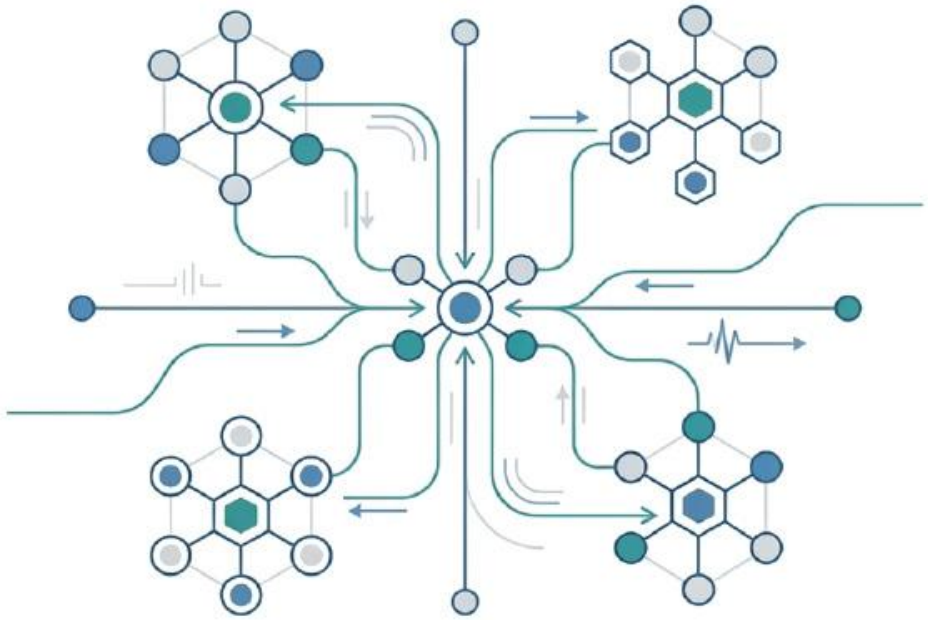
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ



Επιστημονική Ημερίδα της Αρχής:
2η Ημέρα Διαλόγου με την Ερευνητική Κοινότητα

22 Οκτωβρίου 2026

Griefbots, ψηφιακή αθανασία και ιδιωτικότητα: από τη μοντελοποίηση απειλών στον Privacy-by-Design σχεδιασμό

Βασιλική Διαμαντοπούλου, Επ. Καθηγήτρια, Πανεπιστήμιο Αιγαίου, Αν. Μέλος ΑΔΑΕ
Αγγελική Τσώχου, Καθηγήτρια, Ιόνιο Πανεπιστήμιο

Περίγραμμα παρουσίασης

- Τα Griefbots ως συστήματα συνομιλιακής ΤΝ
- Ερευνητικό Κίνητρο και Συμβολή
- Κανονιστικό Πλαίσιο και Κίνδυνοι
- Αρχιτεκτονική συστήματος και μοντελοποίηση απειλών
- Ανάλυση ασφάλειας και ιδιωτικότητας
- Κατευθυντήριες γραμμές σχεδιασμού

Τα Griefbots ως συστήματα συνομιλιακής ΤΝ

- Συστήματα που προσομοιώνουν την επικοινωνία με αποθανόντα πρόσωπα, αξιοποιώντας ψηφιακά ίχνη:
  - Προσωπικά μηνύματα και ιστορικά συνομιλιών
  - Φωνητικές εγγραφές και οπτικοακουστικό υλικό
  - Φωτογραφίες, δημοσιεύσεις και άλλα ψηφιακά δεδομένα
- Μεταφέρουν την ψηφιακή μνημόνευση από τη στατική μορφή στη διαδραστική αναπαράσταση.
- Μετασχηματίζουν το πένθος σε εμπειρία που διαμεσολαβείται τεχνολογικά.



Griefbots και συμβατικά chatbots

- **Συμβατικό chatbot**
  - Απαντά σε ερωτήσεις
  - Εκτελεί συγκεκριμένες εργασίες
  - Χρησιμοποιεί περιορισμένο πλαίσιο
  - Δεν αναπαριστά συγκεκριμένη ταυτότητα
- **Griefbot**
  - Προσομοιώνει συγκεκριμένο πρόσωπο
  - Χρησιμοποιεί οικεία προσωπικά αρχεία
  - Παράγει νέα δεδομένα αλληλεπίδρασης
  - Επηρεάζει μνήμη, εμπιστοσύνη και πένθος

Η επιφάνεια κινδύνου επεκτείνεται
στα δεδομένα, το μοντέλο, τη διεπαφή και την υποδομή.

Ερευνητικό κενό και συμβολή της μελέτης

Το ερευνητικό κενό

- Η υπάρχουσα βιβλιογραφία εξετάζει την ηθική, το πένθος και τη διακυβέρνηση, αλλά δεν παρέχει επαρκώς συστηματική μηχανική ασφάλειας και ιδιωτικότητας ειδικά για τα griefbots.

Η συμβολή μας

1. Γενική αρχιτεκτονική αναφοράς
2. Ανάλυση ασφάλειας με STRIDE
3. Ανάλυση ιδιωτικότητας με LINDDUN
4. Κατευθυντήριες γραμμές σχεδιασμού

Στόχος: ανθεκτικότερα griefbots
με ασφάλεια και προστασία δεδομένων ήδη από τον σχεδιασμό.

Κανονιστικό πλαίσιο και προσέγγιση κινδύνου

AI Act
Διαφάνεια και απαγόρευση ορισμένων χειριστικών πρακτικών

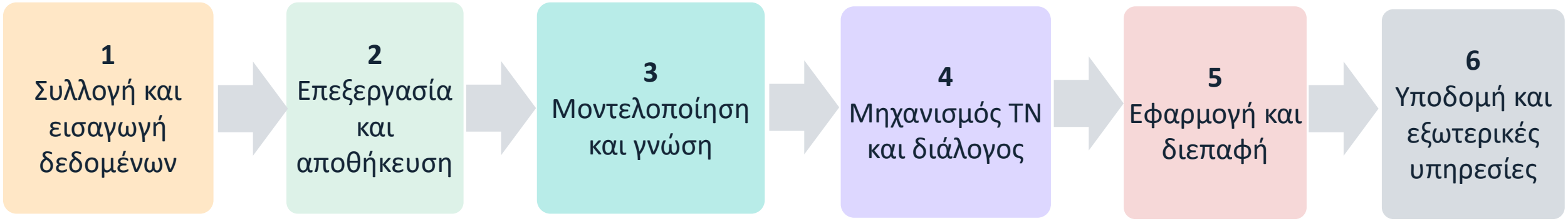
GDPR
Δεδομένα ζώντων προσώπων
Προστασία από τον σχεδιασμό

NIS 2
Ασφάλεια εφοδιαστικής αλυσίδας και κυβερνοανθεκτικότητα

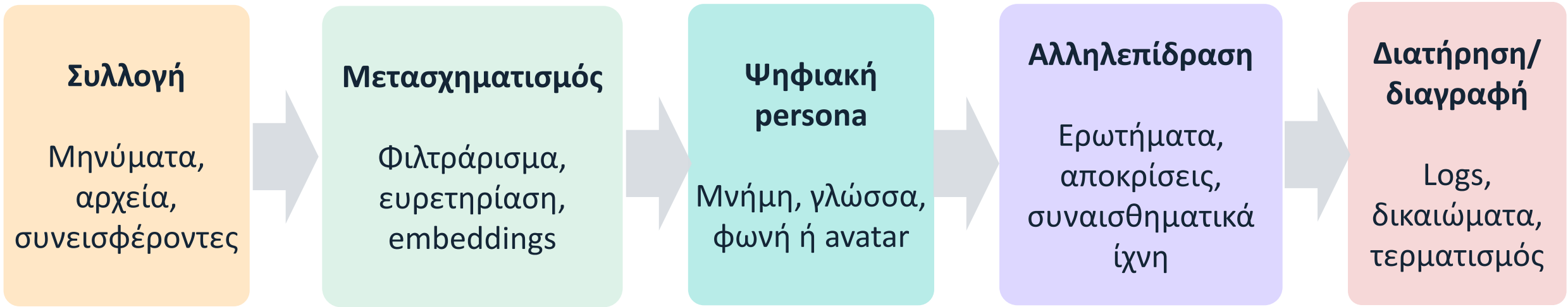
Όχι απαραίτητα «υψηλού κινδύνου» κατά AI Act – αλλά δυνητικά υψηλού αντικτύπου στην πράξη.

* Η εφαρμογή της NIS 2 εξαρτάται από τον πάροχο και το είδος της καλυπτόμενης υπηρεσίας.

Αρχιτεκτονική αναφοράς:
6 διασυνδεδεμένα επίπεδα



Κύκλος ζωής δεδομένων ενός Griefbot



Κάθε μετάβαση μπορεί να προκαλέσει διαρροή, συσχέτιση, χειραγώγηση ή ανεξέλεγκτη διατήρηση δεδομένων.

Κατηγορίες δεδομένων που επεξεργάζονται τα griefbots

Δεδομένα ταυτότητας

Όνομα, φωνή, φωτογραφίες, βιογραφικά στοιχεία

Δεδομένα πενθούντων

Ερωτήματα, συναισθήματα και προφίλ χρήσης

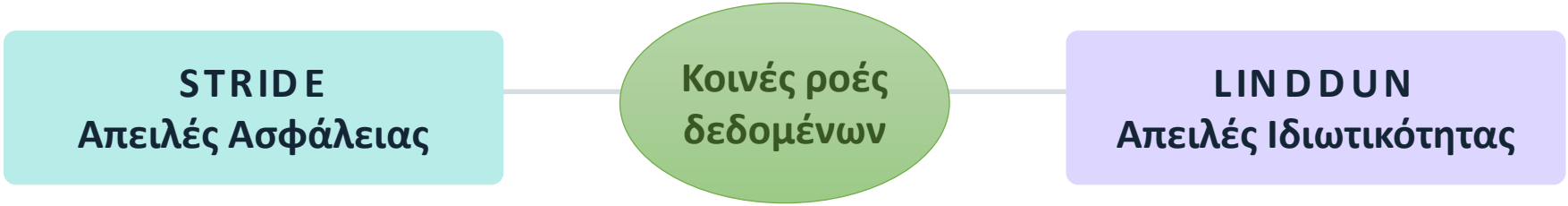
Επικοινωνιακά δεδομένα

Ιστορικά, γλωσσικά, πρότυπα, σχέσεις

Δυναμικά προσωπικά δεδομένα ζώντων προσώπων

Μεθοδολογία μοντελοποίησης απειλών

- **STRIDE – μεθοδολογία μελέτης ασφάλειας συστήματος**
  - Εξετάζει επιθέσεις σε λογισμικό και υποδομές: πλαστοπροσωπία (**S**poofing), αλλοίωση (**T**ampering), αποποίηση (**R**epudiation), αποκάλυψη πληροφοριών (**I**nformation disclosure), άρνηση υπηρεσίας (**D**enial of service – DoS) και κλιμάκωση προνομίων (**E**levation of privilege).
- **LINDDUN – μεθοδολογία μελέτης ιδιωτικότητας**
  - Εξετάζει πώς μπορεί να προκύψει συσχέτιση (**L**inkability), ταυτοποίηση (**I**dentiability), μη αποποίηση (**N**on-Repudiation), ανιχνευσιμότητα (**D**etectability), αποκάλυψη πληροφοριών (**D**isclosure of data), άγνοια/έλλειψη επίγνωσης (**U**nawareness) και μη συμμορφούμενη (**N**on-compliance) επεξεργασία προσωπικών δεδομένων



Ανάλυση STRIDE (1/4)
Βασικές απειλές

- **Spoofing:** Πλαστοπροσωπία χρηστών, συγγενών, διαχειριστών ή υπηρεσιών
- **Tampering:** Αλλοίωση αρχείων, μοντέλου ή παραγόμενης αναπαράστασης
- **Repudiation:** Αδυναμία απόδειξης ποιος τροποποίησε ή προσπέλασε δεδομένα
- **Information Disclosure:** Διαρροή προσωπικών συνομιλιών και ηχογραφήσεων
- **Denial of Service:** Διακοπή πρόσβασης σε συναισθηματικά σημαντικές στιγμές
- **Elevation of Privilege:** Μη εξουσιοδοτημένη πρόσβαση σε διαχειριστικές λειτουργίες

Ανάλυση STRIDE(2/4)
Σενάρια επιθέσεων

Εισαγωγή δεδομένων
Ψευδή αρχεία από υποτιθέμενο συγγενή – κακόβουλα uploads

Αποθήκευση
Αποκάλυψη ή αλλοίωση ιστορικών επικοινωνίας

Μοντελοποίηση
Αλλοίωση παραμέτρων persona ή ευρετηρίων

Αλληλεπίδραση
Prompt injection και αποκάλυψη ιδιωτικού περιεχομένου

Διεπαφή
Υποκλοπή συνεδρίας ή ελλιπής έλεγχος πρόσβασης

Εξωτερικές υπηρεσίες
Παραβίαση API keys ή υποδομών cloud

Μία επίθεση μπορεί ταυτόχρονα να θίξει την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα της αναπαράστασης.

Ανάλυση STRIDE (3/4)
Ιεράρχηση απειλών

Η ανάλυση δίνει ιδιαίτερη προτεραιότητα σε:

Αποκάλυψη πληροφοριών (Information disclosure)	Πρόσβαση σε οικείο προσωπικό υλικό και δεδομένα πένθους.
Αλλοίωση δεδομένων (Tampering)	Παραμόρφωση της ψηφιακής ταυτότητας του αποθανόντος.
Κλιμάκωση προνομίων (Elevation of privilege)	Παράκαμψη ελέγχων και εκτεταμένη μη εξουσιοδοτημένη πρόσβαση.

> Άρνηση Παροχής Υπηρεσίας (Denial of Service – DoS) έχει επίσης σημασία λόγω της χρονικής συγκυρίας και της συναισθηματικής κατάστασης του χρήστη
> Πλαστοπροσωπία (spoofing) και **αποποίηση ευθύνης ή ενεργειών (repudiation)** παραμένουν σημαντικές απειλές, καθώς η ταυτότητα και η δυνατότητα καταλογισμού ευθύνης αποτελούν κεντρικά στοιχεία του συστήματος.

Ανάλυση STRIDE (4/4)
Προτεινόμενες στρατηγικές αντιμετώπισης απειλών

Spoofing
Ισχυρή αυθεντικοποίηση
Προστασία συνεδριών
RBAC / ABAC

Tampering
Έλεγχοι ακεραιότητας
Ελεγχόμενες τροποποιήσεις
Προστασία ρυθμίσεων μοντέλου

Repudiation
Καταγραφή ενεργειών
Ελεγκτικά ίχνη με σεβασμό στην ιδιωτικότητα

Information Disclosure
Κρυπτογράφηση
Έλεγχος πρόσβασης
Ασφαλείς πάροχοι

Denial of Service
Περιορισμοί αιτημάτων
Εφεδρικοί μηχανισμοί
Σχέδια επιχειρησιακής συνέχειας

Elevation of Privilege
Ελάχιστα προνόμια
Ασφαλή APIs
Περιοδικοί έλεγχοι

Ανάλυση LINDDUN (1/4)
Απειλές ιδιωτικότητας

- Οι κίνδυνοι για την ιδιωτικότητα μπορούν να προκύψουν ακόμη και χωρίς την ύπαρξη μιας κλασικής «επίθεσης»
  - Τα δεδομένα ενδέχεται να **συσχετιστούν**, να χρησιμοποιηθούν για την εξαγωγή **συμπερασμάτων**, να **αποκαλυφθούν** ή να υποβληθούν σε **επεξεργασία**, χωρίς οι χρήστες να έχουν ουσιαστική επίγνωση αυτών των διαδικασιών.
- Η μεθοδολογία LINDDUN διευρύνει την ανάλυση απειλών πέρα από τις επιθέσεις μη εξουσιοδοτημένων τρίτων
  - Εξετάζει κατά πόσο τα δεδομένα μπορούν να συσχετιστούν (Linkability), τα άτομα να ταυτοποιηθούν (Identifiability), η χρήση του συστήματος να ανιχνευθεί (Detectability), οι πληροφορίες να αποκαλυφθούν (Disclosure of Information), οι χρήστες να παραμένουν χωρίς επαρκή επίγνωση (Unawareness) ή η επεξεργασία δεδομένων να πραγματοποιείται κατά παράβαση του κανονιστικού πλαισίου (Non-compliance).
  - Αυτό είναι ιδιαίτερα σημαντικό, καθώς τα griefbots επεξεργάζονται δεδομένα που αφορούν διαπροσωπικές σχέσεις και μπορούν να επηρεάσουν τόσο τα εν ζωή άτομα όσο και την ψηφιακή αναπαράσταση του αποθανόντος.

Ανάλυση LINDDUN (2/4)
Σενάρια ιδιωτικότητας

Συλλογή
Τρίτα πρόσωπα αγνοούν ότι επαναχρησιμοποιούνται τα δεδομένα τους

Αποθήκευση
Ασύνδετα αποσπάσματα συνθέτουν συνεκτικά προσωπικά προφίλ

Μοντελοποίηση
Η persona αποκαλύπτει σχέσεις και πληροφορίες ζώντων προσώπων

Αλληλεπίδραση
Τα prompts φανερώνουν πένθος, συνήθειες, πεποιθήσεις

Διεπαφή
Τα μοτίβα χρήσης γίνονται ορατά σε τρίτους

Εξωτερικοί πάροχοι
Συσχέτιση δεδομένων μεταξύ διαφορετικών πλατφορμών

Ανάλυση LINDDUN (3/4)
Ιεράρχηση απειλών

- Η ανάλυση δίνει ιδιαίτερη έμφαση στην **Αποκάλυψη Πληροφοριών (Disclosure of Information)**, λόγω της εξαιρετικά ευαίσθητης και προσωπικής φύσης των δεδομένων μνήμης των αποθανόντων, των συνομιλιών που σχετίζονται με το πένθος, των φωνητικών καταγραφών και των προφίλ συμπεριφοράς.
- Ωστόσο, η **Συσχετισιμότητα (Linkability)**, η **Ταυτοποιησιμότητα (Identifiability)**, η **Ανιχνευσιμότητα (Detectability)** και η **Μη Συμμόρφωση (Non-compliance)** αποτελούν επίσης σημαντικές απειλές, καθώς το σύστημα έχει σχεσιακό χαρακτήρα. Ενδέχεται, δηλαδή, να επηρεάζει και άτομα που δεν έχουν επιλέξει άμεσα να αλληλεπιδράσουν με το griefbot.

Ανάλυση LINDDUN (4/4)
Προτεινόμενες στρατηγικές αντιμετώπισης

Περιορισμός συσχέτισης
Ελαχιστοποίηση δεδομένων
Διαχωρισμός αποθετηρίων
Ελεγχόμενη επαναχρήση

Περιορισμός της έκθεσης πληροφοριών
Απόκρυψη ή απαλοιφή ευαίσθητων πληροφοριών
Επιλεκτική αποκάλυψη πληροφοριών
Μηχανισμοί ελέγχου των παραγόμενων αποτελεσμάτων

Μείωση ανιχνευσιμότητας
Διακριτική διεπαφή
Λιγότερες ειδοποιήσεις
Ελαχιστοποίηση των μεταδεδομένων

Ενίσχυση ενημέρωσης
Σαφείς ειδοποιήσεις
Εξήγηση ορίων μοντέλου
Κατανοητές ενδείξεις

Διασφάλιση συμμόρφωσης
Περιορισμός σκοπού
Διαχείριση συγκατάθεσης
Διατήρηση και διαγραφή

Διακυβέρνηση παρόχων
Τεκμηρίωση εξαρτήσεων
Έλεγχος διαβιβάσεων
Επαλήθευση εγγυήσεων

Εκτίμηση της σοβαρότητας των απειλών στο περιβάλλον ενός Griefbot

- Οι ίδιες απειλές αποκτούν μεγαλύτερη σοβαρότητα στα οικοσυστήματα των griefbots.
- Οι τεχνικές αστοχίες μπορούν να οδηγήσουν σε **προσβολή της μνήμης** και της **αξιοπρέπειας**, καθώς και σε **υπονόμευση της εμπιστοσύνης** και της **φροντίδας**.

1 **Οικειότητα**

Ιδιωτικά μηνύματα, φωνή, φωτογραφίες, συναισθηματικές εκμυστηρεύσεις

2 **Ταυτότητα**

Οι αποκρίσεις εκλαμβάνονται ως αναπαράσταση συγκεκριμένου αποθανόντος

3 **Σχέσεις**

Τα δεδομένα περιλαμβάνουν οικογένεια, φίλους και συνομιλητές

4 **Χρονική ευαλωτότητα**

Η διαθεσιμότητα και οι επιπτώσεις έχουν ιδιαίτερο βάρος σε στιγμές πένθους

Κατευθυντήριες γραμμές σχεδιασμού (1/4)

1. Πειθαρχία στον κύκλο ζωής των δεδομένων

Ο σχεδιασμός των griefbots απαιτεί ελαχιστοποίηση δεδομένων και περιορισμό σκοπού, σαφή διάκριση των εμπλεκόμενων ρόλων και εφαρμογή κατάλληλων μέτρων ασφάλειας από την αρχή.

Αυθεντικοποίηση
Ισχυρή ταυτοποίηση και προστασία συνεδριών

Έλεγχος πρόσβασης
Λεπτομερής διαχείριση ρόλων και δικαιωμάτων

Ασφάλεια δεδομένων
Κρυπτογράφηση, ακεραιότητα, ασφαλής αποθήκευση

Διατήρηση / διαγραφή
Σαφείς κανόνες, οριοθέτηση χρόνου και διαδικασίες

Κατευθυντήριες γραμμές σχεδιασμού (2/4)

2. Σχεδιασμός Μοντέλου και Διαχείριση Μνήμης (Model and Memory Design)

- Το μοντέλο θα πρέπει να:
  - αποφεύγει την περιττή έκθεση δεδομένων που έχουν χρησιμοποιηθεί κ ατά την εκπαίδευσή του.
  - περιορίζει την απομνημόνευση προσωπικών και ευαίσθητων πληροφοριών από τα δεδομένα εκπαίδευσης.
  - περιορίζει τη διατήρηση των δεδομένων των χρηστών που βιώνουν πένθος μόνο σε όσα είναι απαραίτητα για τη διασφάλιση της συνέχειας της αλληλεπίδρασης.
- Διαφάνεια (Transparency): Οι χρήστες πρέπει να γνωρίζουν ότι αλληλεπιδρούν με σύστημα Τεχνητής Νοημοσύνης (AI), ποια δεδομένα υποβάλλονται σε επεξεργασία, πώς χρησιμοποιούνται και ποιες λειτουργίες το σύστημα δεν μπορεί να εκτελέσει με αξιοπιστία.

Κατευθυντήριες γραμμές σχεδιασμού (3/4)

3. Αυτονομία του χρήστη

- Το σύστημα θα πρέπει να αποφεύγει σχεδιαστικές πρακτικές που αποσκοπούν στη *χειραγώγηση* ή ενδέχεται να προκαλέσουν *συναισθηματική εξάρτηση*, παρέχοντας στους χρήστες τη δυνατότητα να διακόπτουν προσωρινά, να περιορίζουν, να εξάγουν τα δεδομένα τους ή να τερματίζουν οριστικά τη χρήση της υπηρεσίας.

Προστασία δεδομένων τρίτων

- Τα μηνύματα, οι φωτογραφίες και οι ηχογραφήσεις ενδέχεται να περιλαμβάνουν προσωπικά δεδομένα συγγενών, φίλων, ατόμων με τα οποία υπήρξε επικοινωνία και άλλων τρίτων. Συνεπώς, απαιτούνται *μηχανισμοί φιλτραρίσματος*, *απόκρυψης ευαίσθητων πληροφοριών*, *επιλεκτικού αποκλεισμού δεδομένων* και *αυστηρότεροι έλεγχοι* για την περαιτέρω επαναχρησιμοποίησή τους.

Η συγκατάθεση ενός προσώπου δεν συνεπάγεται απεριόριστη χρήση δεδομένων όλων των συνομιλητών του.

Κατευθυντήριες γραμμές σχεδιασμού (4/4)

4. Διακυβέρνηση Εξωτερικών Παρόχων, Καταγραφών, Περιστατικών και Δικαιωμάτων

Εξωτερικοί πάροχοι
Οι εξαρτήσεις από τρίτους παρόχους πρέπει να περιορίζονται, να τεκμηριώνονται και να υπόκεινται σε κατάλληλους μηχανισμούς διακυβέρνησης και ελέγχου

Καταγραφή συμβάντων
Υποστήριξη λογοδοσίας και αντιμετώπιση περιστατικών ασφάλειας, χωρίς να αποθηκεύονται περιττές λεπτομέρειες από τις συνομιλίες των χρηστών.

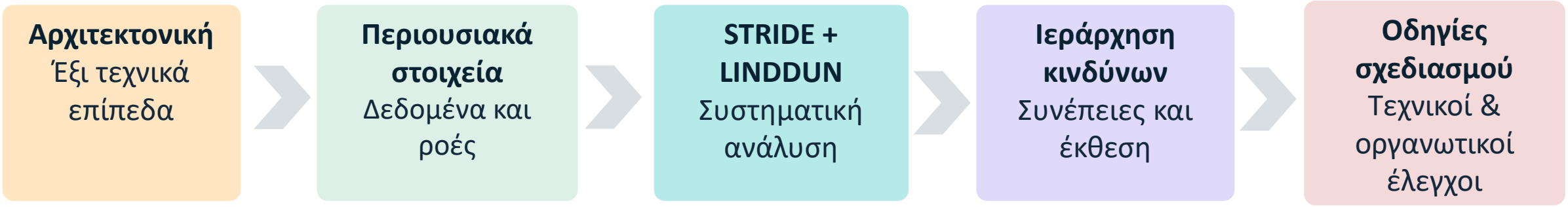
Δικαιώματα και έλεγχος
Οι χρήστες θα πρέπει να γνωρίζουν ποια δεδομένα διατηρούνται, να μπορούν να ζητούν τη διαγραφή ή τον περιορισμό της επεξεργασίας τους, όπου αυτό προβλέπεται, και να διαχειρίζονται τη συμμετοχή τους στο σύστημα.

Οριστικός τερματισμός
Η οριστική απόσυρση ή ο τερματισμός λειτουργίας του συστήματος απαιτεί προσοχή, λόγω της συναισθηματικής σημασίας που μπορεί να έχει για τους χρήστες, εφόσον πρόκειται για griefbots που αναπαριστούν ψηφιακά αγαπημένα τους πρόσωπα που έχουν αποβιώσει.

Η προστασία καλύπτει όχι μόνο το τεχνικό σύστημα αλλά και τις σχέσεις και το συναισθηματικό πλαίσιο.

Από τη μοντελοποίηση απειλών στον υπεύθυνο σχεδιασμό

- Η συμβολή της παρούσας εργασίας δεν περιορίζεται μόνο στην πρόταση ενός συνόλου μέτρων προστασίας, αλλά επεκτείνεται στην ανάπτυξη μιας **συστηματικής και επαναλήψιμης μεθοδολογικής προσέγγισης μηχανικής**, η οποία μπορεί να εφαρμοστεί και σε άλλα αντίστοιχα συστήματα.
- Η Ασφάλεια από τον Σχεδιασμό (Security by Design) και η Προστασία της Ιδιωτικότητας από τον Σχεδιασμό (Privacy by Design) πρέπει να συνδυάζονται κατά την ανάπτυξη και λειτουργία των griefbots ώστε να διασφαλίζεται τόσο η ασφάλεια των συστημάτων όσο και η προστασία των προσωπικών δεδομένων των χρηστών.



Συμπεράσματα και μελλοντική έρευνα

- Τα griefbots εγείρουν σημαντικά ζητήματα ασφάλειας, προστασίας της ιδιωτικότητας και κανονιστικής συμμόρφωσης.
- Η λειτουργία τους μπορεί να επηρεάσει όχι μόνο την ψηφιακή αναπαράσταση του αποθανόντος, αλλά και τα δικαιώματα και την ευημερία των εν ζωή χρηστών και τρίτων προσώπων.

Μελλοντική Έρευνα

- Εφαρμογή της προτεινόμενης μεθοδολογικής προσέγγισης σε πραγματικές υλοποιήσεις συστημάτων griefbots, με στόχο την πρακτική αξιολόγηση της αποτελεσματικότητάς της.
- Ανάπτυξη πιο λεπτομερών μοντέλων ιεράρχησης απειλών, για τη συστηματικότερη αξιολόγηση της πιθανότητας εμφάνισης και της σοβαρότητας των επιπτώσεών τους.
- Μετατροπή των προτεινόμενων κατευθυντήριων γραμμών σε συγκεκριμένα τεχνικά και οργανωτικά μέτρα προστασίας, τα οποία θα μπορούν να εφαρμοστούν στην ανάπτυξη και λειτουργία των εν λόγω συστημάτων.

Αναφορές

1. Hollanek, T., Nowaczyk-BasiÅĎska, K.: Griefbots, deadbots, postmortem avatars: on responsible applications of generative AI in the digital afterlife industry. Philos. Technol. 37, 63 (2024).
2. Lei, Y., Ma, S., Sun, Y., Ma, X.: “AI Afterlife” as digital legacy: perceptions, expectations, and concerns. In: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems, Article 981. ACM, New York (2025).
3. Harbinja, E., Edwards, L., McVey, M.: Governing ghostbots. Comput. Law Secur. Rev. 48, 105791 (2023).
4. Ciani Sciolla, J., Pagallo, U.: No peace after death? The impact of AI-driven memorial chatbots on privacy and data protection. Information 16(6), 426 (2025).
5. European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Off. J. Eur. Union L 119, 1–88 (2016)
6. European Union: Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Off. J. Eur. Union L 2024/1689
7. European Union: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Off. J. Eur. Union L 333, 80–152 (2022)

Αναφορές

8. Holt, J., Nicholson, J., Smeddinck, J.D.: From personal data to digital legacy: explor ing conflicts in the sharing, security and privacy of post-mortem data. In: Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, pp. 1–7. ACM, New York (2021). Cheng, K.Y.: The law of digital afterlife: the Chinese experience of AI ‘resurrection’ and ‘grief tech’. Int. J. Law Inf. Technol. 33(1), eaae029 (2025).
9. Xygkou, A., Siriaraya, P., Covaci, A., Prigerson, H.G., Neimeyer, R.A., Ang, C.S., She, W.J.: The “conversation” about loss: understanding how chatbot technology was used in supporting people in grief. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI ’23), Hamburg, Germany, pp. 1–15. ACM, New York (2023).
10. Holt, J., Smeddinck, J.D., Nicholson, J., Vlachokyriakos, V., Durrant, A.C.: Post mortem information management: exploring contextual factors in appropriate personal data access after death. Hum.-Comput. Interact. 41(1), 26–61 (2026).
11. Holt, J., Smeddinck, J.D., Nicholson, J., Vlachokyriakos, V., Durrant, A.C.: Post mortem information management: exploring contextual factors in appropriate personal data access after death. Hum.-Comput. Interact. 41(1), 26–61 (2026)
12. Khan, R.U., et al.: Chatbot development strategies: a review of current stud ies and future directions. Knowl. Inf. Syst. (2025)
13. Sun, Z., et al.: A survey on large language model security and privacy: the good, the bad, and the ugly. Array 24, 100382 (2024)

Αναφορές

14. ENISA: Artificial intelligence cybersecurity challenges. European Union Agency for Cybersecurity (2020).
15. ENISA Threat Landscape 2025. European Union Agency for Cybersecurity (2025)
16. PÃĺrez, J.Q., Alonso, R.S., Corchado, J.M.: A survey on chatbots and large language models: testing and evaluation techniques. Comput. Electr. Eng. 123, 110008 (2025)
17. Adamopoulou, E., Moussiades, L.: An overview of chatbot technology. In: Artifi cial Intelligence Applications and Innovations, IFIP AICT, vol. 584, pp. 373–383. Springer, Cham (2020)
18. Shostack, A.: Threat Modeling: Designing for Security. Wiley, Indianapolis (2014).
19. Microsoft: Threats– Microsoft Threat Modeling Tool– STRIDE model. Microsoft Learn.
20. Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requir. Eng. 16(1), 3–32 (2011)
21. Shostack, A.: Threat Modeling: Designing for Security. Wiley, Indianapolis (2014)

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ

Σας ευχαριστώ για την προσοχή σας