
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

# Ανάλυση και Αξιολόγηση των Εργαλείων Μοντελοποίησης των Απαιτήσεων Ασφάλειας Πληροφοριακών Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

**Ζερβού Δωροθέας**

Επιβλέπουσα:
Δρ. Διαμαντοπούλου Βασιλική, Επίκουρη Καθηγήτρια του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου

Μέλη εξεταστικής επιτροπής:
Δρ. Καρύδα Μαρία, Επίκουρη Καθηγήτρια του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου

Δρ. Κοκολάκης Σπυρίδων, Καθηγητής του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου

Σάμος, 2024

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

# Ευχαριστίες

Η ολοκλήρωση της διπλωματικής μου εργασίας σηματοδοτεί το τέλος μιας σημαντικής εκπαιδευτικής πορείας και ταυτόχρονα αποτελεί μια αφετηρία για νέες προκλήσεις και στόχους. Πρώτα απ' όλα, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στην επιβλέπουσα καθηγήτρια μου, Δρ. Βασιλική Διαμαντοπούλου, για τη σταθερή καθοδήγηση, τις χρήσιμες συμβουλές και την υποστήριξή σε κάθε στάδιο της μελέτης. Ιδιαίτερη μνεία αξίζει στην οικογένειά μου, που υπήρξε πηγή στήριξης και ενθάρρυνσης, όχι μόνο στην περίοδο της εκπόνησης της παρούσας εργασίας αλλά και σε κάθε μου βήμα. Η αμέριστη υπομονή και η ενθάρρυνσή τους υπήρξαν καθοριστικά στη δική μου επιμονή και προσήλωση. Τέλος, θα ήθελα να ευχαριστήσω τους φίλους μου που ακόμα και χωρίς την φυσική παρουσία τους μου υπενθύμιζαν όλα αυτά τα όνειρα που έχουμε πει ότι θα υλοποιήσουμε και κατόρθωναν να επαναφέρουν στο προσκήνιο τα κίνητρα που είχα θέσει. Η ενθάρρυνση και η υποστήριξή τους μέχρι να περατωθεί η εργασία ήταν συγκινητική.

# Περιεχόμενα

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ....5
ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ....6
Περίληψη....7
Abstract....9
Κεφάλαιο 1 – Εισαγωγή....10
1.1 Εισαγωγή-Θεωρητικό υπόβαθρο....10
1.2 Κίνητρα και Ερευνητικές Ερωτήσεις....12
1.3 Μεθοδολογία....13
1.4 Πεδίο και Σημασία....14
1.5 Ερευνητικό Κενό και Συνεισφορά....14
Κεφάλαιο 2 – Κοινωνική μηχανική....16
2.1 Εργαλεία και αμυντικοί μηχανισμοί της Κοινωνικής Μηχανικής....17
2.2 Χαρτογράφηση των αμυντικών μηχανισμών....18
2.3 Μέθοδοι για την κοινωνική μηχανική....20
2.4 HATCH....22
*2.4.1 Πραγματικό σενάριο....25*
2.5 Επιθέσεις ευρείας κλίμακας....26
*2.5.1 Phising....26*
*2.5.2 Baiting....28*
*2.5.3 Spear Phishing....29*
*2.5.3 Επιθέσεις Watering Hole....30*
*2.5.4 Επίθεση σε πολλαπλά μέτωπα....30*
*2.5.5 Physical baiting....32*
*2.5.6 Τρόποι αντιμετώπισης απειλών....32*
Κεφάλαιο 3 – Απαιτήσεις και μηχανική ασφάλειας....35
3.1 Ανάλυση κενών σε διαδικασίες (Gap analysis)....36
Κεφάλαιο 4 – Ανασκόπηση μεθόδων ελέγχου....40
4.1 Απαιτήσεις ανάπτυξης του λογισμικού....40
4.2 Στρατηγική αναζήτησης και πηγές δεδομένων....41
4.3 Επιλογή προσεγγίσεων SRE....42
*4.3.1 KAOS (Keep All Objectives Satisfied)....43*
*4.3.2 Secure i*....43*
*4.3.3 Secure tropos....44*
*4.3.4 GBRAM (Goal-Based Requirements Analysis Methods)....45*
*4.3.5 Abuse Frames....46*
*4.3.6 (SEPP) Security Engineering Process Using Patterns....46*
*4.3.7 SREF (Security Requirements Engineering Framework)....48*
*4.3.8 CORAS....48*

*4.3.9 SREP (Security Requirements Engineering Process)* ..... *49*
*4.3.10 Microsoft's Threat Modeling* ..... *50*
*4.3.11 CLASP (Comprehensive, Lightweight Application Security Process)* ..... *51*
*4.3.12 SQUARE (Security Quality Requirements Engineering Method)* ..... *51*
*4.3.13 MSRA (Multilateral Security Requirements Analysis)* ..... *52*
*4.3.14 SRE Methods Based on AGILE* ..... *52*
*4.3.15 SecureUML* ..... *53*
*4.3.16 UMLsec* ..... *53*
*4.3.17 Misuse case* ..... *54*
*4.3.18 MOSRE (Model-Oriented Security Requirements Engineering Framework)* ..... *56*
*4.3.19 ISSRM (Information System Security Risk Management)* ..... *57*
*4.3.20 Ontology-Based SRE Approaches* ..... *58*
4.6 Συγκριτική ανάλυση των εργαλείων μοντελοποίησης απαιτήσεων ασφαλείας ..... 72
Κεφάλαιο 5 –Εργαλεία που υποστηρίζουν τις Προσεγγίσεις SRE ..... 82
5.1 Objectiver's methodology: KAOS ..... 83
5.2 ReqView ..... 87
5.3 Microsoft's Threat Modeling Tool: ..... 90
5.4 CORAS Tool ..... 93
5.5 ST-Tool (Secure Tropos) ..... 95
5.6 Αξιολόγηση Εργαλείων ..... 100
Κεφάλαιο 6 – Συμπεράσματα ..... 108
Βιβλιογραφία ..... 111

# ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1 Η σχέση μεταξύ HATCH, PROTECT και Κουίζ ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο (Pape et al., 2020). ..... 20
Εικόνα 2 Η προηγμένη πλατφόρμα εκπαίδευσης THREAT-ARREST (Krombholz et al., 2013). ..... 22
Εικόνα 3 Κάρτες HATCH όπου διακρίνονται οι ψυχολογικές Αρχές, η επίθεση της κοινωνικής μηχανικής και ο τύπος του επιτιθέμενου. ..... 25
Εικόνα 4 HATCH: Προσαρμογή του σχεδίου έκτακτης ανάγκης και διαφυγής για το παιχνίδι. ..... 26
Εικόνα 5 KAOS Modeling with Objectiver ..... 83
Εικόνα 6 Γενικό μοτίβο στόχου ..... 84
Εικόνα 7 Γενικό μοτίβο στόχου ..... 85
Εικόνα 8 Γενικοί στόχοι: "Ασφαλές σύστημα" ..... 86
Εικόνα 9 Γενικοί στόχοι: "Μη Ασφαλές σύστημα" ..... 86
Εικόνα 10 Αρχική Οθόνη εγκατάστασης του ReqView ..... 87
Εικόνα 11 Case Scenario στο ReqView -Ρόλοι του Scenario ..... 88
Εικόνα 12 Απαιτήσεις Ασφαλείας του Use Case Scenario ..... 89
Εικόνα 13 Risks, Potential Effects and Rating ..... 89
Εικόνα 14 Αρχική οθόνη Microsoft's Threat Modeling Tool ..... 90
Εικόνα 15 Use case Διάγραμμα αρχείου TM.7 ..... 91
Εικόνα 16 Εργαλείο Μοντελοποίησης Απειλών, το οποίο χρησιμοποιεί προσέγγιση SDL ..... 92
Εικόνα 17 Δημιουργία απειλής με πιθανά ελαττώματα σχεδιασμού ..... 92
Εικόνα 18 Ένα στιγμιότυπο οθόνης της εφαρμογής CORAS ..... 94
Εικόνα 19 SWOT διάγραμμα στο CORAS Tool ..... 94
Εικόνα 20 Workspace selection ..... 96
Εικόνα 21 GUI overview ..... 97
Εικόνα 22 Sequence of views ..... 98
Εικόνα 23 Λειτουργίες σχεδίασης ..... 99

# ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

Πίνακας 1 Αναλυτικός πίνακας που συνοψίζει κάθε προσέγγιση Απαιτήσεων Ασφαλείας (SRE) και περιλαμβάνει τον σκοπό του πλαισίου, τα κύρια βήματα ή τις μεθόδους, την εστίαση εντός του SDLC, τα εργαλεία και τους περιορισμούς ..... 60
Πίνακας 2 Πίνακας σύγκρισης μεθοδολογιών για τις απαιτήσεις ασφάλειας χαρτογράφησης ..... 77
Πίνακας 3 Απαιτήσεις ασφάλειας ανά μεθοδολογία ..... 80
Πίνακας 4 Αξιολόγηση εργαλείων μοντελοποίησης απαιτήσεων ασφαλείας…… 108

## Περίληψη

Προκειμένου να αντιμετωπιστούν στην πράξη τα προβλήματα ασφάλειας και προστασίας της ιδιωτικότητας, η παρούσα εργασία επικεντρώνεται στην ανάλυση και αξιολόγηση εργαλείων που στόχο έχουν τη μοντελοποίηση απαιτήσεων ασφαλείας πληροφοριακών συστημάτων. Σε αυτή την εργασία θα αναλυθούν συγκεκριμένα εργαλεία καθώς και προκλήσεις στους τομείς της κοινωνικής μηχανικής, της διαχείρισης ασφάλειας και των τεχνολογιών ενίσχυσης της ιδιωτικής ζωής.

**Κοινωνική Μηχανική**. Παρέχεται μια επισκόπηση των υφιστάμενων εργαλείων που μπορούν να χρησιμοποιηθούν για την κοινωνική μηχανική και αναλύονται οι διαθέσιμες άμυνες έναντι της κοινωνικής μηχανικής. Τα παιχνίδια σοβαρού σκοπού προτείνονται ως ο πιο ευχάριστος τρόπος για την ευαισθητοποίηση των εργαζομένων και την περαιτέρω εκπαίδευσή τους.

**Διαχείριση Ασφάλειας**. Η διαχείριση Ασφάλειας εξετάζεται ως ένας κρίσιμος τομέας για τη διασφάλιση της προστασίας των πληροφοριών. Γι' αυτό το λόγο, αναλύονται μέθοδοι οι οποίες υποστηρίζουν τόσο τη βελτίωση της ασφάλειας σε έναν οργανισμό όσο και την αξιολόγηση των κινδύνων που ελλοχεύουν.

**Τεχνολογίες ενίσχυσης της ιδιωτικής ζωής**. Η παρούσα εργασία εξετάζει τις προκλήσεις που προκύπτουν με την ενσωμάτωση τεχνολογιών ενίσχυσης της ιδιωτικότητας από εταιρείες και χρήστες και τα εμπόδια που υπάρχουν και δυσκολεύουν τη χρήση των τεχνολογιών αυτών.

Η εργασία, επίσης, παρουσιάζει μια ολοκληρωμένη ανάλυση των πιο ευρέως διαδεδομένων μεθοδολογιών απαιτήσεων ασφαλείας, επισημαίνοντας τις μοναδικές προσεγγίσεις τους για τον καθορισμό και την ιεράρχηση των αναγκών ασφαλείας στον σχεδιασμό ενός συστήματος. Κατηγοριοποιούνται μεθοδολογίες όπως η MOSRE, η Secure Tropos, η KAOS, η GBRAM, το M-N Framework και η NFR ως προσανατολισμένες στους στόχους του συστήματος, ευθυγραμμίζοντας τις απαιτήσεις ασφάλειας με τους οργανωτικούς στόχους. Επιπλέον, αναλύονται μεθοδολογίες επικεντρωμένες στον κίνδυνο όπως η SQUARE, που δίνουν προτεραιότητα στην αξιολόγηση των απειλών ενός συστήματος. Παρά τα πλεονεκτήματα αυτών των

μεθοδολογιών, υπάρχει ένα αξιοσημείωτο κενό στην ενσωμάτωση ολοκληρωμένης ανάλυσης κινδύνου που λαμβάνει υπόψη τόσο τις πιθανές απειλές όσο και την αξία των κρίσιμων περιουσιακών στοιχείων. Τελικά, τα ευρήματα υποδεικνύουν ότι η ανάπτυξη υβριδικών προσεγγίσεων που συνδυάζουν στρατηγικές βασισμένες σε στόχους και βασισμένες στον κίνδυνο θα παράσχουν ένα πιο αποτελεσματικό και προσαρμόσιμο πλαίσιο για την αντιμετώπιση του εξελισσόμενου τοπίου των προκλήσεων ασφάλειας στα πληροφοριακά συστήματα.

## Abstract

In order to address security and privacy problems, this paper focuses on the analysis and evaluation of tools that aim to model security requirements of information systems. In this paper, specific tools as well as challenges in the areas of social engineering, security management and privacy-enhancing technologies will be analyzed.

**Social Engineering**. An overview of existing tools that can be used for social engineering is provided and the available defenses against social engineering are analyzed. "Serious" games are suggested as the most enjoyable way to raise awareness and further educate employees.

**Security Management**. is considered as a critical area for ensuring information protection. For this reason, methods that support both the improvement of security in an organization and the assessment of the risks involved are analyzed.

**Privacy-Enhancing Technologies**. This paper examines the challenges that arise with the integration of privacy-enhancing technologies by companies and users and the barriers that exist that make it difficult to use these technologies.

The paper also presents a comprehensive comparison of various security requirements methodologies, highlighting their unique approaches to defining and prioritizing security needs in system design. He categorizes methodologies such as MOSRE, Secure Tropos, KAOS, GBRAM, M-N Framework and NFR as goal-oriented, aligning security requirements with organizational goals, while contrasting them with risk-focused methodologies such as SQUARE, which give priority in threat assessment. Despite the advantages of these methodologies, there is a notable gap in incorporating comprehensive risk analysis that considers both potential threats and the value of critical assets. Ultimately, the findings suggest that the development of hybrid approaches that combine goal-based and risk-based strategies will provide a more effective and adaptable framework for addressing the evolving landscape of security challenges in information systems.

# Κεφάλαιο 1 – Εισαγωγή

## 1.1 Εισαγωγή-Θεωρητικό υπόβαθρο

Λόγω των αυξανόμενων περιστατικών παραβίασης και διαρροής δεδομένων σε μηνιαία βάση (Hill *et al.*, 2017), τα ζητήματα ασφάλειας δεδομένων και προστασίας προσωπικών πληροφοριών έχουν αναδειχθεί ως κορυφαία θέματα στην κοινωνία. Ωστόσο, η αντιμετώπιση θεμάτων ασφάλειας και της προστασίας της ιδιωτικότητας κρίνουν προσοχής. Συχνά τα όρια μεταξύ ασφάλειας και προστασίας της ιδιωτικότητας είναι ασαφή και προς τις δύο κατευθύνσεις: εάν τα χρησιμοποιούμενα κοινωνικο-τεχνικά συστήματα δεν είναι ασφαλή, όλα τα δεδομένα του χρήστη κινδυνεύουν να διαρρεύσουν εάν συμβεί οποιαδήποτε παραβίαση. Σύμφωνα με την Cloud Security Alliance, οι παραβιάσεις δεδομένων κατατάσσονται διαχρονικά ως μία από τις κορυφαίες απειλές για το υπολογιστικό νέφος. (Cloud Security Alliance, 2024) Αντίθετα, σε περίπτωση διαρροής προσωπικών δεδομένων, αυτά τα δεδομένα μπορούν επίσης να χρησιμοποιηθούν για περαιτέρω επιθέσεις σε άτομα ή στις εταιρείες τους, με επιθέσεις στο μηχανισμό «επαναφοράς κωδικού πρόσβασης» ή άλλων μέσων κοινωνικής μηχανικής.

Έχει αποδειχθεί ότι τα προβλήματα ασφάλειας και ιδιωτικότητας είναι συχνά δύσκολα και αν ακόμη υπάρχει λύση στη θεωρία ή στον ακαδημαϊκό χώρο, δεν είναι ακόμα αυτονόητο ότι οι προτεινόμενες λύσεις λειτουργούν στην πράξη. Μια προτεινόμενη λύση που είναι ασφαλής θεωρητικά, δε σημαίνει αυτόματα ότι είναι και ασφαλής στην πράξη. Αυτό ισχύει για διάφορα τεχνικά μέτρα, π.χ. κρυπτογραφικοί αλγόριθμοι των οποίων οι υλοποιήσεις μπορούν να επιτεθούν από δομές πλευρικού καναλιού (Kocher *et al.*, 2019), αλλά και για ανθρώπους που δυσκολεύονται να χρησιμοποιήσουν προγράμματα και μηχανισμούς που έχουν σχεδιαστεί από μηχανικούς (Gerber, Zimmermann and Volkamer, 2019). Για την αποτελεσματική αντιμετώπιση των προβλημάτων στην πράξη, κρίνεται απαραίτητη η συστηματική και ακριβής καταγραφή των απαιτήσεων πριν από οποιαδήποτε προσπάθεια επίλυσής τους. Στη συνέχεια αναλύονται οι συγκεκριμένες προκλήσεις στους τομείς της κοινωνικής μηχανικής, της διαχείρισης ασφάλειας και των τεχνολογιών ενίσχυσης της ιδιωτικής ζωής:

- Κοινωνική μηχανική. Η κύρια πρόκληση κατά την παραβίαση της κοινωνικής

μηχανικής είναι ότι όλες οι άμυνές της πρέπει να λαμβάνουν υπόψη την ανθρώπινη συμπεριφορά, η οποία –σε αντίθεση με τα τεχνικά συστήματα– δεν είναι γενικά ντετερμινιστική, αλλά εξαρτάται από διάφορους άλλους παράγοντες. Ενώ υπάρχει μια ποικιλία εργαλείων, τα περισσότερα από αυτά υποστηρίζουν περισσότερο επιτιθέμενους. Αυτό δεν αποτελεί ευθύνη των εργαλείων, αφού πολλά από αυτά δε σχεδιάστηκαν για επιθέσεις κοινωνικής μηχανικής. Εκτός από το μειονέκτημα από την πλευρά των εργαλείων, είναι επίσης ένα δύσκολο έργο η ευαισθητοποίηση και η εκπαίδευση των εργαζομένων, καθώς γενικά το κύριο καθήκον τους δεν είναι να καταπολεμήσουν τις επιθέσεις κοινωνικής μηχανικής. Επίσης, παρέχεται μια επισκόπηση των υφιστάμενων εργαλείων που μπορούν να χρησιμοποιηθούν για την κοινωνική μηχανική και αναλύει τις άμυνες κατά της κοινωνικής μηχανικής. Επιπλέον, προτείνονται σοβαρά παιχνίδια ως ένας πιο ευχάριστος τρόπος ευαισθητοποίησης και εκπαίδευσης των εργαζομένων.

- Διαχείριση Ασφαλείας. Λόγω της συνεχής ανάπτυξης και βελτίωσης των μεθοδολογιών της ασφάλειας υπογραμμίζεται η σημασία της χρήσης αξιόπιστων μετρήσεων για την αποτελεσματική διαχείριση της ασφάλειας, π.χ. χρησιμοποιώντας μετρήσεις που στοχεύουν να προσεγγίσουν την πραγματική κατάσταση της ασφάλειας των πληροφοριών. Δυστυχώς, η διαχείριση της ασφάλειας συχνά συνδυάζεται με τη συμμόρφωση, πράγμα που σημαίνει ότι μερικές φορές δεν εφαρμόζονται μέτρα για την αύξηση της ασφάλειας, αλλά για την απόδειξη της συμμόρφωσης προκειμένου να προβλεφθούν επιπτώσεις για ζημιές σε περίπτωση επιτυχούς επίθεσης στην εταιρεία. Αυτό σημαίνει επίσης ότι η αξιολόγηση κινδύνου ασφάλειας πρέπει να αποτελεί θεμελιώδες μέρος της διαχείρισης της ασφάλειας και συχνά απαιτεί την εφαρμογή συστημάτων διαχείρισης ασφάλειας πληροφοριών. Επομένως, αναλύονται οι συγκεκριμένες απαιτήσεις για μικρομεσαίους παρόχους ενέργειας και προτείνεται ένα σύνολο εργαλείων για την υποστήριξή τους στην αξιολόγηση των κινδύνων για την ασφάλεια και τη βελτίωση της ασφάλειάς τους. Οι μεγαλύτερες επιχειρήσεις υποστηρίζονται από μια μέθοδο συλλογής δεικτών απόδοσης κλειδιών ασφαλείας για διαφορετικές θυγατρικές και με μια μέθοδο αξιολόγησης κινδύνου για εφαρμογές σε κινητές συσκευές. Επιπλέον, ως η πιο δημοφιλής σήμερα μορφή εξωτερικής ανάθεσης, συζητείται η επιλογή ενός ασφαλούς παρόχου cloud.
- Τεχνολογίες ενίσχυσης της ιδιωτικότητας. Για τις τεχνολογίες που ενισχύουν

την ιδιωτικότητα, η κύρια πρόκληση είναι η διάδοσή τους. Συχνά οι εταιρείες δε θέλουν να ενσωματώσουν τεχνολογίες ενίσχυσης της ιδιωτικής ζωής στις υπηρεσίες τους, επειδή το επιχειρηματικό τους μοντέλο βασίζεται στη συλλογή δεδομένων των χρηστών ή πιστεύουν ότι μπορεί να χρειαστούν αργότερα τα δεδομένα που συλλέγονται ή επειδή απλά δε ξέρουν πώς να τα ενσωματώσουν χωρίς να βλάπτεται η χρηστικότητα ή η απόδοση. Από την άλλη πλευρά, ακόμη και αν υπάρχουν αυτόνομες τεχνολογίες ενίσχυσης της ιδιωτικής ζωής, η υιοθέτηση από τους χρήστες είναι αρκετά χαμηλή και ιδιαίτερα για τους μη ειδικούς μπορεί να είναι μια δύσκολη εργασία για να ενσωματωθεί στην καθημερινότητα (Gerber, Zimmermann and Volkamer, 2019). Ως εκ τούτου, οι τεχνολογίες αυτές στοχεύουν στον εντοπισμό σχετικών παραγόντων για την υιοθέτηση από τους χρήστες τεχνολογιών ενίσχυσης της ιδιωτικής τους ζωής. Εκτός αυτού, συμπεριλαμβάνονται οικονομικά κίνητρα και εμπόδια και εφαρμόζεται η προστασία της ιδιωτικότητας από το σχεδιασμό στις περιπτώσεις χρήσης του ηλεκτρονικού εμπορίου και του Διαδικτύου των πραγμάτων.

### 1.2 Κίνητρα και Ερευνητικές Ερωτήσεις

Το κύριο κίνητρο πίσω από αυτήν την εργασία είναι να γεφυρωθεί το χάσμα μεταξύ των θεωρητικών πλαισίων ασφαλείας και των πρακτικών τους εφαρμογών, συγκεκριμένα με τον εντοπισμό, την ανάλυση και την αξιολόγηση εργαλείων που μπορούν να μοντελοποιήσουν αποτελεσματικά τις απαιτήσεις ασφάλειας. Καθώς οι οργανισμοί προσπαθούν να προστατεύσουν τα δεδομένα τους και να προστατεύσουν το απόρρητο των χρηστών, ιδιαίτερα ενόψει ολοένα και πιο εξελιγμένων επιθέσεων, υπάρχει ανάγκη για ολοκληρωμένα εργαλεία που μπορούν να αντιμετωπίσουν τόσο την τεχνική όσο και την ανθρώπινη διάσταση της ασφάλειας. Αυτή η έρευνα καθοδηγείται από τον στόχο να εξοπλίσει τους επαγγελματίες ασφαλείας και τους οργανισμούς με μια σαφέστερη κατανόηση των διαθέσιμων εργαλείων και μεθόδων, μαζί με τα δυνατά τους σημεία, τις αδυναμίες και τα κατάλληλα πλαίσια εφαρμογής.

Τα ακόλουθα ερευνητικά ερωτήματα καθοδηγούν αυτή τη μελέτη:

- *Ποια εργαλεία και μέθοδοι είναι διαθέσιμα επί του παρόντος για τη*

*μοντελοποίηση απαιτήσεων ασφάλειας, ιδιαίτερα στους τομείς της κοινωνικής μηχανικής, της διαχείρισης ασφάλειας και των τεχνολογιών που βελτιώνουν την προστασία της ιδιωτικότητας;*

- *Πόσο αποτελεσματικά είναι αυτά τα εργαλεία για την αντιμετώπιση συγκεκριμένων προκλήσεων σε κάθε τομέα, λαμβάνοντας υπόψη την πρακτική εφαρμογή και την ευθυγράμμιση με τις ανάγκες του οργανισμού;*
- *Ποια κενά υπάρχουν μεταξύ των τρεχουσών δυνατοτήτων αυτών των εργαλείων και των απαιτήσεων που είναι απαραίτητες για την αποτελεσματική προστασία της ασφάλειας και της ιδιωτικής ζωής, και πώς θα μπορούσαν να γεφυρωθούν αυτά τα κενά;*

Απαντώντας σε αυτά τα ερωτήματα, αυτή η εργασία στοχεύει να χαρτογραφήσει το τοπίο των εργαλείων μοντελοποίησης απαιτήσεων ασφάλειας, να αξιολογήσει την αποτελεσματικότητά τους και να εντοπίσει κρίσιμους τομείς για μελλοντική βελτίωση.

### 1.3 Μεθοδολογία διπλωματικής εργασίας

Για την αντιμετώπιση των ερευνητικών ερωτημάτων, χρησιμοποιήθηκε μια προσέγγιση μεικτών μεθόδων, που συνδυάζει μια περιεκτική βιβλιογραφική ανασκόπηση με συγκριτική ανάλυση και πρακτικές περιπτωσιολογικές μελέτες. Αυτή η μεθοδολογία διαρθρώνεται σε διάφορες βασικές φάσεις:

- Ανασκόπηση βιβλιογραφίας: Πραγματοποιήθηκε συστηματική ανασκόπηση βιβλιογραφίας για τον εντοπισμό και την κατηγοριοποίηση των υφιστάμενων εργαλείων και μεθοδολογιών που χρησιμοποιούνται για τη μοντελοποίηση των απαιτήσεων ασφαλείας. Οι πηγές περιλάμβαναν ακαδημαϊκές εργασίες, εκθέσεις του κλάδου και περιπτωσιολογικές μελέτες, διασφαλίζοντας ένα ευρύ φάσμα προοπτικών.

- Ανάλυση και αξιολόγηση εργαλείων: Τα εργαλεία που προσδιορίστηκαν από τη βιβλιογραφία αξιολογήθηκαν με βάση προκαθορισμένα κριτήρια, όπως η ευκολία χρήσης, η τεχνική ευρωστία, η προσαρμοστικότητα σε διαφορετικά οργανωτικά πλαίσια και η συνολική αποτελεσματικότητα στην εκπλήρωση των απαιτήσεων ασφαλείας. Διεξήχθη συγκριτική ανάλυση σε βασικούς τομείς

ασφάλειας – κοινωνική μηχανική, διαχείριση ασφάλειας και τεχνολογίες ενίσχυσης της ιδιωτικής ζωής – για να αντληθούν πληροφορίες σχετικά με τα σχετικά δυνατά και αδύνατα σημεία κάθε εργαλείου.

- Πρακτική εφαρμογή: Για να γεφυρωθεί η θεωρία με την πράξη, η φάση αξιολόγησης περιλάμβανε μελέτες περιπτώσεων που απεικονίζουν τον τρόπο απόδοσης επιλεγμένων εργαλείων σε σενάρια για την καλύτερη αξιολόγηση των εργαλείων. Αυτές οι περιπτωσιολογικές μελέτες εξέτασαν ειδικά τις πρακτικές προκλήσεις σε κάθε τομέα και τα εμπόδια στην υιοθέτηση τεχνολογιών που βελτιώνουν την ιδιωτικότητα.

## 1.4 Πεδίο και Σημασία

Το εύρος της διπλωματικής εργασίας δομείται γύρω από τρεις διακριτούς, αλλά αλληλένδετους τομείς απαιτήσεων ασφάλειας και της προστασίας της ιδιωτικότητας: κοινωνική μηχανική, διαχείριση ασφάλειας και τεχνολογίες ενίσχυσης της ιδιωτικότητας. Εστιάζοντας σε αυτούς τους τομείς, η μελέτη παρέχει μια ολοκληρωμένη επισκόπηση των διαθέσιμων εργαλείων, τα οποία κατηγοριοποιούνται ανά τομέα εφαρμογής και αξιολογούνται ως προς την ικανότητά τους να μοντελοποιούν απαιτήσεις σε πολύπλοκα σενάρια ασφαλείας.
Αυτή η εργασία έχει σημαντική αξία τόσο σε ακαδημαϊκό όσο και σε πρακτικό πλαίσιο. Για τον ακαδημαϊκό κόσμο, ενοποιεί μια σειρά εργαλείων μοντελοποίησης ασφάλειας και προστασίας της ιδιωτικότητας, παρέχοντας έναν πόρο για τους ερευνητές που αναζητούν να αναπτύξουν ή να βελτιώσουν αυτές τις μεθόδους. Για τους επαγγελματίες, τα ευρήματα προσφέρουν χρήσιμες πληροφορίες για την επιλογή των κατάλληλων εργαλείων για την κάλυψη συγκεκριμένων αναγκών ασφαλείας, ιδιαίτερα σε κλάδους που χειρίζονται ευαίσθητα δεδομένα, όπως τα οικονομικά, η υγειονομική περίθαλψη και τα προσωπικά δεδομένα.

## 1.5 Ερευνητικό Κενό και Συνεισφορά

Ενώ προηγούμενες μελέτες έχουν διερευνήσει μεμονωμένες πτυχές της μοντελοποίησης των απαιτήσεων ασφαλείας, υπάρχει ένα αξιοσημείωτο κενό σε

ολοκληρωμένες αξιολογήσεις που καλύπτουν πολλούς τομείς ασφάλειας, λαμβάνοντας υπόψη τόσο τεχνικούς όσο και ανθρώπινους παράγοντες. Αυτή η έρευνα αντιμετωπίζει αυτό το κενό παρέχοντας μια ολιστική ανάλυση εργαλείων σε τρεις κρίσιμους τομείς ασφάλειας, δίνοντας έμφαση στην πρακτική εφαρμογή τους και αξιολογώντας την αποτελεσματικότητα τους. Επιπλέον, αυτή η μελέτη υπογραμμίζει προκλήσεις που δεν έχουν διερευνηθεί, όπως η περιορισμένη υιοθέτηση τεχνολογιών ενίσχυσης της ιδιωτικής ζωής, και προτείνει στρατηγικές για την αντιμετώπιση αυτών των ζητημάτων, όπως το gamification για ευαισθητοποίηση στην άμυνα κοινωνικής μηχανικής.

Με τον συστηματικό εντοπισμό, ανάλυση και αξιολόγηση αυτών των εργαλείων, αυτή η εργασία συμβάλλει στο ευρύτερο πεδίο της μηχανικής απαιτήσεων ασφάλειας, προσφέροντας μια δομημένη προσέγγιση σε επαγγελματίες και ερευνητές να επιλέγουν και να εφαρμόζουν εργαλεία ευθυγραμμισμένα με τους στόχους ασφαλείας.

## Κεφάλαιο 2 – Κοινωνική μηχανική

Ο Ευρωπαϊκός Οργανισμός για την Κυβερνοασφάλεια (ENISA) ορίζει την κοινωνική μηχανική ως μια τεχνική που εκμεταλλεύεται τις ανθρώπινες αδυναμίες και στοχεύει να χειραγωγήσει τους ανθρώπους ώστε να παραβιάσουν τις συνήθεις διαδικασίες ασφαλείας. Στις περισσότερες περιπτώσεις, οι επιτιθέμενοι με κακόβουλο κίνητρο στοχεύουν να αποκτήσουν πρόσβαση στις εμπορικές, οικονομικές, ευαίσθητες ή ιδιωτικές πληροφορίες του θύματός τους προκειμένου να τις χρησιμοποιήσουν εναντίον τους ή να προκαλέσουν βλάβη με άλλο τρόπο (Aladawy, Beckers and Pape, 2018).

«Η μεγαλύτερη απειλή για την ασφάλεια μιας εταιρείας δεν είναι ένας ιός υπολογιστή, ένα μη επιδιορθωμένο κενό σε ένα βασικό πρόγραμμα ή ένα κακώς εγκατεστημένο τείχος προστασίας. Στην πραγματικότητα, η μεγαλύτερη απειλή θα μπορούσε να είναι οι παράγοντες που χρησιμοποιούν την τεχνολογία. Οι επιθέσεις κοινωνικής μηχανικής αντιπροσωπεύουν μια συνεχή απειλή για τους υπαλλήλους των οργανισμών. Με μια ευρεία διαθεσιμότητα διαφορετικών εργαλείων και πηγών πληροφοριών (Beckers *et al.*, 2017), είναι μια πρόκληση να ενημερώνονται για τις πρόσφατες επιθέσεις σε εργαζόμενους, καθώς αναπτύσσονται νέες επιθέσεις και εμφανίζονται τροποποιήσεις γνωστών σεναρίων επιθέσεων. Για παράδειγμα, οι κακόβουλοι χρήστες έχουν ήδη διαφοροποιήσει την προσέγγισή τους και ζητούν επίσης αγορά και μεταφορά διαδικτυακών δωροκαρτών σε υπαλλήλους. Επιπλέον, οι κακόβουλοι χρήστες βασίζουν τις επιθέσεις τους στην κατάσταση ειδήσεων, όπως ο COVID-19, τα Ransomware (Tarik Saleh., 2020) ή σε ψεύτικους ιστότοπους (BBC News., 2020). Επιπλέον, μια επίθεση κοινωνικής μηχανικής είναι συχνά μόνο το πρώτο βήμα μιας μεγαλύτερης επίθεσης, στην οποία ο εισβολέας χρησιμοποιεί τις πληροφορίες που αποκτά εκεί για περαιτέρω επιθέσεις. Μια επίθεση κοινωνικής μηχανικής από μόνη της αποτελείται από πολλαπλές φάσεις. Στην πρώτη φάση, ο εισβολέας διεξάγει έρευνα για να εντοπίσει άτομα με πρόσβαση στις πληροφορίες που επιθυμεί. Η δεύτερη φάση επικεντρώνεται στην εύρεση όσο το δυνατόν περισσότερων πληροφοριών για αυτά τα άτομα για να βοηθήσει τον εισβολέα να χειραγωγήσει τα θύματά του. Με βάση αυτές τις πληροφορίες, ο εισβολέας αρχίζει να χτίζει μια σχέση με το θύμα (φάση προσχήματος). Στη συνέχεια, ο εισβολέας εκμεταλλεύεται τη χτισμένη εμπιστοσύνη στη σχέση και αξιολογεί τις πληροφορίες που συγκεντρώθηκαν στη φάση μετά την εκμετάλλευση. Ωστόσο, οι περισσότεροι οργανισμοί έχουν δυσκολίες να

αντιμετωπίσουν αυτό το ζήτημα επαρκώς. Υποστηρίζεται ότι θα πρέπει να εφαρμόζονται τεχνολογικά αντίμετρα όποτε είναι δυνατόν. Ωστόσο, κανένα υλικό ή λογισμικό δεν είναι σε θέση να προστατεύσει πλήρως έναν οργανισμό από επιθέσεις βασισμένες στην κοινωνική μηχανική. Ωστόσο οι περισσότερες στρατηγικές άμυνας δημιουργούνται από ειδικούς σε θέματα ασφάλειας πληροφορικής που έχουν ένα ισχυρό υπόβαθρο στα πληροφοριακά συστήματα.

### 2.1 Εργαλεία και αμυντικοί μηχανισμοί της Κοινωνικής Μηχανικής

Ακόμα κι αν οι εταιρείες γνωρίζουν τις επιθέσεις κοινωνικής μηχανικής, έχουν μόνο περιορισμένο αριθμό εργαλείων διαθέσιμα για να τις υποστηρίξουν. Αυτός μπορεί να είναι ένας από τους λόγους της προαναφερθείσας προτίμησης των πολύ τυποποιημένων προϊόντων ασφαλείας. Παρακάτω θα συζητηθούν τα ευρήματα μιας έρευνας για εργαλεία κοινωνικής μηχανικής. Προκειμένου να παρέχεται μια επισκόπηση περαιτέρω λύσεων, εκτός από εκπαιδεύσεις και εκστρατείες ευαισθητοποίησης, θα συγκριθούν αμυντικοί μηχανισμοί που προτείνονται στην ασφάλεια πληροφορικής και στην ανθρώπινη συμπεριφορά. Στη διαδικασία της κοινωνικής μηχανικής, οι δύο πρώτες φάσεις βασίζονται σε μεγάλο βαθμό στη συλλογή πληροφοριών. Για το σκοπό αυτό, διατίθενται διάφορα εργαλεία. Από τη μία πλευρά, αυτά τα εργαλεία μπορούν να χρησιμοποιηθούν από έναν κοινωνικό μηχανικό για να προετοιμάσουν τα άτομα για μια επίθεση. Από την άλλη πλευρά, αυτά τα εργαλεία θα μπορούσαν επίσης να προσφέρουν σε έναν οργανισμό μια εξαιρετική εναλλακτική λύση για τη δοκιμή αμυντικών μηχανισμών ή την εκπαίδευση ευαισθητοποίησης, καθώς επιτρέπουν την ανάλυση πιθανών τρωτών σημείων. Για το σκοπό αυτό, πραγματοποιήθηκε μια δομημένη έρευνα σχετικά με τις δυνατότητες των εργαλείων και βρέθηκαν τα εξής:

- ταξινόμηση των υπαρχόντων εργαλείων σχετικά με κατηγορίες όπως ο προτεινόμενος σκοπός, η τιμή, η αντιληπτή χρηστικότητα, η οπτικοποίηση των αποτελεσμάτων,
- μια έρευνα τύπου πληροφοριών που ανακτώνται από τα εργαλεία σχετικά με πληροφορίες ή με τους υπαλλήλους μιας εταιρείας και τα κανάλια επικοινωνίας τους, καθώς και σχετικές πληροφορίες π.χ. εταιρικές πολιτικές
- μια αντιστοίχιση εργαλείων σε ορισμένους τύπους επιθέσεων κοινωνικής μηχανικής (ψάρεμα, δόλωμα, πλαστοπροσωπία).

Για τη μελέτη της χαρτογράφησης, πρώτα για κάθε τύπο πληροφοριών (π.χ. email,

φίλοι, (ιδιωτική) τοποθεσία, συνάδελφοι, τοποθεσία εταιρείας) και κάθε εξεταζόμενη επίθεση κοινωνικής μηχανικής (ψάρεμα, δόλωμα, πλαστοπροσωπία) καθορίστηκε αν ήταν χρήσιμη για εκτέλεση μιας επίθεσης. Στη συνέχεια, για καθένα από τα εργαλεία που ερευνήθηκαν (π.χ. Cree-py, Maltego) ή ιστότοπους (π.χ. LinkedIn, Xing) διερευνήθηκε στη βάση των ποιων πληροφορίων μπορούσαν να παρέχουν. Συνδυάζοντας όλα αυτά τα δεδομένα, φαίνεται ποια από τα εργαλεία μπορεί να είναι χρήσιμα και για ποια από τις επιθέσεις κοινωνικής μηχανικής.

Ρίχνοντας μια πιο προσεκτική ματιά, μπορεί να παρατηρηθεί ότι ο μόνος τύπος πληροφοριών που τα εργαλεία κοινωνικής μηχανικής δεν παρέχουν σήμερα είναι το λεγόμενο εταιρικό lingo, οι συντομογραφίες και συγκεκριμένες λέξεις που χρησιμοποιούνται σε μια εταιρεία ή τομέα. Ωστόσο, αναλύοντας τις αναρτήσεις σε ιστότοπους κοινωνικών δικτύων με προσανατολισμό τις επιχειρήσεις, μπορεί να είναι θέμα χρόνου να εφαρμοστεί η μηχανική εκμάθηση και η ανάλυση μεγάλων δεδομένων θα καλύψει αυτό το κενό. Περαιτέρω αποτελέσματα της έρευνάς ήταν ότι κανένα από τα ερευνητικά εργαλεία ή ιστότοπους δεν πρόσφερε συγκεκριμένη βοήθεια για την άμυνα έναντι επιθέσεων κοινωνικής μηχανικής. Κανένα από τα εργαλεία δεν παρείχε κανενός είδους εκτίμηση κινδύνου για τις συλλεγόμενες πληροφορίες σχετικά με τους ίδιους τους υπαλλήλους ή για τους επικεφαλής πληροφοριών (ασφάλειας). Επιπλέον, κανένα από τα εργαλεία δε μπόρεσε να προτείνει την κατάργηση ορισμένων πληροφοριών ή να προτείνει την προσθήκη ψεύτικων ή ψευδών πληροφοριών στις δημοσίως καταχωρισμένες πληροφορίες. Οι πλαστές πληροφορίες θα επέτρεπαν τον εύκολο εντοπισμό επιθέσεων κοινωνικής μηχανικής αργότερα, οι οποίες θα μπορούσαν να βασίστηκαν σε αυτές. Επιπλέον, τα περισσότερα από τα εργαλεία ήταν εύχρηστα, ανοίγοντας το πεδίο όχι μόνο σε ειδικευμένους επαγγελματίες, αλλά και σε μη ειδικούς.

### 2.2 Χαρτογράφηση των αμυντικών μηχανισμών

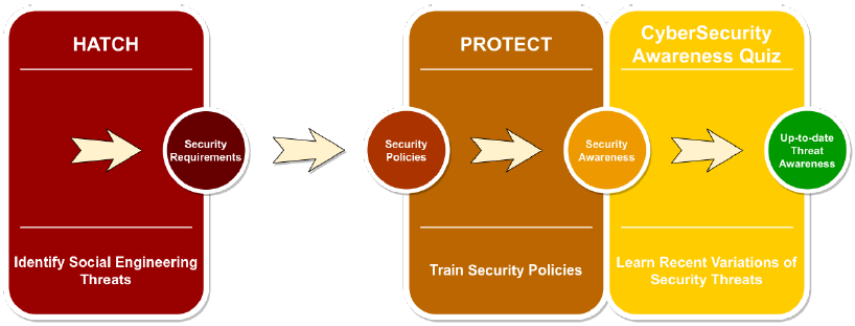
Όπως διαπιστώθηκε στην προηγούμενη ενότητα, τα περισσότερα εργαλεία υποστηρίζουν τον κακόβουλο χρήστη. Ως εκ τούτου, αξίζει μια πιο προσεκτική ματιά σε διαφορετικές άμυνες ενάντια στην κοινωνική μηχανική. Για το σκοπό αυτό, ερευνήθηκε η κατάσταση της τεχνολογίας από την επιστήμη των υπολογιστών, δηλαδή από την άποψη της ασφάλειας πληροφορικής. Σύμφωνα με τους (Kruger and Kearney, 2006), η συνειδητοποίηση της κοινωνικής μηχανικής θεωρήθηκε ότι αποτελείται από τις τρεις διαστάσεις γνώση, στάση και συμπεριφορά. Ως εκ τούτου, οι προσδιορισμένοι αμυντικοί μηχανισμοί χαρτογραφήθηκαν σε αυτές τις τρεις διαστάσεις. Επιπλέον, οι

μηχανισμοί άμυνας από την ασφάλεια πληροφορικής και την κοινωνική ψυχολογία μπορούν να αντιστοιχιστούν μεταξύ τους. Κατά τη σύγκριση των διαφορετικών μηχανισμών, είναι ορατό ότι οι μηχανισμοί άμυνας στο πλαίσιο της ασφάλειας πληροφορικής δεν έχουν ακόμη αξιοποιήσει πλήρως τις δυνατότητές τους. Στο πλαίσιο της διάστασης της στάσης, αποτελούνται κυρίως από εκπαιδεύσεις και προγράμματα ευαισθητοποίησης σχετικά με την ασφάλεια και τον καθορισμό των απαραίτητων πολιτικών ασφαλείας. Συγκριτικά, η κοινωνική ψυχολογία προσφέρει με προειδοποίηση ένα μηχανισμό παρόμοιο με την ευαισθητοποίηση. Ωστόσο, η γνώση της πειθούς (συμπεριλαμβανομένης της γνώσης σχετικά με τις στρατηγικές πειθούς) και η ενίσχυση της στάσης (η οποία βασίζεται σε μια καλή γνώση σχετικά με τις πολιτικές ασφαλείας και τις συνέπειές της για τη δημιουργία μιας ενισχυτικής νοοτροπίας) υπερβαίνουν κατά πολύ τους περιγραφόμενους αμυντικούς μηχανισμούς από την ασφάλεια πληροφορικής. Τελευταίο αλλά όχι λιγότερο σημαντικό, οι προσεκτικά σχεδιασμένοι έλεγχοι πραγματικότητας θα μπορούσαν να βοηθήσουν τους ανθρώπους να συνειδητοποιήσουν ότι στην πραγματικότητα είναι ευάλωτοι. Ωστόσο, οι πραγματικοί έλεγχοι πρέπει να διεξάγονται πολύ προσεκτικά, προκειμένου να αποφευχθεί η απογοήτευση των ατόμων που υπόκεινται σε αυτούς και να δημιουργηθούν παρόμοια αποτελέσματα με αυτά των δοκιμών διείσδυσης κοινωνικής μηχανικής. Από άποψη συμπεριφοράς, οι έλεγχοι (συμπεριλαμβανομένου του ελέγχου ασφαλείας ειδικά για την κοινωνική μηχανική) είναι ένας τυπικός αμυντικός μηχανισμός στη διάσταση της συμπεριφοράς. Ωστόσο, δεδομένου ότι γενικά οι επαγγελματίες αξιολόγησης ασφαλείας εστιάζουν έντονα στον εντοπισμό επιθέσεων και όχι σε οποιοδήποτε άλλο είδος εκπαίδευσης ή πραγματικούς ελέγχους των θυμάτων τους, πρέπει να ληφθεί μέριμνα ώστε να μην αποθαρρύνονται τα άτομα της εταιρείας. Από την άλλη, από κοινωνική ψυχολογική άποψη, η συνεχής εκπαίδευση που βάζει τους υπαλλήλους σε παρόμοια κατάσταση, είναι ένας κοινωνικός μηχανισμός που θα τους οδηγούσε στην αποφυγή παρορμητικών αποφάσεων, που συχνά ωφελούν τους επιτιθέμενους εισβολείς και θα μπορούσε να βοηθήσει τους υπαλλήλους, ώστε να επιμείνουν σε μια πραγματική επίθεση. Συνολικά, η ανάλυση του χάσματος δείχνει ότι οι μηχανισμοί άμυνας από την ασφάλεια πληροφορικής μπορούν να βελτιωθούν, και ειδικότερα να λάβουμε υπόψη τη διάσταση της συμπεριφοράς. Μια άλλη συνεισφορά της βιβλιογραφικής έρευνας είναι η ανασκόπηση των ψυχολογικών αρχών που υποστηρίζουν τις παρορμητικές αποφάσεις και αποφεύγουν τη βαθύτερη συλλογιστική. Ταξινομώντας τα παραπάνω με την εφαρμοσιμότητα των

(ψυχολογικών) μηχανισμών άμυνας, μπορεί να διαπιστωθεί εύκολα ότι οι επιθέσεις που εκμεταλλεύονται την εξουσία, την κοινωνική απόδειξη ή την απόσπαση της προσοχής εμπίπτουν στο μηχανισμό διάστασης της στάσης, ενώ οι επιθέσεις που βασίζονται στη συμπάθεια, την ομοιότητα, την εξαπάτηση, την ανταπόδοση και η συνέπεια απαιτούν την εκπαίδευση και των δύο διαστάσεων, στάσης και συμπεριφοράς. Ως αποτέλεσμα, συνιστούμε την ενσωμάτωση γνώσεων πειθούς και εκπαίδευσης αντίστασης σε εκπαιδεύσεις ή εκστρατείες ευαισθητοποίησης για την καταπολέμηση της κοινωνικής μηχανικής. Επιπλέον, η ενίσχυση της στάσης έχει αποδειχθεί ότι είναι αποτελεσματική στη μείωση της αποτελεσματικότητας των προσπαθειών πειθούς και θα μπορούσε να είναι ζωτικής σημασίας όταν στους χρήστες δε δείχνουν μόνο τις αποτυχίες τους αλλά και τις επιτυχημένες προσπάθειές τους να αποτρέψουν μια επίθεση κοινωνικής μηχανικής.

## 2.3 Μέθοδοι για την κοινωνική μηχανική

Για να αντιμετωπισθούν τα ζητήματα που εντοπίστηκαν και αναπτύχθηκαν στις προηγούμενες ενότητες, σχεδιάσαμε τρία σοβαρά παιχνίδια. Τα σοβαρά παιχνίδια έχουν χτίσει τη φήμη ότι κάνουν τους υπαλλήλους των εταιρειών να συμμετέχουν σε δραστηριότητες ασφάλειας με ευχάριστο και βιώσιμο τρόπο. Διατηρώντας ακόμη έναν παιχνιδιάρικο χαρακτήρα, χρησιμοποιούνται σοβαρά παιχνίδια για π. σολ. εκπαίδευση ασφάλειας και ανάλυση απειλών. Δεδομένου ότι εκείνη την εποχή, κανένα από τα παιχνίδια δεν αναπτύχθηκε ειδικά για κοινωνική μηχανική, και τα τρία παιχνίδια που προτείνονται σε αυτήν την ενότητα, στοχεύουν στην αντιμετώπιση της κοινωνικής μηχανικής, αν και με διαφορετικό τρόπο (Εικόνα 1). Ξεκινά μια σύντομη επισκόπηση των παιχνιδιών και τη σχέση τους σε αυτή την ενότητα. Περιγράφονται αναλυτικότερα παρακάτω.

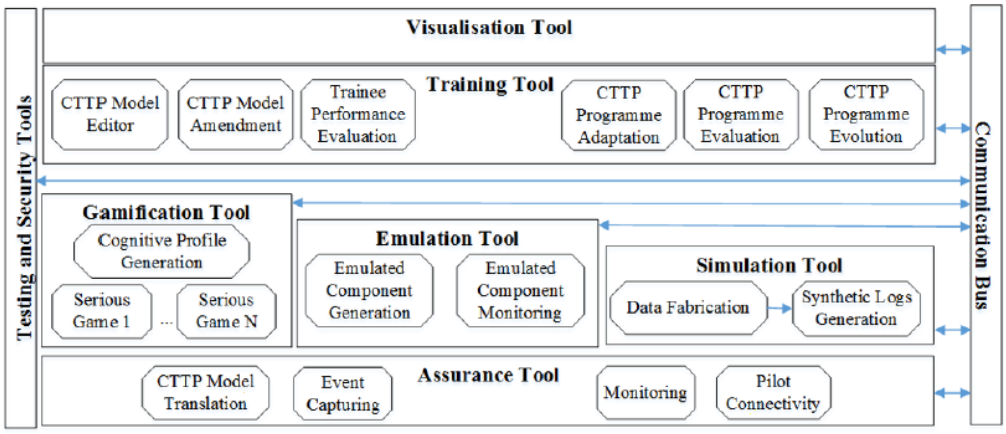



**Εικόνα 1 Η σχέση μεταξύ HATCH, PROTECT και Κουίζ ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο (Pape et al., 2020).**

Το HATCH (Beckers and Pape, 2016) στοχεύει στον εντοπισμό απειλών κοινωνικής μηχανικής και την ανάπτυξη τους σύμφωνα με τις απαιτήσεις ασφάλειας. Εφόσον παρατηρήθηκε ότι τα περισσότερα εργαλεία κοινωνικής μηχανικής δε βοηθούν τους αμυνόμενους, η κύρια ιδέα αυτού του παιχνιδιού είναι να υποστηρίξει τους αμυνόμενους σε μια συστηματική πρόκληση απειλής. Οι παίκτες αναπτύσσουν επιθέσεις στους συναδέλφους τους με βάση τις υπάρχουσες γνώσεις τους για τις διαδικασίες εργασίας, τις δεξιότητες και τις προτιμήσεις τους. Ως αποτέλεσμα, δημιουργείται μια λίστα με πιθανές απειλές SE που μπορούν να χρησιμοποιηθούν για τη βελτίωση των διαδικασιών εργασίας και των πολιτικών ασφαλείας. Το πλεονέκτημα έναντι της ανάλυσης απειλών από ειδικούς είναι ότι οι υπάλληλοι ενός τμήματος ή μιας εταιρείας γνωρίζουν πολύ καλά τις πραγματικές διαδικασίες της εργασίας τους, επομένως είναι πιο εύκολο να τους εκπαιδεύσουν στην κοινωνική μηχανική παρά να βρουν και να εκπαιδεύσουν ειδικούς σε όλες τις διαθέσιμες διαδικασίες εργασίας. Επιπλέον, όταν ερωτηθούν για πραγματικές διαδικασίες, πολλοί εργαζόμενοι πιθανότατα δε θα αποκαλύψουν τι κάνουν πραγματικά, αλλά θα επιδείξουν τις γνώσεις τους σχετικά με το πώς φαίνεται η διαδικασία. Ενώ η μεθοδολογία HATCH βοηθά στην ανάπτυξη και τη βελτίωση των πολιτικών ασφαλείας, το PROTECT (Tselios, Tsolis and Athanatos, 2020) στοχεύει να προσφέρει στους εργαζόμενους ένα περιβάλλον όπου μπορούν να μάθουν και να εκπαιδεύσουν την εφαρμογή άμυνας. Μακροπρόθεσμα, το παιχνίδι αυξάνει την ευαισθητοποίηση των εργαζομένων σε θέματα ασφάλειας και βοηθά επίσης στην ενίσχυση της στάσης τους απέναντι σε αυτά. Δεδομένου ότι το PROTECT βασίζεται σε πολιτικές ασφαλείας, είναι φυσικά κάπως γενικό και δε μπορεί να αντιμετωπίσει όλες τις πρόσφατες παραλλαγές ορισμένων επιθέσεων. Επομένως, η ιδέα του Cyber Security Awareness Quiz (Pape *et al.*, 2020) είναι να υπάρχει ένα κουίζ βασισμένο στις τελευταίες επιθέσεις και τις παραλλαγές τους. Αφού εμφανιστεί μια νέα επίθεση ή παραλλαγή, το μόνο που χρειάζεται είναι η ανάπτυξη μιας νέας ερώτησης η οποία στη συνέχεια μπορεί να χρησιμοποιηθεί αμέσως στο κουίζ. Εκτός από την αλληλεπίδραση των τριών παιχνιδιών, η οποία ήδη παρέχει μια αλυσίδα εργαλείων για την άμυνα ενάντια στην κοινωνική μηχανική, είναι επίσης σημαντικό να επιτραπεί η ενσωμάτωση των παιχνιδιών σε μια γενικότερη πλατφόρμα εκπαίδευσης, όπως η προηγμένη εκπαίδευση THREAT-ARREST (Krombholz *et al.*, 2013) πλατφόρμα. Το έργο THREAT-ARREST έλαβε χρηματοδότηση από το πρόγραμμα έρευνας και καινοτομίας Horizon 2020 της Ευρωπαϊκής Ένωσης και στοχεύει στην ανάπτυξη μιας προηγμένης εκπαιδευτικής πλατφόρμας που

ενσωματώνει δυνατότητες εξομοίωσης, προσομοίωσης, σοβαρού παιχνιδιού και οπτικοποίησης για να προετοιμάσει επαρκώς τα ενδιαφερόμενα μέρη με διαφορετικούς τύπους ευθύνης και επίπεδα τεχνογνωσίας στην υπεράσπιση συστήματα και οργανισμοί στον κυβερνοχώρο υψηλού κινδύνου για την αντιμετώπιση προηγμένων, γνωστών και νέων επιθέσεων στον κυβερνοχώρο.

Η ενσωμάτωση στην πλατφόρμα επιτρέπει τον συνδυασμό των προσπαθειών στο σοβαρό παιχνίδι με άλλα στοιχεία όπως η εξομοίωση και το εργαλείο προσομοίωσης. Αυτό συμβάλλει στη συνεχή αξιολόγηση της απόδοσης των μεμονωμένων εκπαιδευομένων και της αποτελεσματικότητας των εκπαιδευτικών προγραμμάτων. Μέσα στην πλατφόρμα για κάθε εκπαιδευόμενο τα αποτελέσματα των σοβαρών παιχνιδιών, η εξομοίωση, η προσομοίωση και το εκπαιδευτικό εργαλείο συγκεντρώνονται για να εντοπίσουν πιθανά κενά στη γνώση ή την ευαισθητοποίηση του υπαλλήλου. Εάν εντοπιστούν κενά γνώσης, μπορεί να ελεγχθεί εάν υπάρχει ήδη εκπαίδευση στο συγκεκριμένο θέμα ως σοβαρό παιχνίδι, προσομοίωση ή εξομοίωση του συστήματος εμβέλειας στον κυβερνοχώρο. Εάν δε μπορεί να εντοπιστεί κατάλληλη εκπαίδευση, αυτό μπορεί να υποδηλώνει την ανάγκη παραγωγής για μια νέα εκπαίδευση, προσαρμοσμένη στις οργανωτικές ανάγκες και τους τύπους των ασκουμένων.




**Εικόνα 2 Η προηγμένη πλατφόρμα εκπαίδευσης THREAT-ARREST (Krombholz et al., 2013).**

## 2.4 HATCH

To Hack and Trick Capricious Humans (HATCH) είναι ένα φυσικό (επιτραπέζιο) σοβαρό παιχνίδι για την κοινωνική μηχανική. Το παιχνίδι είναι διαθέσιμο σε δύο εκδόσεις, ένα πραγματικό σενάριο και μια γενική έκδοση. Κάθε έκδοση του παιχνιδιού επιδιώκει έναν ελαφρώς διαφορετικό στόχο: Το σενάριο της πραγματικής ζωής

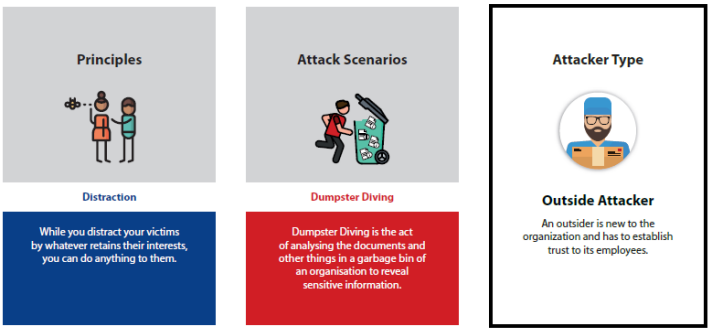
στοχεύει στην εξαγωγή των απαιτήσεων ασφάλειας κοινωνικής μηχανικής μιας εταιρείας ή ενός από τα τμήματα της. Επομένως, μοντελοποιείται ένα πραγματικό περιβάλλον και οι παίκτες επιτίθενται στους συναδέλφους τους προκειμένου να εντοπίσουν πραγματικούς φορείς επίθεσης. Η γενική έκδοση του παιχνιδιού στοχεύει να αυξήσει την ευαισθητοποίηση των παικτών για απειλές κοινωνικής μηχανικής και να τους εκπαιδεύσει στον εντοπισμό αυτού του είδους επιθέσεων. Προκειμένου να μην εκτίθενται άσκοπα και να κατηγορούνται οι συνάδελφοι κατά τη διάρκεια μιας εκπαιδευτικής συνεδρίας, βασίζεται σε ένα εικονικό σενάριο με πρόσωπα ως θύματα επίθεσης (Sebastian Pape and Dennis-Kenji Kipker., 2020). Το αρχικό σενάριο αποτελείται από μια διάταξη ενός γραφείου μεσαίου μεγέθους και δέκα υπαλλήλους ως πρόσωπα, τυπωμένα σε κάρτες που περιέχουν φανταστικές περιγραφές τους. Εξ ορισμού, τα πρόσωπα είναι φανταστικά, ωστόσο, ρεαλιστικές περιγραφές ενδιαφερομένων ή μελλοντικών χρηστών μιας υπηρεσίας ή προϊόντος, που έχουν ονόματα, θέσεις εργασίας, συναισθήματα, στόχους, ορισμένες ανάγκες και απαιτήσεις (Shamal Faily and Ivan Flechais., 2011). Και στις δύο εκδόσεις χρησιμοποιούνται δύο τράπουλες: ψυχολογικές αρχές και επιθέσεις κοινωνικής μηχανικής. Οι κάρτες ψυχολογικών αρχών δηλώνουν και περιγράφουν ανθρώπινες συμπεριφορές ή πρότυπα που συχνά εκμεταλλεύονται οι κοινωνικοί μηχανικοί, όπως για παράδειγμα: «Απόσπαση της προσοχής - ενώ αποσπάτε την προσοχή των θυμάτων σας με οτιδήποτε διατηρεί τα ενδιαφέροντά τους, μπορείτε να τους κάνετε τα πάντα». Τα πρότυπα ψυχολογικής αρχής βασίζονται στην εργασία των (Stajano and Wilson, 2011), οι οποίοι περιγράφουν γιατί οι επιθέσεις σε θύματα απάτης μπορεί να πετύχουν. Επεκτείναμε το σύνολο των προτύπων συμπεριφοράς με μοτίβα που βρέθηκαν στην εργασία για την κοινωνική μηχανική από τους (Radha Gulati., 2003) και (Peltier, 2006). Από την άλλη πλευρά, οι κάρτες κοινωνικής μηχανικής ονομάζουν και ορίζουν μερικές από τις πιο κοινές επιθέσεις κοινωνικής μηχανικής, για παράδειγμα την κατάδυση σε σκουπίδια, που είναι «η πράξη της ανάλυσης εγγράφων και άλλων πραγμάτων σε έναν κάδο σκουπιδιών ενός οργανισμού για την αποκάλυψη ευαίσθητων πληροφοριών». Οι χρησιμοποιούμενες τεχνικές επίθεσης βασίζονται κυρίως στο έργο των (Krombholz *et al.*, 2013). Και πάλι, επεκτείναμε το σύνολο των τεχνικών επίθεσης με τη δουλειά των (Radha Gulati., 2003), (Peltier, 2006) και (Chitrey, Singh and Singh, 2012). Όταν παίζει το παιχνίδι, κάθε παίκτης τραβάει μια κάρτα ψυχολογικής αρχής και τρεις κάρτες επίθεσης κοινωνικής μηχανικής και διαβάζει τις αντίστοιχες περιγραφές. Κάθε παίκτης έχει τότε το καθήκον να επιλέξει ένα θύμα4 που ταιριάζει στην κάρτα ψυχολογικής

αρχής και να επεξεργαστεί μια επίθεση χρησιμοποιώντας μία από τις κάρτες επίθεσης κοινωνικής μηχανικής που ταιριάζει καλύτερα με το θύμα και την ψυχολογική αρχή. Οι παίκτες με τη σειρά τους αποκαλύπτουν τις κάρτες τους και περιγράφουν την επίθεση κοινωνικής μηχανικής που σκέφτηκαν. Άλλοι παίκτες συζητούν την προτεινόμενη επίθεση και τους πόντους απονομής για τη σκοπιμότητα και τη βιωσιμότητα της επίθεσης και βαθμολογούν εάν είναι συμβατή με τις περιγραφές των φύλλων αυτού του παίκτη. Η συνολική βαθμολογία κάθε παίκτη υπολογίζεται με το τέλος της βαθμολογίας του ομίλου και τον παίκτη με την υψηλότερη βαθμολογία κερδίζει το παιχνίδι. Στο τέλος του παιχνιδιού, όλοι οι παίκτες αναλογίζονται εν συντομία τις προτεινόμενες επιθέσεις κοινωνικής μηχανικής και αντλούν πιθανές απειλές για την ασφάλεια. Η παρακάτω λίστα παρέχει μια επισκόπηση των βημάτων του παιχνιδιού:

1. Κάθε παίκτης τραβάει ένα φύλλο από την τράπουλα των αρχών ανθρώπινης συμπεριφοράς, π.χ. σολ. την αρχή «Ανάγκη και Απληστία».
2. Κάθε παίκτης τραβάει τρία φύλλα από την τράπουλα των τεχνικών επίθεσης κοινωνικής μηχανικής, π.χ. phishing.
3. Κάθε παίκτης αναπτύσσει μια επίθεση με στόχο μια από τις περσόνες του σεναρίου με βάση τα χαρτιά που έχουν τραβηχτεί.
4. Κάθε παίκτης παρουσιάζει την επίθεσή του/της στην ομάδα και τα άλλα μέλη της ομάδας συζητούν εάν η επίθεση είναι εφικτή.
5. Οι παίκτες παίρνουν πόντους με βάση το πόσο βιώσιμη είναι η επίθεσή τους και αν η επίθεση ήταν σύμφωνη με τα τραβηχτά φύλλα. Ο παίκτης με τους περισσότερους πόντους κερδίζει το παιχνίδι.
6. Ως απολογισμός, συζητούνται οι αντιληπτές απειλές και οι παίκτες αντανακλούν τις επιθέσεις τους.

Η Εικόνα 3 δείχνει δείγματα των διαθέσιμων καρτών. Όπως συζητήθηκε, το παιχνίδι μπορεί να παιχτεί είτε με ένα φανταστικό (εικονικό) σενάριο, είτε με ένα ρεαλιστικό σενάριο που αντικατοπτρίζει το πραγματικό περιβάλλον εργασίας. Περιγράφονται και οι δύο τύποι σεναρίων στη συνέχεια με περισσότερες λεπτομέρειες.


(a) Card Version 1 [16]




(b) Card Version 2

**Εικόνα 3 Κάρτες HATCH όπου διακρίνονται οι ψυχολογικές Αρχές, η επίθεση της κοινωνικής μηχανικής και ο τύπος του επιτιθέμενου.**

### 2.4.1 Πραγματικό σενάριο

Ο βασικός τρόπος παιχνιδιού του HATCH έχει ήδη περιγραφεί παραπάνω. Για το ρεαλιστικό σενάριο, ο στόχος ήταν να προσδιοριστεί μια λίστα απειλών κοινωνικής μηχανικής. Οι παίκτες θα πρέπει να αναπτύξουν επιθέσεις στους συναδέλφους τους με βάση τις υπάρχουσες γνώσεις τους για τις διαδικασίες εργασίας, τις δεξιότητες και τις προτιμήσεις τους. Προκειμένου να ενισχυθεί η δημιουργικότητα, αναπτύσσεται ένα σχέδιο παιχνιδιού με βάση ένα υπάρχον σχέδιο έκτακτης ανάγκης και διαφυγής. Τα σχέδια έκτακτης ανάγκης και εκκένωσης είναι μια καλή πηγή για αξιοποίηση, καθώς περιλαμβάνουν ένα σχέδιο τοποθεσίας που ταιριάζει στις ανάγκες μας και η διάταξή τους είναι τυποποιημένη (International Organization for Standardization (ISO)., 2009). Επιπλέον, είναι δημόσια διαθέσιμα στους διαδρόμους, πρέπει να ενημερώνονται συχνά και –ανάλογα με τον τύπο του κτιρίου– στις περισσότερες χώρες απαιτούνται από τη νομοθεσία. Με αυτόν τον τρόπο, μπορεί να δημιουργηθεί ένα σχέδιο παιχνιδιού με χαμηλή προσπάθεια, προσθέτοντας απλώς εικόνες ή εικονίδια των συναδέλφων και ορισμένα στοιχεία. Εκτός από την εκπαίδευση και την ευαισθητοποίηση, το αποτέλεσμα είναι μια λίστα με πιθανές απειλές κοινωνικής μηχανικής που μπορούν να

χρησιμοποιηθούν για τη βελτίωση των διαδικασιών εργασίας και των πολιτικών ασφάλειας.


(a) Emergency and Escape Plan (b) Adapted Game Plan

**Εικόνα 4 HATCH: Προσαρμογή του σχεδίου έκτακτης ανάγκης και διαφυγής για το παιχνίδι.**

Το πλεονέκτημα έναντι της ανάλυσης απειλών από ειδικούς είναι ότι οι υπάλληλοι ενός τμήματος ή μιας εταιρείας γνωρίζουν πολύ καλά τις πραγματικές διαδικασίες εργασίας, επομένως είναι πιο εύκολο να τους εκπαιδεύσουν στην κοινωνική μηχανική παρά να μελετήσουν ειδικούς όλες τις διαδικασίες εργασίας. Οι Beckers και Pape (Beckers and Pape, 2016) έδειξαν ότι το ρεαλιστικό σενάριο ήταν χρήσιμο για την πρόκληση επιθέσεων με συγκεκριμένο πλαίσιο, χρησιμοποιώντας τη γνώση του τομέα των παικτών και τις παρατηρήσεις και τις γνώσεις τους σχετικά με την καθημερινή εργασία και διαδικασίες.

## 2.5 Επιθέσεις ευρείας κλίμακας

### 2.5.1 Phishing

Το phishing ξεχωρίζει ως η πιο διαδεδομένη μορφή κοινωνικής μηχανικής, που περιλαμβάνει περίπου το 77% όλων των επιθέσεων που βασίζονται σε κοινωνικά δίκτυα, με ανησυχητικούς 37 εκατομμύρια χρήστες να αναφέρουν απόπειρες phishing το 2013. Αυτή η δόλια τακτική περιλαμβάνει απόπειρα κλοπής προσωπικών ή ευαίσθητων πληροφοριών πλαστοπροσωπώντας ένα πηγάδι -γνωστή ή αξιόπιστη οντότητα. Ενώ το email παραμένει η κύρια πλατφόρμα για επιθέσεις phishing, οι δράστες εκμεταλλεύονται επίσης άλλα κανάλια επικοινωνίας, όπως τηλεφωνικές κλήσεις, μηνύματα κειμένου, φαξ και μέσα κοινωνικής δικτύωσης.

Πολλές ευρέως διαδεδομένες προσπάθειες ηλεκτρονικού ψαρέματος είναι σχετικά απλές και μπορούν να αναγνωριστούν από τους περισσότερους χρήστες υπολογιστών ως δόλιες. Ωστόσο, οι τακτικές phishing εξελίσσονται, με τους εισβολείς να χρησιμοποιούν διάφορες στρατηγικές είτε για να κάνουν τα email τους να φαίνονται νόμιμα είτε για να ζητήσουν άμεση δράση από το θύμα. Για παράδειγμα, οι εισβολείς

μπορούν να πλαστογραφήσουν διευθύνσεις email για να μιμηθούν αξιόπιστους οργανισμούς όπως τράπεζες, εταιρείες κοινής ωφέλειας ή κρατικούς φορείς. Επιπλέον, εκμεταλλεύονται σημαντικά ειδησεογραφικά γεγονότα για να χειραγωγήσουν τους παραλήπτες ώστε να αναλάβουν δράση, όπως η δωρεά χρημάτων ή η υπογραφή αναφορών που σχετίζονται με την εκδήλωση. Παρά την αυξανόμενη πολυπλοκότητα των καμπανιών ηλεκτρονικού "ψαρέματος" (phishing), αρκετοί κοινοί δείκτες μπορούν να βοηθήσουν στον εντοπισμό των μηνυμάτων ηλεκτρονικού ψαρέματος:

- Τα μηνύματα είναι αυτόκλητα και στερούνται εξατομικευμένων πληροφοριών.
- Τα μηνύματα ηλεκτρονικού ταχυδρομείου περιέχουν αόριστο περιεχόμενο και μπορεί να περιλαμβάνουν κακή γραμματική, ορθογραφικά λάθη ή περίεργες φράσεις.
- Συχνά παρουσιάζουν μη ρεαλιστικές προσφορές ή απειλές με την αίσθηση του επείγοντος.
- Η διεύθυνση email του αποστολέα μπορεί να μοιάζει με αυτή ενός νόμιμου οργανισμού, αλλά διαφέρει ελαφρώς.
- Τα μηνύματα ηλεκτρονικού ψαρέματος ενδέχεται να περιέχουν εσφαλμένες ή χαμηλής ποιότητας εκδόσεις του λογότυπου ενός οργανισμού, μαζί με συνδέσμους προς παραπλανητικούς ιστότοπους.

Τα μηνύματα ηλεκτρονικού ψαρέματος συνήθως προτρέπουν τους χρήστες να κάνουν κλικ σε κακόβουλους συνδέσμους, να ανοίξουν συνημμένα ή να συμμετάσχουν σε ανταλλαγές ηλεκτρονικού ταχυδρομείου για να αποκαλύψουν εμπιστευτικές πληροφορίες. Αυτοί οι σύνδεσμοι μπορεί να φαίνεται ότι οδηγούν σε νόμιμους ιστότοπους, αλλά ανακατευθύνουν τους χρήστες σε δόλιους ιστότοπους, μια τεχνική γνωστή ως συσκότιση. Κατά την επίσκεψη σε αυτούς τους ιστότοπους, τα θύματα ενδέχεται να αποκαλύψουν εν αγνοία τους ευαίσθητα δεδομένα ή να κατεβάσουν κατά λάθος κακόβουλο λογισμικό. Ομοίως, τα συνημμένα σε μηνύματα ηλεκτρονικού ψαρέματος συχνά περιέχουν κακόβουλο λογισμικό, που αποτελεί σημαντική απειλή για την ασφάλεια στον κυβερνοχώρο των χρηστών. Ακόμη πιο προηγμένα συστήματα phishing μπορεί να φτάσουν στο να κατευθύνουν τα θύματα σε ένα σχεδόν τέλειο αντίγραφο ενός γνήσιου ιστότοπου. Αυτά τα αντίγραφα είναι σχολαστικά κατασκευασμένα για να παραπλανούν τα άτομα να εισάγουν τα ονόματα χρήστη, τους κωδικούς πρόσβασης ή άλλες ευαίσθητες λεπτομέρειες.

### 2.5.2 Baiting

Μια άλλη μέθοδος εκτεταμένης επίθεσης περιλαμβάνει το δόλωμα των χρηστών μέσω διαδικτυακών διαφημίσεων και ιστότοπων. Παρόμοια με το phishing, αυτές οι τακτικές παρουσιάζουν συχνά δελεαστικές προσφορές που φαίνονται πολύ καλές για να είναι αληθινές ή επείγουσες προειδοποιήσεις. Για παράδειγμα, ορισμένοι ιστότοποι προσφέρουν δωρεάν λήψεις ή ροή βίντεο, όπως ταινίες ή τηλεοπτικές εκπομπές, ενώ άλλοι εμφανίζουν αναδυόμενα παράθυρα που ισχυρίζονται ότι έχουν εντοπίσει προβλήματα με το σύστημα του χρήστη, προτρέποντάς τους να κάνουν κλικ για λύση. Ακολουθώντας αυτούς τους δολωματικούς συνδέσμους, οι χρήστες ενδέχεται να αποκαλύπτουν άθελά τους προσωπικές πληροφορίες ή να έχουν αυτόματη λήψη κακόβουλου λογισμικού στις συσκευές τους. Ενώ ορισμένες από αυτές τις επιθέσεις μπορεί να είναι στοιχειώδεις, άλλες είναι εξαιρετικά εξελιγμένες και επίμονες. Μια άλλη ευρέως διαδεδομένη μέθοδος δολώματος περιλαμβάνει τη χρήση «δωρεάν» σημείων πρόσβασης WiFi, αν και απαιτεί ένα ορισμένο επίπεδο τεχνικής εξειδίκευσης. Σε αυτό το σενάριο, ο εισβολέας δημιουργεί ένα σημείο πρόσβασης WiFi που διαφημίζεται σαφώς ως "δωρεάν", συνήθως σε δημόσιους χώρους όπως καφετέριες, αεροδρόμια και λόμπι ξενοδοχείων. Ενώ παρέχουν στους ανυποψίαστους χρήστες πρόσβαση στο διαδίκτυο, αυτά τα hotspot επιτρέπουν στους εισβολείς να παρεμποδίζουν τα δεδομένα που μεταδίδονται μέσω της σύνδεσης χρησιμοποιώντας μια τεχνική γνωστή ως επίθεση "man-in-the-middle". Αυτή η δυνατότητα παρακολούθησης επεκτείνεται σε ασφαλείς συνδέσεις, συμπεριλαμβανομένων εκείνων που χρησιμοποιούνται για διαδικτυακές τραπεζικές υπηρεσίες. Επιπλέον, οι εισβολείς μπορούν να αναπτύξουν εξ αποστάσεως κακόβουλο λογισμικό στα συστήματα των θυμάτων, επιτρέποντας έτσι μια ποικιλία πρόσθετων εκμεταλλεύσεων.

Το Shylock, ένα εξελιγμένο και δύσκολα εντοπίσιμο κακόβουλο λογισμικό, αποτελεί σημαντική απειλή επιτρέποντας στους εγκληματίες του κυβερνοχώρου να κλέβουν τα διαπιστευτήρια των θυμάτων και να διευκολύνουν τα οικονομικά εγκλήματα στον κυβερνοχώρο. Παρά τις προσπάθειες επιβολής του νόμου στο Ηνωμένο Βασίλειο στα μέσα του 2014 που διέκοψαν με επιτυχία τις λειτουργίες του Shylock και μείωσαν την επικράτηση του, συνεχίζει να χρησιμοποιείται από εγκληματίες. Στοχεύοντας ιδιαίτερα το Ηνωμένο Βασίλειο, ο Shylock μόλυνε περίπου το 61% όλων των παραβιασμένων ιστοσελίδων στο απόγειό του, με την πλειοψηφία να ανήκει στον τομέα λιανικής.

Αυτό το κακόβουλο λογισμικό διαδίδεται μέσω διαφόρων καναλιών, συμπεριλαμβανομένης της ενσωμάτωσης κακόβουλου κώδικα σε διαδικτυακές διαφημίσεις που εμφανίζονται σε νόμιμους ιστότοπους, καθώς και μέσω της άμεσης στόχευσης και παραβίασης δημοφιλών ιστότοπων. Ορισμένοι παραβιασμένοι ιστότοποι ενδέχεται να εμφανίζουν μηνύματα που ζητούν από τους χρήστες να εγκαταστήσουν πρόσθετα που λείπουν, τα οποία, όταν κάνουν κλικ, έχουν ως αποτέλεσμα την ακούσια εγκατάσταση του Shylock στο σύστημα του θύματος.
Μόλις ενεργοποιηθεί, το Shylock είναι σε θέση να μεταδίδει κρυφά στον εισβολέα τυχόν δεδομένα που έχουν εισαχθεί σε έναν υπολογιστή, περιλαμβάνοντας διαπιστευτήρια ιστότοπου και άλλες ευαίσθητες πληροφορίες. Μπορεί ακόμη και να προσομοιώσει ένα κατασκευασμένο παράθυρο "chat" σε τραπεζικούς ιστότοπους, επιτρέποντας στους εισβολείς να εμπλακούν απευθείας με τα θύματα, ενθαρρύνοντάς τα έτσι να αποκαλύψουν πρόσθετες ευαίσθητες πληροφορίες - μια τακτική παρόμοια με ένα δευτερεύον επίπεδο κοινωνικής μηχανικής.

### 2.5.3 Spear Phishing

Το Spear phishing αντιπροσωπεύει μια πιο εκλεπτυσμένη προσέγγιση που χρησιμοποιείται από εξελιγμένους επιτιθέμενους, που χαρακτηρίζεται από ένα περιορισμένο κοινό-στόχο και προσαρμοσμένα μηνύματα για να ενισχύσουν την ελκυστικότητα και τη φαινομενική νομιμότητά τους. Αυτές οι επιθέσεις συχνά επικεντρώνονται σε συγκεκριμένα άτομα σε έναν συγκεκριμένο επιχειρηματικό τομέα, εταιρεία, τμήμα ή σε άτομα που μοιράζονται κοινά χαρακτηριστικά. Σε ορισμένες περιπτώσεις, ένα email ηλεκτρονικού ψαρέματος με δόρυ μπορεί να απευθύνεται σε ένα μεμονωμένο άτομο που θεωρείται πολύτιμο για τον εισβολέα, μειώνοντας έτσι τον αριθμό των πιθανών θυμάτων αυξάνοντας παράλληλα την πιθανότητα επιτυχίας. Ενώ ορισμένες απόπειρες ψαρέματος με δόρυ μπορεί να εξακολουθούν να παρουσιάζουν εμφανή σημάδια εξαπάτησης, άλλες είναι σχολαστικά κατασκευασμένες και είναι εξαιρετικά δύσκολο να εντοπιστούν ως κακόβουλες.
Οι ειδικευμένοι επιτιθέμενοι επενδύουν χρόνο στην έρευνα των στόχων τους για να βελτιστοποιήσουν τις πιθανότητες επιτυχίας τους. Συλλέγουν πληροφορίες για τον οργανισμό, συμπεριλαμβανομένων οργανογραμμάτων και στοιχείων επικοινωνίας, που συμπληρώνονται από πληροφορίες που προέρχονται από τα προφίλ των θυμάτων στα μέσα κοινωνικής δικτύωσης και δημόσια διαθέσιμα δεδομένα. Αντί να χρησιμοποιούν γενικούς χαιρετισμούς, τα μηνύματα ηλεκτρονικού ψαρέματος συχνά

απευθύνονται στους παραλήπτες ονομαστικά και μπορεί να περιλαμβάνουν εξατομικευμένες λεπτομέρειες. Οι εισβολείς αξιοποιούν τις ταυτότητες αξιόπιστων τρίτων μερών, όπως οι προμηθευτές, για να εκμεταλλευτούν τις υπάρχουσες σχέσεις εμπιστοσύνης. Μπορούν να αντιγράψουν τις διευθύνσεις ηλεκτρονικού ταχυδρομείου αυτών των τρίτων μερών και να χρησιμοποιήσουν την έρευνά τους για να πλαστοπροσωπήσουν άτομα που είναι γνωστά στα επιδιωκόμενα θύματα, πιθανώς ακόμη και να επιχειρήσουν να παραβιάσουν τους λογαριασμούς email αυτών των τρίτων.

### 2.5.3 Επιθέσεις Watering Hole

Οι επιθέσεις που μοιάζουν με τακτικές δολώματος, εκμεταλλεύονται την εμπιστοσύνη που σχετίζεται με αξιόπιστους ιστότοπους για να διεισδύσουν στους υπολογιστές των θυμάτων. Αυτές οι επιθέσεις συνήθως επιδεικνύουν υψηλότερο επίπεδο πολυπλοκότητας σε σύγκριση με άλλες τεχνικές κοινωνικής μηχανικής, που συχνά απαιτούν έναν βαθμό τεχνικής εξειδίκευσης. Σε μια επίθεση με νερό, ένας αξιόπιστος ιστότοπος τρίτου μέρους παραβιάζεται για να παραδώσει κακόβουλο κώδικα στον υπολογιστή του θύματος.

Παρόμοια με άλλες στοχευμένες στρατηγικές κοινωνικής μηχανικής, οι εισβολείς διεξάγουν διεξοδική έρευνα στα θύματά τους για να εντοπίσουν αξιόπιστους ιστότοπους που είναι πιθανό να επισκεφτούν. Αυτοί οι ιστότοποι μπορεί να περιλαμβάνουν πύλες προμηθευτών, δημοσιεύσεις του κλάδου, δεξαμενές σκέψης ή οποιονδήποτε άλλο ιστότοπο κρίνεται σχετικός με τα συμφέροντα του θύματος. Μόλις εντοπιστεί ένας κατάλληλος ιστότοπος (ή ιστότοποι), ο εισβολέας προχωρά στον εντοπισμό τρωτών σημείων στον διακομιστή που φιλοξενεί τον ιστότοπο. Με την ανακάλυψη μιας ευπάθειας, ο εισβολέας εισάγει κώδικα που διευκολύνει τη λήψη κακόβουλου λογισμικού στον υπολογιστή του θύματος, μερικές φορές χωρίς καμία αλληλεπίδραση που απαιτείται από το θύμα (αναφέρεται ως επίθεση "drive-by").

### 2.5.4 Επίθεση σε πολλαπλά μέτωπα

Ένας αποφασισμένος εισβολέας μπορεί να χρησιμοποιήσει μια προσέγγιση πολλαπλών επιπέδων μαζί με πρόσθετες τακτικές για να ενισχύσει την εμπιστοσύνη του στόχου του ή να προκαλέσει σύγχυση, μεγιστοποιώντας έτσι τις πιθανότητες επιτυχίας. Αν και είναι κάπως αδιάκριτος, ένας εισβολέας θα μπορούσε να ξεκινήσει τυχαίες τηλεφωνικές κλήσεις μέσα σε έναν οργανισμό, παριστάνοντας ως προσωπικό

υποστήριξης IT (ενδεχομένως χρησιμοποιώντας πραγματικό όνομα που λαμβάνεται από τα μέσα κοινωνικής δικτύωσης). Στόχος τους είναι να εντοπίσουν ένα θύμα που αντιμετωπίζει ένα πραγματικό πρόβλημα πληροφορικής. Υποτίθεται ότι βοηθούν τον χρήστη στην επίλυση του προβλήματος, τον χειραγωγούν ώστε να αποκαλύψουν διαπιστευτήρια σύνδεσης, κωδικούς πρόσβασης ή άλλες ευαίσθητες πληροφορίες, οι οποίες μπορούν να βοηθήσουν στην παραβίαση του υπολογιστή τους.

Εναλλακτικά, ο εισβολέας μπορεί να μεταμφιεστεί σε υψηλόβαθμο στέλεχος, ζητώντας επειγόντως από το θύμα να στείλει ένα σημαντικό (και εμπιστευτικό) έγγραφο στην προσωπική του διεύθυνση email, επικαλούμενος την αδυναμία πρόσβασης στον λογαριασμό εργασίας του. Και στα δύο σενάρια, το θύμα μπορεί να αισθάνεται ότι πιέζεται να συμμορφωθεί με τα αιτήματα, φοβούμενο τις συνέπειες για την ανάκριση κάποιου που φαίνεται να διαθέτει ανώτερες γνώσεις (υποστήριξη πληροφορικής) ή εξουσία (το στέλεχος). Η άρνηση συμμόρφωσης θα μπορούσε ενδεχομένως να έχει αρνητικές συνέπειες για το θύμα.

Ορισμένοι επιτιθέμενοι μπορεί να χρησιμοποιούν ακόμη πιο εξελιγμένες τακτικές. Αυτές οι περίτεχνες επιθέσεις, που συχνά προορίζονται για στόχους με πρόσβαση σε πολύτιμες πληροφορίες, όπως τα διευθυντικά στελέχη, είναι γνωστές ως «Whalebaiting» και αντιπροσωπεύουν μια μορφή επίθεσης Spear Phishing. Ένα τυπικό παράδειγμα τέτοιας επίθεσης δίνεται στη συνέχεια.

Ως μέρος μιας αξιολόγησης ευπάθειας για έναν οργανισμό, ένας αξιολογητής διεξήγαγε συλλογή πληροφοριών και αποκάλυψε ευαίσθητες λεπτομέρειες όπως τοποθεσίες διακομιστών, διευθύνσεις IP, διευθύνσεις email, αριθμούς τηλεφώνου, φυσικές διευθύνσεις, διακομιστές αλληλογραφίας, ονόματα υπαλλήλων, τίτλοι και άλλα. Επιπλέον, μέσω του Facebook, ο αξιολογητής έλαβε προσωπικές πληροφορίες για τον Διευθύνοντα Σύμβουλο, συμπεριλαμβανομένου του αγαπημένου του εστιατορίου, της αθλητικής ομάδας και της συμμετοχής του σε δραστηριότητες συγκέντρωσης χρημάτων για τον καρκίνο.

Χρησιμοποιώντας αυτές τις πληροφορίες που συγκεντρώθηκαν, ο υπεύθυνος κάλεσε τον Διευθύνοντα Σύμβουλο, παρουσιάζοντας τον έρανο από μια φιλανθρωπική οργάνωση για τον καρκίνο με την οποία ο Διευθύνων Σύμβουλος είχε προηγουμένως αλληλεπιδράσει. Ο υπεύθυνος ενημέρωσε τον Διευθύνοντα Σύμβουλο για μια κλήρωση που διοργάνωσε η φιλανθρωπική οργάνωση, προσφέροντας έπαθλα όπως εισιτήρια για έναν αγώνα της αγαπημένης του αθλητικής ομάδας και δείπνο στο εστιατόριο της προτίμησής του. Ενδιαφερόμενος, ο Διευθύνων Σύμβουλος συμφώνησε

να λάβει ένα PDF που θα περιέχει περαιτέρω λεπτομέρειες σχετικά με τη συγκέντρωση κεφαλαίων και την κλήρωση. Είναι αξιοσημείωτο ότι ο υπεύθυνος έπεισε μάλιστα τον Διευθύνοντα Σύμβουλο να αποκαλύψει την έκδοση του Adobe Reader που χρησιμοποιούσε.
Στη συνέχεια, ο υπεύθυνος έστειλε το αρχείο PDF στον Διευθύνοντα Σύμβουλο, το οποίο, κατά το άνοιγμα, οδήγησε στην εγκατάσταση κακόβουλου λογισμικού στον υπολογιστή του Διευθύνοντος Συμβούλου, παρέχοντας μη εξουσιοδοτημένη πρόσβαση στο σύστημά του.

### 2.5.5 Physical baiting

Ένας εισβολέας μπορεί επίσης να χρησιμοποιήσει υλικό ως δόλωμα για να στοχεύσει είτε ένα άτομο είτε μια ομάδα. Συνήθως, αυτή η μέθοδος κοινωνικής μηχανικής χρησιμοποιείται από πιο προηγμένους επιτιθέμενους που εστιάζουν σε έναν συγκεκριμένο τομέα, οργανισμό ή άτομο. Μια συνήθης τακτική είναι να αφήνετε έναν τύπο ψηφιακών μέσων, όπως μια μονάδα flash USB, CD ή DVD, χωρίς επίβλεψη σε μια τοποθεσία όπου συχνάζει το θύμα που επιθυμείτε, όπως ένα πάρκινγκ, που συχνά φέρει ετικέτα με δελεαστικό περιεχόμενο. Ο στόχος είναι να το παραλάβει το θύμα και να το χρησιμοποιήσει σε προσωπικό ή υπολογιστή εργασίας, μολύνοντας άθελά του τον υπολογιστή με κακόβουλο λογισμικό.
Μια άλλη προσέγγιση περιλαμβάνει το φυσικό δόλωμα σε συνέδρια ή παρόμοιες εκδηλώσεις, όπου ο εισβολέας μπορεί να διανείμει δωρεάν μονάδες USB ή να παρέχει πληροφορίες σε ψηφιακά μέσα, τα οποία είναι κρυφά φορτωμένα με κακόβουλο λογισμικό.

### 2.5.6 Τρόποι αντιμετώπισης απειλών

Τεχνικές λύσεις όπως φίλτρα ανεπιθύμητης αλληλογραφίας, λογισμικό προστασίας από ιούς και αποκλεισμός γνωστών ιστότοπων ηλεκτρονικού ψαρέματος μπορούν να παρέχουν κάποιο επίπεδο προστασίας έναντι αυτών των επιθέσεων. Ωστόσο, αποφασισμένοι κοινωνικοί μηχανικοί θα βρουν συχνά τρόπους να παρακάμψουν αυτές τις άμυνες. Επομένως, η πιο αποτελεσματική στρατηγική πρόληψης κατά της κοινωνικής μηχανικής είναι η εκπαίδευση και η ευαισθητοποίηση των χρηστών:

- Εκπαίδευση των χρηστών σχετικά με τα σημάδια των μηνυμάτων ηλεκτρονικού "ψαρέματος" (phishing), με πόρους που διατίθενται από το Cyber Streetwise και το Get Safe Online.
- Χρήση πόρων από το Cyber Security Information Sharing Partnership (CiSP) για να αναζήτηση συμβουλών και βελτίωση την ευαισθητοποίηση των χρηστών.
- Διεξαγωγή συνεδρίων ευαισθητοποίησης των χρηστών, πιθανώς ως μέρος προγραμμάτων εκπαίδευσης ή εισαγωγής, που συμπεριλαμβάνονται επιδείξεις επιτυχημένων επιθέσεων κοινωνικής μηχανικής.
- Ενθάρρυνση των χρηστών να επαληθεύουν ασυνήθιστα αιτήματα ή μηνύματα καλώντας τον αποστολέα σε έναν επιβεβαιωμένο αριθμό.
- Ενημέρωση των χρηστών για την παρουσία τους στο διαδίκτυο και συμβουλή να είναι προσεκτικοί σχετικά με τις πληροφορίες που μοιράζονται στα μέσα κοινωνικής δικτύωσης.
- Αξιολόγηση του όγκου των δημοσίως διαθέσιμων πληροφοριών σχετικά με τον οργανισμό σας που θα μπορούσαν να αξιοποιηθούν σε μια επίθεση κοινωνικής μηχανικής.
- Εφαρμογή πολιτικών για τον μετριασμό του κινδύνου επιθέσεων ηλεκτρονικού ψαρέματος, όπως η μη αποστολή ευαίσθητων πληροφοριών εκτός του δικτύου του οργανισμού και διασφάλιση ότι οι χρήστες αισθάνονται σίγουροι ότι ακολουθούν αυτούς τους κανόνες.
- Ενθάρρυνση των χρηστών να αναφέρουν τυχόν ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου ή απόπειρες κοινωνικής μηχανικής σε συναδέλφους και υποστήριξη πληροφορικής.
- Διαμοιρασμός πληροφοριών σχετικά με πιθανές προσπάθειες κοινωνικής μηχανικής με άλλους οργανισμούς μέσω του CiSP.
- Προετοιμασία για την πιθανότητα ενός επιτυχημένου συμβιβασμού και να επιβεβαίωση ότι υπάρχουν σχέδια αντιμετώπισης συμβάντων και αποκατάστασης καταστροφών.

- Συμμόρφωση με καθιερωμένα πλαίσια κυβερνοασφάλειας, όπως τα "10 βήματα για την ασφάλεια στον κυβερνοχώρο" και τα "20 κρίσιμοι έλεγχοι για την άμυνα στον κυβερνοχώρο" για να βελτιώσετε τη συνολική στάση της κυβερνοασφάλειας, συμπεριλαμβανομένης της άμυνας έναντι επιθέσεων κοινωνικής μηχανικής.

# Κεφάλαιο 3 – Απαιτήσεις και μηχανική ασφάλειας

Οι Απαιτήσεις Ασφαλείας είναι οι περιορισμοί στις λειτουργικές απαιτήσεις του συστήματος στο πλαίσιο των απαραίτητων στόχων ασφαλείας (El-Attar, 2012). Είναι οι περιορισμοί στις λειτουργίες του συστήματος που λειτουργούν σε έναν ή και περισσότερους στόχους ασφαλείας. Με άλλα λόγια, αυτοί είναι οι στόχοι ασφάλειας που πρέπει να ικανοποιούνται στο πλαίσιο του περιβάλλοντος του συστήματος και όχι στην εφαρμογή μέτρων και πολιτικών ασφαλείας. Είναι δυναμικής φύσης και εξελίσσονται καθώς αναπτύσσεται το λογισμικό. Οι περισσότεροι από τους ερευνητές τις ταξινομούν ως μη λειτουργικές απαιτήσεις, επειδή δεν έχουν ξεκάθαρα κριτήρια ναι/όχι για τις προδιαγραφές και την ικανοποίησή τους.

Τα Κοινά Κριτήρια (CC99) ορίζουν τις απαιτήσεις ασφαλείας ως «η βελτίωση των στόχων ασφάλειας πληροφορικής σε τεχνικές απαιτήσεις για τη διασφάλιση της ασφάλειας και της διασφάλισης του συστήματος και του περιβάλλοντος του» (El-Attar, 2012). Οι περισσότεροι από τους επαγγελματίες ασφαλείας μπερδεύουν τις απαιτήσεις ασφάλειας με αρχιτεκτονικούς μηχανισμούς ασφαλείας, όπως κωδικούς πρόσβασης, τεχνικές κρυπτογράφησης, τείχη προστασίας, ελέγχους πρόσβασης, επιβάλλοντας έτσι περιττούς περιορισμούς ασφαλείας στις απαιτήσεις συστημάτων. Οι ερευνητές υποστήριξαν ότι η εξέταση των απαιτήσεων ασφαλείας μαζί με τις λειτουργικές απαιτήσεις τείνει να ενσωματώνει λύσεις ασφάλειας στο σύστημα αρκετά νωρίς, αποφεύγοντας έτσι σοβαρά ελαττώματα ασφαλείας κατά τις πρώτες φάσεις του SDLC (El-Attar, 2014).

Η μηχανική απαιτήσεων ασφαλείας είναι η διαδικασία εξαγωγής, ανάλυσης και καθορισμού των απαιτήσεων ασφαλείας για το σύστημα. Περιλαμβάνει τη χρήση επαναλαμβανόμενων διαδικασιών και συστηματικών κατευθυντήριων γραμμών για να διασφαλιστεί ότι το σύνολο των καθορισμένων απαιτήσεων ασφαλείας είναι πλήρες, συνεπές, κατανοητό και επαληθεύσιμο. Οι SRE παρέχουν τεχνικές, μεθόδους και κατευθυντήριες γραμμές για την αντιμετώπιση θεμάτων ασφάλειας κατά τα πρώτα στάδια της διαδικασίας ανάπτυξης λογισμικού (Banerjee, Banerjee and D. Murarka, 2014). Οι προσεγγίσεις SRE είναι οι διαθέσιμες μέθοδοι/πλαίσια/μοντέλα, που χρησιμοποιούν αυτές τις τεχνικές για τη μοντελοποίηση απειλών, την προστασία περιουσιακών στοιχείων, τον καθορισμό απαιτήσεων ασφαλείας και την πρόληψη του κινδύνου με προληπτικό τρόπο.

### 3.1 Ανάλυση κενών σε διαδικασίες (Gap analysis)

Πολλές εξέχουσες μελέτες σχετίζονται με την αναθεώρηση των απαιτήσεων ασφαλείας έχουν αναφερθεί στη βιβλιογραφία, οι οποίες περιγράφονται ως εξής:

– Οι (Mellado *et al.*, 2010) διεξήγαγαν μια συστηματική ανασκόπηση της υπάρχουσας βιβλιογραφίας SRE (μέχρι το 2010) και παρείχε μια περίληψη πληροφοριών σχετικά με τις απαιτήσεις ασφαλείας. Ωστόσο, η κύρια εστίασή τους δεν ήταν σχετικά με την αξιολόγηση των προσεγγίσεων SRE, αλλά παρουσιάζοντας στους ερευνητές μια περίληψη των πρωτοβουλιών απαιτήσεων ασφαλείας με ενδελεχή και αμερόληπτο τρόπο. Το μόνο ερευνητικό ερώτημα που αντιμετωπίζουν είναι ο «προσδιορισμός πρωτοβουλιών και αναφορών εμπειρίας στη μηχανική λογισμικού» οι οποίες λαμβάνουν υπόψη τις απαιτήσεις ασφάλειας από την αρχή της ανάπτυξης του Πληροφοριακού Συστήματος, προκειμένου να αναπτυχθούν ασφαλή συστήματα.' Ωστόσο, η μελέτη που διεξάγεται στην εργασία βασίζεται σε 5 ερευνητικά ερωτήματα που καλύπτουν διάφορες πτυχές των προσεγγίσεων SRE, όπως οι τεχνικές εξαγωγής και τα πρότυπα ασφαλείας που υιοθετήθηκαν, η υποστήριξη της χρηστικότητας, η υποστήριξη κατά τη διάρκεια των διαφόρων υποφάσεων της φάσης απαιτήσεων και ορολογιών που χρησιμοποιούνται για διαφορετικές έννοιες ασφάλειας. Επιπλέον, πολλές πρωτοβουλίες και εξελίξεις SRE, που έχουν προκύψει τα τελευταία 9 χρόνια, προστίθενται στη μελέτη.

– Οι (Fabian *et al.*, 2010) παρείχαν ένα εννοιολογικό πλαίσιο που προσπαθεί να ευθυγραμμίσει διαφορετικές έννοιες που χρησιμοποιούνται στο SRE. Επιπλέον, έχουν συγκρίνει 18 διαφορετικές προσεγγίσεις SRE (δημοσιευμένες έως το 2010) με βάση αυτό το πλαίσιο. Αν και το πλαίσιο που προτείνουν είναι αρκετά εξαντλητικό και παρέχει ένα ευρύ σύνολο κριτηρίων για τη σύγκριση των προσεγγίσεων SRE, δεν πραγματοποιήθηκε συστηματική ανασκόπηση της βιβλιογραφίας για τον προσδιορισμό των προσεγγίσεων SRE. Ωστόσο, στην εργασία περιλαμβάνονται και τα δύο, πρώτα μια συστηματική ανασκόπηση της βιβλιογραφίας για τον εντοπισμό των σχετικών προσεγγίσεων SRE και στη συνέχεια τη σύγκριση αυτών των προσεγγίσεων με διάφορα κριτήρια που καθοδηγούνται από τα ερευνητικά ερωτήματα.

– Οι (Karpati, Sindre and Opdahl, 2011) έχουν προτείνει ένα σύνολο όψεων και υποκατηγοριών κατηγοριοποίησης για πρωτοβουλίες απαιτήσεων ασφάλειας μετά από εξέταση δέκα εγγράφων ανασκόπησης και σύγκρισης που σχετίζονται με τον χαρακτηρισμό μοντέλων ασφαλείας. Με άλλα λόγια, διεξήγαγαν βασικά μια

τριτοβάθμια μελέτη (ανασκόπηση εγγράφων ανασκόπησης) για να προτείνουν ένα πλαίσιο για χαρακτηρισμό που θα καθοδηγεί την επιλογή των πρωτοβουλιών απαιτήσεων ασφάλειας που εξαρτώνται από το πλαίσιο. Ωστόσο, η εργασία τους στερείται ποιοτικού ελέγχου που βασίζεται σε μια διαδικασία συστηματικής αναθεώρησης και περιορίζεται μόνο στον καθορισμό ενός πλαισίου σύγκρισης και όχι στην πραγματική σύγκριση των προσεγγίσεων SRE που βασίζονται σε αυτό το πλαίσιο.

– Οι (Iankoulova and Daneva, 2012) έχουν πραγματοποιήσει μια συστηματική ανασκόπηση σχετικά με τις απαιτήσεις και τις λύσεις ασφάλειας στον τομέα του υπολογιστικού νέφους. Έχουν αναλύσει 55 τελικά επιλεγμένες μελέτες και τις έχουν ταξινομήσει σε 9 διαφορετικές περιοχές ασφαλείας. Έχουν επίσης αναλύσει αυτό που από αυτές τις περιοχές έχουν ερευνηθεί περισσότερο και ποιες από αυτές είναι λιγότερο. Αν και το έργο τους είναι σύμφωνο με τις οδηγίες συστηματικής αναθεώρησης στη μηχανική λογισμικού, αλλά η εστίασή τους περιορίστηκε μόνο στις απαιτήσεις ασφάλειας στον τομέα του cloud computing.

– Οι (Salini and Kanmani, 2012) διεξήγαγε μια ανασκόπηση των προσεγγίσεων SRE, προσδιόρισε 11 προσεγγίσεις και τις συνέκρινε με διαφορετικά κριτήρια όπως υποστήριξη μοντελοποίησης απειλών, ανάλυση κινδύνου και επιχειρησιακή φάση του SDLC. Η εργασία τους παρέχει μια σύντομη συνοπτική σύγκριση των 11 SRE προσεγγίσεις, αλλά στερείται συστηματικής διαδικασίας αναθεώρησης που προτείνεται για τη διεξαγωγή επισκοπήσεων στον κλάδο της μηχανικής λογισμικού.

– Οι (Raspotnig and Opdahl, 2013) διεξήγαγαν μια συστηματική ανασκόπηση για να σκιαγραφήσουν τεχνικές αναγνώρισης κινδύνου στον τομέα της ασφάλειας και της ασφάλειας. Με βάση την ανασκόπηση, καθορίστηκαν συγκεκριμένα κριτήρια από τους συγγραφείς προς επισήμανση η δύναμη και η αδυναμία των τεχνικών και πώς οι τεχνικές από αυτούς τους δύο τομείς μπορούν να αλληλοσυμπληρώνονται. Ωστόσο, η εργασία μας είναι αρκετά διαφορετική υπό την έννοια ότι οι συγγραφείς εδώ έχουν επικεντρωθεί ειδικά σε τεχνικές αναγνώρισης κινδύνου, ενώ έχουμε αναλύσει τις μηχανολογικές προσεγγίσεις απαιτήσεων ασφαλείας, συμπεριλαμβανομένων των τεχνικών αναγνώρισης κινδύνου, αλλά περιορίζονται μόνο στον τομέα ασφάλειας. Επίσης, τα κριτήρια για τη σύγκριση των προσεγγίσεων σε αυτό το έγγραφο είναι αρκετά διαφορετικά από τα δικά μας, καθώς ο κύριος σκοπός του είναι να προσδιορίσει πώς οι τεχνικές αναγνώρισης κινδύνου από τους δύο τομείς ασφάλειας και ασφάλειας ανταποκρίνονται μεταξύ τους.

– Οι (Muñante *et al.*, 2014) πραγματοποίησαν μια ανασκόπηση 13 προσεγγίσεων SRE

που περιλαμβάνει μια συγκριτική ανάλυση των προσεγγίσεων με βάση ορισμένα κριτήρια που σχετίζονται με την ανάλυση κινδύνου και τη μηχανική βάσει μοντέλου. Η προσέγγιση ανασκόπησης που χρησιμοποιούν οι συγγραφείς σε αυτό το άρθρο δεν είναι αυστηρή και βασίζεται απλώς στον εντοπισμό σχετικών προσεγγίσεων SRE.

– Οι (Kriaa *et al.*, 2015) διεξήγαγαν μια έρευνα προσεγγίσεων που συνδυάζουν την ασφάλεια και την ασφάλεια των βιομηχανικών συστημάτων ελέγχου. Έχουν ταξινομήσει διαφορετικές προσεγγίσεις σε τρεις μεγάλες κατηγορίες ως γενικές προσεγγίσεις, γραφικές προσεγγίσεις βάσει μοντέλων και άτυπες μη γραφικές προσεγγίσεις. Οι περισσότερες από τις προσεγγίσεις που συζητούνται σε αυτό το έγγραφο επικεντρώνονται στην ασφάλεια και την ασφάλεια στον βιομηχανικό έλεγχο συστημάτων, που εφαρμόζονται σε όλες τις φάσεις του SDLC, ενώ οι προσεγγίσεις που συζητούνται στην εργασία μας στοχεύουν πιο συγκεκριμένα στην ανάλυση απειλών κατά τη φάση των απαιτήσεων. Επιπλέον, η έρευνα δε διαθέτει συστηματική αναθεώρηση και διαδικασίες ποιότητας.

– Οι (Silva *et al.*, 2016) έχουν εντοπίσει 19 διαφορετικές μεθοδολογίες για τον εντοπισμό και τον μετριασμό των απειλών στο SDLC μετά από δύο συστηματικές μελέτες χαρτογράφησης. Από τις 19 μεθοδολογίες που προσδιορίστηκαν, οι 17 υποστήριξαν τον εντοπισμό απειλών και οι 14 υποστήριξαν τον μετριασμό της απειλής. Είναι αξιοσημείωτο ότι οι συγγραφείς έχουν περιγράψει διάφορες μεθοδολογίες ανάπτυξης ασφαλούς λογισμικού από τη βιβλιογραφία σε μια συστηματική και ποιοτικά ελεγχόμενη διαδικασία. Η μελέτη στοχεύει να απαντήσει σε ένα ερευνητικό ερώτημα που μοιάζει πολύ με το πρώτο ερώτημα της μελέτης μας, σχετικό στον εντοπισμό προσεγγίσεων που βοηθούν στον εντοπισμό απειλών. Ωστόσο, η περιοχή εστίασής τους δεν είναι συγκεκριμένη για τη φάση των απαιτήσεων. Δεύτερον, οι συγγραφείς σε αυτό το άρθρο δεν έχουν περιγράψει άλλες σημαντικές προσεγγίσεις όπως τα SecureUML, UMLsec, Secure i*, ISSRM και η προσέγγιση μοντελοποίησης απειλών της Microsoft και η μελέτη τους καλύπτει πρωτοβουλίες μόνο έως το 2015.

– Οι (Mohammed *et al.*, 2017) έχουν εντοπίσει 52 προσεγγίσεις ασφάλειας λογισμικού σε όλο τον κύκλο ζωής ανάπτυξης λογισμικού και τις ταξινομούν σε έξι ευρείες κατηγορίες, πραγματοποιώντας συστηματική ανασκόπηση της βιβλιογραφίας μέχρι το έτος 2015. Η κύρια έρευνά τους ήταν να προσδιορίσουν τις προσεγγίσεις ασφάλειας και το στάδιο στο οποίο είναι ενσωματωμένο στο SDLC. Ωστόσο, το επίκεντρο στην εργασία μας ήταν να προσδιορίσουμε τις προσεγγίσεις ασφαλείας που ισχύουν κυρίως στη φάση των απαιτήσεων, τη συγκριτική τους ανάλυση σε διάφορες παραμέτρους και

πώς αυτές ενσωματώνονται σε διάφορες υποφάσεις της φάσης των απαιτήσεων.

Είναι προφανές ότι οι περισσότερες από τις εργασίες που αναφέρονται παραπάνω διερευνούν τον τομέα της μηχανικής απαιτήσεων ασφαλείας ολοκληρωμένα με ποικίλους στόχους και ερευνητικά ερωτήματα. Ωστόσο, πολύ λίγες από τις εργασίες που αναφέρονται παραπάνω παρουσιάζουν μια συστηματική ανασκόπηση και σύγκριση των προσεγγίσεων SRE. Οι (Fabian *et al.*, 2010) και (Salini and Kanmani, 2012) έχουν αξιολογήσει και συνέκριναν τις προσεγγίσεις SRE, αλλά λείπει από την εργασία τους μια αυστηρή και συστηματική ανασκόπηση της σχετικής βιβλιογραφίας. Επίσης, το ερευνητικό ερώτημα που εξετάζεται στην εργασία μας, όπως η αξιολόγηση των προσεγγίσεων SRE σε διάφορες υποφάσεις της φάσης των απαιτήσεων, είναι διαφορετικό από σχεδόν όλες τις εργασίες, καθώς οι περισσότεροι από τους συγγραφείς έχουν προσπαθήσει να διερευνήσουν την ενσωμάτωση των προσεγγίσεων SRE σε ευρείες φάσεις του SDLC. Ομοίως, άλλα ερευνητικά ερωτήματα, όπως ο εντοπισμός προσεγγίσεων που αφορούν την ασφάλεια αποκλειστικά κατά τη φάση των απαιτήσεων και η σύγκρισή τους με βάση τις ορολογίες που χρησιμοποιούνται για την αντιμετώπιση εννοιών που σχετίζονται με την ασφάλεια, όπως απειλές, τρωτά σημεία, στόχοι ασφάλειας κ.λπ., δίνουν νέες πληροφορίες για τον τομέα. Τέλος, η εργασία μας είναι η πιο πρόσφατη και καλύπτει τις πιο πρόσφατες προσεγγίσεις SRE που έχουν δημοσιευτεί στη βιβλιογραφία μέχρι σήμερα (μέχρι τον Μάιο του 2019).

Αυτή η συστηματική ανασκόπηση πραγματοποιήθηκε χρησιμοποιώντας κατάλληλες οδηγίες για συστηματικές ανασκοπήσεις στη μηχανική λογισμικού που προτείνει ο (Kitchenham B., 2007). Σύμφωνα με τις οδηγίες, η υπάρχουσα βιβλιογραφία συντίθεται με επίσημο και συστηματικό τρόπο. Η ερευνητική διαδικασία ακολουθεί μια καλά καθορισμένη ακολουθία βημάτων (P1–P5) που πλαισιώνεται με τη δημιουργία του πρωτοκόλλου ανασκόπησης που αναπτύχθηκε από τους (de Almeida Biolchini *et al.*, 2007). Λόγω του μεγάλου όγκου βιβλιογραφίας για το θέμα, χρησιμοποιήθηκε το λογισμικό Mendeley ως εργαλείο για την αποτελεσματική διαχείριση των ανακτημένων πληροφοριών.

# Κεφάλαιο 4 – Ανασκόπηση μεθόδων ελέγχου

## 4.1 Απαιτήσεις ανάπτυξης του λογισμικού

Η παρούσα εργασία εστιάζει στον εντοπισμό για τις προσεγγίσεις SRE στη βιβλιογραφία και λαμβάνει υπόψη τις απαιτήσεις ασφάλειας κατά τα αρχικά στάδια ανάπτυξης λογισμικού μαζί με την κριτική τους σύγκριση και έρευνα σε διαφορετικές διαστάσεις. Ως εκ τούτου, διαμορφώθηκαν πέντε ερευνητικά ερωτήματα τα οποία προσδιορίζονται ως εξής:

- RQ1 Ποιες προσεγγίσεις SRE φέρεται να έχουν καθιερωθεί;
- RQ2 Ποιες τεχνικές εκκίνησης, μοντέλα και πρότυπα ασφαλείας έχουν προσαρμοστεί σημαντικά από τις καθιερωμένες προσεγγίσεις SRE;
- RQ3 Πώς διαφέρουν αυτές οι προσεγγίσεις SRE ως προς τη χρηστικότητα σε σχέση με διάφορες παραμέτρους όπως η υποστήριξη μοντελοποίησης απειλών, η υποστήριξη ανάλυσης κινδύνου, η υποστήριξη εργαλείων, η προσαρμογή του κλάδου και το μέγεθος του έργου;
- RQ4 Τι επίπεδο υποστήριξης παρέχουν αυτές οι προσεγγίσεις SRE κατά τις διάφορες υποφάσεις της φάσης των απαιτήσεων;
- RQ5 Ποιες ορολογίες χρησιμοποιούνται από τις προσεγγίσεις SRE για την κάλυψη διαφορετικών πτυχών ασφάλειας;

Το RQ1 πλαισιώθηκε για να προσδιορίσει τις προσεγγίσεις SRE που είναι διαθέσιμες στη βιβλιογραφία για τη λεπτομερή μελέτη. Το RQ2 διατυπώθηκε για να αναλύσει τις επιλεγμένες προσεγγίσεις SRE από την άποψη των τεχνικών πρόκλησης. Περαιτέρω, διερευνήθηκε η τεχνική μοντελοποίησης και τα πρότυπα ασφαλείας που προσαρμόστηκαν από αυτές τις προσεγγίσεις. Στο RQ3, ο στόχος ήταν να συγκριθούν οι προσεγγίσεις SRE από την άποψη διαφορετικών κριτηρίων, όπως η υποστήριξη μοντελοποίησης απειλών, η υποστήριξη ανάλυσης κινδύνου, η υιοθέτηση του κλάδου και η διαθεσιμότητα του εργαλείου. Επιπλέον, αναλύθηκε η χρηστικότητα των προσεγγίσεων σε σχέση με το μέγεθος και την πολυπλοκότητα του έργου. Το RQ4 σχεδιάστηκε για να διερευνήσει το επίπεδο υποστήριξης από προσεγγίσεις SRE σε σχέση με τις υποφάσεις της φάσης απαιτήσεων. Το RQ5 σχεδιάστηκε για να συγκρίνει τις ορολογίες που χρησιμοποιούνται από διαφορετικές προσεγγίσεις SRE για την αντιμετώπιση εννοιών που σχετίζονται με την ασφάλεια, όπως απειλές, τρωτά σημεία,

κίνδυνος, περιουσιακά στοιχεία, στόχους ασφάλειας και απαιτήσεις ασφάλειας.

### 4.2 Στρατηγική αναζήτησης και πηγές δεδομένων

Η στρατηγική αναζήτησης για τη μελέτη βασίζεται γενικά σε τρία βήματα, τα οποία συζητούνται παρακάτω. Κατασκευή των όρων αναζήτησης: Κατασκευάσαμε τους όρους αναζήτησης σύμφωνα με τις λέξεις-κλειδιά που προσδιορίστηκαν από τον πληθυσμό και την παρέμβαση:

– Πληθυσμός: Απαιτήσεις ή απαιτήσεις ασφάλειας μηχανική
– Παρέμβαση: Υπάρχουσες προσεγγίσεις για τη μοντελοποίηση της ασφάλειας κατά τη φάση των απαιτήσεων.

Προσδιορισμός των λέξεων-κλειδιών από τους επιλεγμένους όρους: Δοκιμάστηκαν οι όροι αναζήτησης στις μηχανές αναζήτησης και μετά από πολλές επαναλήψεις, προσδιορίστηκαν οι λέξεις-κλειδιά με βάση τους πιο σχετικούς όρους που προέκυψαν από τα αποτελέσματα των δοκιμών. Οι λέξεις-κλειδιά που προσδιορίζονται και αντιστοιχούν στους όρους αναζήτησης παρατίθενται παρακάτω:

– Απαιτήσεις ασφαλείας: απαιτήσεις ή ασφάλεια
– Τεχνολογία Απαιτήσεων: απαιτήσεις ή απαιτήσεις μηχανική
– προσεγγίσεις: προσεγγίσεις ή μοντέλα ή εργαλεία ή πρωτοβουλίες ή πλαίσιο ή μεθόδους ή τεχνικές ή προτάσεις.

Κατασκευή της συμβολοσειράς αναζήτησης: Αφού δοκιμάστηκαν οι συμβολοσειρές αναζήτησης με βάση τις παραπάνω λέξεις-κλειδιά σε διάφορες βάσεις δεδομένων, έγινε εντοπισμός ορισμένων τιμών που θα μπορούσαν να αποκλίνουν την αναζήτησή σε άλλους τομείς. Εξαιρέθηκαν λέξεις-κλειδιά όπως τεχνικές, προτάσεις και πρωτοβουλίες πριν από τη δημιουργία της συμβολοσειράς αναζήτησης. Η λίστα των λέξεων-κλειδιών που περιλαμβάνονται είναι ασφάλεια, μηχανική απαιτήσεων, απαιτήσεις, προσεγγίσεις, εργαλεία, μοντέλα, πλαίσια και μέθοδοι. Συνδέθηκαν οι λέξεις-κλειδιά με λογικούς τελεστές AND και OR για να σχεδιαστεί η συμβολοσειρά αναζήτησής ως εξής: (ασφάλεια) ΚΑΙ (απαιτήσεις μηχανικής Ή απαιτήσεις) AND (προσεγγίζει OR μοντέλα Ή πλαίσια Ή μεθόδους Ή εργαλείο) Ο χώρος αναζήτησης περιλάμβανε ψηφιακές βιβλιοθήκες. Αφού εντοπιστούν οι πηγές των μελετών, είναι απαραίτητο να περιγραφεί η στρατηγική αναζήτησης. Η έρευνα διεξήχθη σε δύο φάσεις. Σε πρώτη φάση, όλες οι σχετικές μελέτες ανακτήθηκαν χρησιμοποιώντας τη

συμβολοσειρά αναζήτησης από έξι ηλεκτρονικές βάσεις δεδομένων (Google scholar, Science direct, IEEEXplore, Scopus, SpringerLink, ACM). Δεδομένου ότι κάθε ψηφιακή βιβλιοθήκη έχει τα δικά της χαρακτηριστικά μηχανή αναζήτησης, προσαρμόστηκαν οι συμβολοσειρές αναζήτησης για κάθε βιβλιοθήκη χρησιμοποιώντας επαναλαμβανόμενες δοκιμές και μικρές τροποποιήσεις. Οι συμβολοσειρές δευτερεύουσας αναζήτησης ειδικά για κάθε βάση δεδομένων που χρησιμοποιείται στη μελέτη δίνονται στο «Παράρτημα Α.» Αυτή η απλή αναζήτηση οδήγησε σε μεγάλο αριθμό εγγράφων (N = 15.585). Για να περιοριστούν τα αποτελέσματά, πραγματοποιήθηκε η διαδικασία αναζήτησης σε διαφορετικές φάσεις. Επιπλέον, σαρώνοντας καθεμία από αυτές τις ανακτημένες μελέτες σύμφωνα με τη στρατηγική αναζήτησης, φιλτραρίστηκαν 773 έγγραφα που σχετίζονται με τη μελέτη. Η διαδικασία φιλτραρίσματος αποτελείται από δύο υποβήματα: πρώτα χειροκίνητη σάρωση των τίτλων όλων των επιλεγμένων εγγράφων (15.585) για φιλτράρισμα σχετικών εγγράφων και περαιτέρω διερεύνηση ενός υποσυνόλου αυτών των εργασιών (1685 περίπου) διαβάζοντας την περίληψη, τις λέξεις-κλειδιά και σε ορισμένες θέτει το κείμενο σύμφωνα με τη στρατηγική επιλογής για να φιλτράρει 773 σχετικές εργασίες. Μετά από αυτό το βήμα, εφαρμόστηκαν τα κριτήρια συμπερίληψης και αποκλεισμού στις μελέτες που οδήγησαν σε συνολικά 157 εργασίες ακολουθούμενες από μια δεύτερη φάση διαδικασίας αναζήτησης χρησιμοποιώντας αναζητήσεις αναφοράς (Snowballing) και αναζήτηση συγκεκριμένου συγγραφέα στη βάση δεδομένων DBLP (Digital Bibliographic Library Browser). Αυτή η συμπληρωματική στρατηγική βοήθησε να συμπεριληφθεί οποιαδήποτε πιθανή εργασία που θα μπορούσε να έχει παραλειφθεί κατά λάθος. Συνολικά προστέθηκαν 31 ακόμη εργασίες μετά τη συμπληρωματική αναζήτηση που αύξησε τον απολογισμό των εργασιών σε 188. Τέλος, τα κριτήρια αξιολόγησης ποιότητας εφαρμόστηκαν σε αυτές τις 188 μελέτες. Στο τέλος της άσκησης, τελικά επιλέχθηκαν 108 μελέτες που κρίθηκαν κατάλληλες για να απαντήσουν στα διατυπωμένα ερευνητικά ερωτήματα.

### 4.3 Επιλογή προσεγγίσεων SRE

Οι πληροφορίες που εξάγονται από τα επιλεγμένα έγγραφα περιλαμβάνουν μεθόδους, διαδικασίες, μοντέλα ή πλαίσια για τον καθορισμό απαιτήσεων ασφαλείας στο στάδιο απαιτήσεων του SDLC. Η φόρμα εξαγωγής δεδομένων σχεδιάστηκε για να καταγράφει τον τύπο της έρευνας και τη μέθοδο μελέτης που χρησιμοποιήθηκε, προσδιορίζοντας

20 διαφορετικούς τύπους προσεγγίσεων SRE και ταξινομώντας τις διάφορες μεθόδους SRE που ελήφθησαν από τη μελέτη μας σε αυτές τις ευρείες κατηγορίες. Επίσης διερευνήθηκαν βασικές πληροφορίες όπως τίτλος, περίληψη, ημερομηνία δημοσίευσης, τύπος εξαγωγής και τεχνικές μοντελοποίησης που χρησιμοποιούνται για απαιτήσεις ασφαλείας, υποστήριξη για μοντελοποίηση απειλών και ανάλυση κινδύνου, διαθεσιμότητα υποστήριξης εργαλείων και υιοθέτηση από τον κλάδο. Χρησιμοποιήθηκε μια κλίμακα Likert 4 σημείων για να αξιολογηθεί το επίπεδο υποστήριξης διαφορετικών προσεγγίσεων SRE σε διάφορες υποφάσεις της φάσης των απαιτήσεων. Επιπλέον, καταγράφηκαν διάφορες ορολογίες που χρησιμοποιούνται για την αντιμετώπιση των εννοιών ασφάλειας. Οι ακόλουθες υποενότητες παρέχουν μια σύντομη περιγραφή των 20 προσεγγίσεων SRE που εξήχθησαν από τις μελέτες, σύμφωνα με τη στρατηγική εξαγωγής δεδομένων.

### 4.3.1 KAOS (Keep All Objectives Satisfied)

Ο Van Lamsweerde επέκτεινε την προηγούμενη έρευνά του (Lamsweerde, 2007) σχετικά με τη μέθοδο ανάλυσης απαιτήσεων προσανατολισμένη στο στόχο, γνωστή ως KAOS, ενσωματώνοντας γραμμική χρονική λογική, αντιμοντέλα και ανάλυση συγκρούσεων για να επεξεργαστεί και να επισημοποιήσει τις απαιτήσεις ασφαλείας (van Lamsweerde, no date). Το KAOS εστιάζει στην εξαγωγή στόχων του συστήματος, στην εννοιολόγηση αυτών των στόχων σε απαιτήσεις και υποθέσεις, στην ανάθεση ευθυνών σε παράγοντες όπως ανθρώπους, συσκευές ή λογισμικό και στη διαχείριση των εξελισσόμενων απαιτήσεων με την πάροδο του χρόνου (Dardenne, van Lamsweerde and Fickas, 1993). Η μέθοδος περιλαμβάνει δραστηριότητες όπως μοντελοποίηση στόχων συστήματος, αντικειμένων συστήματος, πράκτορες συστήματος, λειτουργίες συστήματος, εμπόδια στους στόχους, απειλές ασφαλείας και συμπεριφορές πρακτόρων. Αυτή η μέθοδος υποστηρίζει μια ελαφριά ημιτυπική διαδικασία για γραφική μοντελοποίηση και μια επίσημη διαδικασία επαλήθευσης και επικύρωσης απαιτήσεων. Η προσέγγιση δίνει έμφαση στη συνοχή, την πληρότητα και τον καθορισμό των απαιτήσεων και όχι την πρόκληση. Το KAOS έχει ενσωματωθεί με τη γλώσσα B για την επίσημη κατασκευή ενός πλήρους, συνεπούς και σαφούς μοντέλου απαιτήσεων ασφαλείας.

### 4.3.2 Secure i*

Το πλαίσιο μοντελοποίησης i* αναπτύχθηκε για να υποστηρίξει την ανάλυση και το σχεδιασμό απαιτήσεων χρησιμοποιώντας την προσέγγιση προσανατολισμένη στον πράκτορα. Προσπαθεί να μοντελοποιήσει τις σχέσεις εξάρτησης μεταξύ διαφόρων παραγόντων χρησιμοποιώντας την έννοια των δρώντων, των πρακτόρων και των στόχων. Διάφορες επεκτάσεις (Liu, Yu and Mylopoulos, 2003), (Elahi, Yu and Zannone, 2010) του μοντέλου i* έχουν προταθεί για να μοντελοποιήσουν έννοιες ασφάλειας και ιδιωτικότητας. Το Secure i*, μια επέκταση του μοντέλου i*, αναλύει τις ανταλλαγές ασφαλείας μεταξύ των διαφόρων ενδιαφερόμενων μερών και του συστήματος που θα κατασκευαστεί. Προσπαθεί να ευθυγραμμίσει τις απαιτήσεις ασφαλείας με άλλες απαιτήσεις του συστήματος. Βασίζεται σε ένα γενικό μοντέλο που λαμβάνει υπόψη σημαντικές έννοιες ασφάλειας όπως στόχος, καθήκον, περιουσιακά στοιχεία, απειλές και πόρους. Ένα μετα-μοντέλο που στοχεύει να συλλάβει την πράξη των επιτιθέμενων και την αντεπίθεση των θυμάτων χρησιμοποιώντας το μοντέλο i* συζητείται στο (Yasin *et al.*, 2021). Ισχύει σε όλες τις φάσεις του SDLC και καλύπτει τους τρεις στόχους της CIA. Η άτυπη επικύρωση σε αυτή την προσέγγιση γίνεται με τον αλγόριθμο επισήμανσης στόχων.

### 4.3.3 Secure tropos

Η προσέγγιση Tropos βασίζεται στο παράδειγμα μηχανικής λογισμικού προσανατολισμένη σε πράκτορες (AOSE) και στο πλαίσιο μοντελοποίησης i*, το οποίο βλέπει το σύστημα ως ένα σύστημα πολλαπλών πρακτόρων με διαφορετικούς παράγοντες που εξαρτώνται ο ένας από τον άλλο για την εκπλήρωση των στόχων τους (Susi, A.; Perini, A.; Mylopoulos, J.; Giorgini, 2005). Οι προγραμματιστές βλέπουν το σύστημα ως μια ανθρώπινη κοινωνία, με οντότητες που διαθέτουν ανθρώπινα χαρακτηριστικά όπως κινητικότητα, ευφυΐα και ικανότητα, που επικοινωνούν μεταξύ τους. Η διαδικασία περιλαμβάνει μοντελοποίηση παραγόντων, μοντελοποίηση εξαρτήσεων μεταξύ των παραγόντων, μοντελοποίηση εμπιστοσύνης και βελτίωση στόχων.

Οι έννοιες τόσο της εμπιστοσύνης όσο και της ασφάλειας είναι ενσωματωμένες στο μοντέλο Tropos. Μουρτάδης κ.ά. πρότεινε την ενσωμάτωση του Secure Tropos για την ανάπτυξη συστημάτων πολλαπλών πρακτόρων (Mouratidis and Giorgini, 2009). Στο (Matulevičius *et al.*, 2008), οι συγγραφείς διερεύνησαν την ενσωμάτωση της ανάλυσης κινδύνου με το Secure Tropos. Μια επέκταση, το Secure Tropos-SPL, αναπτύχθηκε για τη μοντελοποίηση απαιτήσεων ασφαλείας σε σειρές προϊόντων λογισμικού (SPL). Η

ενσωμάτωση των παραγώγων απαιτήσεων ασφαλείας που βασίζονται σε πρότυπα στο μοντέλο έχει μελετηθεί στο (Rrenja and Matulevičius, 2015). Μια άλλη επέκταση, που συζητήθηκε στο (Pavlidis *et al.*, 2017), μοντελοποιεί και βελτιστοποιεί επίσημα μηχανισμούς ασφαλείας που ευθυγραμμίζονται με τις απαιτήσεις ασφαλείας.
Ένα Secure Tropos με επίγνωση του κινδύνου, ευθυγραμμισμένο με τις έννοιες διαχείρισης κινδύνου ασφάλειας πληροφοριών, συζητείται στο (Matulevičius, 2017). Το πλαίσιο Στόχου-Κινδύνου Tropos για τη μοντελοποίηση και την αξιολόγηση των κινδύνων ασφαλείας κρίσιμων συστημάτων με βάση τις σχέσεις εμπιστοσύνης μεταξύ των παραγόντων προτείνεται στο (Anwar Mohammad, Nazir and Mustafa, 2019). Αυτό το πλαίσιο χρησιμοποιεί την εμπιστοσύνη ως απόδειξη για την αξιολόγηση του κινδύνου, αξιολογεί εναλλακτικούς στόχους και αναλύει πιθανά αντίμετρα για τον μετριασμό του κινδύνου με βάση το οργανωτικό πλαίσιο του συστήματος. Επιπλέον, το SecTro, ένα εργαλείο CASE, έχει αναπτυχθεί για να καθοδηγήσει και να υποστηρίξει τους προγραμματιστές στην κατασκευή κατάλληλων μοντέλων για το Secure Tropos.

### 4.3.4 GBRAM (Goal-Based Requirements Analysis Methods)

Αυτή η μέθοδος χρησιμοποιεί προσέγγιση με γνώμονα στόχους και σενάρια για την επιβολή πολιτικών ασφάλειας και απορρήτου κατά τα αρχικά στάδια ανάπτυξης λογισμικού. Οι (Jürjens, 2001) έχουν προτείνει ένα πλαίσιο που μοντελοποιεί τις απαιτήσεις απορρήτου χρησιμοποιώντας τη διαδικασία της μηχανικής ρόλων. Η διαδικασία μηχανικής ρόλων λειτουργεί με τον προσδιορισμό των ρόλων, την άδεια και την αντιστοίχιση των ρόλων στα δικαιώματα. Ο ρόλος ενός ατόμου υποδηλώνεται με μια πλειάδα τριών (u, r, p) όπου u είναι ο χρήστης που μπορεί να έχει πρόσβαση σε ένα αντικείμενο, εάν του/της έχει εκχωρηθεί ένας ρόλος r με άδεια p. Αυτή η προσέγγιση μειώνει το χάσμα μεταξύ των απαιτήσεων απορρήτου και των πολιτικών ελέγχου πρόσβασης. Ένα πλαίσιο PFIRES έχει προταθεί από τους Rees et al. για ανάλυση κινδύνου στη ρύθμιση του ηλεκτρονικού επιχειρείν. Ένα πλαίσιο DIGS, το οποίο υποστηρίζει τον αναλυτή στη συστηματική και ολοκληρωμένη ανακάλυψη στόχων ασφαλείας κατά τη μηχανική απαιτήσεων ασφαλείας, προτείνεται στο (Rrenja and Matulevičius, 2015). Το GBRAM χρησιμοποιείται κυρίως για την επεξεργασία και την πρόσβαση οργανωτικών στόχων που έχουν ήδη καλά καθορισμένες πολιτικές ασφαλείας. Μπορεί να χρησιμοποιηθεί κατά την εκκίνηση των απαιτήσεων καθώς και στη φάση του σχεδιασμού.

### 4.3.5 Abuse Frames

Χρησιμοποιείται για τη συστηματική ανάλυση και αναπαράσταση των συνθηκών υπό τις οποίες μπορεί να εμφανιστεί ευπάθεια στο σύστημα. Δομεί και περιορίζει το εύρος του προβλήματος ασφάλειας, διευκολύνοντας έτσι την πρόκληση απαιτήσεων ασφαλείας. Το πλαίσιο κατάχρησης μοιράζεται την ίδια σημείωση με αυτή των προβληματικών πλαισίων του Jackson, με μια μικρή αλλαγή ότι περιλαμβάνει antirequirements (απαιτήσεις κακόβουλου εισβολέα). Κάθε διάγραμμα πλαισίου κατάχρησης αντιπροσωπεύει μια κατηγορία απειλών που μπορεί να παραβιάσει έναν συγκεκριμένο στόχο ασφαλείας. Μερικές από τις γενικές κατηγορίες απειλών περιλαμβάνουν υποκλοπή, τροποποίηση και άρνηση υπηρεσίας. Με βάση την έννοια των πλαισίων κατάχρησης, οι συγγραφείς στο (Lin *et al.*, no date) έχουν προτείνει μια επαναληπτική μέθοδο που συνίσταται στη διάσπαση των προβλημάτων σε υποπροβλήματα που μπορούν να πλαισιωθούν σε ένα γενικό πλαίσιο προβλημάτων, προσδιορίζοντας τις αντι-απαιτήσεις ως περιορισμούς στις λειτουργικές ανάγκες για την κατασκευή το διάγραμμα πλαισίου κατάχρησης, εντοπίζοντας τα τρωτά σημεία και, τέλος, αντιμετωπίζοντας κάθε ευπάθεια για την εξαγωγή ενός συνόλου απαιτήσεων ασφαλείας. Δεν υποστηρίζει επίσημη επαλήθευση και επικύρωση. Ωστόσο, οι συγγραφείς έχουν συζητήσει μια μέθοδο κατασκευής ABA (κατάχρηση όρισμα πλαισίου) για να ελέγξουν την ικανοποίηση των αντι-απαιτήσεων. Στο (Luncheng Lin *et al.*, no date), οι συγγραφείς έχουν συζητήσει μια μέθοδο ακριβούς καθορισμού των απαιτήσεων ασφαλείας, δεσμεύοντας έτσι το εύρος των προβλημάτων ασφαλείας χρησιμοποιώντας πλαίσια κατάχρησης. Μια μεθοδολογία έχει αναπτυχθεί στο (El-Hadary and El-Kassas, 2014) που βοηθά τους προγραμματιστές να προκαλέσουν επαρκείς απαιτήσεις ασφαλείας χρησιμοποιώντας πλαίσια κατάχρησης.

### 4.3.6 (SEPP) Security Engineering Process Using Patterns

Η ιδέα της χρήσης προτύπων έχει αποδειχθεί πολύ πολύτιμη στον τομέα της μηχανικής λογισμικού. Μας δίνουν μια εικόνα μιας κατηγορίας προβλημάτων. Μας βοηθούν στο σχεδιασμό λογισμικών παρέχοντάς μας ένα συσσωρευμένο σώμα γνώσεων, ώστε να μην χρειάζεται να ξεκινήσουμε απευθείας από το μηδέν. Τα πλαίσια προβλημάτων εισήχθησαν από τον Jackson, ο οποίος ορίζει ένα πρόβλημα διαισθητικά χρησιμοποιώντας ήδη καθορισμένη κατηγορία προβλημάτων όσον αφορά τον τομέα,

τα χαρακτηριστικά, τις διεπαφές και τις απαιτήσεις του. Οι (El-Hadary and El-Kassas, 2014), παρουσίασαν δύο νέα πλαίσια προβλημάτων, γνωστά ως πλαίσια προβλημάτων ασφαλείας (SPF) και συγκεκριμένα πλαίσια προβλημάτων ασφαλείας (CSPF). Το SPF συμβάλλει στην εκπλήρωση των απαιτήσεων ασφαλείας του συστήματος. Αναφέρονται στα προβλήματα ασφάλειας που επιλύονται χωρίς να προτείνουν λύση. Ο χώρος λύσης ορίζεται με τη συγκεκριμένη εφαρμογή των προβληματικών πλαισίων με γενικό μηχανισμό ασφαλείας (όπως τεχνικές κρυπτογράφησης για ασφαλή μετάδοση δεδομένων), μετατρέποντας το SPF σε CSPF. Το CSPF αποτελείται από προϋποθέσεις και μετασυνθήκες σε επίσημους συμβολισμούς που πρέπει να εκπληρωθούν για να δημιουργηθεί μια παρουσία του SPF. Οι συγγραφείς έχουν περιγράψει μια μεθοδολογία τριών βημάτων που διαμορφώνει προβλήματα που σχετίζονται με την ασφάλεια. Το πρώτο βήμα συνίσταται στην αποσύνθεση του προβλήματος σε υποπροβλήματα μέχρι να βρεθεί ένα συγκεκριμένο πλαίσιο προβλήματος ασφαλείας αναλόγως. Στο δεύτερο βήμα, εισάγονται γενικοί μηχανισμοί ασφάλειας για την επίλυση των προβλημάτων ασφάλειας με τη συγκεκριμένη εφαρμογή ενός SPF με ένα γνωστό μέτρο ασφαλείας. Τέλος, το τελευταίο βήμα εισάγει συγκεκριμένα μέτρα ασφαλείας και γενικό διάγραμμα ακολουθίας για να επιτευχθεί η τέλεια λύση στο πρόβλημα ασφάλειας. Η ιδέα της χρήσης προτύπων ασφαλείας χρησιμοποιήθηκε επίσης στο (Hatebur, Heisel and Schmidt, 2008) για τον εντοπισμό, την ανάλυση και την ολοκλήρωση των απαιτήσεων ασφαλείας. Η προσέγγιση δεν είναι εφαρμόσιμη για την πρόκληση αρχικών απαιτήσεων ασφάλειας. Η μέθοδος μπορεί να καλύπτει και τους τρεις στόχους της CIA. Επί του παρόντος, δε διατίθεται αυτοματοποιημένο εργαλείο για την εφαρμογή της παραπάνω προσέγγισης. Τα πρότυπα ασφαλείας που βασίζονται σε πρότυπα (Sindre and Opdahl, 2005), μαζί με το σύστημα ταξινόμησης, έχουν χρησιμοποιηθεί και εφαρμοστεί χρησιμοποιώντας διάφορες μελέτες περιπτώσεων. Μοτίβο κατάχρησης (Fernandez, Yoshioka and Washizaki, 2009), ένας τύπος προτύπου ασφαλείας που χρησιμοποιεί το μοντέλο περίπτωσης κατάχρησης, έχει αναπτυχθεί το οποίο περιγράφει με ακρίβεια τον τρόπο μοντελοποιήστε μια επίθεση, το πλαίσιο της, τα μέτρα αντιμετώπισης και τους τρόπους εντοπισμού του εισβολέα. Στο (Schmidt, 2010) έχει προταθεί μια ανάλυση κινδύνου που βασίζεται σε γνώσεις και πρότυπα σχετικά με την ασφάλεια. Ο Donald Firesmith πρότεινε τη χρήση επαναχρησιμοποιήσιμων παραμετροποιημένων προτύπων για ανάλυση και προδιαγραφή απαιτήσεων ασφαλείας. Στο (Wirtz and Heisel, 2019) οι συγγραφείς έχουν προτείνει ένα πρότυπο βασισμένο στο Common Vulnerability

Scoring System (CVSS) για την περιγραφή των απειλών ασφαλείας και μια ημιαυτόματη διαδικασία για τον εντοπισμό σχετικών απειλών χρησιμοποιώντας αυτές τις πρότυπα. Ένα μοτίβο ασφαλείας με τη μορφή περιπτώσεων μετριαστικής χρήσης προτάθηκε, το οποίο προτείνει λύσεις για επαναλαμβανόμενες απειλές στο σύστημα κατά τη φάση των απαιτήσεων. Μια τεχνική ταξινόμησης προτύπων ασφαλείας που περιλαμβάνει διάφορες διαθέσιμες στο κοινό βάσεις δεδομένων ασφαλείας και διευκολύνει τον σχεδιαστή στην επιλογή του καλύτερου διαθέσιμου μοτίβου ασφαλείας προτείνεται στο (Salva and Regainia, 2019). Η τεχνική επιλέγει τον συνδυασμό προτύπων με βάση τη σχέση μεταξύ επιθέσεων λογισμικού, αρχών ασφάλειας και προτύπων ασφαλείας.

### 4.3.7 SREF (Security Requirements Engineering Framework)

Οι (Haley *et al.*, 2008), έχουν προτείνει ένα πλαίσιο που ενσωματώνει τη μηχανική απαιτήσεων με την ασφάλεια. Ο κύριος στόχος αυτού του πλαισίου είναι η ανάδειξη, η ανάλυση και η ικανοποίηση των απαιτήσεων ασφαλείας. Οι Haley et al. να επεξεργαστεί περαιτέρω μια επαναληπτική διαδικασία για τη μοντελοποίηση των απαιτήσεων ασφαλείας. Τα βήματα της διαδικασίας είναι: (1) προσδιορισμός επιχειρηματικών απαιτήσεων. (2) προσδιορισμός στόχων ασφάλειας. (3) προσδιορισμός απαιτήσεων ασφαλείας. και (4) κατασκευή επιχειρημάτων ικανοποίησης. Η ικανοποίηση των απαιτήσεων ασφαλείας χρησιμοποιώντας επίσημα και ημιτυπικά επιχειρήματα έχει συζητηθεί. Οι (Haley *et al.*, 2008) έχουν ασχοληθεί με τον ρόλο των υποθέσεων εμπιστοσύνης στην εκκίνηση και επεξεργασία απαιτήσεων ασφάλειας. Στο (Rehman and Gruhn, 2018), οι συγγραφείς έχουν προτείνει ένα πλαίσιο Μηχανικής Απαιτήσεων Ασφαλείας για κυβερνοφυσικά συστήματα που εξετάζει διάφορα στοιχεία όπως αισθητήρες, πρωτόκολλο δέκτη και άλλα ζητήματα δικτύου μαζί με ανησυχίες λογισμικού. Το πλαίσιο έχει αξιολογηθεί μέσω μιας μελέτης περίπτωσης για το έξυπνο σύστημα στάθμευσης.

### 4.3.8 CORAS

Είναι μια μέθοδος ανάλυσης ασφάλειας που βασίζεται σε μοντέλα που αναπτύχθηκαν ως ερευνητικό έργο στο πλαίσιο του Προγράμματος Τεχνολογιών της Κοινωνίας της Πληροφορίας (IST). Αυτή η μέθοδος χρησιμοποιεί διαγράμματα μοντελοποίησης κινδύνων ασφαλείας εμπνευσμένα από το UML για τη μοντελοποίηση απειλών, τρωτών σημείων και κινδύνων. Το CORAS αποτελείται από επτά βήματα:

- Αρχική συνάντηση με τον πελάτη και τον αναλυτή για την κατανόηση του γενικού στόχου του πελάτη.
- Διευκρίνιση των θεμάτων που συζητήθηκαν μέσω μιας δεύτερης συνάντησης μεταξύ του αναλυτή και του πελάτη.
- Συμπλήρωση υποθέσεων και σαφής περιγραφή του στόχου.
- Ανάλυση όλων των πιθανών απειλών, στόχων ασφαλείας και τρωτών σημείων για το σύστημα-στόχο με τη βοήθεια συνεργείων και ειδικού σε θέματα ασφάλειας.
- Περαιτέρω εργαστήρια για τον εντοπισμό της πιθανότητας και εκτίμησης των απειλών.
- Παροχή στον πελάτη εκτίμησης ανάλυσης κινδύνου για προσαρμογές.
- Προσδιορισμός των απαραίτητων διορθωτικών μέτρων για τις απειλές μαζί με το κόστος/ωφέλειά τους.

Το CORAS είναι μια συνταγογραφική μέθοδος που βοηθά στον εντοπισμό στόχων ασφάλειας, απειλών, τρωτών σημείων και συναφών κινδύνων, καλύπτοντας και τους τρεις στόχους της CIA (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα). Μια σημασιολογία για την ερμηνεία του διαγράμματος CORAS έχει προταθεί. Μια τεχνική ανάλυσης κινδύνου για δυναμικά συστήματα έχει αναπτυχθεί και ενσωματωθεί στο πλαίσιο CORAS. Επιπλέον, η μεθοδολογία CORAS έχει χρησιμοποιηθεί για τη μοντελοποίηση απειλών και κινδύνων στα κοινωνικά δίκτυα (Larionovs, Teilans and Grabusts, 2015).

### 4.3.9 SREP (Security Requirements Engineering Process)

Είναι μια καθιερωμένη, επαναληπτική και βασισμένη στην επαναχρησιμοποίηση σταδιακή προσέγγιση για την αντιμετώπιση των απαιτήσεων ασφαλείας κατά τις αρχικές φάσεις της ανάπτυξης λογισμικού. Αυτή η προσέγγιση αξιοποιεί την επαναχρησιμοποίηση προηγούμενων γνώσεων σχετικά με τις απειλές, τα περιουσιακά στοιχεία, τους στόχους ασφαλείας και τις απαιτήσεις ασφάλειας ενσωματώνοντας ένα χώρο αποθήκευσης πόρων ασφαλείας που βασίζεται στα πρότυπα Κοινών Κριτηρίων (CC). Χρησιμοποιεί περιπτώσεις κακής χρήσης και χρήσης για τη μοντελοποίηση απειλών, με πρότυπα υποθέσεων κακής χρήσης που καθορίζουν απειλές και πρότυπα

υποθέσεων χρήσης που πλαισιώνουν τις απαιτήσεις ασφαλείας. Η μέθοδος SREP περιλαμβάνει μια σειρά από εννέα βήματα:

- Συμφωνία σε όρους και ορισμούς.
- Προσδιορισμός κρίσιμων περιουσιακών στοιχείων.
- Προσδιορισμός στόχων ασφάλειας.
- Εντοπισμός απειλών με χρήση του αποθετηρίου πόρων ασφαλείας (SRR) / περιπτώσεων κακής χρήσης.
- Αξιολόγηση του κινδύνου που σχετίζεται με τις απειλές.
- Προκαλώντας απαιτήσεις ασφαλείας.
- Προτεραιότητα απαιτήσεων ασφαλείας.
- Επικύρωση των απαιτήσεων.
- Τροποποίηση του αποθετηρίου πόρων γνώσης.

Οι (Mellado, Fernández-Medina and Piattini, 2007) παρουσιάζουν μια συστηματική προσέγγιση που βασίζεται σε κοινά κριτήρια που αντιμετωπίζει τις απαιτήσεις ασφάλειας στα αρχικά στάδια ανάπτυξης λογισμικού.

### 4.3.10 Microsoft's Threat Modeling

Είναι μια πρακτική, φιλική προς το χρήστη τεχνική για τη μοντελοποίηση απειλών, βασισμένη κυρίως σε διαγράμματα ροής δεδομένων (DFD) και στη μεθοδολογία STRIDE (τεχνική απαρίθμησης απειλών). Αυτή η κοινή τεχνική χρησιμοποιείται για την αποκάλυψη αδυναμιών σε ένα σύστημα λογισμικού και εφαρμόζεται μόλις γίνουν γνωστές οι λειτουργικές απαιτήσεις του συστήματος. Η μοντελοποίηση απειλών σε αυτήν την προσέγγιση βοηθά τους αναλυτές να εντοπίσουν τρωτά σημεία και πιθανές απειλές για το σύστημα. Οι βασικές δραστηριότητες σε αυτή την προσέγγιση περιλαμβάνουν:

- Μοντελοποίηση του συστήματος με χρήση διαγραμμάτων ροής δεδομένων (DFD).
- Αντιστοίχιση κάθε στοιχείου DFD σε στοιχεία STRIDE (πλαστογράφηση, παραποίηση, απόρριψη, αποκάλυψη πληροφοριών, άρνηση υπηρεσίας, ανύψωση προνομίου).
- Προκαλώντας απειλές.
- Τεκμηρίωση των απειλών.

Η ανάλυση κινδύνου αποτελεί επίσης μέρος αυτής της προσέγγισης και διεξάγεται χωριστά χρησιμοποιώντας τη μεθοδολογία DREAD. Μια εμπειρική μελέτη που διεξήχθη σε ελεγχόμενο περιβάλλον για να αναλυθεί η αποτελεσματικότητα αυτής της προσέγγισης. Οι προκλήσεις στην εφαρμογή αυτής της προσέγγισης σε ένα ευέλικτο περιβάλλον περιγράφονται και συζητούνται στο (Soares Cruzes *et al.*, 2018).

### 4.3.11 CLASP (Comprehensive, Lightweight Application Security Process)

Είναι μια ελαφριά διαδικασία για την ανάπτυξη ασφαλών συστημάτων λογισμικού. Προτείνει μια σειρά από δραστηριότητες σε όλο τον κύκλο ζωής ανάπτυξης λογισμικού. Αυτές οι δραστηριότητες μπορούν να επιλεγούν ανάλογα με την ανάγκη και το είδος του έργου. Σε υψηλότερο επίπεδο, η διαδικασία CLASP για τον καθορισμό των απαιτήσεων ασφαλείας μπορεί να περιγραφεί με τέσσερα βήματα: (1) προσδιορισμός ρόλων και πόρων (2) κατηγοριοποίηση των πόρων (3) προσδιορίζοντας τις αλληλεπιδράσεις και τις εξαρτήσεις μεταξύ των πόρων και (4) καθορισμός μηχανισμών για την αντιμετώπιση των βασικών θεμάτων ασφάλειας.

### 4.3.12 SQUARE (Security Quality Requirements Engineering Method)

Είναι μια ολοκληρωμένη μέθοδος που αναπτύχθηκε για την εξαγωγή, την κατηγοριοποίηση και την ιεράρχηση των απαιτήσεων ασφαλείας σε έναν οργανισμό. Στόχος του είναι να ενσωματώσει τις απαιτήσεις ασφάλειας στα αρχικά στάδια ανάπτυξης λογισμικού. Είναι εφαρμόσιμο σε έργα λογισμικού πραγματικού κόσμου, καθώς παρέχει μια εύκολα προσαρμόσιμη μεθοδολογία και συνιστά τεχνικές που έχουν ήδη αναπτυχθεί στον τομέα της Μηχανικής Απαιτήσεων Ασφαλείας. Η SQUARE υποστηρίζει εννέα βήματα τα οποία είναι: (1) συμφωνία όλων των ενδιαφερομένων σε κοινούς ορισμούς; (2) προσδιορισμός των στόχων ασφάλειας; (3) ανάπτυξη αντικειμένων; (4) εκτελεί ανάλυση κινδύνου; (5) επιλογή της κατάλληλης τεχνικής εξαγωγής; (6) πρόκληση απαιτήσεων ασφαλείας; (7) κατηγοριοποίηση απαιτήσεων; (8) ιεράρχηση των απαιτήσεων και (9) επιθεώρηση των τελικών απαιτήσεων. Κάθε βήμα έχει ορισμένα κριτήρια εξόδου τα οποία πρέπει να πληρούνται πριν μεταβείτε στο επόμενο βήμα, αν και ορισμένα από τα βήματα μπορούν να εκτελεστούν παράλληλα. Μια συγκριτική μελέτη (Mead and Abu-Nimeh, 2019) του SQUARE με άλλες προσεγγίσεις όπως CLASP, SREP και Tropos έχει διεξαχθεί, παρέχοντας κάποιες βασικές κατευθυντήριες γραμμές για την επιλογή προσεγγίσεων SRE ανάλογα

με τις ανάγκες του έργου. Η αποτελεσματικότητα της μεθοδολογίας SQUARE μελετήθηκε χρησιμοποιώντας διάφορα σχετικά κριτήρια που σχετίζονται με τις απαιτήσεις ασφαλείας. Μια μέθοδος έχει αναπτυχθεί χρησιμοποιώντας το SQUARE για τον προσδιορισμό των απαιτήσεων απορρήτου. Το eSQUARE, ένα διαδικτυακό εργαλείο, αναπτύχθηκε με βάση τη γλώσσα Z για τη μοντελοποίηση και τον έλεγχο της συνέπειας των απαιτήσεων ασφαλείας. Το Ametrics έχει αναπτυχθεί για τη μέτρηση των απαιτήσεων ασφαλείας και ευθυγραμμίστηκε με τη μεθοδολογία SQUARE. Στο (Mead and Abu-Nimeh, 2019), οι συγγραφείς έχουν ενσωματώσει απαιτήσεις απορρήτου στη μεθοδολογία SQUARE προκειμένου να προσδιορίσουν τους κινδύνους απορρήτου εκτός από τους κινδύνους ασφαλείας. Το SQUARE έχει εφαρμοστεί με επιτυχία σε πολλά έργα ανάπτυξης λογισμικού σε ακαδημαϊκούς.

### 4.3.13 MSRA (Multilateral Security Requirements Analysis)

Σε ένα δικτυακό περιβάλλον, διαφορετικοί χρήστες που αλληλεπιδρούν με το σύστημα έχουν διαφορετικές και αντικρουόμενες απαιτήσεις ασφαλείας. Οι χρήστες ενδέχεται να έχουν διαφορετικούς στόχους ασφαλείας όχι μόνο έναντι των κακόβουλων χρηστών αλλά και έναντι άλλων τελικών χρηστών των συστημάτων. Αυτές οι απαιτήσεις είναι συχνά αντικρουόμενες και εξαρτώνται από το πλαίσιο του συστήματος. Οι (Anwar Mohammad, Nazir and Mustafa, 2019) έχουν περιγράψει μια μεθοδολογία που ενσωματώνει τους στόχους ασφαλείας των τελικών χρηστών και διευκολύνει την πρόκληση απαιτήσεων ασφαλείας. Η μέθοδος που προτείνεται από τους συγγραφείς αποτελείται από επτά βήματα: καθορισμός ρόλων και υποομάδων, πραγματοποίηση λειτουργικής ανάλυσης του συστήματος, ομαδοποίηση λειτουργιών σε λίστα επεισοδίων, χρήση προτιμήσεων ασφαλείας για διαφορετικά επεισόδια, δημιουργία λίστας στόχων ασφαλείας, διαμόρφωση στόχων ασφαλείας και τέλος συνθέτοντας όλους τους στόχους ασφαλείας για να καταλήξουμε σε ένα σύνολο απαιτήσεων ασφαλείας. Οι (Gregoire *et al.*, 2007) έχουν προτείνει μια πολυμερή προσέγγιση για την ενσωμάτωση και τη διατήρηση της ιδιωτικής ζωής σε πανταχού παρόντα περιβάλλοντα. Η προσέγγιση αρθρώνει τους στόχους ασφαλείας και τις απαιτήσεις του συστήματος.

### 4.3.14 SRE Methods Based on AGILE

Οι ιστορίες κατάχρησης χρησιμοποιούνται ευρέως στη μεθοδολογία AGILE για την εξαγωγή και τη διατύπωση απαιτήσεων ασφαλείας. Προσδιορίζουν όλους τους

πιθανούς τρόπους με τους οποίους ένας εισβολέας μπορεί να βλάψει το σύστημα. Ο Peeters (Daneva and Wang, 2018) πρότεινε μια νέα έννοια των ιστοριών καταχρήσεων για την επίτευξη διασφάλισης ασφάλειας και ιχνηλασιμότητας των απαιτήσεων ασφαλείας στο AGILE. Χρησιμοποιούνται επίσης άλλες μέθοδοι AGILE όπως το Scrum και ο Extreme Programming (XP) στην ανάπτυξη ασφαλών συστημάτων λογισμικού. Το μοντέλο FLAMIRA υιοθετεί ιστορίες χρηστών και καταχραστών για να ενσωματώσει τις ανάγκες ασφαλείας με τις απαιτήσεις λογισμικού με επαναληπτικό τρόπο. Ένα υβριδικό πλαίσιο που περιλαμβάνει ιστορίες καταχραστών και δέντρα επιθέσεων έχει αναπτυχθεί για την εξαγωγή απαιτήσεων στο Agile Software Development (ASD). Οι Bostrom et al. πρότειναν μια επέκταση των πρακτικών Extreme Programming (XP) που εφαρμόζουν ιστορίες χρήστη, καταχραστών και χρήστες που σχετίζονται με την ασφάλεια ιστορίες, για να βοηθήσει τους προγραμματιστές στις απαιτήσεις ασφάλειας μηχανικής. Οι (Bezerra, Sampaio and Marinho, 2020) πρότειναν μια προσέγγιση για τις απαιτήσεις ασφάλειας εξόρυξης από το αποθετήριο Common Vulnerabilities and Exposure (CVE) στο Agile Software Development. Η προσέγγιση βοηθά στην εξαγωγή απαιτήσεων ασφαλείας που μπορεί να παραμεληθούν από τον αναλυτή κατά τη διαδικασία ανάπτυξης.

### 4.3.15 SecureUML

Είναι μια γλώσσα μοντελοποίησης που βασίζεται σε aUML για την ανάπτυξη ασφαλών και κατανεμημένων συστημάτων. Ενσωματώνει πολιτικές ελέγχου πρόσβασης βάσει ρόλου (RBAC) στο διάγραμμα κλάσης UML χρησιμοποιώντας μια σημείωση γνωστή ως UMLprofile, παρέχοντας έτσι τη σημασιολογία που απαιτείται για τον σχολιασμό των διαγραμμάτων με χαρακτηριστικά ελέγχου πρόσβασης. Ο έλεγχος εξουσιοδότησης διαχειρίζεται επίσημα το OCL (Object Constraint Language) που αντιπροσωπεύει τις πολιτικές RBAC για διάφορα στοιχεία. Το πεδίο εφαρμογής αυτού του μοντέλου περιορίζεται μόνο στις προδιαγραφές και το σχεδιασμό ασφαλών συστημάτων. Δεν υποστηρίζει την εκκίνηση, επαλήθευση, επικύρωση και διαχείριση απαιτήσεων ασφαλείας. Έχει πραγματοποιηθεί μια συγκριτική μελέτη (Matulevicius, Lakk and Lepmets, 2011) του SecureUML με UMLsec. Μια διαδικασία μετασχηματισμού μεταξύ διαγραμμάτων SecureUML και UMLsec έχει συζητηθεί.

### 4.3.16 UMLsec

Αυτή η προσέγγιση επεκτείνει γνωστά διαγράμματα UML, όπως διαγράμματα κλάσεων, διαγράμματα διαγραμμάτων καταστάσεων και διαγράμματα ακολουθίας, χρησιμοποιώντας ελαφρούς μηχανισμούς επέκτασης, όπως στερεότυπα, ετικέτες και περιορισμούς για να ενσωματωθούν απαιτήσεις ασφαλείας. Υποστηρίζει την επίσημη σημασιολογία και εξετάζει το μοντέλο ενός εισβολέα που βασίζεται σε γνώσεις αντιπάλου και τομέα που βασίζεται σε υποθέσεις. Αυτή η επέκταση, που αναπτύχθηκε από εμπειρίες με διάφορα κυβερνητικά έργα στη Γερμανία, επιτρέπει την επίσημη επαλήθευση των απαιτήσεων ασφαλείας, αλλά δεν υποστηρίζει την επαλήθευση, την επικύρωση και την πληρότητα άλλων λειτουργικών και μη λειτουργικών απαιτήσεων. Χρησιμοποιείται κυρίως για τον καθορισμό και το σχεδιασμό των απαιτήσεων ασφαλείας ενός συστήματος.

Ένα αυτοματοποιημένο εργαλείο επαλήθευσης έχει αναπτυχθεί για την επαλήθευση του μοντέλου UMLsec και ένα άλλο εργαλείο έχει δημιουργηθεί για τη διαχείριση και την ανάλυση μηχανισμών ελέγχου πρόσβασης βάσει αδειών ασφαλείας εντός του μοντέλου. Τα μοντέλα UMLsec που βασίζονται στις απαιτήσεις ασφαλείας του συστήματος συζητούνται στο (Hatebur *et al.*, 2011). Επίσης, προτείνεται μια επέκταση της σημειογραφίας των καταστάσεων UML για να μοντελοποιηθούν πτυχές ασφάλειας. Αν και παρόμοια με το UMLsec, αυτή η επέκταση διαφέρει κυρίως στον στερεότυπο συμβολισμό: ο στερεότυπος συμβολισμός του UMLsec βοηθά στην επίσημη δήλωση απαιτήσεων που περιορίζουν τη συμπεριφορά των γραφημάτων καταστάσεων, ενώ ο προτεινόμενος συμβολισμός βοηθά στη διάκριση διαφορετικών τύπων καταστάσεων.

Επιπλέον, μια ασφαλής μεθοδολογία ανάπτυξης λογισμικού για το σχεδιασμό εφαρμογών Ιστού χρησιμοποιώντας τη γλώσσα μοντελοποίησης UMLsec προτείνεται στο (Lee *et al.*, 2019).

### 4.3.17 Misuse case

Αποτελεί ένα εργαλείο μοντελοποίησης που έχει σχεδιαστεί για να προσομοιώνει τη συμπεριφορά εχθρικών προς το υπό ανάπτυξη σύστημα παραγόντων. Αυτό το εργαλείο χρησιμοποιείται παράλληλα με το τυπικό διάγραμμα περιπτώσεων χρήσης UML για τη μοντελοποίηση ανεπιθύμητων συμπεριφορών εντός του συστήματος. Το διάγραμμα περίπτωσης κακής χρήσης απεικονίζει απειλές και επιτιθέμενους, μαζί με τις

κατευθυνόμενες συσχετίσεις τους. Διάφορες σχέσεις μέσα στο διάγραμμα περιλαμβάνουν απειλές, περιλαμβάνει και επεκτείνεται. Παρόλο που το διάγραμμα περίπτωσης κακής χρήσης καταγράφει μόνο μια βασική επισκόπηση των απειλών, έχει προταθεί ένα πρότυπο για να παρέχει μια λεπτομερή περιγραφή των απειλών και των επιτιθέμενων. Αυτά τα πρότυπα διευκολύνουν την επαναχρησιμοποίηση των απαιτήσεων ασφαλείας με την αφαίρεση τους σε μια αποθήκη γενικών απειλών. Η προσέγγιση που βασίζεται στην επαναχρησιμοποίηση που προτείνεται από τους (Guttorm and Andreas L., 2008) η χρήση υποθέσεων κατάχρησης περιλαμβάνει τα ακόλουθα βήματα: (1) αναγνώριση περιουσιακών στοιχείων, (2) τον καθορισμό στόχων ασφάλειας για κάθε περιουσιακό στοιχείο, (3) ανάλυση απειλών για την ασφάλεια, (4) τον προσδιορισμό του κινδύνου που σχετίζεται με τις απειλές. και (5) καθορισμός των απαιτήσεων ασφαλείας.

Ένα πλαίσιο έχει αναπτυχθεί για την αντιμετώπιση ελαττωμάτων στα μοντέλα περιπτώσεων κακής χρήσης, βελτιώνοντας έτσι την ποιότητα του μοντέλου. Στο (El-Attar, 2014), οι συγγραφείς προτείνουν μια επίσημη δομή για την καταγραφή περιγραφών περιπτώσεων κακής χρήσης και μια τεχνική μετασχηματισμού μοντέλων βασισμένη σε εργαλεία για τη συστηματική μετατροπή αυτών των δομών σε διαγράμματα κακής δραστηριότητας. Διάφορες μετρήσεις έχουν αναπτυχθεί για να βοηθήσουν τους προγραμματιστές να εντοπίσουν και να διορθώσουν ελαττώματα και ελαττώματα στα μοντέλα περιπτώσεων κακής χρήσης. Η οπτική σύνταξη του μοντέλου βελτιώθηκε με χρώματα και εικονίδια για καλύτερη αναγνωσιμότητα. Το μοντέλο επεκτάθηκε (Guttorm and Andreas L., 2008) για να αντιμετωπίσει άλλους παράγοντες αξιοπιστίας όπως η διαθεσιμότητα, η αξιοπιστία και η ευρωστία. Έχει δημιουργηθεί μια μέθοδος για τη δημιουργία περιπτώσεων κακής χρήσης χρησιμοποιώντας την ταξινόμηση STRIDE κατά τη φάση ανάλυσης κινδύνου της ανάπτυξης ασφαλούς λογισμικού. Οι El-Attar et al. πρότεινε ένα πλαίσιο για την ανάπτυξη συνεπών μοντέλων περιπτώσεων κακής χρήσης. Μια προσέγγιση για τη μοντελοποίηση τρωτών σημείων, κινδύνων και αντίμετρων έχει επίσης αναπτυχθεί χρησιμοποιώντας το μοντέλο περίπτωσης κακής χρήσης. Οι (Faily and Fléchais, 2016) συζητούν ζητήματα που σχετίζονται με περιπτώσεις κακής χρήσης (σενάρια για τη μοντελοποίηση αποφάσεων ασφαλούς σχεδιασμού και χρηστικότητας) και πώς αυτά μπορούν να βοηθήσουν στην αντιμετώπιση ακατάλληλων σχεδίων ασφαλείας και επακόλουθης κακής χρήσης του συστήματος. Το μοντέλο περιορισμένης κακής χρήσης (RMCM), μια προσέγγιση μοντελοποίησης βασισμένη σε περιπτώσεις χρήσης για τον καθορισμό

και την ανάλυση των απαιτήσεων ασφάλειας και απορρήτου, προτείνεται στο (Mai *et al.*, 2018). Αυτή η προσέγγιση βοηθά στην ανάλυση απειλών για την ασφάλεια, σεναρίων απειλών και στον μετριασμό τους σε μια δομημένη και αναλύσιμη μορφή. Banerjee et al. πρότεινε έναν αλγόριθμο για τον εντοπισμό τρωτών σημείων και περιπτώσεων κακής χρήσης κατά τη φάση των απαιτήσεων χρησιμοποιώντας πρότυπα προσαρμοσμένα στον κλάδο όπως το Common Vulnerability Scoring System (CVSS) και το Common Vulnerabilities Enumeration (CVE). Αναπτύχθηκε μια προσέγγιση για την ευθυγράμμιση των μετρήσεων απαιτήσεων ποιότητας που προσανατολίζονται στην κακή χρήση με τις τεχνικές μηχανικής εκμάθησης για την ανάλυση και τον καθορισμό απαιτήσεων ασφαλείας.

### 4.3.18 MOSRE (Model-Oriented Security Requirements Engineering Framework)

Αυτή η προσέγγιση ακολουθεί μια επαναληπτική διαδικασία που χρησιμοποιεί διάφορες μεθόδους, όπως περιπτώσεις κακής χρήσης, περιπτώσεις χρήσης και πολλά άλλα για την πρόκληση, την επαναχρησιμοποίηση, την ανάλυση και την ιχνηλασιμότητα των απαιτήσεων ασφαλείας. Εφαρμόζεται σε όλες τις υποφάσεις της φάσης των απαιτήσεων, με ιδιαίτερη έμφαση στις δραστηριότητες ασφάλειας. Εκτός από τις απαιτήσεις ασφάλειας, αυτή η προσέγγιση βοηθά στον εντοπισμό στόχων, στόχων και λειτουργικών απαιτήσεων IS. Τα βήματα που εμπλέκονται βασίζονται εν μέρει στη μεθοδολογία SQUARE και περιγράφουν 16 βήματα για την απόκτηση απαιτήσεων ασφαλείας:

- Προσδιορισμός των στόχων του συστήματος.
- Διαμόρφωση των ενδιαφερόμενων μερών.
- Εντοπισμός των περιουσιακών στοιχείων.
- Επιλογή μιας τεχνικής εξαγωγής.
- Απόκτηση ενός αρχιτεκτονικού διαγράμματος υψηλού επιπέδου.
- Καθορισμός στόχων και απαιτήσεων που δεν αφορούν την ασφάλεια.
- Δημιουργία διαγράμματα περίπτωσης χρήσης.
- Προσδιορισμός στόχων ασφάλειας.
- Προσδιορισμός απειλών και τρωτών σημείων.
- Προκαθορισμός εκτίμησης κινδύνου.

- Να δοθεί προτεραιότητα και κατηγοριοποιήστε τις απειλές και τα τρωτά σημεία.
- Δημιουργία διαγραμμάτων περιπτώσεων κακής χρήσης.
- Να γίνει προσδιορισμός των απαιτήσεων ασφαλείας.
- Απαραίτητο είναι η δημιουργία διαγραμμάτων περιπτώσεων χρήσης με βάση τις απαιτήσεις ασφαλείας.
- Δημιουργία μοντέλων δομικής ανάλυσης.
- Ανάπτυξη διαγραμμάτων UML.

Αυτή η προσέγγιση έχει επικυρωθεί σε μια κρίσιμη για την ασφάλεια εφαρμογή web για τον καθορισμό και την ανάλυση απαιτήσεων ασφαλείας. Έχει επίσης εφαρμοστεί με επιτυχία για την πρόκληση απαιτήσεων ασφαλείας σε ασφαλή συστήματα ηλεκτρονικής ψηφοφορίας, εφαρμογές ηλεκτρονικής υγείας και συστήματα λογισμικού ηλεκτρονικής διακυβέρνησης.

### 4.3.19 ISSRM (Information System Security Risk Management)

Αυτή η συστηματική προσέγγιση αντιμετωπίζει ζητήματα που σχετίζονται με τον κίνδυνο ασφάλειας σε ένα σύστημα πληροφοριών (Oueslati, Rahman and Othmane, 2015). Το μοντέλο έχει σχεδιαστεί με βάση μια εκτενή έρευνα διαφόρων προτύπων διαχείρισης κινδύνου, προτύπων ασφαλείας, μεθόδων διαχείρισης κινδύνου και πλαισίων μηχανικής λογισμικού. Υποστηρίζει την ευθυγράμμιση άλλων γλωσσών μοντελοποίησης ασφάλειας με τη διαχείριση κινδύνου και αντιμετωπίζει ζητήματα που σχετίζονται με τον κίνδυνο με εστιασμένο και συστηματικό τρόπο, που υποστηρίζεται από τα προαναφερθέντα πρότυπα. Η διαδικασία ISSRM είναι επαναληπτική και περιλαμβάνει έξι βήματα:

- Προσδιορισμός των περιουσιακών στοιχείων και καθορισμός του πλαισίου του οργανισμού.
- Προσδιορισμός των στόχων ασφαλείας για τα προσδιορισμένα περιουσιακά στοιχεία.
- Ανάλυση των κινδύνων για τα προσδιορισμένα περιουσιακά στοιχεία.
- Προσδιορισμός των αποφάσεων αντιμετώπισης κινδύνου (αποφυγή κινδύνου, μείωση κινδύνου, μεταφορά κινδύνου ή διατήρηση κινδύνου).

- Καθορισμός των απαιτήσεων ασφαλείας ως πιθανές λύσεις για τον μετριασμό του κινδύνου.
- Εφαρμογή των απαιτήσεων ασφαλείας με τη μορφή ελέγχων ασφαλείας (αντίμετρα).

Δεδομένου ότι η διαδικασία είναι επαναληπτική, μπορεί να εντοπίσει νέους κινδύνους και ελέγχους ασφαλείας μετά από κάθε επανάληψη. Ένα σύνολο μετρήσεων έχει αναπτυχθεί για τη βελτίωση του μοντέλου ISSRM. Οι συγγραφείς στο (Mead, Miyazaki and Zhan, 2011) έχουν ευθυγραμμίσει το μοντέλο ISSRM με διαγράμματα κακής δραστηριότητας και Secure TROPOS, αντίστοιχα, για τη διαχείριση του κινδύνου ασφαλείας στη φάση των απαιτήσεων.

### 4.3.20 Ontology-Based SRE Approaches

Οι οντολογίες είναι πολύτιμες για τον χαρακτηρισμό και τη χαρτογράφηση διαφόρων τύπων γνώσης σε παρόμοιους τομείς. Μια καλά σχεδιασμένη οντολογία απαιτήσεων ασφαλείας μπορεί να βοηθήσει τους μηχανικούς απαιτήσεων να αναφέρουν αποτελεσματικά συμβάντα, να επαναχρησιμοποιήσουν απαιτήσεις ασφαλείας από παρόμοιους τομείς και να συζητήσουν ζητήματα συνεργατικά, εναρμονίζοντας έτσι αόριστα καθορισμένη ορολογία. Οι (Elahi, Yu and Zannone, 2009) προσδιόρισε τις βασικές έννοιες που είναι απαραίτητες για την εξαγωγή απαιτήσεων ασφάλειας από τη βιβλιογραφία και πρότεινε μια οντολογία για την ενσωμάτωση των τρωτών σημείων σε διαφορετικά πλαίσια μοντελοποίησης. Στο (Pavlidis *et al.*, 2017), οι συγγραφείς ανέπτυξαν και συνδύασαν μια οντολογία ανάλυσης κινδύνου και μια οντολογία απαιτήσεων για να αντιπροσωπεύουν επίσημα επαναχρησιμοποιήσιμες απαιτήσεις ασφαλείας. Με βάση αυτό το πλαίσιο, ανέπτυξαν μια ελαφριά μέθοδο για να προκαλέσουν και να καθορίσουν απαιτήσεις ασφαλείας.

Αναπτύχθηκε μια οντολογία (Massacci *et al.*, 2011) για να ενοποιήσει διάφορες έννοιες από τα πλαίσια προβλημάτων και τις μεθοδολογίες Secure i* για τις απαιτήσεις ασφάλειας μηχανικής. Μια οντολογία για την εξαγωγή απαιτήσεων ασφάλειας σε συστήματα πληροφοριών προτάθηκε στο (Souag *et al.*, 2015) και οι συγγραφείς αξιολόγησαν την πληρότητά της σε σχέση με άλλες υπάρχουσες οντολογίες ασφάλειας. Επιπλέον, δημιουργήθηκε ένα διαδραστικό περιβάλλον για τη διευκόλυνση της χρήσης και επαναχρησιμοποίησής του. Ένα σύστημα συστάσεων βασισμένο σε οντολογία για την εξαγωγή σχετικών απαιτήσεων ασφαλείας έχει προταθεί στο (Williams, 2018).

Ακολουθεί ένας αναλυτικός πίνακας που συνοψίζει κάθε προσέγγιση Απαιτήσεων Ασφαλείας (SRE) και περιλαμβάνει τον σκοπό του πλαισίου, τα κύρια βήματα ή τις μεθόδους, την εστίαση εντός του SDLC, τα εργαλεία και τους περιορισμούς:

**Πίνακας 1 Αναλυτικός πίνακας που συνοψίζει κάθε προσέγγιση Απαιτήσεων Ασφαλείας (SRE) και περιλαμβάνει τον σκοπό του πλαισίου, τα κύρια βήματα ή τις μεθόδους, την εστίαση εντός του SDLC, τα εργαλεία και τους περιορισμούς**

| Προσέγγιση SRE | Περιγραφή & Σκοπός | Βασικά Βήματα ή Μέθοδοι | Υποστήριξη εργαλείων | Περιορισμοί |
|---|---|---|---|---|
| **SREF (Security Requirements Engineering Framework)** | Ενσωματώνει τη μηχανική απαιτήσεων με την ασφάλεια για τον εντοπισμό, την ανάλυση και την ικανοποίηση των απαιτήσεων ασφαλείας. | 1. Προσδιορίζει επιχειρηματικές απαιτήσεις 2. Θέτει στόχους ασφάλειας 3. Προσδιορίζει τις απαιτήσεις ασφάλειας 4. Διαμορφώνει επιχειρήματα ικανοποίησης που στοχεύουν στο να ανταποκριθούν πλήρως στις απαιτήσεις | Περιορισμένα επίσημα/ημι-επίσημα εργαλεία επιχειρημάτων | Περιορισμένη επεκτασιμότητα. Η πολυπλοκότητα της διαδικασίας μπορεί να περιορίσει την ευελιξία για δυναμικά περιβάλλοντα |
| **CORAS** | Ανάλυση ασφάλειας βάσει μοντέλου χρησιμοποιώντας διαγράμματα μοντελοποίησης κινδύνου εμπνευσμένα από το UML, με στόχο | 1. Συναντήσεις πελατών για τον εντοπισμό στόχων 2. Καθορισμός στόχων και υποθέσεων ασφαλείας 3. Ανάλυση απειλών, ευπάθειας και κινδύνου 4. Εργαστήρια για την αξιολόγηση πιθανοτήτων απειλών 5. Εκτίμηση ανάλυσης κινδύνου | Εργαλεία που βασίζονται σε UML, διαγράμματα CORAS | Μπορεί να είναι πολύπλοκο για μικρά έργα. η αρχική δέσμευση πελατών είναι χρονοβόρα |

| | | | | |
|---|---|---|---|---|
| | τον εντοπισμό απειλών, τρωτών σημείων και σχετικών κινδύνων. | 6. Προτάσεις για διορθωτικά μέτρα. | | |
| **SREP (Security Requirements Engineering Process)** | Επαναληπτική και βασισμένη σε επαναχρησιμοποίηση εξελικτική προσέγγιση χρησιμοποιώντας πρότυπα απειλών και περιπτώσεων χρήσης, επιτρέποντας την επαναχρησιμοποίηση της γνώσης για τον έγκαιρο εντοπισμό των απαιτήσεων ασφαλείας. | 1. Συμφωνία σχετικά με τους ορισμούς 2. Προσδιορισμός κρίσιμων περιουσιακών στοιχείων 3. Καθορισμός στόχων ασφάλειας 4. Προσδιορισμός απειλών (SRR/περιπτώσεις κακής χρήσης) 5. Εκτίμηση κινδύνου 6. Αιτίες ασφαλείας 7. Προτεραιότητα απαιτήσεων 8. Επικύρωση απαιτήσεων 9. Τροποποίηση του αποθετηρίου γνώσης. | Αποθετήριο πόρων ασφαλείας (SRR) | Περιορισμένη επεκτασιμότητα λόγω εξάρτησης από το χώρο αποθήκευσης. απαιτεί εκτεταμένη ρύθμιση για SRR |
| **Microsoft's Threat Modeling** | Πρακτική μοντελοποίηση απειλών με χρήση διαγραμμάτων ροής | 1. Μοντέλο συστήματος μέσω DFD 2. Αντιστοίχιση στοιχείων DFD σε στοιχεία STRIDE 3. Αναγνώριση απειλών 4. Έγγραφο απειλών. | μεθοδολογίες STRIDE και DREAD. Εργαλεία που βασίζονται στο STRIDE | Μπορεί να μην ταιριάζει σε όλα τα ευέλικτα περιβάλλοντα λόγω της εστίασης σε |

| | | | | |
|---|---|---|---|---|
| | δεδομένων και STRIDE για την αποκάλυψη τρωτών σημείων του συστήματος με βάση λειτουργικές απαιτήσεις. | | | DFD. Οι μετρήσεις DREAD χρειάζονται τακτικό έλεγχο |
| **CLASP** | Ελαφριά προσέγγιση για ασφαλή ανάπτυξη λογισμικού, προσαρμόσιμη στις ανάγκες του έργου, με επαναληπτικές δραστηριότητες σε όλο το SDLC. | 1. Προσδιορισμός ρόλων και πόρων 2. Κατηγοριοποίηση πόρων 3. Προσδιορισμός αλληλεπιδράσεων και εξαρτήσεων 4. Ορισμός μηχανισμών για την αντιμετώπιση ζητημάτων ασφάλειας. | Ελαφρά, ευέλικτα εργαλεία ενσωμάτωσης | Περιορισμένη κάλυψη απειλών για την ασφάλεια. Όχι τόσο ολοκληρωμένη για μεγάλα συστήματα |
| **SQUARE** | Δομημένη μεθοδολογία για τον προσδιορισμό, την κατηγοριοποίηση και την ιεράρχηση των απαιτήσεων ασφαλείας | 1. Συμφωνεί στους ορισμούς 2. Θέτει στόχους ασφαλείας 3. Αναπτύσσει τα απαραίτητα στοιχεία 4. Διεξάγει ανάλυση κινδύνου 5. | eSQUARE (εργαλείο που βασίζεται στο web). Μοντελοποίηση γλώσσας Z | Η πολυπλοκότητα στην ανάλυση κινδύνου μπορεί να επιβραδύνει τα ευέλικτα έργα. απαιτεί εκπαιδευμένο |

| | | | | |
|---|---|---|---|---|
| | στην αρχή του SDLC με έμφαση στη συναίνεση των ενδιαφερομένων. | Επιλέγει την κατάλληλη τεχνική εξαγωγής 6. Πρόκληση απαιτήσεων ασφάλειας 7. Κατηγοριοποίηση απαιτήσεων 8. Προτεραιότητα απαιτήσεων 9. Επιθεώρηση τελικών απαιτήσεων. | | προσωπικό για ανάλυση κινδύνου και εργαλεία ειδικά για το SQUARE |
| **MSRA (Multilateral Security Requirements Analysis)** | Διαχειρίζεται τις αντικρουόμενες ανάγκες ασφαλείας διαφορετικών χρηστών σε δικτυακά περιβάλλοντα ενσωματώνοντας στόχους ασφαλείας και εκμαιεύοντας απαιτήσεις ασφάλειας μέσω μιας διαδικασίας επτά βημάτων. | 1. Καθορισμός ρόλων/υποομάδων 2. Ανάλυση λειτουργικού συστήματος 3. Καταχώρηση λειτουργιών σε επεισόδια 4. Ορισμός προτιμήσεων ασφαλείας για επεισόδια 5. Δημιουργία λίστας στόχων ασφαλείας 6. Διαμόρφωση στόχων ασφαλείας 7. Σύνθεση στόχων ασφαλείας σε απαιτήσεις. | Εργαλεία διαμόρφωσης που βασίζονται σε ρόλους/υποομάδες | Πολυπλοκότητα στη διαχείριση αντικρουόμενων απαιτήσεων. μπορεί να είναι δύσκολο να εφαρμοστεί σε δυναμικά περιβάλλοντα |

| | | | | |
|---|---|---|---|---|
| **Μέθοδοι SRE που βασίζονται σε ευέλικτο τρόπο** | Χρησιμοποιεί ιστορίες κατάχρησης, Scrum και XP για την εξαγωγή και τη διαμόρφωση απαιτήσεων ασφαλείας σε ευέλικτες ρυθμίσεις με έμφαση στη διασφάλιση ασφάλειας και την ιχνηλασιμότητα. | 1. Ορισμός ιστοριών κατάχρησης 2. Δημιουργία ιστοριών εκμετάλλευσης 3. Ανάπτυξη ιστοριών χρηστών/καταχραστών 4. Ανάλυση κινδύνου χρησιμοποιώντας δεδομένα CVE/CVSS. | CVE, CVSS ενσωμάτωση αποθετηρίου. Agile εργαλεία (Scrum, XP) | Έχει τη δυνατότητα να αγνοήσει τις εις βάθος απαιτήσεις ασφάλειας. Απαιτεί συχνές ενημερώσεις για κατάχρηση ιστοριών και εκμετάλλευση ιστοριών |
| **SecureUML** | Μια γλώσσα μοντελοποίησης που βασίζεται σε aUML που ενσωματώνει πολιτικές RBAC σε διαγράμματα UML για τη διαχείριση του ελέγχου πρόσβασης σε ασφαλή, κατανεμημένα συστήματα. | 1. Ενσωματώνει πολιτικές RBAC σε διαγράμματα κλάσης UML 2. Χρησιμοποιεί τη γλώσσα περιορισμού αντικειμένου για έλεγχο πρόσβασης 3. Ενσωμάτωση του προφίλ UML για σχολιασμούς σημασιολογίας ασφαλείας. | Εργαλεία που βασίζονται σε UML και OCL | Περιορίζεται στον έλεγχο πρόσβασης. δεν υποστηρίζει την προετοιμασία, την επαλήθευση και την επικύρωση των απαιτήσεων ασφαλείας |

| | | | | |
|---|---|---|---|---|
| **UMLsec** | Επεκτείνει τα διαγράμματα UML με στερεότυπα, ετικέτες και περιορισμούς για να μοντελοποιήσει επίσημα τις απαιτήσεις ασφαλείας, με έμφαση στη γνώση των επιτιθέμενων και στις απαιτήσεις που βασίζονται σε απειλές. | 1. Επεκτείνονται τα διαγράμματα UML (κλάση, ακολουθία, κατάσταση) 2. Εκτελούνται γνώσεις αντιπάλου και μοντελοποίηση βάσει υποθέσεων 3. Χρησιμοποιούνται αυτοματοποιημένα εργαλεία επαλήθευσης. | Εργαλεία ειδικά για UMLsec. αυτοματοποιημένη επαλήθευση | Περιορισμένη επεκτασιμότητα για περιβάλλοντα που δεν είναι UML. περιορισμένη υποστήριξη για λειτουργικές απαιτήσεις που δεν αφορούν την ασφάλεια |
| **Misuse case** | Μοντελοποιεί ανεπιθύμητες συμπεριφορές σε συστήματα για την προσομοίωση και την αντιμετώπιση πιθανών απειλών, υποστηρίζοντας την ανάλυση απειλών, την | 1. Προσδιορισμός περιουσιακών στοιχείων 2. Καθορισμός στόχων ασφάλειας για περιουσιακά στοιχεία 3. Διεξαγωγή ανάλυσης απειλών 4. Εκτίμηση κινδύνου που σχετίζεται με απειλές 5. Καθορισμός απαιτήσεων ασφάλειας. | Διαγράμματα περιπτώσεων κακής χρήσης που βασίζονται σε UML | Καταγράφει μόνο βασική επισκόπηση απειλών. ενδέχεται να απαιτούνται πρόσθετα εργαλεία για την αντιμετώπιση σύνθετων σεναρίων απειλών |

| | | | | |
|---|---|---|---|---|
| | αξιολόγηση κινδύνου και τον επαναληπτικό καθορισμό απαιτήσεων ασφαλείας. | | | |
| **MOSRE (Model-Oriented Security Requirements Engineering)** | Επαναληπτικό πλαίσιο SRE για την εξαγωγή και ανάλυση απαιτήσεων ασφαλείας με χρήση υποθέσεων χρήσης και κακής χρήσης, επιτρέποντας την ιχνηλασιμότητα και υποστήριξη για λειτουργικούς στόχους ασφάλειας. | 1. Προσδιορισμός στόχων συστήματος και ενδιαφερόμενων μερών<br>2. Προσδιορισμός περιουσιακών στοιχείων 3. Επιλογή τεχνικής εξόρυξης 4. Δημιουργία αρχιτεκτονικών διαγραμμάτων υψηλού επιπέδου<br>5. Καθορισμός στόχων ασφάλειας<br>6. Εκτέλεση αξιολόγησης κινδύνου<br>7. Δημιουργία διαγραμμάτων περίπτωσης κακής χρήσης/χρήσης<br>8. Ανάπτυξη δομικής ανάλυσης/διαγραμμάτων UML | Εργαλεία UML, πρότυπα χρήσης/κακής χρήσης | Η πολύπλοκη διαδικασία πολλαπλών βημάτων μπορεί να είναι δύσκολο να εφαρμοστεί σε ευέλικτα έργα. εξαιρετικά λεπτομερείς για μικρότερα έργα |

| | | | | |
|---|---|---|---|---|
| **ISSRM (Information System Security Risk Management)** | Αντιμετωπίζει τους κινδύνους ασφαλείας στα συστήματα πληροφοριών, με ένα επαναληπτικό μοντέλο που υποστηρίζει πρότυπα και ελέγχους ασφάλειας που σχετίζονται με τον κίνδυνο. | 1. Προσδιορισμός των περιουσιακών στοιχείων και ορισμός του πλαισίου 2. Ορισμός στόχων ασφαλείας 3. Εκτέλεση ανάλυση κινδύνου 4. Λήψη των αποφάσεων διαχείρισης κινδύνου 5. Καθορισμός απαιτήσεων ασφαλείας 6. Εφαρμογή ελέγχων ασφαλείας. | Ασφαλής TROPOS, κακά διαγράμματα δραστηριότητας | Επαναληπτική διαδικασία χρονοβόρα. απαιτεί εκτεταμένες γνώσεις διαχείρισης κινδύνου |
| **Ontology-Based SRE** | Χρησιμοποιεί οντολογίες για την υποστήριξη της αναφοράς περιστατικών, της επαναχρησιμοποίησης απαιτήσεων και της συνοχής της ορολογίας στη μηχανική απαιτήσεων ασφαλείας. | 1. Ανάπτυξη οντολογίας απαιτήσεων ασφαλείας 2. Ευθυγράμμιση οντολογίας με πλαίσια ασφαλείας 3. Χρήση οντολογίας για ανάλυση κινδύνου και προδιαγραφές απαιτήσεων 4. Ενσωμάτωση οντολογίας ασφάλειας με μηχανισμούς επαναχρησιμοποίησης. | Εργαλεία συστάσεων που βασίζονται σε οντολογία | Η αρχική πολυπλοκότητα και οι ανάγκες πόρων για τη ρύθμιση οντολογίας ενδέχεται να απαιτούν εξειδίκευση στον τομέα |

| | | | | |
|---|---|---|---|---|
| **GBRAM (Goal-Based Requirements Analysis Methods)** | Επικεντρώνεται στον προσδιορισμό των απαιτήσεων ασφαλείας με βάση τους στρατηγικούς στόχους ενός οργανισμού, διασφαλίζοντας ότι τα μέτρα ασφαλείας ευθυγραμμίζονται με τους επιχειρηματικούς στόχους και τις ανάγκες των χρηστών. | 1. Προσδιορισμός των επιχειρηματικών στόχων και των στόχων ασφάλειας<br>2. Συντονισμός των στόχων ασφάλειας με τους οργανωτικούς στόχους<br>3. Διαμόρφωση απαιτήσεων βάσει προσδιορισμένων στόχων 4. Επικύρωση και ιεράρχηση απαιτήσεων<br>5. Επανάληψη της διαδικασίας όπως απαιτείται για τη βελτίωση των απαιτήσεων. | Εργαλεία ανάλυσης βάσει στόχων, πλαίσια | Απαιτεί σαφή καθορισμό των επιχειρηματικών στόχων. Μπορεί να χρειάζεται προσαρμογή για συγκεκριμένα περιβάλλοντα ή οργανισμούς |
| **KAOS** | Προσέγγιση προσανατολισμένη στο στόχο που ενσωματώνει τη λογική και την ανάλυση συγκρούσεων για επίσημες απαιτήσεις | Δίνει έμφαση στη συνέπεια και την πληρότητα. | Υποστηρίζεται εν μέρει από επίσημα εργαλεία μοντελοποίησης | Περιορισμένα δωρεάν εργαλεία. ημι-επίσημο, όχι πλήρως αυτοματοποιημένο |

| | | | | |
|---|---|---|---|---|
| | ασφάλειας (Van Lamsweerde). | | | |
| **Secure i*** | Μοντελοποίηση προσανατολισμένη σε πράκτορες με εστίαση στους συμβιβασμούς ασφαλείας μεταξύ των ενδιαφερομένων. περιλαμβάνει έννοιες όπως στόχος, καθήκον και απειλές (Liu, Yu, Mylopoulos). | Μοντελοποίηση απειλών, Ανάλυση Κινδύνων, Στόχοι της CIA | Γενικό μοντέλο, ανεπίσημα επικυρωμένο με χρήση επισήμανσης στόχου | Περιορισμένη υποστήριξη για συγκεκριμένο εργαλείο. |
| **Secure Tropos** | Προβολή συστήματος πολλαπλών πρακτόρων. ενσωματώνει ανάλυση εμπιστοσύνης και κινδύνου για να μοντελοποιήσει τις εξαρτήσεις και τους | Secure Tropos-SPL για σειρές προϊόντων λογισμικού (Susi et al., Mouratidis et al.). | Σχεδιασμός, Απαιτήσεις εργαλείο SecTro CASE για υποστήριξη μοντέλου | Περιορισμένη διαθεσιμότητα. ορισμένες επεκτάσεις δεν είναι ευρέως προσβάσιμες |

| | | | | |
|---|---|---|---|---|
| | στόχους μεταξύ των πρακτόρων. | | | |
| **Abuse frames** | Μια μέθοδος βασισμένη σε σενάρια που εστιάζει στον εντοπισμό και την ανάλυση απειλών του συστήματος μοντελοποιώντας ανεπιθύμητες συμπεριφορές. | Μοντελοποίηση απειλών, περιπτώσεις κατάχρησης | Περιορισμένη εργαλειοθήκη. χειροκίνητη δημιουργία πλαισίων κατάχρησης | Περιορισμένη επεκτασιμότητα για πολύπλοκα συστήματα |
| **SEPP** | Χρησιμοποιεί μοτίβα ασφαλείας για να αντιμετωπίζει συστηματικά ζητήματα ασφάλειας στο σχεδιασμό του συστήματος, εφαρμόζοντας | Μοτίβα ασφαλείας, Ανάλυση κινδύνου, Αναγνώριση απειλών | Μέτρια υποστήριξη μέσω βιβλιοθηκών προτύπων ασφαλείας | Περιορισμένη ευελιξία. η δυνατότητα εφαρμογής του μοτίβου ποικίλλει |

| | | | | |
|---|---|---|---|---|
| | επαναχρησιμοποιήσιμες λύσεις βασισμένες σε μοτίβα. | | | |

### 4.6 Συγκριτική ανάλυση των εργαλείων μοντελοποίησης απαιτήσεων ασφαλείας

Τα ευρήματα αυτής της μελέτης προέρχονται από συνοπτικές πληροφορίες από επιλεγμένες εργασίες, παρατηρούμενες τάσεις στη βιβλιογραφία, συγκριτική ανάλυση και αναλυτική αξιολόγηση, ακολουθούμενες από συζητήσεις μεταξύ των τριών συγγραφέων. Τα περισσότερα ευρήματα συνδέονται άμεσα με τα αποτελέσματα που προέκυψαν από την ανασκόπηση, τις γενικές πληροφορίες σχετικά με τις προσεγγίσεις SRE και οι ορολογίες που χρησιμοποιούνται από τις προσεγγίσεις SRE για την αντιμετώπιση των εννοιών ασφάλειας. Οι πληροφορίες σε αυτούς τους πίνακες βασίζονται στη βιβλιογραφική ανασκόπηση και, σε κάποιο βαθμό, στην αναλυτική αξιολόγηση από τους συγγραφείς. Ωστόσο, βασίζεται εξ ολοκλήρου στην αναλυτική αξιολόγηση και την κρίση των συγγραφέων σχετικά με τη χρηστικότητα των προσεγγίσεων SRE σε διάφορες υποφάσεις. Ενώ τα αποτελέσματα που σχετίζονται με αυτόν τον πίνακα μπορεί να είναι υποκειμενικά, η αυστηρότητα διατηρήθηκε μέσω των μέσων μετρήσεων βαθμολογίας και των ανεξάρτητων βαθμολογιών που κατανεμήθηκαν από όλους τους συγγραφείς στις προσεγγίσεις SRE στις διάφορες υποδραστηριότητες της φάσης των απαιτήσεων. Τα ευρήματα αυτής της μελέτης βασίζονται σε μια σύνθεση πληροφοριών από επιλεγμένες εργασίες, παρατηρούμενες τάσεις στη βιβλιογραφία, συγκριτικές αναλύσεις και αναλυτικές αξιολογήσεις, ακολουθούμενες από συζητήσεις και συζητήσεις μεταξύ των συγγραφέων. Τα βασικά ευρήματα της μελέτης συνοψίζονται ως εξής:

- Η περίπτωση κακής χρήσης, το Secure Tropos, το SQUARE και το SEPP εμφανίζονται ως οι πιο δημοφιλείς προσεγγίσεις μεταξύ των ερευνητών, όπως αποδεικνύεται από τη συχνότητα δημοσίευσής τους.
- Η μοντελοποίηση απειλών αναγνωρίζεται ευρέως ως μια κρίσιμη δραστηριότητα στον τομέα των απαιτήσεων ασφαλείας και υιοθετείται από την πλειονότητα των προσεγγίσεων SRE.
- Ενώ η ανάλυση κινδύνου είναι σημαντική για τη λεπτομέρεια των απειλών και την κατηγοριοποίησή τους, μόνο οι μισές από τις προσεγγίσεις SRE υποστηρίζουν αυτή τη δραστηριότητα.
- Η υποστήριξη εργαλείων βοηθά σημαντικά τους προγραμματιστές και τους ειδικούς σε θέματα ασφάλειας στη μοντελοποίηση απειλών, ωστόσο λιγότερες από τις μισές προσεγγίσεις SRE αναφέρουν ότι έχουν υποστήριξη εργαλείων.

- Οι προσεγγίσεις που βασίζονται σε UML όπως το SecureUML, το UMLsec και η περίπτωση κατάχρησης είναι κατάλληλες κυρίως για μεσαίου μεγέθους ή μικρά έργα, μια λεπτομέρεια που δεν τονίστηκε σε προηγούμενη έρευνα.
- Παρά την ύπαρξη διαφόρων προτύπων ασφαλείας, πολλές προσεγγίσεις SRE αποτυγχάνουν να τα ενσωματώσουν στις μεθοδολογίες τους.
- Οι επίσημες μέθοδοι παρέχουν μια αυστηρή βάση για την προδιαγραφή απαιτήσεων ασφαλείας, αλλά υιοθετούνται μόνο με λίγες προσεγγίσεις.
- Το SQUARE αναδεικνύεται ως η πιο αποτελεσματική και επιδραστική προσέγγιση στη φάση εξαγωγής απαιτήσεων, ακολουθούμενη από το MOSRE στη φάση της ανάλυσης απαιτήσεων.
- Οι KAOS και SREF προσδιορίζονται ως οι καλύτερες προσεγγίσεις στη φάση προδιαγραφής απαιτήσεων, ενώ οι KAOS, Secure Tropos και SREP είναι οι πιο αποτελεσματικές στην επικύρωση και διαχείριση απαιτήσεων.
- Η σύγκριση με βάση την ορολογία αποκαλύπτει κοινά σημεία στη χρήση όρων όπως "απειλή" και "τρωτότητα" μεταξύ των προσεγγίσεων SRE.

Η μελέτη διερευνά πολλές νέες οδούς στις απαιτήσεις ασφάλειας μηχανικής, συμπεριλαμβανομένων γνώσεων σχετικά με την αποτελεσματικότητα διαφορετικών μεθοδολογιών στα μεγέθη έργων, την υιοθέτηση επίσημων μεθόδων και την απόδοση προσεγγίσεων σε διάφορες υποφάσεις της φάσης των απαιτήσεων. Επιπλέον, καλύπτει νεότερες προσεγγίσεις όπως το MOSRE, τις προσεγγίσεις SRE που βασίζονται στην οντολογία και τις προσεγγίσεις SRE που βασίζονται σε ευέλικτο, οι οποίες έχουν κερδίσει εξέχουσα θέση αλλά δεν έχουν αναθεωρηθεί προηγουμένως. Αυτά τα ευρήματα συμβάλλουν στην κατανόηση των τρεχουσών βέλτιστων πρακτικών στον τομέα των SRE.

Τα ευρήματά αποκαλύπτουν ότι οι προσεγγίσεις SRE όπως η περίπτωση κακής χρήσης (Misuse Case), η Secure Tropos, η SQUARE και η SEPP έχουν την υψηλότερη συχνότητα δημοσίευσης και είναι ευρέως δημοφιλείς μεταξύ των ερευνητών. Αυτή η παρατήρηση επιβεβαιώνεται από προηγούμενες μελέτες, όπως αυτές των συγγραφέων (Mohammed *et al.*, 2017) και (Silva *et al.*, 2016), οι οποίες υπογραμμίζουν επίσης τη δημοτικότητα μεθόδων όπως η Secure Tropos. Επιπλέον, οι συγγραφείς (Mohammed *et al.*, 2017) εντόπισαν ότι οι προσεγγίσεις στην «εκτεταμένη κατηγορία που βασίζεται σε UML» έχουν τη δεύτερη υψηλότερη συχνότητα δημοσίευσης. Υποστηρίζονται ότι οι προσεγγίσεις SRE που βασίζονται σε UML είναι εξαιρετικά προσαρμόσιμες και

προτιμώνται από τους χρήστες. Βρέθηκε ότι οι μισές από τις προσεγγίσεις SRE υποστηρίζουν την ανάλυση κινδύνου, σύμφωνα με τα ευρήματα των συγγραφέων (Fabian *et al.*, 2010) και (Salini and Kanmani, 2012), οι οποίοι ανέφεραν παρόμοια υποστήριξη για την ανάλυση κινδύνου στις επισκοπήσεις τους.

Επιπλέον, σκιαγραφείται ότι η μοντελοποίηση απειλών είναι μια κρίσιμη δραστηριότητα που υποστηρίζεται από την πλειονότητα των προσεγγίσεων SRE, όπως αναφέρεται από τους συγγραφείς (Salini and Kanmani, 2012). Ωστόσο, πολύ λίγες προσεγγίσεις SRE ενσωματώνουν καθιερωμένα πρότυπα ασφαλείας, ένα εύρημα που σημειώθηκε επίσης σε προηγούμενες έρευνες, αν και πολλές πρόσφατες προσεγγίσεις SRE που εξετάστηκαν στη μελέτη μας δεν συμπεριλήφθηκαν στην ανάλυσή τους.

Μέσα από μια ανασκόπηση της βιβλιογραφίας και την αναλυτική αξιολόγηση, διαπιστώθηκε ότι προσεγγίσεις που βασίζονται σε UML, όπως το SecureUML, το UMLsec και η Misuse Case, είναι κατάλληλες κυρίως για μεσαίου μεγέθους ή μικρά έργα. Είναι ενδιαφέρον ότι προηγούμενες εργασίες ανασκόπησης δεν εξέτασαν προσεγγίσεις SRE σχετικά με το μέγεθος του έργου. Ομοίως, οι περισσότερες προσεγγίσεις SRE δεν υιοθετούν επίσημες μεθόδους, μια ιδιαίτερη πτυχή που δεν έχει τονιστεί από τους περισσότερους ερευνητές στις μελέτες τους. Επιπλέον, η μελέτη παρέχει νέες γνώσεις σχετικά με την απόδοση των προσεγγίσεων SRE σε διάφορες υποφάσεις της φάσης των απαιτήσεων, ένα θέμα που δεν είχε διερευνηθεί προηγουμένως στην υπάρχουσα έρευνα.

Επιπλέον, καλύπτονται νεότερες προσεγγίσεις όπως το MOSRE, τις προσεγγίσεις SRE που βασίζονται στην οντολογία και τις προσεγγίσεις SRE που βασίζονται σε ευέλικτο, οι οποίες έχουν αποκτήσει θέση μεταξύ των ερευνητών τα τελευταία χρόνια, αλλά δεν συμπεριλήφθηκαν σε προηγούμενες εργασίες ανασκόπησης. Αυτά τα αποτελέσματα και τα ευρήματα αποκαλύπτουν νέους δρόμους που είναι ζωτικής σημασίας για τις απαιτήσεις μηχανικής ασφάλειας και βοηθούν στον προσδιορισμό των τρεχουσών βέλτιστων πρακτικών στον τομέα των SRE.

Ο Πίνακας 2 παρέχει μια δομημένη σύγκριση διαφορετικών μεθοδολογιών Μηχανικών Απαιτήσεων Ασφαλείας (SRE) που βασίζονται σε διάφορα βασικά χαρακτηριστικά που σχετίζονται με την ανάπτυξη λογισμικού που εστιάζει στην ασφάλεια. Οι μεθοδολογίες ποικίλλουν ως προς την κύρια προσέγγισή τους, τη δυνατότητα εφαρμογής φάσης SDLC και τις συγκεκριμένες μεθόδους ασφαλείας που

υποστηρίζουν. Αυτή η συγκριτική ανάλυση υπογραμμίζει τις διακρίσεις και τις επικαλύψεις μεταξύ της αξιολόγησης κινδύνου, του προσανατολισμού των στόχων, των στρατηγικών που βασίζονται σε προβλήματα και των προσεγγίσεων που βασίζονται στην απειλή.

Προσέγγιση: Οι μεθοδολογίες διαφέρουν ως προς τη θεμελιώδη προσέγγισή τους για την εξαγωγή απαιτήσεων ασφάλειας. Για παράδειγμα, μέθοδοι προσανατολισμένες στον στόχο, όπως οι MOSRE, Secure Tropos, KAOS και GBRAM δίνουν προτεραιότητα στην ευθυγράμμιση των απαιτήσεων ασφαλείας με τους πρωταρχικούς στόχους του οργανισμού. Οι μέθοδοι που βασίζονται στον κίνδυνο όπως το SQUARE, το CLASP και το ISSRM επικεντρώνονται στην αξιολόγηση πιθανών κινδύνων και τρωτών σημείων, διασφαλίζοντας ότι τα μέτρα ασφαλείας αντιμετωπίζουν τις εντοπισμένες απειλές του συστήματος. Οι προσεγγίσεις που βασίζονται σε απειλές - εμφανείς στο SREP, το Microsoft Threat Modeling και τις περιπτώσεις κακής χρήσης - επικεντρώνονται στον εντοπισμό και την ανάλυση απειλών για την προληπτική αντιμετώπιση πιθανών παραβιάσεων της ασφάλειας. Ορισμένες μεθοδολογίες, όπως το SEPP, χρησιμοποιούν προσεγγίσεις που βασίζονται σε πρότυπα, εφαρμόζοντας επαναχρησιμοποιήσιμα μοτίβα για κοινές απαιτήσεις ασφαλείας.

Στάδιο: Διαφορετικές μεθοδολογίες εφαρμόζονται σε διάφορα στάδια του κύκλου ζωής ανάπτυξης λογισμικού (SDLC). Τα περισσότερα συγκεντρώνονται στην πρώιμη φάση του σχεδιασμού για να ενσωματώσουν την ασφάλεια νωρίς στη διαδικασία (π.χ. SQUARE, MOSRE, SecureUML και KAOS). Οι επαναληπτικές προσεγγίσεις όπως οι μέθοδοι ISSRM και Agile-based SRE Methods εκτείνονται σε πολλαπλά στάδια, διευκολύνοντας τη συνεχή αξιολόγηση κινδύνου και την προσαρμογή των απαιτήσεων ασφαλείας καθώς εξελίσσεται το σύστημα. Ορισμένα, όπως το CLASP, χρησιμοποιούνται σε όλες τις φάσεις SDLC, υποστηρίζοντας μια ολιστική, συνεχή εστίαση στην ασφάλεια.

Ανάλυση κινδύνου και απειλών: Πολλές από αυτές τις μεθοδολογίες περιλαμβάνουν βήματα για ανάλυση κινδύνου και ανάλυση απειλών σε διάφορους βαθμούς. Για παράδειγμα, το SQUARE και το ISSRM παρέχουν εκτεταμένη υποστήριξη για την αξιολόγηση κινδύνου, ενώ το Microsoft Threat Modeling and Misuse Cases έχουν σχεδιαστεί ειδικά για ολοκληρωμένη ανάλυση απειλών. Αυτές οι αναλύσεις βοηθούν

στην ιεράρχηση των απαιτήσεων ασφαλείας με βάση τον πιθανό αντίκτυπο των κινδύνων και των απειλών στα κρίσιμα περιουσιακά στοιχεία του συστήματος.

Κατηγοριοποίηση και ταξινόμηση: Η κατηγοριοποίηση και ταξινόμηση των απαιτήσεων ασφαλείας είναι ένα άλλο αξιοσημείωτο χαρακτηριστικό που υποστηρίζεται από μεθοδολογίες όπως το SQUARE, το MOSRE και το ISSRM. Αυτή η διαδικασία επιτρέπει τη δομημένη οργάνωση των απαιτήσεων, βοηθώντας τους προγραμματιστές να εκτιμήσουν τη σχετική σημασία διαφορετικών στόχων ασφάλειας και να κατανείμουν αποτελεσματικά τους πόρους.

Αναγνώριση απειλών: Ορισμένες μεθοδολογίες, όπως το ISSRM, το CORAS και το M-N Framework, δίνουν έμφαση στην αναγνώριση περιουσιακών στοιχείων, διασφαλίζοντας ότι τα κρίσιμα περιουσιακά στοιχεία του συστήματος προστατεύονται σύμφωνα με την αξία τους για τον οργανισμό. Αυτό το βήμα είναι απαραίτητο για τη δημιουργία μιας στοχευμένης στρατηγικής ασφάλειας που μετριάζει τις απειλές για τους πιο πολύτιμους πόρους.

Επικύρωση απαιτήσεων και επίλυση συγκρούσεων: Η επικύρωση του τελικού συνόλου απαιτήσεων ασφαλείας είναι ένα σημαντικό στοιχείο σε μεθοδολογίες όπως το MOSRE, το SREP και το Secure Tropos. Η επίλυση συγκρούσεων είναι μια άλλη κρίσιμη πτυχή, η οποία αντιμετωπίζεται σε μεθόδους προσανατολισμένες στο στόχο, όπως το MOSRE και το Secure Tropos, οι οποίες εξετάζουν πιθανές συγκρούσεις μεταξύ των στόχων ασφαλείας και άλλων στόχων του συστήματος.
Συμπερασματικά, κάθε μεθοδολογία προσφέρει μοναδικά πλεονεκτήματα και περιορισμούς με βάση το συγκεκριμένο πλαίσιο στο οποίο χρησιμοποιείται. Ενώ οι μεθοδολογίες προσανατολισμένες στον στόχο υπερέχουν στην ευθυγράμμιση της ασφάλειας με τους οργανωτικούς στόχους, οι προσεγγίσεις που βασίζονται στον κίνδυνο προσφέρουν ισχυρές άμυνες έναντι γνωστών τρωτών σημείων. Οι μελλοντικές εξελίξεις στο SRE θα μπορούσαν να ωφεληθούν από υβριδικές προσεγγίσεις που συνδυάζουν τα πλεονεκτήματα αυτών των μεθοδολογιών—όπως η ενσωμάτωση αξιολογήσεων κινδύνου με επίκεντρο τα περιουσιακά στοιχεία με πλαίσια προσανατολισμένα στον στόχο—για την παροχή ολοκληρωμένων λύσεων ασφάλειας σε όλες τις φάσεις ανάπτυξης συστήματος.

**Πίνακας 2 Πίνακας σύγκρισης μεθοδολογιών για τις απαιτήσεις ασφάλειας**

| *Μεθοδολογία* | *Στόχοι Ασφαλείας* | *Προσέγγιση* | *Στάδιο* | *Ανάλυση Κινδύνου* | *Ανάλυση Απειλών* | *Κατηγοριοποίηση/ Ταξινόμηση* | *Απειλές* | *Έλεγχος Απαιτήσεων* | *Προσδιορισμός συγκρούσεων* |
|---|---|---|---|---|---|---|---|---|---|
| KAOS | Security | Goal-Oriented | Early Design | X | X | | | | |
| Secure i* | Security / Privacy | Goal-Oriented | Early Design | X | X | | X | | |
| Secure Tropos | Security | Goal-Oriented | Early/Late Design | X | | | X | X | X |
| GBRAM | Security | Goal-Oriented | Early Design | | X | X | | X | X |
| Abuse Frames | Security | Problem based | UML Based | | X | | | | |
| SEPP | Security | Pattern-driven | Design | | X | | | | |
| SREF | Security | Problem based | Early Design | X | X | X | X | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| CORAS | Security | Risk Assessment Oriented | Early Design | X | X | X | X | | |
| SREP | Security | Threat-driven | Early Design | X | X | | | | |
| Microsoft's Threat Modeling | Security | Threat-driven | Early Design | X | X | | | | |
| CLASP | Security | Risk- driven | All system stages | X | X | | X | | |
| SQUARE | Security | Risk- driven | Early Design | X | X | X | | X | |
| MSRA | Security | Multi-party Goal-Oriented | Early Design | | | X | | X | |
| SRE METHODS | Security | Agile-driven | Iterative | X | | | | X | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| AGILE-BASED | | | | | | | | | |
| SecureUML | Security | Model-driven | Design | | | X | | | |
| UMLsec | Security | Model-driven | Design | X | | | | X | |
| Misuse Cases | Security | Threat-driven | Early Design | X | X | | | X | |
| MOSRE | Security | Goal-Oriented | Early Design | X | X | X | | X | X |
| ISSRM | Security | Risk- driven | Iterative | X | X | X | X | X | |
| Ontology-Based SRE Approaches | Security | Knowledge-based | Early Design | | | X | | | |

Ο Πίνακας 3 περιγράφει τις απαιτήσεις ασφαλείας που αντιμετωπίζει κάθε μεθοδολογία κατά τη διάρκεια του σχεδιασμού του συστήματος. Σε περιπτώσεις που επισημαίνονται με '~', οι υποστηρικτές της μεθοδολογίας δεν προσδιορίζουν τις απαιτήσεις ασφαλείας που εξετάζουν.

**Πίνακας 3 Απαιτήσεις ασφάλειας ανά μεθοδολογία**

| ***Μεθοδολογία*** | ***Απαιτήσεις Ασφαλείας*** |
|---|---|
| KAOS | Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Ιδιωτικότητα, Αυθεντικοποίηση, Μη αποποίηση |
| Secure i* | Εμπιστευτικότητα, Ιδιωτικότητα, Αυθεντικοποίηση, Έλεγχος πρόσβασης |
| Secure Tropos | Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Αυθεντικοποίηση, Μη αποποίηση, Λογοδοσία |
| GBRAM (Μέθοδος Ανάλυσης Απαιτήσεων Βάσει Στόχων) | ~ |
| Abuse frames (Πλαίσια Καταχώρησης) | ~ |
| SEPP (Security Engineering Process Using Patterns) | Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Εξουσιοδότηση |
| SREF (Security Requirements Engineering Framework) | Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Λογοδοσία |
| CORAS | Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα |
| SREP (Security Requirements Engineering Process) | ~ |
| Microsoft’s Threat Modeling | Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Τεκμηριωμένη Αξιοπιστία |
| CLASP (Comprehensive, Lightweight Application Security Process) | Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Ανθεκτικότητα, Επεκτασιμότητα |
| SQUARE (Security Quality Requirements Engineering Method) | Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα |
| MSRA (Multilateral Security Requirements Analysis) | Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Αυθεντικοποίηση, Βεβαιότητα |
| SRE Methods Based on AGILE | Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα |
| SecureUML | Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Αυθεντικοποίηση ,Έλεγχος πρόσβασης |
| UMLsec | Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα |
| Misuse case (Υποθέσεις Κατάχρησης) | ~ |

| | |
|---|---|
| MOSRE (Model-Oriented Security Requirements Engineering Framework) | Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Αυθεντικοποίηση, Εξουσιοδότηση, Έλεγχος πρόσβασης |
| ISSRM (Information System Security Risk Management) | Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Εκτίμηση Ρίσκου, Έλεγχος πρόσβασης |
| Ontology - Based SRE Approaches | Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Λογοδοσία |

Στον Πίνακα 3, παρουσιάζονται οι απαιτήσεις ασφάλειας που λαμβάνει υπόψη κάθε μεθοδολογία κατά τη διάρκεια του σχεδιασμού ενός συστήματος, αποδεικνύοντας ποικιλομορφία στη διαχείριση μη λειτουργικών απαιτήσεων ασφαλείας. Οι μέθοδοι αυτοί επικεντρώνονται σε διάφορα χαρακτηριστικά, όπως η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων, αλλά και σε πιο εξειδικευμένες απαιτήσεις όπως η αυθεντικοποίηση, ο έλεγχος πρόσβασης και η λογοδοσία.

Γίνεται σαφές ότι οι διαφορετικές μεθοδολογίες ασφάλειας επικεντρώνονται σε ποικίλες απαιτήσεις, αναδεικνύοντας τις προτεραιότητες και τους στόχους της καθεμιάς. Ορισμένες μεθοδολογίες, όπως οι KAOS, Secure Tropos και SREF, καλύπτουν ευρεία γκάμα απαιτήσεων, όπως η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα, προσφέροντας ένα πιο ολοκληρωμένο πλαίσιο ασφαλείας.

Αντίθετα, οι GBRAM και Abuse frames, δεν προσδιορίζουν σαφείς απαιτήσεις ασφαλείας, γεγονός που μπορεί να περιορίσει την εφαρμοσιμότητά τους σε πιο εξειδικευμένα περιβάλλοντα ασφάλειας.

Η ποικιλία στις απαιτήσεις ασφαλείας που καλύπτονται από κάθε μεθοδολογία υποδηλώνει την ανάγκη για προσεκτική επιλογή της κατάλληλης μεθόδου, ανάλογα με τις συγκεκριμένες ανάγκες του εκάστοτε συστήματος. Επιπλέον, οι μεθοδολογίες που περιλαμβάνουν εξειδικευμένα χαρακτηριστικά, όπως ο έλεγχος πρόσβασης και η λογοδοσία, φαίνεται να προσφέρουν μεγαλύτερη ευελιξία και ασφάλεια, ιδιαίτερα σε περιβάλλοντα με αυξημένες απαιτήσεις προστασίας. Συνεπώς, η επιλογή της μεθοδολογίας πρέπει να γίνεται με βάση τις συγκεκριμένες ανάγκες ασφαλείας του οργανισμού και τη φύση των δεδομένων που διαχειρίζεται.

# Κεφάλαιο 5 –Εργαλεία που υποστηρίζουν τις Προσεγγίσεις SRE

Στον τομέα της ασφάλειας των πληροφοριακών συστημάτων, η αποτελεσματική μοντελοποίηση των απαιτήσεων ασφαλείας είναι κρίσιμης σημασίας για τη διασφάλιση στιβαρού σχεδιασμού και λειτουργίας του συστήματος. Το παρόν κεφάλαιο παρουσιάζει μια λεπτομερή εξερεύνηση των εργαλείων που υποστηρίζουν τις προσεγγίσεις της Μηχανικής Απαιτήσεων Ασφαλείας (SRE), επισημαίνοντας τις μεθοδολογίες, τις δυνατότητες και τις εφαρμογές τους σε περιβάλλοντα εστιασμένα στην ασφάλεια. Κάθε εργαλείο που εξετάζεται σε αυτό το κεφάλαιο ευθυγραμμίζεται με συγκεκριμένες μεθοδολογίες SRE, προσφέροντας διακριτά χαρακτηριστικά για τον εντοπισμό, την ανάλυση και την αντιμετώπιση προβλημάτων ασφάλειας κατά τη διάρκεια του κύκλου ζωής ανάπτυξης του συστήματος. Το κεφάλαιο ξεκινά με μια συζήτηση της μεθοδολογίας του Objectiver μέσω του πλαισίου KAOS, το οποίο δίνει έμφαση στην ανάλυση προσανατολισμένη στο στόχο. Στη συνέχεια εξετάζει το ReqView, ένα ευέλικτο εργαλείο για τη διαχείριση της τεκμηρίωσης των απαιτήσεων, ακολουθούμενο από μια επισκόπηση του Threat Modeling Tool της Microsoft, το οποίο παρέχει μια δομημένη προσέγγιση για τον εντοπισμό και τον μετριασμό των απειλών ασφαλείας. Το εργαλείο CORAS, σχεδιασμένο για την αξιολόγηση κινδύνου, αξιολογείται επίσης, μαζί με το ST-Tool (Secure Tropos), το οποίο εστιάζει στην ενσωμάτωση απαιτήσεων ασφαλείας στο σχεδιασμό του συστήματος. Μέσω αυτής της ανάλυσης, το κεφάλαιο στοχεύει να παρέχει μια ολοκληρωμένη κατανόηση των δυνατοτήτων και των εφαρμογών αυτών των εργαλείων, βοηθώντας τους ενδιαφερόμενους φορείς στην επιλογή κατάλληλων λύσεων για ασφαλή ανάπτυξη συστημάτων.

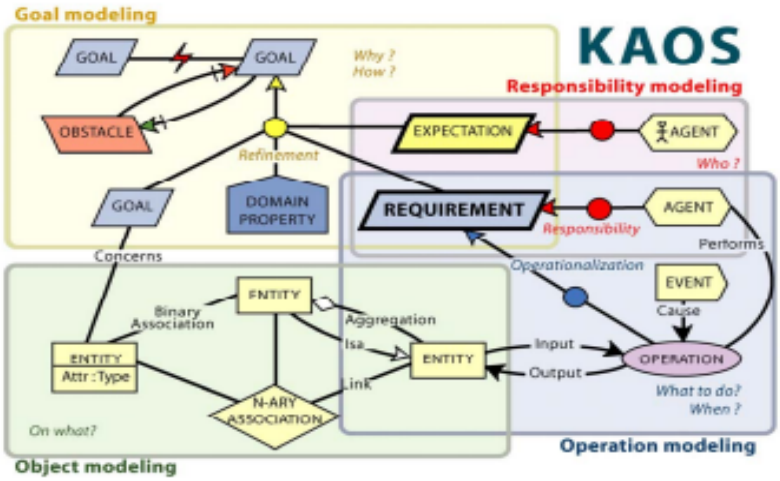
## 5.1 Objectiver's methodology: KAOS

Το Objectiver είναι εργαλείο το οποίο διαμορφώνει τις τεχνικές και επιχειρηματικές απαιτήσεις του KAOS στοχεύοντας στην εξάλειψη των καθυστερήσεων και στις υπερβάσεις κόστους σε ένα ολοκληρωμένο έργο παρέχοντας μια δομημένη διαδικασία για την υποστήριξη μίας εργασίας για την εξαγωγή και την οργάνωση των απαιτήσεων. Ουσιαστικά,

1. Προσδιορίζει όλες τις απαιτήσεις του έργου χρησιμοποιώντας τη προσέγγιση δομημένης μοντελοποίησης KAOS.
2. Δημιουργεί μοντέλα που λαμβάνουν υπόψη τους το χρήστη και το περιβάλλον του συστήματος
3. Αναπαριστά σενάρια χρηστών και μοντελοποιεί επιχειρηματικές διαδικασίες και ροές εργασίας
4. Δημιουργεί έγγραφα δομημένων απαιτήσεων

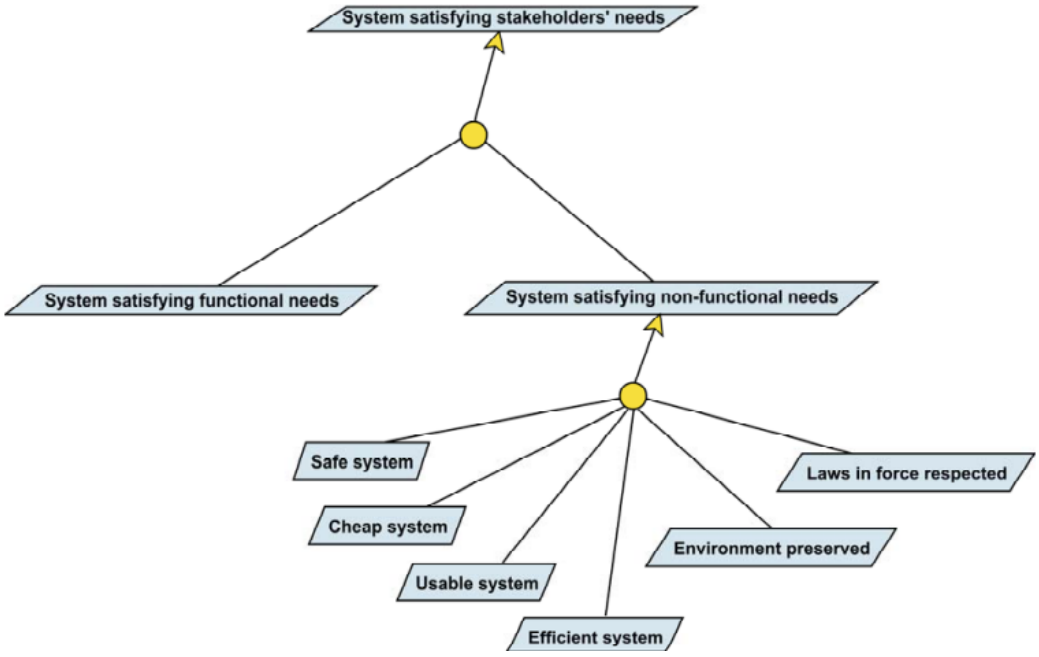
Το Objectiver βασίζεται στην KAOS, την πιο εξέχουσα μεθοδολογία μηχανικής απαιτήσεων που έχει αναπτυχθεί μέχρι τώρα.

Το εργαλείο αυτό παρέχει μια συνολική και λεπτομερής εικόνα ενός συστήματος, εταιρείας ή έργου, χάρη στη συστηματική αναγνώριση των δεσμών μεταξύ:
των στόχων και των στόχων που επιδιώκονται, τους ρόλους και τις ευθύνες (όλων των εμπλεκόμενων ατόμων ή των αυτοματοποιημένων συστημάτων), τις διαδικασίες και τις προτεραιότητές τους.




**Εικόνα 5 KAOS Modeling with Objectiver**

Οι απαιτήσεις μπορούν να συγκεντρωθούν μέσω ανοιχτών συνεντεύξεων. Ένας πιο αποτελεσματικός τρόπος συγκέντρωσης απαιτήσεων είναι η διεξαγωγή λιγότερο ανοιχτών συνεντεύξεων με την επαναχρησιμοποίηση προτύπων απαιτήσεων. Ένα από τα μακροπρόθεσμα οφέλη της επένδυσης στην τεχνολογία KAOS συνίσταται στη σταδιακή μοντελοποίηση γενικών προτύπων απαιτήσεων. Αυτά τα μοτίβα μπορούν να χρησιμοποιηθούν σε νέες περιπτώσεις για να καθοδηγήσουν τον προσδιορισμό των απαιτήσεων. Το σχήμα 1 δείχνει ένα τέτοιο σχέδιο. εφαρμογές αυτών των εργαλείων, βοηθώντας τους ενδιαφερόμενους φορείς στην επιλογή κατάλληλων λύσεων για ασφαλή ανάπτυξη συστημάτων.



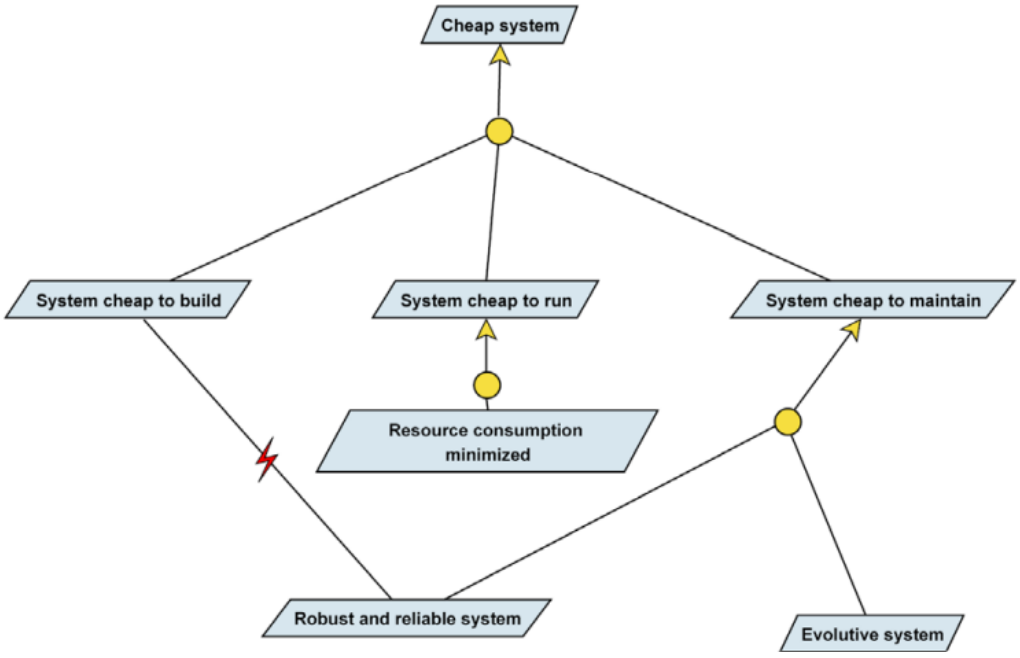

**Εικόνα 6 Γενικό μοτίβο στόχου**

Κάθε παραλληλόγραμμο στο σχήμα αντιπροσωπεύει έναν στόχο. Οι κίτρινοι κύκλοι αντιπροσωπεύουν βελτιώσεις ενός γονικού στόχου (αυτός στον οποίο δείχνει το κίτρινο βέλος) και μια λίστα υποστόχων. Το διάγραμμα μπορεί να διαβαστεί ως εξής:
Ο στόχος του συστήματος είναι να οικοδομήσει ένα σύστημα που να ικανοποιεί όλες τις ανάγκες των κατόχων: λειτουργικές και μη. Οι μη λειτουργικοί στόχοι ταξινομούνται ως εξής:

• το σύστημα πρέπει να είναι ασφαλές, φθηνό, εύχρηστο και αποτελεσματικό.
• το σύστημα πρέπει να διατηρήσει το περιβάλλον του.
• το σύστημα πρέπει να σέβεται τους ισχύοντες νόμους.

Υπάρχουν διαφορετικές τακτικές για την αποσύνθεση των στόχων σε υποστόχους. Η τακτική που χρησιμοποιήθηκε εδώ είναι μια αποσύνθεση με γνώμονα την περίπτωση: οι υποστόχοι απαριθμούν όλες τις περιπτώσεις που πρέπει να καλυφθούν για να εκπληρωθεί ο στόχος του πατέρα. Για παράδειγμα, λειτουργικές και μη λειτουργικές ανάγκες μαζί καλύπτουν όλες τις ανάγκες.

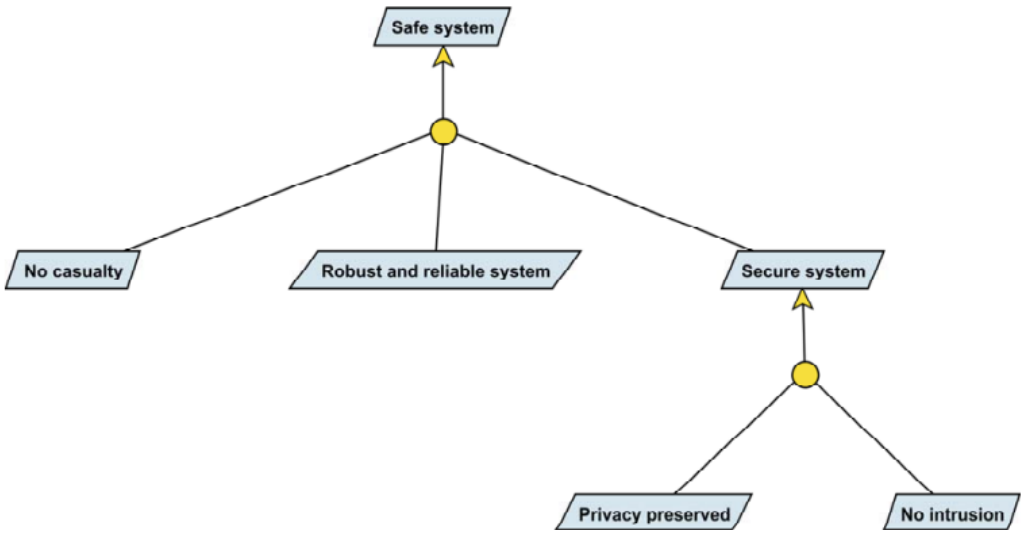
Κάθε φύλλο στο παραπάνω διάγραμμα μπορεί να αποσυντεθεί με τη σειρά του σε υποστόχους. Για παράδειγμα, το ακόλουθο διάγραμμα στόχου διερευνά τις οικονομικές πτυχές. η τακτική που χρησιμοποιείται εδώ είναι μια αποσύνθεση που καθοδηγείται από ορόσημο: πρώτα κατασκευάζονται συστήματα, μετά πρέπει να λειτουργούν. Το σχήμα δείχνει επίσης μια σύγκρουση μεταξύ δύο στόχων: «Σύστημα φθηνό στην κατασκευή» και πρέπει να είναι «Στιβαρό και αξιόπιστο». Η μείωση του κόστους κατά την κατασκευή του συστήματος μπορεί να επηρεάσει αρνητικά την ευρωστία και την αξιοπιστία του συστήματος που προκύπτει. Αντίστροφα, η βελτίωση της ευρωστίας και της αξιοπιστίας του συστήματος θα μπορούσε να αυξήσει σημαντικά το παγκόσμιο κόστος κατασκευής του συστήματος.



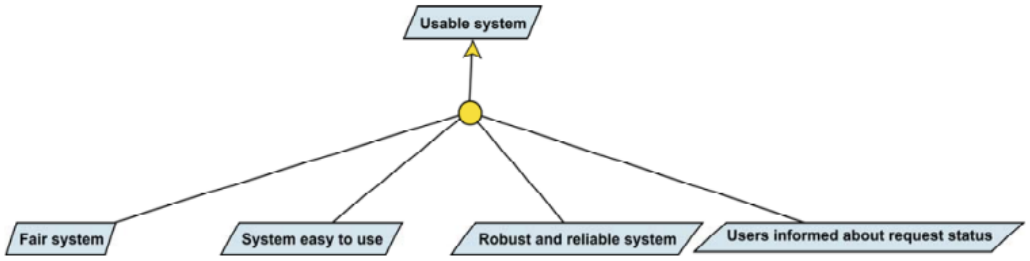

**Εικόνα 7 Γενικό μοτίβο στόχου**

Ένα μοντέλο στόχου KAOS είναι ένα κατευθυνόμενο γράφημα (το οποίο είναι πιο γενικό από ένα απλό δέντρο), που σημαίνει ότι ένας δεδομένος στόχος μπορεί να εμφανιστεί σε διαφορετικά διαγράμματα για να βελτιώσει διαφορετικούς στόχους υψηλότερου επιπέδου. Για παράδειγμα, ο στόχος «Στιβαρό και αξιόπιστο σύστημα»

εμφανίζεται στην Εικόνα 8 και στην Εικόνα 9. Αυτός ο στόχος συμβάλλει στους στόχους ασφάλειας, χρηστικότητας και φθηνής συντήρησης για το σύστημα. Είναι σημαντικό να καταγράψετε στο μοντέλο όλους τους διαφορετικούς λόγους για τους οποίους χρειάζεται ένας στόχος. Διευκολύνει τις μελλοντικές αναλύσεις επιπτώσεων καθώς το μοντέλο καθιστά σαφές ότι η μείωση της ευρωστίας ή της αξιοπιστίας του συστήματος μπορεί να έχει αντίκτυπο στη χρηστικότητα, την ασφάλεια και το κόστος συντήρησης του συστήματος.



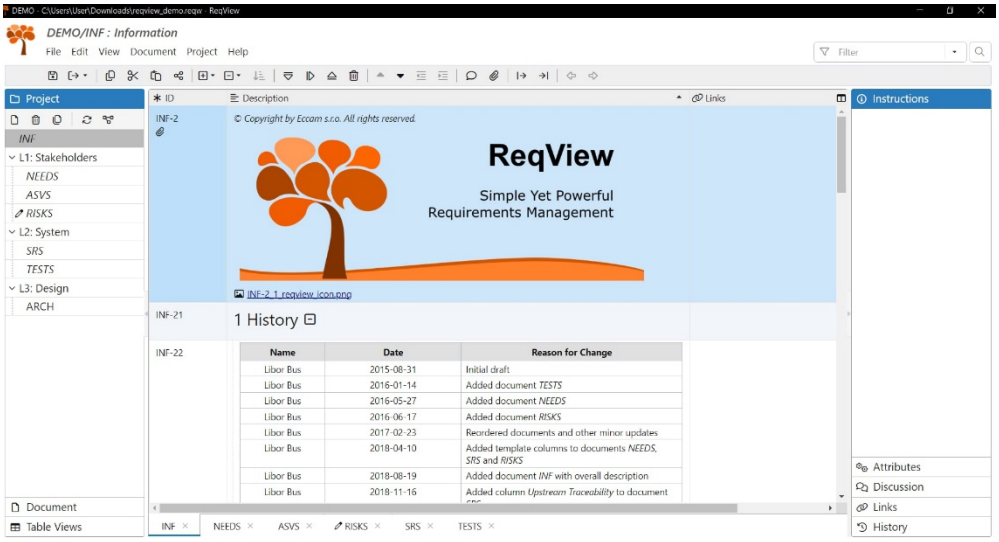

**Εικόνα 8 Γενικοί στόχοι: "Ασφαλές σύστημα"**



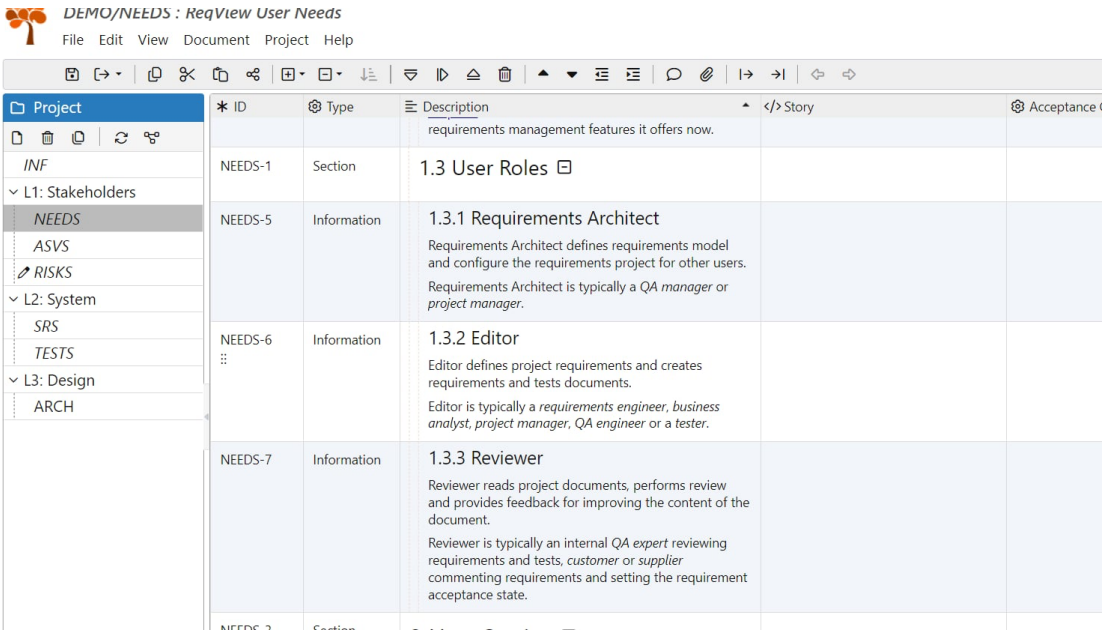

**Εικόνα 9 Γενικοί στόχοι: "Μη Ασφαλές σύστημα"**

## 5.2 ReqView

Το εργαλείο ReqView είναι λογισμικό διαχείρισης απαιτήσεων που βασίζεται σε cloud περιβάλλοντα και έχει σχεδιαστεί για να βοηθά τις επιχειρήσεις όλων των μεγεθών να διαχειρίζονται τις απαιτήσεις λογισμικού και συστήματος. Το ReqView μπορεί να χρησιμοποιηθεί από τις προσεγγίσεις SRE για να εξασφαλιστεί η ύπαρξη σαφών, τεκμηριωμένων απαιτήσεων και της ιχνηλασιμότητάς τους, διευκολύνοντας έτσι την επίτευξη της αξιοπιστίας που είναι ο πρωταρχικός στόχος του SRE. Το εργαλείο ReqView συναντάται πολύ συχνά με την προσέγγιση KAOS αφού στόχος της είναι η ανάλυση και η διάσπαση των στόχων ασφαλείας σε απαιτήσεις. Το ReqView μπορεί να χρησιμοποιηθεί για την καταγραφή των απαιτήσεων που προκύπτουν από την ανάλυση KAOS, παρακολουθώντας την ικανοποίησή τους σε όλη τη διάρκεια του έργου. Επίσης, μέσω της μεθοδολογίας SQUARE και του ReqView καταγράφονται αναλύονται και ιεραρχούνται απαιτήσεις. Το ReqView σε συνεργασία με το πλαίσιο ISSRM (Information System Security Risk Management) πραγματοποιείται καταγραφή των απαιτήσεων που σχετίζονται με την αξιολόγηση κινδύνων που παράγονται από το ISSRM, ειδικά για την παρακολούθηση της συμμόρφωσης με τα μέτρα ασφαλείας. Παρακάτω διαφαίνεται η εγκατάσταση σε δοκιμαστική περίοδο του ReqView και η αρχική του οθόνη απεικονίζει πως ορίζονται και διαχειρίζονται οι απαιτήσεις για ένα έργο ανάπτυξης λογισμικού.




**Εικόνα 10 Αρχική Οθόνη εγκατάστασης του ReqView**

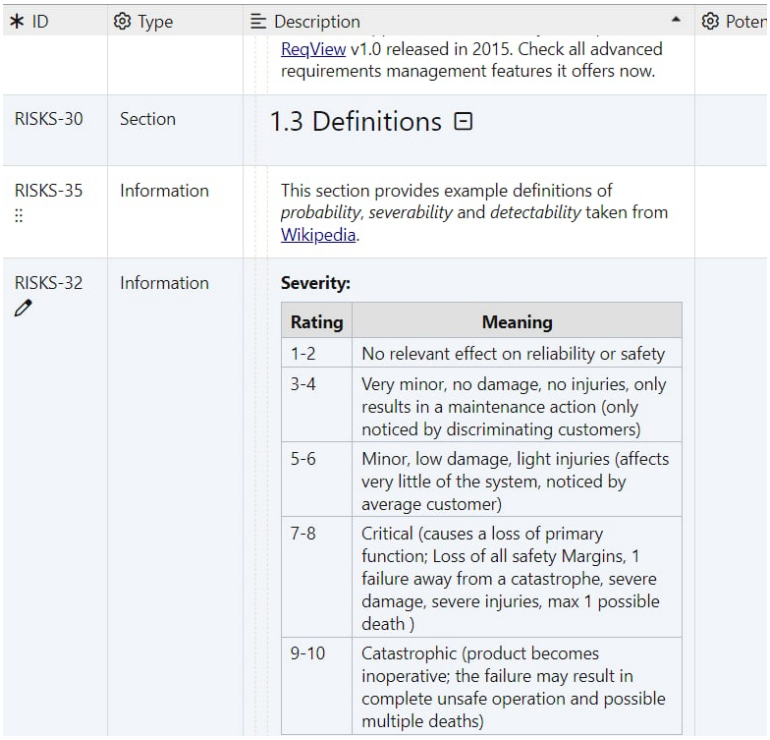



**Εικόνα 11 Case Scenario στο ReqView -Ρόλοι του Scenario**

Στην **Εικόνα 11** έχει δημιουργηθεί ένα project και αναγράφονται οι ρόλοι που συμμετέχουν στο project:

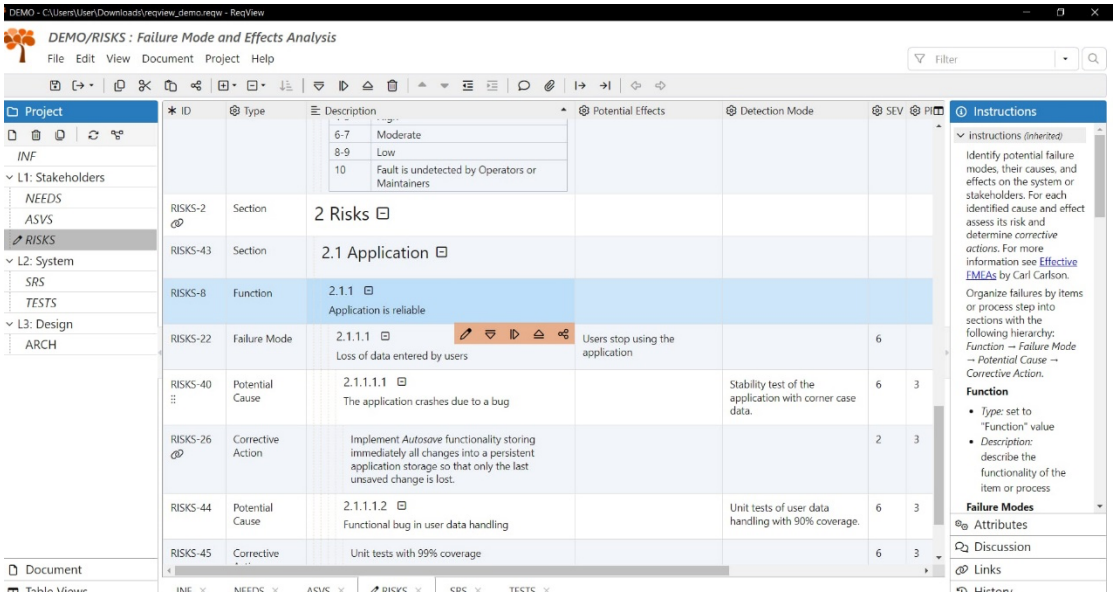
- Ο Architect ο οποίος καθορίζει και διαμορφώνει τις απαιτήσεις του έργου για άλλους χρήστες.
- Ο Editor δημιουργεί απαιτήσεις και ελέγχει δεδομένα.
- Ο Reviewer αναλύει και επεξεργάζεται τα δεδομένα του project και δίνοντας feedback βελτιώνεται το περιεχόμενο των δεδομένων.

Στη συνέχεια φαίνονται ενδεικτικά απαιτήσεις ασφαλείας του συστήματος που επικεντρώνονται στους κινδύνους του έργου.




**Εικόνα 12 Απαιτήσεις Ασφαλείας του Use Case Scenario**

Στη συνέχεια, φαίνονται οι κίνδυνοι των απαιτήσεων ασφαλείας και γίνεται αξιολόγηση με βάση το πόσο σημαντικός είναι ένας κίνδυνος και την πιθανή δυσλειτουργία που θα έχει στο σύστημα.




**Εικόνα 13 Risks, Potential Effects and Rating**

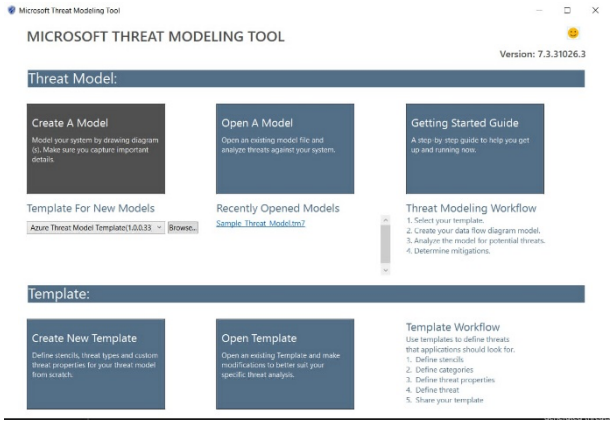
## 5.3 Microsoft’s Threat Modeling Tool:

Είναι εργαλείο που μπορεί να χρησιμοποιηθεί για τη μοντελοποίηση απειλών βοηθά τις ομάδες να εντοπίζουν, να αναλύουν και να διαχειρίζονται πιθανούς κινδύνους ασφαλείας σε εφαρμογές και συστήματα. Αποτελείται από πέντε βασικά βήματα μοντελοποίησης απειλών.

- Καθορισμός απαιτήσεων ασφαλείας.
- Δημιουργία διαγράμματος εφαρμογής.
- Εντοπισμός απειλών.
- Μετριασμός απειλών.
- Επιβεβαίωση ότι οι απειλές έχουν μετριαστεί.

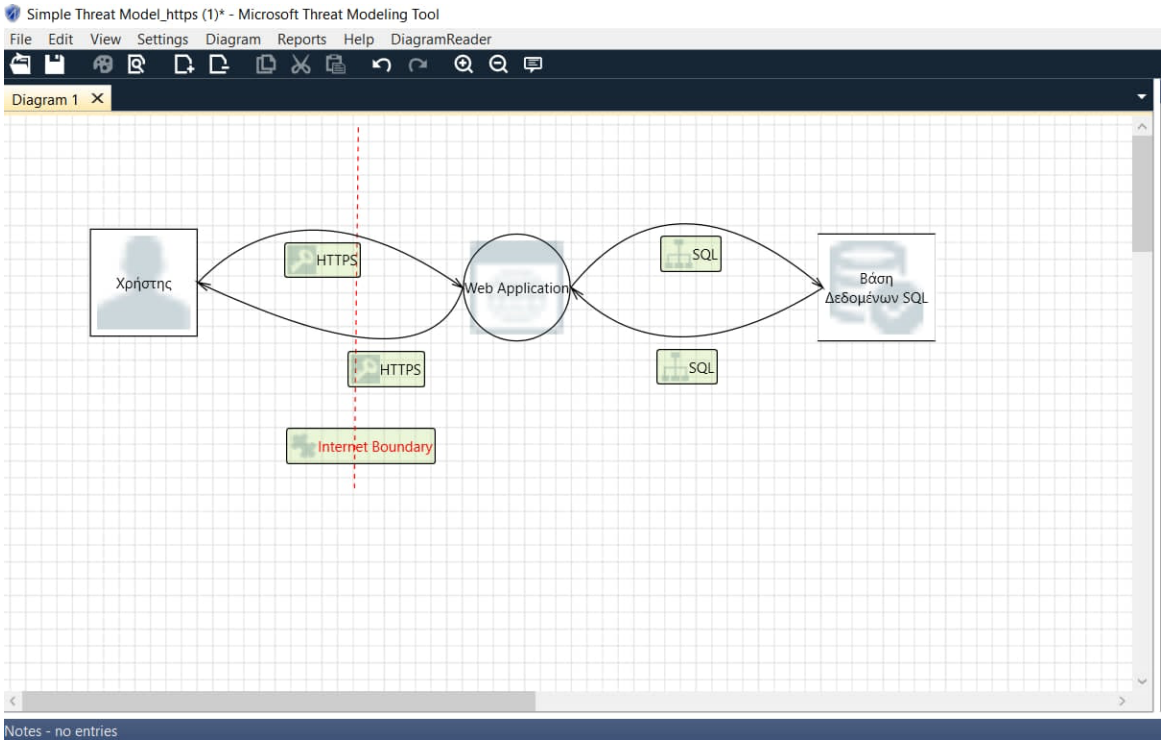
Εγκατάσταση του Microsoft’s Threat Modeling Tool:

Ανοίγει αρχική οθόνη:




**Εικόνα 14 Αρχική οθόνη Microsoft's Threat Modeling Tool**

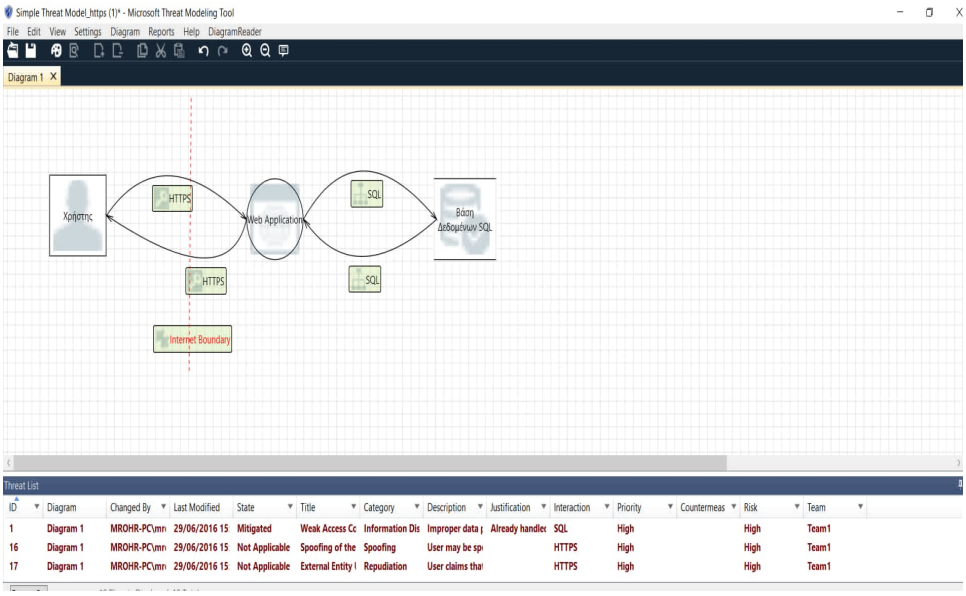
Έπειτα, δίνεται η δυνατότητα να περιηγηθεί ο χρήστης βλέποντας λύσεις και προτάσεις, έτοιμα templates αλλά υπάρχει και η επιλογή για δημιουργία ενός μοντέλου. Ανοίγει έναν κενό καμβά για τον σχεδιασμό το διαγράμματος.




**Εικόνα 15 Use case Διάγραμμα αρχείου TM.7**

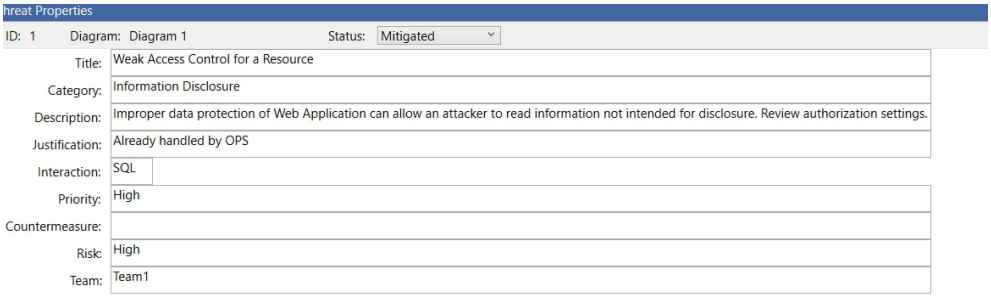
Παρακάτω δημιουργήθηκε ένα απλό σενάριο για ένα μοντέλο απειλής για να γίνει αντιληπτό πως λειτουργεί το Microsoft's Threat Modeling Tool .

- Ο χρήστης σχεδιάζεται ως μια εξωτερική οντότητα—ένα τετράγωνο
- Στέλνουν εντολές στον διακομιστή Ιστού —τον κύκλο
- Ο διακομιστής Web συμβουλεύεται μια βάση δεδομένων (δύο παράλληλες γραμμές)
- Το εργαλείο μοντελοποίησης απειλών επιτρέπει στους χρήστες να προσδιορίζουν όρια εμπιστοσύνης, που υποδεικνύονται με τις κόκκινες διακεκομμένες γραμμές, για να δείχνουν πού ελέγχουν διαφορετικές οντότητες.




**Εικόνα 16 Εργαλείο Μοντελοποίησης Απειλών, το οποίο χρησιμοποιεί προσέγγιση SDL**

Στην **Εικόνα 17** παρατηρείται μια λίστα δημιουργούμενων απειλών που βρήκε το Εργαλείο Μοντελοποίησης Απειλών με βάση το προεπιλεγμένο πρότυπο, το οποίο χρησιμοποιεί την προσέγγιση SDL που ονομάζεται STRIDE και είναι υποστηρικτικό μοντέλο των μεθοδολογιών CLASP και CORAS.



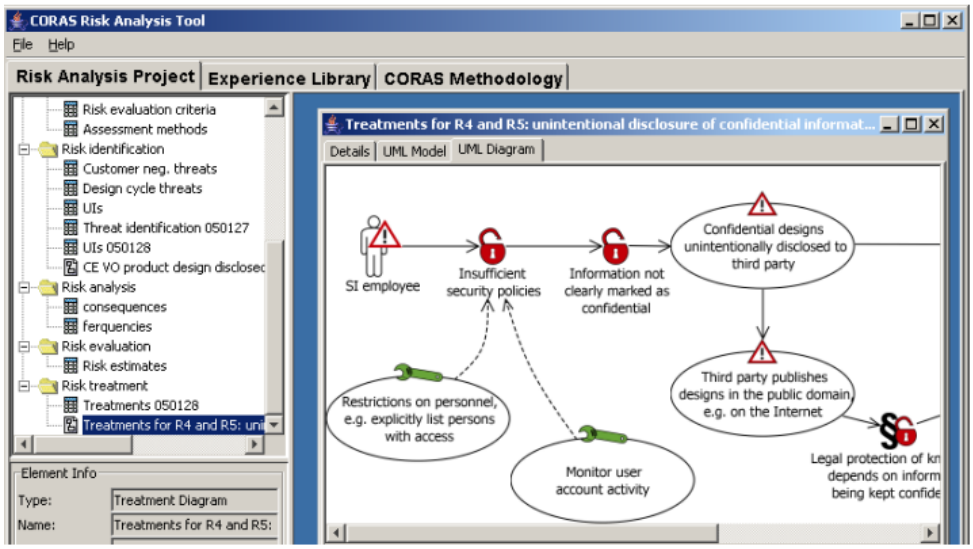

**Εικόνα 17 Δημιουργία απειλής με πιθανά ελαττώματα σχεδιασμού**

Η απειλή που δημιουργείται βοηθά να κατανοήσει ο χρήστης πιθανά ελαττώματα σχεδιασμού. Δίνεται μια ιδέα για πιθανούς φορείς επίθεσης, ενώ η πρόσθετη περιγραφή διασαφηνίζει τι ακριβώς φταίει, μαζί με πιθανούς τρόπους για να μετριαστεί.

## 5.4 CORAS Tool

Το εργαλείο CORAS το οποίο είναι ένα εργαλείο επεξεργασίας γραφικών για τη δημιουργία οποιουδήποτε είδους διαγράμματος CORAS. Είναι κατάλληλο για τη δημιουργία μοντέλων κινδύνου καθώς διευκολύνει την τεκμηρίωση και την παρουσίαση των αποτελεσμάτων της ανάλυσης κινδύνου. Ουσιαστικά, το CORAS παρουσιάζει ακριβείς περιγραφή των στόχων του συστήματος, του πλαισίου CORAS και των χαρακτηριστικών ασφαλείας, διευκολύνει την τεκμηρίωση των αποτελεσμάτων της αξιολόγησης κινδύνου και των πιθανών δυσλειτουργιών από τις οποίες εξαρτώνται αυτά τα αποτελέσματα. Το πλαίσιο CORAS για ανάλυση κινδύνου ασφαλείας βασίζεται σε μια γραφική γλώσσα UML για την υποστήριξη της τεκμηρίωσης και επικοινωνία των αποτελεσμάτων της ανάλυσης ασφάλειας.

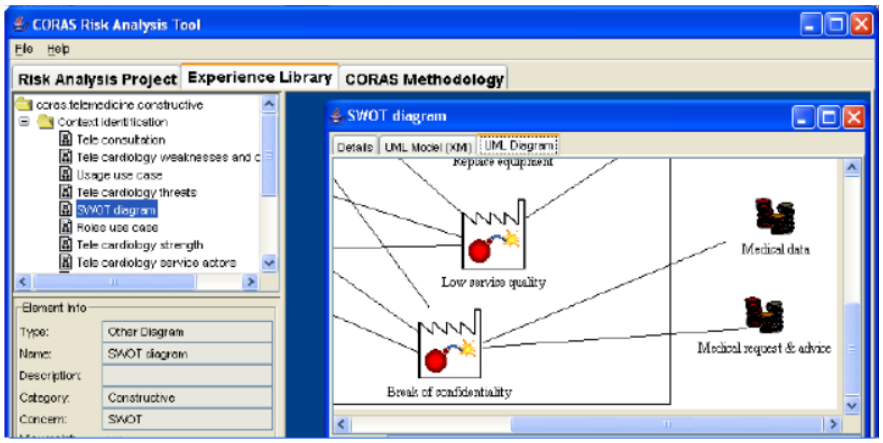
Στη συνέχεια, θα πραγματοποιηθεί ένα σενάριο για να γίνει αντιληπτή η λειτουργικότητα του εργαλείου CORAS όπου παρέχει μηχανογραφική υποστήριξη για την εκτέλεση ανάλυσης ασφαλείας σύμφωνα με τη μεθοδολογία CORAS χρησιμοποιώντας τη γραφική γλώσσα CORAS. Αρχικά πρέπει να γίνει προσδιορισμός, ανάλυση και καταγραφή των απαιτήσεων ασφαλείας του συστήματος. Το εργαλείο ακολουθεί ένα μοντέλο πελάτη-διακομιστή και αναπτύσσεται εξ ολοκλήρου σε Java για να επιτευχθεί η δημιουργία νέων έργων ανάλυσης, η τεκμηρίωση και η επεξεργασία των αποτελεσμάτων ανάλυσης ασφαλείας, η δημιουργία αναφορών ανάλυσης και η διαχείριση και η επαναχρησιμοποίηση εμπειριών από προηγούμενες αναλύσεις. Ένα στιγμιότυπο οθόνης της εφαρμογής CORAS. Τα δεδομένα ανάλυσης αποθηκεύονται σε μια κεντρική βάση δεδομένων στο διακομιστή.




**Εικόνα 18 Ένα στιγμιότυπο οθόνης της εφαρμογής CORAS**

Το εργαλείο CORAS λειτουργεί ως εξής:

Υπάρχουν δύο βάσεις δεδομένων στο εργαλείο CORAS. Η μία βάση δεδομένων αφορά την αξιολόγηση και αποθηκεύει τα αποτελέσματα από τις πραγματικές αναλύσεις ασφάλειας, ενώ δεύτερη βάση δεδομένων αφορά την εμπειρία και περιέχει επαναχρησιμοποιήσιμα αποτελέσματα από προηγούμενες αναλύσεις στη μορφή UML-μοντέλων, λιστών ελέγχου, διαδικασιών και πολλά άλλα. Διευκολύνοντας την επαναχρησιμοποίηση τους, το εργαλείο βοηθά τον χρήστη να αποφεύγει να ξεκινά από την αρχή για κάθε νέα ανάλυση. Στην Εικόνα 19 φαίνεται το UML διάγραμμα στο CORAS εργαλείο.




**Εικόνα 19 UML διάγραμμα στο CORAS Tool**

## 5.5 ST-Tool (Secure Tropos)

Το ST-Tool, είναι ένα εργαλείο CASE για το σχεδιασμό και την επαλήθευση λειτουργικών απαιτήσεων ασφάλειας και εμπιστοσύνης. Έχει σχεδιαστεί για να υποστηρίζει τη Secure Tropos μεθοδολογία. Συγκεκριμένα, αυτό το εργαλείο παρέχει προηγμένες λειτουργίες μοντελοποίησης και ανάλυσης με βάση τη μεθοδολογία Secure Tropos.

Οι κύριοι στόχοι του εργαλείου είναι:

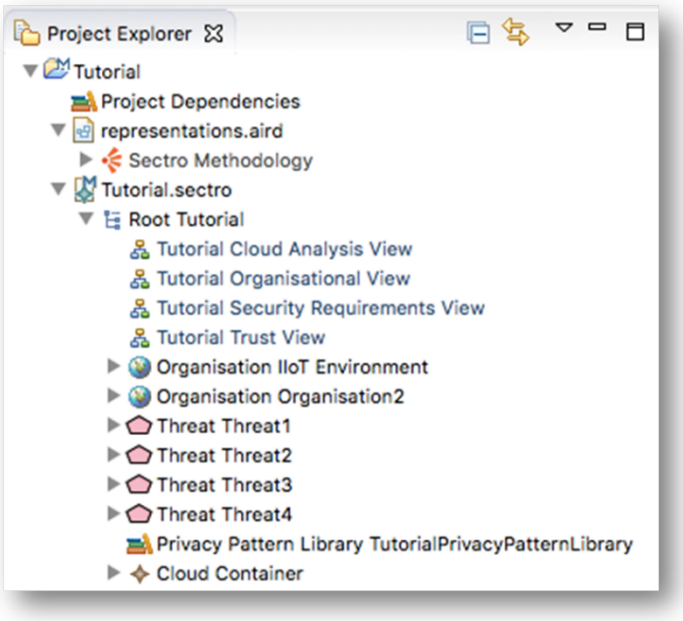
– Γραφικό περιβάλλον: παρέχει ένα οπτικό πλαίσιο για τη σχεδίαση μοντέλων.

– Επισημοποίηση: παροχή υποστήριξης για τη μετάφραση μοντέλων σε επίσημες προδιαγραφές.

– Δυνατότητα ανάλυσης: παροχή υπηρεσιών σε εξωτερικά εργαλεία για επίσημη ανάλυση.

Το Secure Tropos επεκτείνει τη μεθοδολογία Tropos και έχει τις έννοιες των ρόλων που εμπλέκονται στο σύστημα, των στόχων, των πόρων και των κοινωνικών σχέσεων για τον καθορισμό των απαιτήσεων του συστήματος. Στα διαγράμματα που γίνονται αναπαράσταση οι απαιτήσεις ασφαλείας οι ρόλοι – πρόσωπα που εμπλέκονται στο σύστημα αντιπροσωπεύονται ως κύκλοι αντιπροσωπεύονται οι στόχοι, τα καθήκοντα και οι πόροι αντίστοιχα ως οβάλ, εξάγωνα και ορθογώνια. Το ST-Tool είναι ένα εργαλείο CASE που παρέχει μια διεπαφή χρήστη για το σχεδιασμό Secure Tropos μοντέλων, παρέχει υποστήριξη για αυτόματη μετάφραση μοντέλων με γραφικά σε επίσημες προδιαγραφές. Για τη διαχείριση της οπτικής επεξεργασίας και τη συνοχή διαχείρισης δεδομένων, έχει υιοθετηθεί μια λύση δύο επιπέδων: ένα γραφικό επίπεδο και ένα επίπεδο δεδομένων. Σε γραφικό επίπεδο, εμφανίζονται τα μοντέλα ως γραφήματα όπου οι φορείς και οι υπηρεσίες είναι κόμβοι και οι σχέσεις είναι τόξα. Κάθε οπτικό αντικείμενο αναφέρεται σε ένα αντικείμενο δεδομένων. Η συλλογή των αντικειμένων δεδομένων είναι το επίπεδο δεδομένων. Ουσιαστικά, με την ανάλυση διαγραμμάτων με βάση τη μεθοδολογία Secure Tropos εξάγονται αποτελέσματα όπως προειδοποιήσεις και αναφορές για αποτυχία περιορισμών ακεραιότητας, εμπιστευτικότητας και αυθεντικοποίησης.

Μόλις δημιουργηθεί το μοντέλο, δημιουργείται επίσης ένα αρχείο με το παρεχόμενο όνομα και την επέκταση .sectro. Αυτό το αρχείο περιέχει ένα στοιχείο Root που περιέχει όλες τις προβολές του εργαλείου SecTro. Πρέπει να ανοίξουν τέσσερις καρτέλες, αμέσως μετά τη δημιουργία του νέου διαγράμματος. Εάν κάποιο από αυτά τα διαγράμματα κλείσει κατά λάθος, μπορεί να ανοίξει ξανά κάνοντας διπλό κλικ στην αντίστοιχη προβολή στην περιοχή εξερεύνησης έργου




**Εικόνα 20 Workspace selection**

Ένα περιβάλλον του εργαλείου έχει τη μορφή που απεικονίζεται στην Εικόνα 21 και αποτελείται από τα εξής μέρη:

Project Explorer: Όλα τα έργα εμφανίζονται στον χρήστη

Palette: Περιέχει όλες τις έννοιες της Secure Tropos Modeling Language. Εκεί, ο χρήστης μπορεί να επιλέξει οποιαδήποτε έννοια και να την προσθέσει στον χώρο εργασίας

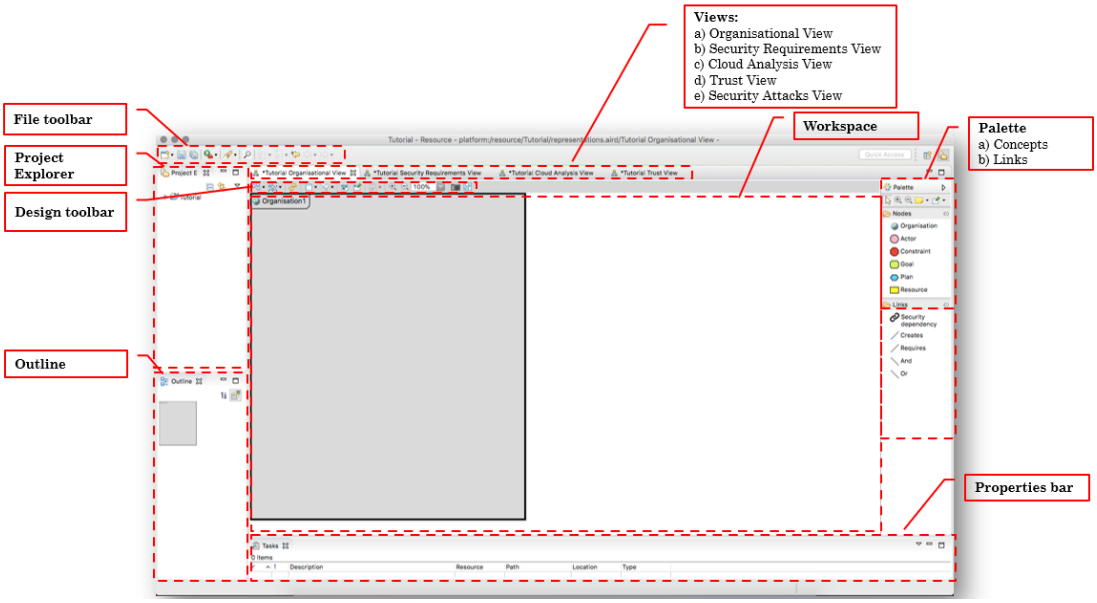
Περίγραμμα: Ο χρήστης μπορεί εύκολα να πλοηγηθεί όταν το διάγραμμα είναι πολύ μεγάλο ή αραιό

Χώρος εργασίας: Μόλις δημιουργηθεί ένα διάγραμμα SecTro, οι καρτέλες φιλοξενούν τις διάφορες προβολές των διαγραμμάτων (Προβολή Οργανισμού, Προβολή Απαιτήσεων Ασφαλείας, Προβολή Ανάλυσης Cloud, Προβολή Εμπιστοσύνης, Προβολή Επιθέσεων Ασφαλείας)

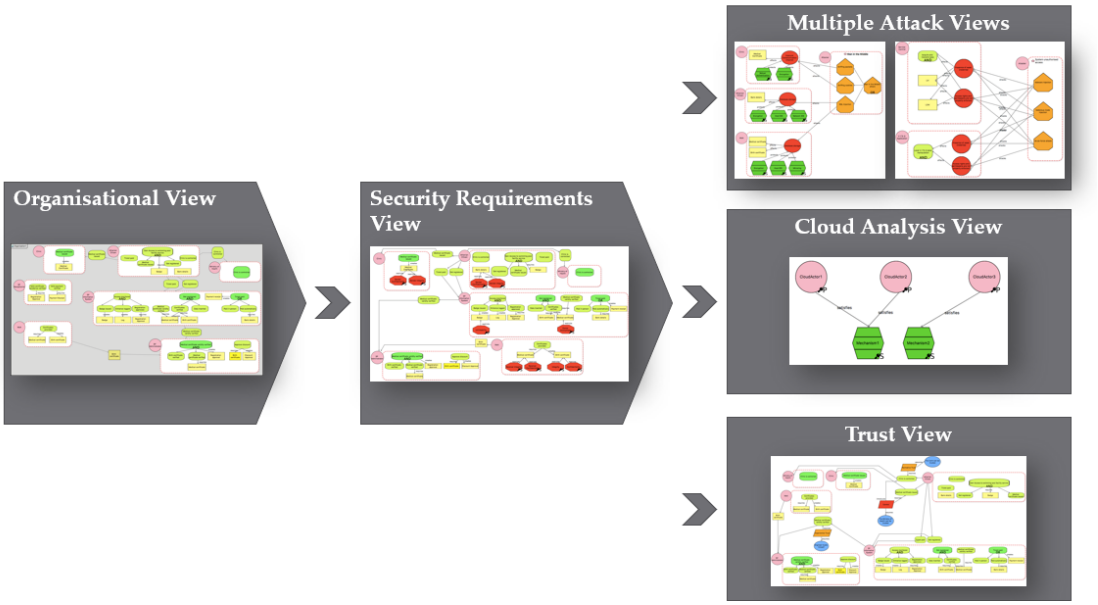
Γραμμή εργαλείων αρχείων: Συντομεύσεις για κύριες επιλογές (νέο έργο, αποθήκευση, ανάλυση, ζουμ, αναζήτηση αρχείων)

Γραμμή εργαλείων σχεδίασης: Συντομεύσεις για τις κύριες επιλογές σχεδίασης (τακτοποίηση στοιχείων, ανανέωση διαγράμματος, εμφάνιση/απόκρυψη στοιχείων, διαγραφή στοιχείων, επιλογές αγάπης, επιλογές χρώματος)

Γραμμή ιδιοτήτων: Περιέχει το σύνολο των ιδιοτήτων κάθε έννοιας. Όταν η καρτέλα είναι ανοιχτή, εμφανίζει τις ιδιότητες οποιωνδήποτε επιλεγμένων από την έννοια του χρήστη

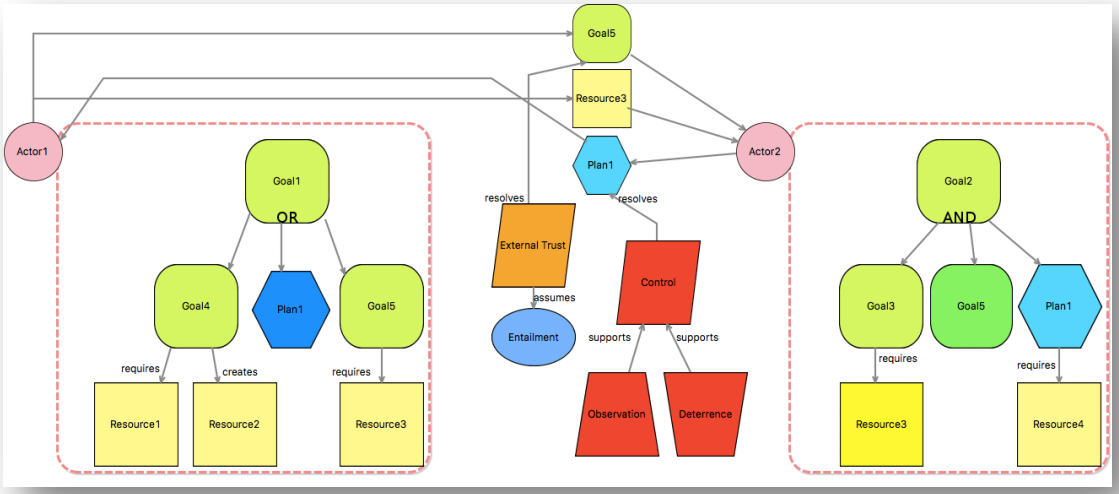



**Εικόνα 21 GUI overview**




**Εικόνα 22 Sequence of views**

Ο χρήστης προσδιορίζει τις σχέσεις εμπιστοσύνης μεταξύ των άλλων χρηστών όταν ο ένας εξαρτάται από τον άλλο για την εκπλήρωση μιας απαίτησης. Αυτή η προβολή συγχρονίζεται με την Προβολή απαιτήσεων ασφαλείας. Οποιοσδήποτε παράγοντας, στόχος, σχέδιο, πόρος ή εξάρτηση που προστίθεται στο ένα θα εμφανίζεται και στον άλλο. Ο χρήστης μπορεί να προσθέσει Αναλύσεις Εμπιστοσύνης ή Ελέγχου και να επιλύσει όλες τις εξαρτήσεις μεταξύ των Αντιπροσώπων, να ορίσει ποιες είναι οι Συνέπειες που θεωρούνται για να είναι έγκυρη μια Ανάλυση Εμπιστοσύνης και τυχόν νέες εξαρτήσεις που εισάγονται από τις Αναλύσεις Ελέγχου (Εικόνα 23).




**Εικόνα 23 Λειτουργίες σχεδίασης**

Κατά τον εντοπισμό και την ανάλυση των εργαλείων μοντελοποίησης διαπιστώθηκε πως υπάρχουν εργαλεία που ικανοποιούν αρκετές από τις προσεγγίσεις SRE με την διαφορά ότι τα περισσότερα από αυτά ήταν είτε παλαιότερες εκδόσεις είτε επι πληρωμή με ελλιπή ανάλυση και επεξήγηση. Στην παρούσα διπλωματική επιλέχθηκε να αναλυθούν και να παρουσιαστούν εκείνα που είτε υπήρχε η δυνατότητα να εγκατασταθούν και να «τρέξουν» με ένα use case scenario είτε επειδή υπήρχε η δυνατότητα να αναλυθούν.

Μερικά από τα εργαλεία που βρέθηκαν αλλά δεν αναλύθηκαν για τους λόγους που αναφέρονται παραπάνω είναι τα εξής:

### OpenOME

Το OpenOME είναι ένα εργαλείο ανοιχτού κώδικα που υποστηρίζει την ανάλυση απαιτήσεων με βάση στόχους και μπορεί να χρησιμοποιηθεί για την υποστήριξη μεθοδολογιών όπως το Secure Tropos και KAOS. Χρησιμοποιείται για τη μοντελοποίηση στόχων ασφαλείας.

Χαρακτηριστικά: Μοντελοποίηση στόχων, ανάλυση εξαρτήσεων, προσδιορισμός ρίσκων.

**MagicDraw**:

Το MagicDraw είναι εργαλείο μοντελοποίησης που με UMLsec επεκτάσεις υποστηρίζει τη UML. Προσφέρει δυνατότητες δημιουργίας, οπτικοποίησης διαγραμμάτων UML τα οποία συνδυαστικά οργανώνουν και συστηματοποιούν απαιτήσεις ασφαλείας ενός έργου. Με την προσθήκη της επέκτασης UMLsec επιτρέπει τη μοντελοποίηση διαγραμμάτων ασφαλείας ενσωματωμένων στις τυπικές UML προδιαγραφές.
Χαρακτηριστικά**:** Σχεδίαση διαγραμμάτων ασφαλείας UML, ανάλυση τρωτών σημείων και ενσωμάτωση προτύπων ασφαλείας.

**Papyrus UML:**

Το Papyrus είναι ένα εργαλείο μοντελοποίησης που υποστηρίζει UML και μπορεί να επεκταθεί με πρότυπα και βιβλιοθήκες ασφαλείας για τη χρήση της UMLsec μεθοδολογίας. Είναι ανοιχτού κώδικα και χρησιμοποιείται ευρέως σε ακαδημαϊκά και επαγγελματικά περιβάλλοντα.
Χαρακτηριστικά: Μοντελοποίηση ασφαλείας με UML, επεκτάσεις για αποτύπωση τρωτών σημείων και σχέσεων ασφαλείας.

**SecReq (Security Requirements Tool):**

Το SecReq βοηθά στην ανάλυση και μοντελοποίηση απαιτήσεων ασφαλείας στο πλαίσιο του ISSRM (Information System Security Risk Management)**,** επικεντρώνοντας στη διαχείριση ρίσκων σε πληροφοριακά συστήματα.
**Χαρακτηριστικά**: Ανάλυση ρίσκων, καθορισμός πολιτικών ασφαλείας, αποτύπωση απαιτήσεων προστασίας.

## 5.6 Αξιολόγηση Εργαλείων

Στην ενότητα αυτή θα γίνει μία αξιολόγηση των εργαλείων που εντοπίστηκαν με βάση κάποια βασικά χαρακτηριστικά. Πιο συγκεκριμένα, τα παραπάνω εργαλεία είναι χρήσιμο να πληρούν κάποιες προϋποθέσεις για να είναι λειτουργικά και να πληρούν

τις απαιτήσεις που έχουν κληθεί να φέρνουν εις πέρας. Αποφασίστηκε πως θα αξιολογηθούν με βάση τη:

**Λειτουργικότητα και Χαρακτηριστικά:** Αν το εργαλείο υποστηρίζει λειτουργίες όπως:

- Διαχείριση απαιτήσεων (αναγνώριση, εντοπισμό, κατηγοριοποίηση, ιχνηλασιμότητα την ικανότητα δηλαδή οι απαιτήσεις ασφαλείας να παρακολουθούνται σε όλα τα στάδια της ανάπτυξης του συστήματος, επικύρωση των απαιτήσεων σημαίνει τη δυνατότητα διασφάλισης πως οι απαιτήσεις ανταποκρίνονται στους αρχικούς στόχους ασφαλείας και ότι υλοποιούνται με τρόπο που να προσφέρεται η επιθυμητή προστασία, αξιολόγηση κινδύνων, διαρκής ενημέρωση και διαχείριση αλλαγών )
- Ανάλυση απαιτήσεων (Συλλογή απαιτήσεων, Αποσαφήνιση και καθορισμός απαιτήσεων, κατηγοριοποίηση και ομαδοποίηση σε λειτουργικές και μη λειτουργικές απαιτήσεις, προτεραιοποίηση, διαχείριση συγκρούσεων απαιτήσεων)

- Μοντελοποίηση με Διαγράμματα

**Υποστήριξη Συνεργασίας**: Αν το εργαλείο παρέχει:

- Συνεργασία μεταξύ πολλών χρηστών, κοινή χρήση και συγχρονισμό σε πραγματικό χρόνο.
- Ενσωμάτωση επιπρόσθετων εργαλείων διαχείρισης έργων.

**Δια λειτουργικότητα**: Αν το εργαλείο δίνει τη δυνατότητα:

- Να εισάγονται και να εξάγονται δεδομένα σε διαφορετικές μορφές και φάσεις.
- Συμβατότητας και με άλλα εργαλεία όπως IDEs και εργαλεία μοντελοποίησης ή με άλλο λογισμικό

**Ευκολία Χρήσης:**

- Αν το εργαλείο είναι εύχρηστο από τον σχεδιασμό του UI μέχρι τη δυνατότητα προσαρμογής του περιβάλλοντος.
- Εύκολο στη χρήση με οδηγίες και templates που μπορούν να χρησιμοποιηθούν, παραμετροποιηθούν και διαχειριστούν με βάση τις ανάγκες που προκύπτουν.

**Υποστήριξη UML:**

- Ποιο εργαλείο παρέχει πιο ισχυρή υποστήριξη σε UML διαγράμματα.
- Αν υπάρχει δυνατότητα προσαρμοσμένων διαγραμμάτων ή συμβολισμών.

**Κόστος:**

- Αν το εργαλείο διανέμεται και σε δωρεάν εκδόσεις, σε άδειες χρήσης, συνδρομές ή κόστος αγοράς.

**Υποστήριξη και Εκπαίδευση:**

- Αν το εργαλείο μελέτης έχει τεχνική υποστήριξη και διαθεσιμότητα online εγχειριδίων, οδηγιών και tutorials.

**Προσαρμοστικότητα:**

- Αν υπάρχει δυνατότητα προσαρμογής της λειτουργικότητας του εργαλείου με plugins, scripts, ή άλλες μορφές επέκτασης.

**Ενημερώσεις λογισμικού:**

- Αν στο εργαλείο παρέχονται συχνά patches και νέες εκδόσεις κάνει το πρόγραμμα πιο αξιόπιστο, ασφαλές και συμβατό με τρέχουσες τεχνολογίες.

**Ικανοποίηση Προσεγγίσεων SRE:**

- Πόσες και ποιες Προσεγγίσεις SRE έχει τη δυνατότητα το κάθε εργαλείο να ικανοποιήσει.

| Κριτήριο | Objectiver's Method | ReqView | Microsoft's Threat Tool | Coras Tool | ST-Tool | OpenOME | MagicDraw | Papyrus UML | SecReq |
|---|---|---|---|---|---|---|---|---|---|
| **Λειτουργικότητα και Χαρακτηριστικά** | 1.Προσδιορίζει όλες τις απαιτήσεις του έργου χρησιμοποιώντας τη προσέγγιση δομημένης μοντελοποίησης KAOS.2.Δημιουργεί μοντέλα που λαμβάνουν υπόψη τους το χρήστη και το περιβάλλον του συστήματος. 3.Αναπαριστά σενάρια χρηστών και μοντελοποιεί επιχειρηματικές διαδικασίες και ροές εργασίας. | 1.Καταγράφει τις απαιτήσεις που προκύπτουν από την ανάλυση KAOS, παρακολουθώντας την ικανοποίησή τους σε όλη τη διάρκεια του έργου. 2.Καταγράφονται αναλύονται και ιεραρχούνται απαιτήσεις. 3.Πραγματοποιείται καταγραφή των απαιτήσεων που σχετίζονται με την αξιολόγηση κινδύνων που παράγονται από το ISSRM, ειδικά για την παρακολούθηση της | 1.Καθορισμός απαιτήσεων ασφαλείας. 2.Δημιουργία διαγράμματος εφαρμογής. 3.Εντοπισμός απειλών. 4.Μετριασμός απειλών. 5. Επιβεβαίωση ότι οι απειλές έχουν μετριαστεί | 1.Δημιουργία μοντέλων κινδύνου καθώς διευκολύνει την τεκμηρίωση και την παρουσίαση των αποτελεσμάτων της ανάλυσης κινδύνου. 2. Παρουσιάζει ακριβείς περιγραφή των στόχων του συστήματος 3. Διευκολύνει την τεκμηρίωση των αποτελεσμάτων της αξιολόγησης κινδύνου και των πιθανών δυσλειτουργιών από τις οποίες εξαρτώνται τα αποτελέσματα | 1.Παρέχει ένα οπτικό πλαίσιο για τη σχεδίαση μοντέλων. 2. Παρέχει υποστήριξης για μετάφραση μοντέλων σε επίσημες προδιαγραφές. 3. Παροχή υπηρεσιών σε εξωτερικά εργαλεία για επίσημη ανάλυση. | 1.Υποστηρίζει την ανάλυση απαιτήσεων με βάση στόχους 2.Μπορεί να χρησιμοποιηθεί για την υποστήριξη μεθοδολογιών | 1. Ενσωματώνει απαιτήσεις και χαρακτηριστικά ασφαλείας στα διαγράμματα UML. 2. Διευκολύνει τη διαδικασία επαλήθευσης, προσδιορίζοντας αν το μοντέλο πληροί τους καθορισμένους περιορισμούς ασφαλείας. 3.Μπορούν να εντοπιστούν πιθανές αδυναμίες ή σημεία μη συμμόρφωσης από νωρίς, μειώνοντας τους κινδύνους ασφαλείας στη φάση ανάπτυξης. | 1. Αποτυπώνει τρωτά σημεία και σχέσεις ασφαλείας | 1.Ανάλυει και μοντελοποίει απαιτήσεις ασφαλείας στο πλαίσιο 2.Επικεντρώνεται στη διαχείριση ρίσκων 3. Ανάλυση ρίσκων, 4.Καθορισμός πολιτικών ασφαλείας, 5.Αποτύπωση απαιτήσεων προστασίας. |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | συμμόρφωσης με τα μέτρα ασφαλείας | | | | | | | |
| **Υποστήριξη Συνεργασίας** | Το objectiver είναι κυρίως εργαλείο το οποίο βασίζεται σε αναλυτές. | Προσφέρει συγχρονισμό σε πραγματικό χρόνο ή cloud. | Δίνει τη δυνατότητα σε οποιονδήποτε να επικοινωνεί σχετικά με το σχεδιασμό ασφαλείας των συστημάτων | Δίνει τη δυνατότητα κοινής χρήσης μεταξύ των αναλυτών | Παρέχει δυνατότητες συνεργασίας σε κοινή χρήση και επεξεργασίας των μοντέλων στόχων από πολλούς χρήστες, αλλά έχει περιορισμένες λειτουργίες . | Το εργαλείο επιτρέπει την υποστήριξη ομαδικής εργασίας. | Υποστηρίζει ομαδική εργασία για να διευκολύνεται η ανάλυση και ο σχεδιασμός συστημάτων | Βασίζεται στην πλατφόρμα Eclipse και υποστηρίζει συνεργασία πολλών χρηστών | Επιτρέπει σε πολλούς χρήστες να συνεγράζονται ταυτόχρονα και να μοιράζονται σχόλια, παρατηρήσεις και ενημερώσεις. |
| **Διαλειτουργικότητα** | Το objectiver σε συνδυασμό με UML γλώσσα δημιουργεί απαιτήσεις ασφαλείας. | Μεταφέρονται ολόκληρα έργα απαιτήσεων από άλλα εργαλεία RM ή απλώς εισάγονται/εξάγονται επιλεγμένες προδιαγραφές απαιτήσεων μέσω αρχείων ReqIF. | Εισάγονται και εξάγονται δεδομένα σε διαφορετικές μορφές και φάσεις. | Εισάγονται δεδομένα με σκοπό την παραμετροποίηση τους | Έχει περιορισμένες δυνατότητες διαλειτουργικότητας | Το OpenOME υποστηρίζει εισαγωγή και εξαγωγή δεδομένων σε μορφές όπως XML. | Δίνεται η δυνατότητα εξαγωγής και εισαγωγής δεδομένων σε μορφές όπως XMI και XML. | Λόγω της υποστήριξης του Eclipse καθιστάται λειτουργικό με άλλα εργαλεία ανάπτυξης. | Δίνεται η δυνατότητα εξαγωγής δεδομένων σε συγκρεκριμένα πρότυπα. |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Ευκολία Χρήσης** | Το objectiver έχει μικρή προσαρμοστικότητα στο σχεδιασμό και δίνει τη δυνατότητα σε πιο ελεύθερα διαγράμματα. | Επαναχρησιμοποίηση προτύπων με βάση τα διεθνή πρότυπα. | Υπάρχει δυνατότητα να εισαχθούν έτοιμα templates και plugins. | Προσαρμόσιμο GUI που δίνει τη δυνατότητα να δημιουργηθούν διαγράμματα UML. | Το εργαλείο είναι εύχρηστο από τον σχεδιασμό του UI | Είναι περιορισμένης διεπαφής καθώς είναι ανοικτού κώδικα δεν δεν προτείνεται για νέους χρήστες. | Το MagicDraw διαθέτει φιλική διεπαφή αλλά είναι αρκετά περίπλοκο σε νέους χρήστες λόγω του μεγάλου αριθμού επιλογών και χαρακτηριστικών. | Ως εργαλείο ανοιχτού κώδικα διαθέτει δύσκολη διεπαφή με το χρήστη και δεν εγκαθιστάτε με ευκολία στην πλατφόρμα Eclipse. | Σχεδιάστηκε με έμφαση στην απλότητα και την αποδοτική ανάλυση απαιτήσεων ασφαλείας. |
| **Υποστήριξη UML** | Το εργαλείο παροτρύνει την ανάπτυξη των UML διαγραμμάτων σε άλλη πλατφόρμα. | Το εργαλείο ReqView καλύπτει κυρίως τις μεθοδολογίες KAOS, SQUARE και ISSRM | Το εργαλείο καλύπτει κυρίως την Προσέγγιση Microsoft's Threat Modeling | Το CORAS Tool δέχεται επεκτάσεις UML για την εξαγωγή διαγραμμάτων UML | ST-Tool δεν είναι φτιαγμένο για τη μοντελοποίηση UML καθώς εστιάζει στη μεθοδολογία KAOS, που είναι σχεδιασμένη για ανάλυση στόχων και διαχείριση απαιτήσεων | Το OpenOME δεν χρησιμοποιεί το UML Αντίθετα, στηρίζεται στη μοντελοποίηση στόχων και απαιτήσεων μέσω της μεθοδολογίας Secure i*, η οποία είναι | Με την προσθήκη του UMLsec υποστηρίζει και ενσωματώνει στα διαγράμματα στοιχεία όπως ακεραιότητα και εμπιστευτικότητα. | Το Papyrus UML παρέχει υποστήριξη UML και όλα τα διαγράμματα UML. | Υποστηρίζει την ενσωμάτωση απαιτήσεων με μοντέλα UML. |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | διαφορετική από την τυπική UML. | | | |
| **Κόστος** | Το objectiver διανέμεται σε τρείς εκδόσεις την τυπική, επαγγελματική και έκδοση κριτικής με το ανάλογο κόστος. | Υπάρχει δυνατότητα Free Trial και αργότερα με ένα κόστος ιδανικό και μικρομεσαία έργα είναι κατάλληλο. | Είναι ένα εργαλείο που διανέμεται δωρεάν για μικρά έργα. | Το Coras Tool διανέμεται δωρεάν. | Το ST-Tool είναι συνήθως διαθέσιμο μέσω αδειοδότησης, καθώς δεν διατίθεται ευρέως στην αγορά. | Το εργαλείο αυτό είναι ανοιχτού κώδικα γι αυτό είναι κατάλληλο για έργα με χαμηλό κόστος. | Το κόστος του MagicDraw ποικίλλει ανάλογα με τη χρήση και τις απαιτήσεις του έργου. Ανάλογα με τις δυνατότητες αυξάνεται και το κόστος. | Διατίθεται δωρεάν μέσω της πλατφόρμας Eclipse και χρησιμοποιείται για project με περιορισμένο προϋπολογισμό | Το κόστος εξαρτάται από τη χρήση και τις απαιτήσεις των χρηστών. |
| **Υποστήριξη και Εκπαίδευση** | Στο εργαλείο Objectiver παρέχεται manual οδηγιών αλλά η παροχή του support υπάρχει μετά από login του χρήστη. | Στην δοκιμαστική περίοδο δίνεται ένα template υποστήριξης και σχεδιασμού των απαιτήσεων. | Υπάρχει οδηγός έναρξης και template για να φανεί η λειτουργικότητα του εργαλείου. | Υπάρχει βιβλίο που εξηγεί την λειτουργικότητα του σε θεωρητικό επίπεδο. | Υπάρχουν κάποια online εγχειρίδια. | Δεν παρέχεται υποστήριξη αλλά μέσω Forum και chat. | Παρέχονται βίντεο με το knowledge base της εφαρμογής | Δεν παρέχεται υποστήριξη αλλά μέσω Forum και chat. | Μέσω Forum και chat ενώ στην εμπορική του χρήση υπάρχει υποστήριξη. |
| **Προσαρμοστικότητα** | Υποστηρίζει τυπική γλώσσα μοντελοποίησης προσανατολισμένη στο στόχο της KAOS | Δέχεται ενημερώσεις από cloud | Η μεθοδολογία που συναντάτε πολύ συχνά | Γίνεται λήψη των Windows GUI for CORAS diagrams και | Υπάρχουν αρκετές μορφές επέκτασης καθώς αναλύονται | UMLsec επεκτάσεις για την υποστήριξη της UML, | Είναι αρκετά προσαρμοστικό καθώς υπάρχουν αρκετά scripts που μπορούν να τρέξουν. | Δεν υπάρχουν αρκετά plugins έτσι ώστε να | Το SeqReq μπορεί να συνδεθεί με εργαλεία όπως είναι |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | είναι η STRIDE | stencils for Microsoft Visio | αρκετές μεθοδολογίες. | | | εγκατασταθεί στο Eclipse. | το Jira και το Git. |
| **Ενημερώσεις λογισμικού** | Συχνές ενημερώσεις λογισμικού και νέες εκδόσεις. | Παρέχονται αλλαγές των απαιτήσεων στο Git ή στο SVN για ο πηγαίο κώδικα. | Ενημερώσεις από τη Microsoft. | Δεν ενημερώνεται καθώς εγκαταστάθηκε αλλά δεν έτρεξε. | Οι ενημερώσεις είναι σχετικά μικρές και όχι αρκετά συχνά. | Οι ενημερώσεις δεν είναι συχνές που αυτό οδηγεί σε περιορισμένη λειτουργικότητα. | Το εργαλείο αυτό ενημερώνεται αρκετά συχνά και προσφέρονται νέες λειτουργίες, εκδόσεις και βελτιώσεις. | Αν συνδυαστεί με εργαλεία όπως το Git επιτρέπει στους χρήστες να διαχειρίζονται αλλαγές. | Οι ενημερώσεις είναι τακτικές με σκοπό να υποστηρίζοντας σύγχρονες απαιτήσεις ασφαλείας. |
| **Ικανοποίηση Προσεγγίσεων SRE** | KAOS | KAOS, SQUARE, ISSRM | Microsoft's Threat Modeling | CORAS | SEPP, SREP, Secure Tropos,KAOS | Secure Tropos KAOS, Secure i* | UMLsec | UMLsec, Misuse case | ISSRM, MOSRE |

**Πίνακας 4 Αξιολόγηση εργαλείων μοντελοποίησης απαιτήσεων ασφαλείας**

# Κεφάλαιο 6 – Συμπεράσματα

Πράγματι, η μηχανική απαιτήσεων ασφαλείας (SRE) κατέχει κρίσιμη θέση στα πρώτα στάδια της ανάπτυξης λογισμικού, διασφαλίζοντας ότι οι ανησυχίες για την ασφάλεια αντιμετωπίζονται από την αρχή του Κύκλου Ζωής Ανάπτυξης Λογισμικού (SDLC). Αναγνωρίζοντας την απουσία συστηματικών ανασκοπήσεων για τις προσεγγίσεις SRE μετά το 2015, οι συγγραφείς ξεκίνησαν μια ολοκληρωμένη μελέτη για να γεφυρώσουν αυτό το χάσμα και να παρουσιάσουν τις τελευταίες εξελίξεις στον τομέα.

Ακολουθώντας τις κατευθυντήριες γραμμές που τέθηκαν από το Kitchenham, πραγματοποιήθηκε μια συστηματική ανασκόπηση των προσεγγίσεων SRE. Αρχικά, αναγνωρίστηκαν 15.585 εργασίες χρησιμοποιώντας σχετικές λέξεις-κλειδιά και κριτήρια αναζήτησης. Μέσα από μια σχολαστική διαδικασία πολλαπλών σταδίων, μόνο 108 εργασίες κρίθηκαν σχετικές, με βάση καλά καθορισμένα κριτήρια επιλογής και αξιολόγηση ποιότητας. Αυτά τα άρθρα στη συνέχεια αναλύθηκαν σχολαστικά για να οριοθετήσουν 20 διαφορετικές προσεγγίσεις SRE, οι οποίες στη συνέχεια συγκρίθηκαν με ένα σύνολο προκαθορισμένων κριτηρίων και παρουσιάστηκαν σε μορφή πίνακα.

Καθ' όλη τη διάρκεια της μελέτης, οι προσεγγίσεις SRE και τα εργαλεία μοντελοποίησης απαιτήσεων ασγαλείας αξιολογήθηκαν με βάση τη χρηστικότητά τους, την απόδοση στη φάση των απαιτήσεων, τη χρήση ορολογίας και τις τάσεις δημοσίευσης. Επιπρόσθετα, προσεγγίσεις που βασίζονται σε UML, όπως η "Misuce case, το SecureUML και το UMLsec" απέκτησαν δημοτικότητα λόγω της απλότητας και της συμβατότητάς τους με τη σύνταξη UML. Το SQUARE αναδείχθηκε ως η πιο αποτελεσματική και επιδραστική προσέγγιση στη φάση εξαγωγής απαιτήσεων, ακολουθούμενη από το MOSRE στη φάση ανάλυσης απαιτήσεων και το KAOS και το SREF στη φάση της προδιαγραφής απαιτήσεων. Ωστόσο, μια αξιοσημείωτη παρατήρηση ήταν η ανεπάρκεια στην προσαρμογή των επίσημων μεθόδων σε πολλές προσεγγίσεις SRE.

Η κύρια συμβολή αυτής της μελέτης χρησιμεύει ως πολύτιμος πόρος για τους επαγγελματίες ασφάλειας στην επιλογή της πιο κατάλληλης προσέγγισης και εργαλείων SRE για τα έργα τους.

Συμπερασματικά, η μελέτη υπογραμμίζει την ανάγκη για περαιτέρω έρευνα σχετικά με τις προσεγγίσεις SRE, ιδιαίτερα όσον αφορά τον αντίκτυπο και τις εφαρμογές τους

στον πραγματικό κόσμο. Επιπλέον, υπάρχει επιτακτική ανάγκη για ένα ενιαίο πλαίσιο ή ταξινόμηση για την τυποποίηση όρων όπως απειλές, ευπάθειες και περιουσιακά στοιχεία. Οι επίσημες μέθοδοι παραμένουν μια περιοχή ώριμη για εξερεύνηση, ειδικά σε κρίσιμα έργα που απαιτούν ακρίβεια. Επομένως, η ανάπτυξη καινοτόμων προσεγγίσεων και μοντέλων για την αντιμετώπιση αυτών των ελλείψεων στη Μηχανική Απαιτήσεων Ασφαλείας είναι επιτακτική. Επιπλέον, η ευθυγράμμιση των υφιστάμενων προσεγγίσεων με τα καθιερωμένα πρότυπα ασφάλειας πληροφοριών είναι ζωτικής σημασίας. Ωστόσο, αξίζει να σημειωθεί ότι η έλλειψη μελετών για προσεγγίσεις SRE με εμπειρικά στοιχεία από βιομηχανίες του πραγματικού κόσμου θέτει έναν περιορισμό σε αυτή την εργασία και μπορεί να εισάγει μεροληψία.

Συμπερασματικά, η συγκριτική ανάλυση των διαφόρων μεθοδολογιών απαιτήσεων ασφαλείας αποκαλύπτει ένα ποικίλο τοπίο προσεγγίσεων, καθεμία προσαρμοσμένη για να αντιμετωπίσει συγκεκριμένες πτυχές της ασφάλειας στο σχεδιασμό του συστήματος. Μεθοδολογίες όπως η MOSRE, η Secure Tropos, η KAOS, η GBRAM, το πλαίσιο M-N και το NFR δίνουν έμφαση σε μια προοπτική προσανατολισμένη στο στόχο, ευθυγραμμίζοντας τις απαιτήσεις ασφάλειας με τους οργανωτικούς στόχους. Αντίθετα, προσεγγίσεις όπως η SQUARE επικεντρώνονται στην αξιολόγηση κινδύνου, αξιολογώντας πιθανές απειλές για τον καθορισμό των απαραίτητων μέτρων ασφαλείας. Αυτό υπογραμμίζει μια θεμελιώδη απόκλιση στον τρόπο με τον οποίο οι απαιτήσεις ασφάλειας εννοιολογούνται και ιεραρχούνται μεταξύ των μεθοδολογιών.

Ενώ πολλές μεθοδολογίες προσδιορίζουν και κατηγοριοποιούν αποτελεσματικά τις απαιτήσεις ασφάλειας, υπάρχει περιθώριο βελτίωσης όσον αφορά την αντιμετώπιση της αλληλεπίδρασης μεταξύ των στόχων ασφάλειας και των κρίσιμων στοιχείων. Ένα αξιοσημείωτο κενό είναι η ενσωμάτωση ολοκληρωμένης ανάλυσης κινδύνου που λαμβάνει υπόψη τόσο τις απειλές όσο και την αξία των περιουσιακών στοιχείων που προστατεύονται. Οι μελλοντικές μεθοδολογίες θα πρέπει να προσπαθήσουν να γεφυρώσουν αυτό το χάσμα, προσφέροντας πιο συνεκτικά πλαίσια που δίνουν προτεραιότητα τόσο στην αξιολόγηση κινδύνου όσο και στην ευθυγράμμιση των στόχων ασφάλειας με τις οργανωτικές στρατηγικές.

Η εξελισσόμενη φύση των απειλών στον κυβερνοχώρο επιβάλλει τη συνεχή προσαρμογή αυτών των μεθοδολογιών. Οι μελλοντικές προσεγγίσεις θα μπορούσαν να ωφεληθούν από την ενσωμάτωση προόδων στη μηχανική μάθηση και την τεχνητή νοημοσύνη για την αυτοματοποίηση του εντοπισμού και της ιεράρχησης των απαιτήσεων ασφαλείας με βάση τη νοημοσύνη απειλών σε πραγματικό χρόνο.

Επιπλέον, η αξιοποίηση οντολογικών πλαισίων μπορεί να ενισχύσει τη συνεργασία και την ανταλλαγή γνώσεων μεταξύ των ενδιαφερόμενων μερών, οδηγώντας σε πιο αποτελεσματική μηχανική απαιτήσεων ασφαλείας.

Τελικά, η ανάπτυξη υβριδικών μεθοδολογιών που συνδυάζουν τα πλεονεκτήματα των υφιστάμενων πλαισίων, όπως η ενσωμάτωση στρατηγικών που βασίζονται σε στόχους και κινδύνους, θα μπορούσε να προσφέρει μια πιο εύρωστη και προσαρμόσιμη προσέγγιση στη μηχανική απαιτήσεων ασφαλείας σε ένα όλο και πιο περίπλοκο ψηφιακό τοπίο. Καθώς οι οργανισμοί συνεχίζουν να αντιμετωπίζουν εξελισσόμενες προκλήσεις ασφάλειας, οι μεθοδολογίες που υιοθετούνται πρέπει να εξελιχθούν ώστε να διασφαλίζεται ότι αντιμετωπίζουν αποτελεσματικά τόσο τις τρέχουσες όσο και τις αναδυόμενες ανάγκες ασφάλειας.

## Βιβλιογραφία


Ackroyd, R. (2014) ‘Supporting an Attack with Technology’, in *Social Engineering Penetration Testing*. Elsevier, pp. 271–309. Available at: https://doi.org/10.1016/B978-0-12-420124-8.00012-0.

Aladawy, D., Beckers, K. and Pape, S. (2018) ‘PERSUADED: Fighting Social Engineering Attacks with a Serious Game’, in, pp. 103–118. Available at: https://doi.org/10.1007/978-3-319-98385-1_8.

de Almeida Biolchini, J.C. *et al.* (2007) ‘Scientific research ontology to support systematic review in software engineering’, *Advanced Engineering Informatics*, 21(2), pp. 133–151. Available at: https://doi.org/10.1016/j.aei.2006.11.006.

Anwar Mohammad, M.N., Nazir, M. and Mustafa, K. (2019) ‘A Systematic Review and Analytical Evaluation of Security Requirements Engineering Approaches’, *Arabian Journal for Science and Engineering*, 44(11), pp. 8963–8987. Available at: https://doi.org/10.1007/s13369-019-04067-3.

Banerjee, C., Banerjee, A. and D. Murarka, P. (2014) ‘Measuring Software Security using MACOQR (Misuse and Abuse Case Oriented Quality Requirement) Metrics: Defensive Perspective’, *International Journal of Computer Applications*, 93(18), pp. 47–54. Available at: https://doi.org/10.5120/16439-6213.

BBC News. (2020) *Nigerian men arrested over German PPE ’scam’*.

Beckers, K. *et al.* (2017) ‘A Structured Comparison of Social Engineering Intelligence Gathering Tools’, in, pp. 232–246. Available at: https://doi.org/10.1007/978-3-319-64483-7_15.

Beckers, K. and Pape, S. (2016) ‘A Serious Game for Eliciting Social Engineering Security Requirements’, in *2016 IEEE 24th International Requirements Engineering Conference (RE)*. IEEE, pp. 16–25. Available at: https://doi.org/10.1109/RE.2016.39.

Bezerra, C.M.M., Sampaio, S.C.B. and Marinho, M.L.M. (2020) ‘Secure Agile Software Development: Policies and Practices for Agile Teams’, in, pp. 343–357. Available at: https://doi.org/10.1007/978-3-030-58793-2_28.

Böhme, R. (2010) ‘Security Metrics and Security Investment Models’, in, pp. 10–24. Available at: https://doi.org/10.1007/978-3-642-16825-3_2.

Chitrey, A., Singh, D. and Singh, V. (2012) ‘A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model’, *International*

*Journal of Information and Network Security (IJINS)*, 1(2). Available at: https://doi.org/10.11591/ijins.v1i2.426.

Christopher Shields. (2000) *Aristotle's psychology. Stanford Encyclopedia of Philosophy.*

Costa, P., Lourenço, J.C. and da Silva, M.M. (2013) 'Evaluating Cloud Services Using a Multiple Criteria Decision Analysis Approach', in, pp. 456–464. Available at: https://doi.org/10.1007/978-3-642-45005-1_34.

Daneva, M. and Wang, C. (2018) 'Security Requirements Engineering in the Agile Era: How Does it Work in Practice?', in *2018 IEEE 1st International Workshop on Quality Requirements in Agile Projects (QuaRAP)*. IEEE, pp. 10–13. Available at: https://doi.org/10.1109/QuaRAP.2018.00008.

Dardenne, A., van Lamsweerde, A. and Fickas, S. (1993) 'Goal-directed requirements acquisition', *Science of Computer Programming*, 20(1–2), pp. 3–50. Available at: https://doi.org/10.1016/0167-6423(93)90021-G.

El-Attar, M. (2012) 'Towards developing consistent misuse case models', *Journal of Systems and Software*, 85(2), pp. 323–339. Available at: https://doi.org/10.1016/j.jss.2011.08.023.

El-Attar, M. (2014) 'From misuse cases to mal-activity diagrams: bridging the gap between functional security analysis and design', *Software & Systems Modeling*, 13(1), pp. 173–190. Available at: https://doi.org/10.1007/s10270-012-0240-5.

El-Hadary, H. and El-Kassas, S. (2014) 'Capturing security requirements for software systems', *Journal of Advanced Research*, 5(4), pp. 463–472. Available at: https://doi.org/10.1016/j.jare.2014.03.001.

El-Attar, M. (2012) 'A framework for improving quality in misuse case models', *Business Process Management Journal*, 18(2), pp. 168–196. Available at: https://doi.org/10.1108/14637151211225162.

Elahi, G., Yu, E. and Zannone, N. (2009) 'A Modeling Ontology for Integrating Vulnerabilities into Security Requirements Conceptual Foundations', in, pp. 99–114. Available at: https://doi.org/10.1007/978-3-642-04840-1_10.

Elahi, G., Yu, E. and Zannone, N. (2010) 'A vulnerability-centric requirements engineering framework: analyzing security attacks, countermeasures, and requirements based on vulnerabilities', *Requirements Engineering*, 15(1), pp. 41–62. Available at: https://doi.org/10.1007/s00766-009-0090-z.

Fabian, B. *et al.* (2010) 'A comparison of security requirements engineering methods', *Requirements Engineering*, 15(1), pp. 7–40. Available at: https://doi.org/10.1007/s00766-009-0092-x.

Faily, S. and Fléchais, I. (2016) 'Finding and resolving security misusability with misusability cases', *Requirements Engineering*, 21(2), pp. 209–223. Available at: https://doi.org/10.1007/s00766-014-0217-8.

Fernandez, E.B., Yoshioka, N. and Washizaki, H. (2009) 'Modeling Misuse Patterns', in *2009 International Conference on Availability, Reliability and Security*. IEEE, pp. 566–571. Available at: https://doi.org/10.1109/ARES.2009.139.

Gerber, N., Zimmermann, V. and Volkamer, M. (2019) 'Why Johnny Fails to Protect his Privacy', in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, pp. 109–118. Available at: https://doi.org/10.1109/EuroSPW.2019.00019.

Gregoire, J. *et al.* (2007) 'On the Secure Software Development Process: CLASP and SDL Compared', in *Third International Workshop on Software Engineering for Secure Systems (SESS'07: ICSE Workshops 2007)*. IEEE, pp. 1–1. Available at: https://doi.org/10.1109/SESS.2007.7.

Guttorm, S. and Andreas L., O. (2008) 'Misuse Cases for Identifying System Dependability Threats', *Journal of Information Privacy and Security*, 4(2), pp. 3–22. Available at: https://doi.org/10.1080/2333696X.2008.10855837.

Haley, C.B. *et al.* (2008) 'Security Requirements Engineering: A Framework for Representation and Analysis', *IEEE Transactions on Software Engineering*, 34(1), pp. 133–153. Available at: https://doi.org/10.1109/TSE.2007.70754.

Hatebur, D. *et al.* (2011) 'Systematic Development of UMLsec Design Models Based on Security Requirements', in, pp. 232–246. Available at: https://doi.org/10.1007/978-3-642-19811-3_17.

Hatebur, D., Heisel, M. and Schmidt, H. (2008) 'Analysis and Component-based Realization of Security Requirements', in *2008 Third International Conference on Availability, Reliability and Security*. IEEE, pp. 195–203. Available at: https://doi.org/10.1109/ARES.2008.27.

Hill, C.G. *et al.* (2017) 'Gender-Inclusiveness Personas vs. Stereotyping', in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, pp. 6658–6671. Available at: https://doi.org/10.1145/3025453.3025609.

Iankoulova, I. and Daneva, M. (2012) ‘Cloud computing security requirements: A systematic review’, in *2012 Sixth International Conference on Research Challenges in Information Science (RCIS)*. IEEE, pp. 1–7. Available at: https://doi.org/10.1109/RCIS.2012.6240421.

International Organization for Standardization (ISO). (2009) *ISO 23601:2009 safety identification – escape and evacuation plan signs.* Available at: https://www.iso.org/standard/41685.html.

Jakobsson, M., Yang, L. and Wetzel, S. (2008) ‘Quantifying the security of preference-based authentication’, in *Proceedings of the 4th ACM workshop on Digital identity management*. New York, NY, USA: ACM, pp. 61–70. Available at: https://doi.org/10.1145/1456424.1456435.

Jürjens, J. (2001) ‘Towards Development of Secure Systems Using UMLsec’, in, pp. 187–200. Available at: https://doi.org/10.1007/3-540-45314-8_14.

Karpati, P., Sindre, G. and Opdahl, A.L. (2011) ‘Characterising and Analysing Security Requirements Modelling Initiatives’, in *2011 Sixth International Conference on Availability, Reliability and Security*. IEEE, pp. 710–715. Available at: https://doi.org/10.1109/ARES.2011.113.

Kevin D. Mitnick and William L. Simon. (2003) *The art of deception: Controlling the human element of security.* John Wiley.

Kitchenham B. (2007) *Guidelines for performing Systematic Literature Reviews in Software Engineering.* Tech. rep., Software Engineering Group, School of Computer Science and Mathematics, Keele University, Keele,.

Kocher, P. *et al.* (2019) ‘Spectre Attacks: Exploiting Speculative Execution’, in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, pp. 1–19. Available at: https://doi.org/10.1109/SP.2019.00002.

Kriaa, S. *et al.* (2015) ‘A survey of approaches combining safety and security for industrial control systems’, *Reliability Engineering & System Safety*, 139, pp. 156–178. Available at: https://doi.org/10.1016/j.ress.2015.02.008.

Krombholz, K. *et al.* (2013) ‘Social engineering attacks on the knowledge worker’, in *Proceedings of the 6th International Conference on Security of Information and Networks*. New York, NY, USA: ACM, pp. 28–35. Available at: https://doi.org/10.1145/2523514.2523596.

Kruger, H.A. and Kearney, W.D. (2006) ‘A prototype for assessing information security awareness’, *Computers & Security*, 25(4), pp. 289–296. Available at: https://doi.org/10.1016/j.cose.2006.02.008.

van Lamsweerde, A. (no date) ‘Elaborating security requirements by construction of intentional anti-models’, in *Proceedings. 26th International Conference on Software Engineering*. IEEE Comput. Soc, pp. 148–157. Available at: https://doi.org/10.1109/ICSE.2004.1317437.

Lamsweerde, A.V. (2007) ‘Engineering requirements for system reliability and security.’, 9(1), p. 196.

Larionovs, A., Teilans, A. and Grabusts, P. (2015) ‘CORAS for Threat and Risk Modeling in Social Networks’, *Procedia Computer Science*, 43, pp. 26–32. Available at: https://doi.org/10.1016/j.procs.2014.12.005.

Lee, J. *et al.* (2019) ‘A Software Development Methodology for Secure Web Application’, *International Journal on Advanced Science, Engineering and Information Technology*, 9(1), pp. 336–341. Available at: https://doi.org/10.18517/ijaseit.9.1.5987.

Lin, L. *et al.* (no date) ‘Introducing abuse frames for analysing security requirements’, in *Journal of Lightwave Technology*. IEEE Comput. Soc, pp. 371–372. Available at: https://doi.org/10.1109/ICRE.2003.1232791.

Liu, L., Yu, E. and Mylopoulos, J. (2003) ‘Security and privacy requirements analysis within a social setting’, in *Journal of Lightwave Technology*. IEEE Comput. Soc, pp. 151–161. Available at: https://doi.org/10.1109/ICRE.2003.1232746.

Luncheng Lin *et al.* (no date) ‘Using abuse frames to bound the scope of security problems’, in *Proceedings. 12th IEEE International Requirements Engineering Conference, 2004.* IEEE, pp. 333–334. Available at: https://doi.org/10.1109/ICRE.2004.1335698.

Mai, P.X. *et al.* (2018) ‘Modeling Security and Privacy Requirements: a Use Case-Driven Approach’, *Information and Software Technology*, 100, pp. 165–182. Available at: https://doi.org/10.1016/j.infsof.2018.04.007.

Massacci, F. *et al.* (2011) ‘An Extended Ontology for Security Requirements’, in, pp. 622–636. Available at: https://doi.org/10.1007/978-3-642-22056-2_64.

Matulevičius, R. *et al.* (2008) ‘Adapting Secure Tropos for Security Risk Management in the Early Phases of Information Systems Development’, in, pp. 541–555. Available at: https://doi.org/10.1007/978-3-540-69534-9_40.

Matulevičius, R. (2017) *Fundamentals of Secure System Modelling*. Cham: Springer International Publishing. Available at: https://doi.org/10.1007/978-3-319-61717-6.

Matulevicius, R., Lakk, H. and Lepmets, M. (2011) 'An approach to assess and compare quality of security models', *Computer Science and Information Systems*, 8(2), pp. 447–476. Available at: https://doi.org/10.2298/CSIS101231014M.

Mead, N.R. and Abu-Nimeh, S. (2019) 'Security and Privacy Requirements Engineering', in *Cyber Law, Privacy, and Security*. IGI Global, pp. 1711–1729. Available at: https://doi.org/10.4018/978-1-5225-8897-9.ch083.

Mead, N.R., Miyazaki, S. and Zhan, J. (2011) 'Integrating privacy requirements considerations into a security requirements engineering method and tool', *International Journal of Information Privacy, Security and Integrity*, 1(1), p. 106. Available at: https://doi.org/10.1504/IJIPSI.2011.043733.

Mellado, D. *et al.* (2010) 'A systematic review of security requirements engineering', *Computer Standards & Interfaces*, 32(4), pp. 153–165. Available at: https://doi.org/10.1016/j.csi.2010.01.006.

Mellado, D., Fernández-Medina, E. and Piattini, M. (2007) 'A common criteria based security requirements engineering process for the development of secure information systems', *Computer Standards & Interfaces*, 29(2), pp. 244–253. Available at: https://doi.org/10.1016/j.csi.2006.04.002.

Mohammed, N.M. *et al.* (2017) 'Exploring software security approaches in software development lifecycle: A systematic mapping study', *Computer Standards & Interfaces*, 50, pp. 107–115. Available at: https://doi.org/10.1016/j.csi.2016.10.001.

Mouratidis, H. and Giorgini, P. (2009) 'Enhancing Secure Tropos to Effectively Deal with Security Requirements in the Development of Multiagent Systems', in, pp. 8–26. Available at: https://doi.org/10.1007/978-3-642-04879-1_2.

Muñante, D. *et al.* (2014) 'A Review of Security Requirements Engineering Methods with Respect to Risk Analysis and Model-Driven Engineering', in, pp. 79–93. Available at: https://doi.org/10.1007/978-3-319-10975-6_6.

Nikola Milosevic. (2013) *Introduction to Social Engineering.* Available at: http://inspiratron.org/%0Aintroduction-to-social-engineering/.

Norman, D.A. (2010) 'The research-practice gap', *Interactions*, 17(4), pp. 9–12. Available at: https://doi.org/10.1145/1806491.1806494.

Oueslati, H., Rahman, M.M. and Othmane, L. ben (2015) 'Literature Review of the Challenges of Developing Secure Software Using the Agile Approach', in *2015 10th*

*International Conference on Availability, Reliability and Security*. IEEE, pp. 540–547. Available at: https://doi.org/10.1109/ARES.2015.69.

Pape, S. *et al.* (2020) 'Conceptualization of a CyberSecurity Awareness Quiz', in, pp. 61–76. Available at: https://doi.org/10.1007/978-3-030-62433-0_4.

Pavlidis, M. *et al.* (2017) 'Selecting Security Mechanisms in Secure Tropos', in, pp. 99–114. Available at: https://doi.org/10.1007/978-3-319-64483-7_7.

Peltier, T.R. (2006) 'Social Engineering: Concepts and Solutions', *EDPACS*, 33(8), pp. 1–13. Available at: https://doi.org/10.1201/1079.07366981/45802.33.8.20060201/91956.1.

Radha Gulati. (2003) *The threat of social engineering and your defense against it.* SANS Readi.

Raspotnig, C. and Opdahl, A. (2013) 'Comparing risk identification techniques for safety and security requirements', *Journal of Systems and Software*, 86(4), pp. 1124–1151. Available at: https://doi.org/10.1016/j.jss.2012.12.002.

Rehman, S. and Gruhn, V. (2018) 'An Effective Security Requirements Engineering Framework for Cyber-Physical Systems', *Technologies*, 6(3), p. 65. Available at: https://doi.org/10.3390/technologies6030065.

Rrenja, A. and Matulevičius, R. (2015) 'Pattern-Based Security Requirements Derivation from Secure Tropos Models', in, pp. 59–74. Available at: https://doi.org/10.1007/978-3-319-25897-3_5.

Salini, P. and Kanmani, S. (2012) 'Survey and analysis on Security Requirements Engineering', *Computers & Electrical Engineering*, 38(6), pp. 1785–1797. Available at: https://doi.org/10.1016/j.compeleceng.2012.08.008.

Salva, S. and Regainia, L. (2019) 'A catalogue associating security patterns and attack steps to design secure applications', *Journal of Computer Security*, 27(1), pp. 49–74. Available at: https://doi.org/10.3233/JCS-171063.

Schaab, P., Beckers, K. and Pape, S. (2017) 'Social engineering defence mechanisms and counteracting training strategies', *Information & Computer Security*, 25(2), pp. 206–222. Available at: https://doi.org/10.1108/ICS-04-2017-0022.

Schmidt, H. (2010) 'Threat- and Risk-Analysis During Early Security Requirements Engineering', in *2010 International Conference on Availability, Reliability and Security*. IEEE, pp. 188–195. Available at: https://doi.org/10.1109/ARES.2010.14.

Sebastian Pape and Dennis-Kenji Kipker. (2020) *Case study: Checking a serious security-awareness game for its legal adequacy. unpublished manuscript*.

Shamal Faily and Ivan Flechais. (2011) ‘Persona cases: a technique for grounding personas.’, in *SIGCHI Conference on Human Factors in Computing Systems.*, pp. 2267–2270.

Silva, P. *et al.* (2016) ‘Software Development Initiatives to Identify and Mitigate Security Threats - Two Systematic Mapping Studies’, *CLEI Electronic Journal* [Preprint]. Available at: https://doi.org/10.19153/cleiej.19.3.5.

Sindre, G. and Opdahl, A.L. (2005) ‘Eliciting security requirements with misuse cases’, *Requirements Engineering*, 10(1), pp. 34–44. Available at: https://doi.org/10.1007/s00766-004-0194-4.

Soares Cruzes, D. *et al.* (2018) ‘Challenges and Experiences with Applying Microsoft Threat Modeling in Agile Development Projects’, in *2018 25th Australasian Software Engineering Conference (ASWEC)*. IEEE, pp. 111–120. Available at: https://doi.org/10.1109/ASWEC.2018.00023.

Souag, A. *et al.* (2015) ‘A Security Ontology for Security Requirements Elicitation’, in, pp. 157–177. Available at: https://doi.org/10.1007/978-3-319-15618-7_13.

Stajano, F. and Wilson, P. (2011) ‘Understanding scam victims’, *Communications of the ACM*, 54(3), pp. 70–75. Available at: https://doi.org/10.1145/1897852.1897872.

Susi, A.; Perini, A.; Mylopoulos, J.; Giorgini, P. (2005) ‘The Tropos Metamodel and its Use.’, *Informatica*, 29(4), pp. 401–408.

Tarik Saleh. (2020) *Covidlock update: Deeper analysis of coronavirus android ransomware.*

Trajce Dimkov, André van Cleeff, Wolter Pieters, and P.H. (2010) ‘Two methodologies for physical penetration testing using social engineering.’, in *26th Annual Computer Security Applications Conference, ACSAC ’10*, pp. 399–408.

Tselios, C., Tsolis, G. and Athanatos, M. (2020) ‘A Comprehensive Technical Survey of Contemporary Cybersecurity Products and Solutions’, in, pp. 3–18. Available at: https://doi.org/10.1007/978-3-030-42051-2_1.

Williams, I. (2018) ‘An Ontology Based Collaborative Recommender System for Security Requirements Elicitation’, in *2018 IEEE 26th International Requirements Engineering Conference (RE)*. IEEE, pp. 448–453. Available at: https://doi.org/10.1109/RE.2018.00060.

Wirtz, R. and Heisel, M. (2019) ‘A Systematic Method to Describe and Identify Security Threats Based on Functional Requirements’, in, pp. 205–221. Available at: https://doi.org/10.1007/978-3-030-12143-3_17.

Yasin, A. *et al.* (2021) 'Understanding and deciphering of social engineering attack scenarios', *SECURITY AND PRIVACY*, 4(4). Available at: https://doi.org/10.1002/spy2.161.

https://www.objectiver.com/fileadmin/download/documents/generalleaflet.pdf

https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started

https://www.uio.no/studier/emner/matnat/ifi/INF5150/h06/undervisningsmateriale/060930.CORAS-handbook-v1.0.pdf

http://www.dit.unitn.it/~pgiorgio/papers/iTrust05-ST-Tool.pdf

https://digi.gov.gr/enisa-threat-landscape-2024/?utm_source.com