/και τεχνικών δημόσιου κλειδιού.

[B3] C. Lambrinoudakis, E. Magkos, V. Chrissikopoulos. "Electronic Voting Systems". (Chapter) In: J. Lopez, S. Furnell, A. Patel, S. Katsikas, (Ed.), "Securing Information and Communication Systems: Principles, Technologies and Applications". Artech House Publishers, Computer Security Series, pp. 307-323, 2008.

Στην εργασία αυτή αναλύονται οι λειτουργικές και μη λειτουργικές απαιτήσεις για τη διενέργεια ενός ηλεκτρονικού συστήματος εκλογών, λαμβάνοντας υπόψη τη κοινοτική νομοθεσία, τις οργανωτικές δομές υπαρκτών (φυσικών) εκλογικών συστημάτων, καθώς επίσης και τους περιορισμούς που επιβάλλονται από την τρέχουσα τεχνολογία. Επίσης, παρέχεται μια επισκόπηση ιστορικών και σύγχρονων κρυπτογραφικών μοντέλων για τη διενέργεια ασφαλών απομακρυσμένων ηλεκτρονικών εκλογών μέσω Internet.

[B4] N. Alexandris, V. Chrissikopoulos and E. Magkos. “The role of Cryptography in Large-Scale Internet Elections”. Volume of essays in honour of Professor Antonios C. Panayotopoulos pp. 93–110, 2006.

Η εργασία αυτή παρουσιάζει μια επισκόπηση της ακαδημαϊκής βιβλιογραφίας σχετικής με την εφαρμογή κρυπτογραφικών τεχνικών κατά τη διενέργεια ηλεκτρονικών εκλογών μέσω Internet. Επίσης, καταδεικνύει τα ανοικτά προβλήματα και τις προκλήσεις που η έρευνα καλείται να επιλύσει τα επόμενα χρόνια.

[B5] M. Burmester, E. Magkos. “Towards Secure and Practical e-Elections in the New Era”. In: Advances in Information Security - Secure Electronic Voting, Kluwer Academic Publishers pp. 63-76, 2003.

Στην εργασία εξετάζονται οι διάφοροι τύποι συστημάτων ηλεκτρονικής ψηφοφορίας από τη σκοπιά της ασφάλειας, αναφέρονται τα κρυπτογραφικά μοντέλα υλοποίησης ηλεκτρονικής ψηφοφορίας που έχουν προταθεί στη διεθνή βιβλιογραφία και συζητούνται τρόποι αντιμετώπισης των προβλημάτων ασφάλειας στα συστήματα ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου. Επίσης περιγράφονται οι μέθοδοι για την επίτευξη προστασίας από καταναγκασμό σε ηλεκτρονικές ψηφοφορίες με τη χρήση Έξυπνων Καρτών που συνεισφέρουν κάποια τυχαιότητα στην κρυπτογράφηση της ψήφου, κατά τρόπο που δεν αφήνει περιθώρια κακόβουλων ενεργειών στον χρήστη ή στην κάρτα.
