Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Σύστήματα Πληροφορικής»

Παρουσίαση Μεταπτυχιακής Εργασίας

«Ανασκόπηση και περιγραφή των μεθοδολογιών, προτύπων και εργαλείων που χρησιμοποιούνται για την ανάλυση ψηφιακών πειστηρίων διαδικτυακών υπηρεσιών *(Web Services Forensics).* ***Επίδειξη κυριοτέρων ανοιχτών εργαλείων με συγκεκριμένες περιπτώσεις χρήσης»***

Ονοματεπώνυμο: **Παπουτσής Δημήτριος**
Αριθμός Μητρώου : **ΜΠΣΠ/ 11034**
Επιβλέπων καθηγητής : **Πολέμη Νινέτα**

Πρόλογος

- Θεωρητική περιγραφή των θεμελιωδών αρχών της «Δικανικής Πληροφορικής».
- Ιδιαίτερη βαρύτητα δίνεται στο τομέα των Υπηρεσιών Ιστού της Δικανικής Πληροφορικής – Web Services Forensics (FWS).
- Γενικές πρακτικές της Δικανικής Πληροφορικής.
- Παρουσίαση μεθοδολογιών της Δικανικής έρευνας.
- Αξιολόγηση των μεθοδολογιών.
- Περιγραφή βέλτιστης μεθοδολογίας της Δικανικής Πληροφορικής στις υπηρεσίες ιστού (Web Services).
- Περιγραφή Προβλήματος.
- Πειραματικό μέρος.

Γενικά

1. Δικανική έρευνα.
2. Είσοδος των υπολογιστικών συστημάτων σε όλους τους τομείς της σύγχρονης ζωής
3. Κίνδυνοι στο Διαδίκτυο – Ηλεκτρονικό έγκλημα.
4. Υπηρεσίες Ιστού.
5. Κίνδυνοι
   - ευαίσθητα δεδομένα πελατών .
   - καταστροφή δεδομένων.
   - παρεμπόδιση επιχειρησιακής συνέχειας.
   - πλήγμα στην αξιοπιστία της εταιρείας.

Ορισμός «Δικανική Πληροφορική»

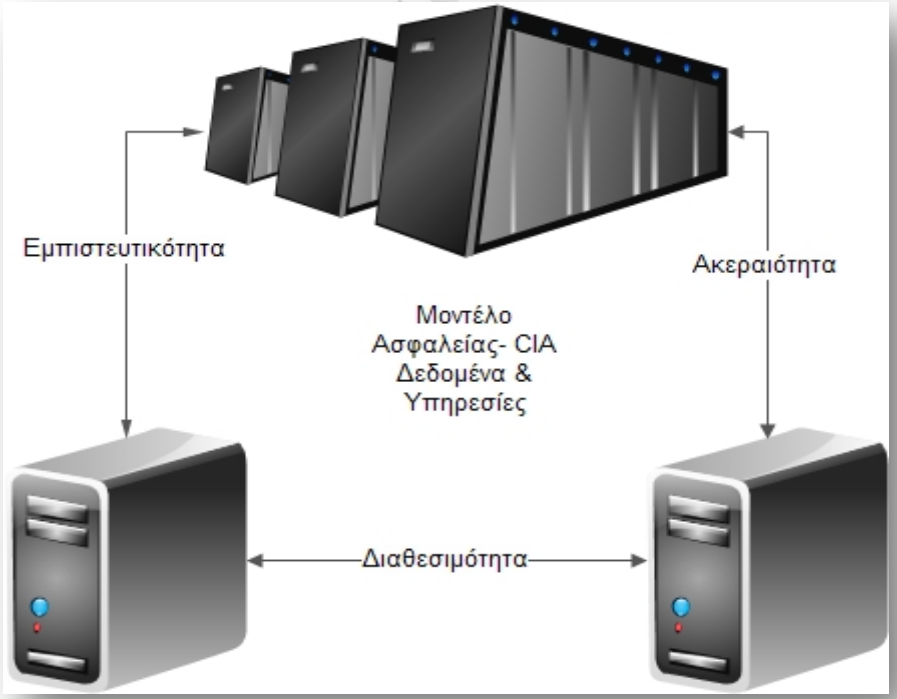
Σαν Δικανική πληροφορική (ή Δικανική Υπολογιστική), ορίζουμε *την πλήρη εφαρμογή των διαδικασιών που συνδυάζουν στοιχεία του νόμου και της επιστήμης των υπολογιστών έτσι ώστε να συλλεχτούν και να αναλυθούν τα δεδομένα από τα συστήματα ηλεκτρονικών υπολογιστών, υπηρεσιών ιστού, δεδομένα δικτύου, ηλεκτρονικών επικοινωνιών και μέσων αποθήκευσης με τρόπο που θα είναι αποδεκτός ως πειστήριο σε ένα δικαστήριο στηριζόμενο στο ισχύον νομοθετικό πλαίσιο ενός κράτους*

Διαδικασίες «Δικανικής Πληροφορικής»

1. Πρόληψη κατά των κακόβουλων πράξεων.
2. Η ανίχνευση «ύποπτων» κινήσεων σε ένα πληροφοριακό δίκτυο.
3. Η συλλογή ψηφιακών αποδείξεων.
4. Διατήρηση των πειστηρίων.
5. Ανάλυση των ψηφιακών αποδείξεων.
6. Ανακατασκευή της επίθεσης.
7. Αποκατάσταση του πληροφοριακού περιβάλλοντος.
8. Παρουσίαση πειστηρίων.

Βασικά χαρακτηρίστηκα Ασφάλειας - CIA

- Εμπιστευτικότητα.
- Ακεραιότητα.
- Διαθεσιμότητα.



Αρχές ασφαλείας

- Ιδιωτικότητα (privacy) .
- Πιστοποίηση (authentication).
- Έλεγχος (auditing).

Μεθοδολογίες
Γενικά 1/2

1. Η μεθοδολογία θα πρέπει να είναι γενική.
2. Η μέθοδος θα πρέπει να είναι εύκολα υλοποιήσιμη.
3. Η μεθοδολογία θα πρέπει να είναι εύκολα προσαρμόσιμη .
4. Η μεθοδολογία θα πρέπει να είναι δομημένη.

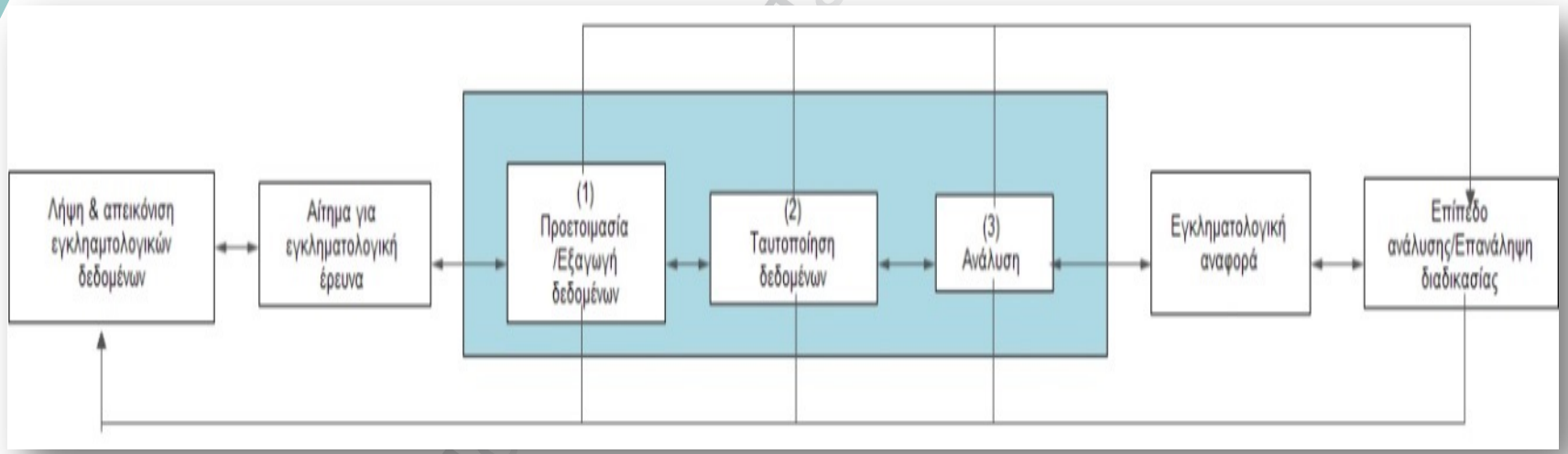
Μεθοδολογίες
Γενικά 2/2

1. Διατήρηση των δεδομένων σε ακέραια μορφή.
2. Πρόληψη για τυχόν κίνδυνο «μόλυνσης» των δεδομένων.
3. Παρουσίαση και τεκμηρίωση των δεδομένων.
4. Χρήση επιστημονικής μεθοδολογίας.

Μεθοδολογία τριών βημάτων 1/3

- Προετοιμασία-Εξαγωγή αποδεικτικών στοιχείων:
  - επικύρωση της καλής λειτουργίας .
  - αντίγραφα των εγκληματολογικών δεδομένων.
  - επαλήθευση της ακεραιότητας των δεδομένων.
  - προθήκη στη σχετική λίστα.
- Εξακρίβωση Δεδομένων:
  - «Λίστα σχετικών δεδομένων».
  - «Λίστα αναζήτησης-αποτελεσμάτων».
- Ανάλυση Δεδομένων:
  - «Λίστα ανάλυσης αποτελεσμάτων».
  - Εγκληματολογικής αναφορά.

Μεθοδολογία τριών βημάτων 2/3



Μεθοδολογία τριών βημάτων 3/3

- Δομημένη διαδικασία με σαφή βήματα.
- Δυνατότητα επανεξέτασης και ταξινόμησης των διαφόρων αντικειμένων .
- Απλότητα στην εφαρμογή της.

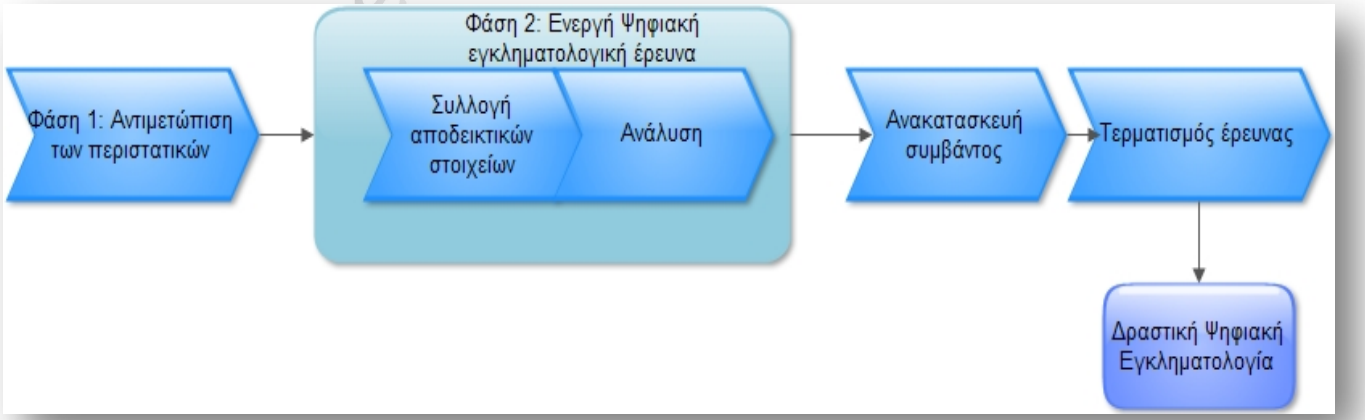
- Συλλογή πειστηρίων μετά το συμβάν της επίθεσης.
- Καλή λειτουργία πληροφοριακών συστημάτων;
- Δύσκολα προσαρμόσιμη στις υπηρεσίες ιστού.

Μεθοδολογία Πολλαπλών Συνιστωσών (Gobler-Louwrens-Solms) – 1/4

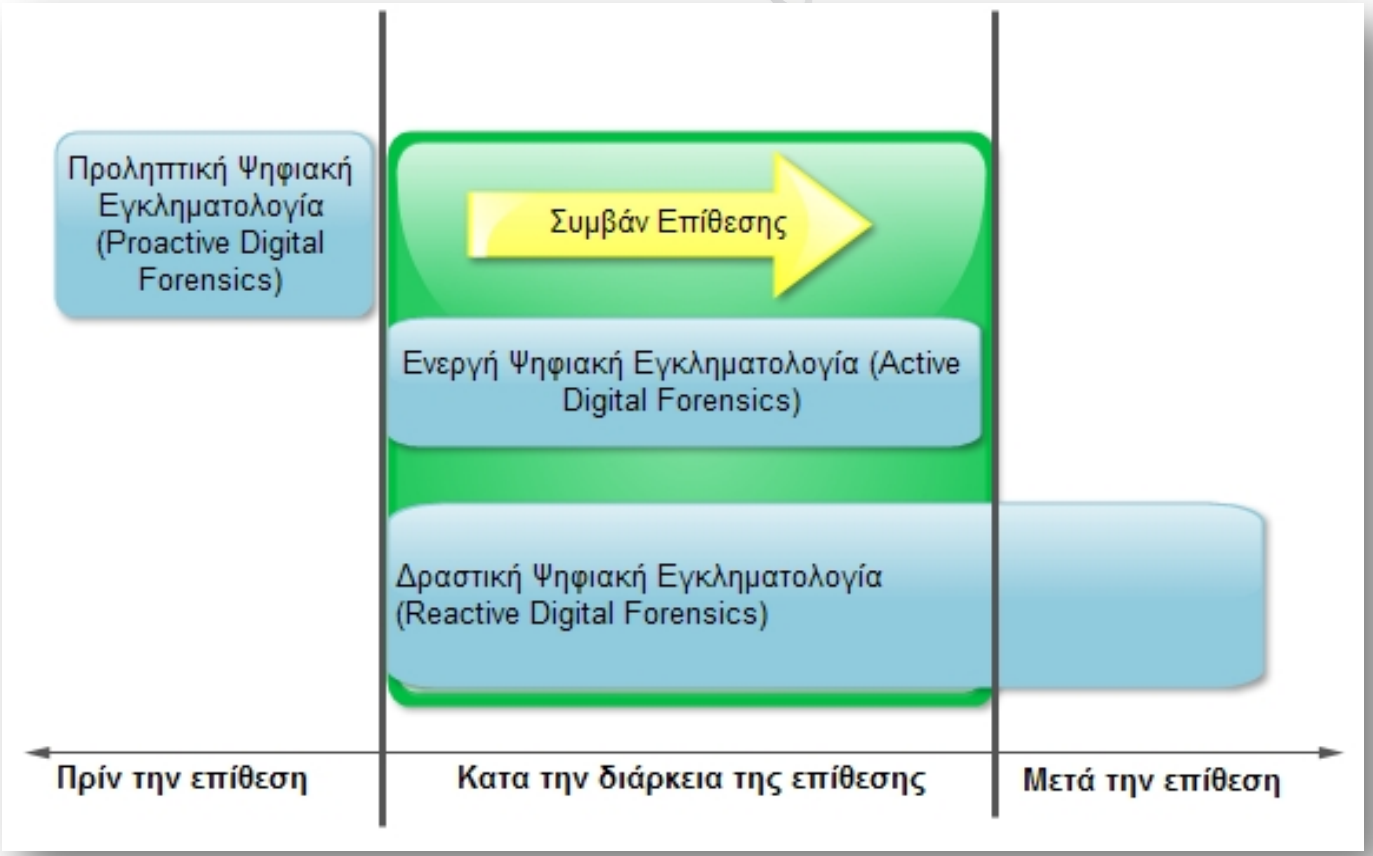
- Προληπτική ψηφιακή εγκληματολογία (Proactive Digital Forensics).
  - Ανάλυση και προετοιμασία πληροφοριακού περιβάλλοντος.
  - ανάπτυξη οργανωτικών σχεδίων αντιμετώπισης κινδύνων και διαχείρισης.
- Ενεργή ψηφιακή εγκληματολογία (Active Digital Forensics).
  - αίτια της εγκληματικής ενέργειας.
  - σύνδεση αποδεικτικών στοιχείων.
  - ελαχιστοποιούνται οι επιπτώσεις της επίθεσης.
  - επιτυχής έρευνα του περιστατικού.

Μεθοδολογία Πολλαπλών Συνιστωσών (Gobler-Louwrens-Solms) – 2/4

- Δραστική ψηφιακή εγκληματολογία(Reactive Digital Forensics).
  - συλλογή σχετικών «ζωντανών» ψηφιακών πειστηρίων.
  - ελαχιστοποίηση των επιπτώσεων στη λειτουργία των πληροφοριακών συστημάτων.
  - σημείο εκκίνησης για μια δραστική έρευνα.



Σχέσεις μεταξύ των Αντικειμένων - 3/4



Μεθοδολογία Πολλαπλών Συνιστωσών (Gobler-Louwrens-Solms) – 4/4

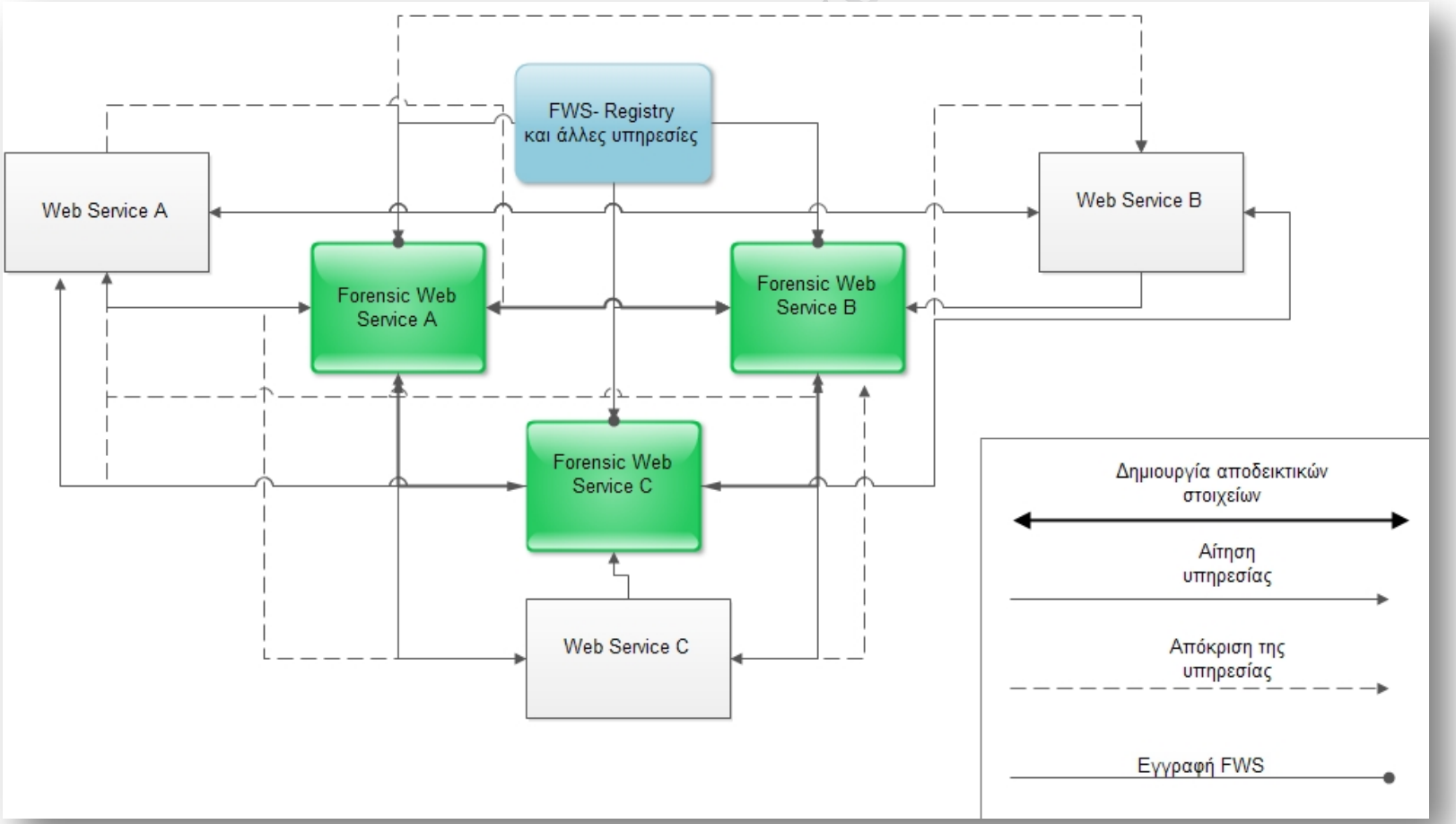
- Καλύπτει όλα τα στάδια της Δικανικής έρευνας.
- Προληπτικές μεθόδους, ακολουθεί αυστηρό πλαίσιο διαδικασιών για τα «ζωντανά» αλλά και για τα κοινά αποδεικτικά στοιχεία.
- Αναθέτει συγκεκριμένους ρόλους.
- Δικλίδες ασφαλείας – τεχνολογικά εργαλεία.

- Υψηλό κόστος.
- Πολυπλοκότητα.
- Αδυναμία στην αντιμετώπιση επιθέσεων υπηρεσιών ιστού.

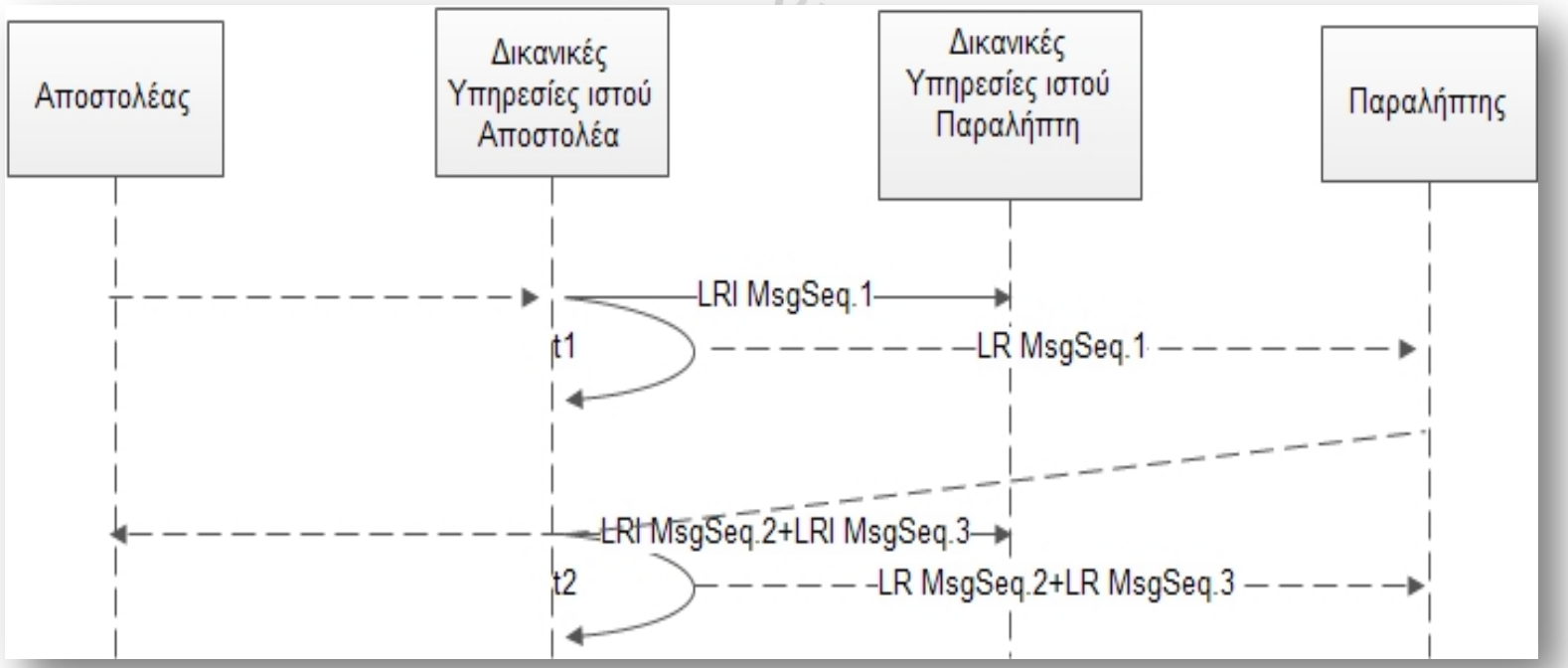
Μεθοδολογία στα Web Services **1/4**

- Αξιόπιστες «τρίτες» οντότητες.
  - Αυθεντικοποίηση όλων των οντοτήτων που λαμβάνουν χώρα.
  - Εμπιστευτικότητα και αξιοπιστία των καναλιών επικοινωνίας.
  - Αξιόπιστη ανταλλαγή μηνυμάτων πάνω από τα κανάλια επικοινωνίας.
- Ζεύγη αποδεικτικών στοιχείων καταγραφής με χρονοσήμανση.
  - Χρόνος αίτησης της υπηρεσίας.
  - Χρόνος ανταπόκρισης της υπηρεσίας.
  - Λήξη της υπηρεσίας αιτήματος.
  - Χρόνος διαθεσιμότητας του εξυπηρετητή.
- Ζεύγη αποδεικτικών στοιχείων καταγραφής με χρονοσήμανση.

Μεθοδολογία στα Web Services
2/4



Μεθοδολογία στα Web Services
3/4



Μεθοδολογία στα Web Services **4/4**

- Αντιμετώπιση «ζωντανών» επιθέσεων.
- Τεχνικές και εργαλεία εύκολα προσαρμόσιμες.
- Εποπτεία κάθε συναλλαγής μεταξύ των υπηρεσιών ιστού.

- Συγκεκριμένο πλαίσιο φάσεων και βημάτων.
- Κατάλληλα εκπαιδευμένο προσωπικό.
- Μηχανισμοί επανάληψης της διαδικασίας .
- Εμπλεκόμενοι ρόλοι.

Σύγκριση μεθοδολογιών

Ψηφιακή Δικανική μεθοδολογία	Προληπτική έρευνα			Ενεργή Ψηφιακή έρευνα					Δραστική έρευνα					Web Services			Αριθμός φάσεων
	Συλλογή δεδομένων	Μηχανισμοί ενεργοποίησης συμβάντων	Προληπτική αντιμετώπιση συμβάντων	Ταυτοποίηση	Διαφύλαξη πειστηρίων	Συλλογή	Ανάλυση	Αναφορά	Ταυτοποίηση	Διαφύλαξη πειστηρίων	Συλλογή	Ανάλυση	Αναφορά	Συλλογή δεδομένων	ενεργοποίησης συμβάντων	Συλλογή\ Ανάλυση	--
«Μεθοδολογίας τριών βημάτων»	--	--	--	- -	- -	- -	- -	- -	✓	✓	✓	✓	✓	--	--	--	3 φάσεις
«Μεθοδολογία Πολλαπλών Συνιστωσών»	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	--	--	--	3 κυρίως φάσεις συμπεριλα - μβανομέν ων υπο- φάσεων
«Μεθοδολογία Web Services»	✓	✓	✓	- -	- -	- -	- -	- -	- -	- -	- -	- -	- -	✓	✓	✓	2 φάσεις

Βέλτιστη μεθοδολογία 1/2

1. Ανάγκη για μια ολοκληρωμένη μέθοδο.
2. Εύκολα προσαρμόσιμη.
3. Προληπτικά μέτρα – Διασφάλιση πληροφοριακού περιβάλλοντος.
4. Συλλογή «ζωντανών» πειστηρίων των υπηρεσιών ιστού.
5. Κατάλληλα εργαλεία για ανακατασκευή του συμβάντος.
6. Παγίωση αποτελεσμάτων – τεκμηριωμένη έκθεση πειστηρίων.

Βέλτιστη μεθοδολογία 2/2

- Τρείς κυρίως φάσεις:
  - προληπτικά (Proactive) μέτρα (5 επιμέρους βήματα).
  - διατήρηση - συλλογή ψηφιακών αποδεικτικών στοιχείων (6 επιμέρους βήματα).
  - τερματισμό της εγκληματολογικής έρευνας (4 επιμέρους βήματα).

Πρακτικό μέρος..