PROJECT 458

Άννα Μακρίδου ΑΜ:4934

Αλέξανδρος Φουρτούνης ΑΜ:5031

Γεώργιος Ξηρουδάκης ΑΜ:5067

Παντελεήμων Τσαγκαράκης ΑΜ:5075

Table Of Contents

Part 1

Στο πλαίσιο του Preparatory Phase του έργου, αναλύσαμε τις βασικές αρχές της κρυπτογραφικής ευελιξίας, τις ορολογίες που δόθηκαν ως πηγές, καθώς και τις προκλήσεις που προκύπτουν από τη μετάβαση στις Post-Quantum Cryptography τεχνολογίες. Στόχος μας ήταν η αναγνώριση ευάλωτων κρυπτογραφικών μηχανισμών που απειλούνται από κβαντικούς υπολογιστές ή έχουν ξεπεραστεί.

Αρχικά, μελετήσαμε και κατανοήσαμε τις ορολογίες που δόθηκαν ως πηγές. Παραθέτουμε συνοπτικά ορισμούς:

Harvert Now, Decrypt Later: Βασίζεται στην αποθήκευση κρυπτογραφημένων δεδομένων που δεν μπορούν προς το παρόν να αποκρυπτογραφηθούν. Τα δεδομένα αυτά διατηρούνται μέχρι τη στιγμή που η τεχνολογία αποκρυπτογράφησης εξελιχθεί τόσο ώστε να μπορούν να αποκρυπτογραφηθούν.

Cryptographic Agility: Η ικανότητα ενός συστήματος να αλλάζει και να προσαρμόζεται γρήγορα σε νέους κρυπτογραφικούς αλγορίθμους χωρίς να απαιτούνται σημαντικές αλλαγές στην υποδομή του συστήματος.

Cryptographic Primitives: Τα βασικά δομικά στοιχεία της κρυπτογραφίας, που είναι απλές λειτουργίες χαμηλού επιπέδου, όπως αλγόριθμοι κρυπτογράφησης, συναρτήσεις κατακερματισμού, ψηφιακές υπογραφές.

Post Quantum Cryptography: Αλγόριθμοι που αντέχουν σε επιθέσεις κβαντικών υπολογιστών

Cryptography Inventory: Περιλαμβάνει λεπτομέρειες για τους αλγορίθμους, τις λειτουργίες, τα κλειδιά, τα πιστοποιητικά και τα πρωτόκολλα που εφαρμόζονται.

Στη συνέχεια, μελετήσαμε τα guidelines, τα οποία τονίζουν την ανάγκη για τους οργανισμούς να προετοιμαστούν για την απειλή που θέτουν οι κβαντικοί υπολογιστές στην κρυπτογραφία. Συγκεκριμένα, προτείνουν τη δημιουργία ενός χάρτη για τη μετάβαση στην Post Quantum Cryptography, ξεκινώντας με την απογραφή των συστημάτων που χρησιμοποιούν κρυπτογραφία ευάλωτη σε κβαντικές επιθέσεις. Επιπλέον, τονίζεται η σημασία της ανάπτυξης λύσεων PQC και της εφαρμογής υβριδικών συστημάτων που συνδυάζουν υπάρχουσες κρυπτογραφικές μεθόδους με νέες τεχνολογίες, όπως η Quantum Key Distribution. Σύμφωνα με το NIST PQC Migration Fact Sheet (2023), οι οργανισμοί πρέπει να ξεκινήσουν την προετοιμασία για τη μετάβαση σε κρυπτογραφία ανθεκτική σε κβαντικούς υπολογιστές, εντοπίζοντας και αντικαθιστώντας ευάλωτους αλγορίθμους. Παράλληλα, η Ευρωπαϊκή Επιτροπή (2024) εξέδωσε σύσταση που ενθαρρύνει τα κράτη μέλη να αναπτύξουν μια συντονισμένη στρατηγική μετάβασης στην Post-Quantum Cryptography (PQC), καθορίζοντας σαφείς στόχους και χρονοδιαγράμματα για την υιοθέτησή της. Επιπλέον, το PQC Migration Handbook του TNO παρέχει λεπτομερείς οδηγίες για την αξιολόγηση των τρεχουσών κρυπτογραφικών υποδομών και τη σταδιακή αντικατάσταση αδύναμων αλγορίθμων. Σύμφωνα με τις διεθνείς αυτές κατευθυντήριες γραμμές, η επιτυχής μετάβαση απαιτεί καταγραφή των υφιστάμενων κρυπτογραφικών στοιχείων, ανάλυση των κινδύνων και σχεδιασμό μιας δομημένης στρατηγικής, ώστε να διασφαλιστεί η διαλειτουργικότητα και η ασφάλεια των συστημάτων στην κβαντική εποχή.

Έπειτα επιλέξαμε τα εξής Cryptographic Primitives:

1) One-Way Hash Functions : Μονοκατευθυνόμενες Συναρτήσεις

- MD5: Ευάλωτο σε επιθέσεις σύγκρουσης που καθιστούν τον αλγόριθμο μη ασφαλή.
- SHA-1: Επίσης ευάλωτο σε επιθέσεις σύγκρουσης και έχει αποσυρθεί από το NIST.
- SHA-2: Παρόλο που παραμένει ασφαλές, η ασφάλειά του μειώνεται με τον αλγόριθμο Grover, απαιτώντας μεγαλύτερα μήκη εξόδου.

2)Symmetric Key Cryptography: Συμμετρική Κρυπτογραφία

- DES: Το μικρό μέγεθος κλειδιού (56 bits) το καθιστά ευάλωτο σε επιθέσεις brute force.
- 3DES: Ευάλωτο σε επιθέσεις meet-in-the-middle και έχει αποσυρθεί από το NIST.
- ECB Mode: Διαρρέει μοτίβα δεδομένων λόγω έλλειψης διάχυσης.
- CBC Mode: Δεν έχει padding και κατάλληλους ελέγχους ακεραιότητας.
- AES με μικρά κλειδιά: Ευάλωτο στον αλγόριθμο Grover, προτιμώνται μεγαλύτερα κλειδιά.

3)Asymmetric Key Cryptography: Ασύμμετρη Κρυπτογραφία

- RSA: Βασίζεται στην παραγοντοποίηση ακεραίων, που καταρρίπτεται από τον αλγόριθμο Shor.
- DSA: Ευάλωτο σε κβαντικές επιθέσεις και προβλήματα επαναχρησιμοποίησης παραμέτρων.

- ECC: Βασίζεται στους διακριτούς λογάριθμους, που είναι ευάλωτοι σε κβαντικές επιθέσεις.
- Diffie Hellman: Ευάλωτο σε κβαντικές επιθέσεις.
- Στατικό Diffie Hellman χωρίς εφήμερα κλειδιά: Δεν παρέχει forward secrecy.

4)Digital Signatures: Ψηφιακές Υπογραφές

- RSA Signatures: Ευάλωτες σε επιθέσεις padding oracle.
- MD5 και SHA-1 Signature Schemes: Ευάλωτες σε επιθέσεις σύγκρουσης.

5)Cryptographically secure pseudorandom number generator: Κρυπτογραφικά Ασφαλής Γεννήτρια Ψευδοτυχαίων Αριθμών (CSPRNG)

- SHA-2: Παρόμοια με το hashing, μειωμένη ασφάλεια υπό τον αλγόριθμο Grover.
- Μη κρυπτογραφικά ασφαλείς RNG: Ακατάλληλες για παραγωγή κλειδιών.

Part 2

Αφού δοκιμάσαμε διάφορα εργαλεία, καταλήξαμε στο Semgrep. Το Semgrep είναι ένα ανοιχτού κώδικα εργαλείο που χρησιμοποιείται για:

- Ανίχνευση deprecated πρακτικών.
- Κατηγοριοποίηση ευπαθειών βάσει επιπέδων σοβαρότητας.
- Αναγνώριση ευάλωτων κρυπτογραφικών αλγορίθμων.

Παρόλαυτα επιλέξαμε να φτιάξουμε έναν δικό μας custom parser με τον οποίον κατηγοριοποιήσαμε τις ευπάθειες ως εξής:

1. **High**
2. **Medium**
3. **Low**

HIGH

Οι περιπτώσεις αυτές υποδεικνύουν σοβαρά προβλήματα ασφάλειας. Η παρουσία τέτοιων ευπαθειών εκθέτει το σύστημα σε σημαντικούς κινδύνους και απαιτείται άμεση διόρθωση. Σε αυτή την κατηγορία εντάξαμε το MD5 και τα DES/3DES, που είναι γνωστά για τις ευπάθειές τους (collisions, brute-force attacks). Παρόμοια, τα μικρά κλειδιά RSA (<2048 bits), οι στατικοί IVs και το ECB mode στον AES παραβιάζουν βασικές αρχές ασφάλειας και επιτρέπουν προβλέψιμες επιθέσεις ή διαρροές μοτίβων δεδομένων. Οι μη κρυπτογραφικά ασφαλείς RNGs (π.χ. random()) οδηγούν σε αδύναμα κλειδιά, ενώ αλγόριθμοι όπως το RC4 και το Blowfish δεν θεωρούνται πλέον κατάλληλοι για σύγχρονες εφαρμογές. Οι ευπάθειες αυτές απαιτούν άμεση αντιμετώπιση για να διασφαλιστεί η συμμόρφωση με τα σύγχρονα πρότυπα ασφάλειας.

MEDIUM

Οι ευπάθειες αυτής της κατηγορίας δεν είναι άμεσα κρίσιμες αλλά πρέπει να εξεταστούν για τη μείωση των κινδύνων. Το SHA-1 αξιολογήθηκε ως WARNING, καθώς, αν και έχει αντικατασταθεί σε πολλές εφαρμογές, παραμένει σε χρήση σε legacy συστήματα. Η χρήση του CBC mode χωρίς ελέγχους ακεραιότητας το καθιστά ευάλωτο σε padding oracle attacks, ενώ το AES-128 είναι δυνητικά ευάλωτο σε κβαντικές επιθέσεις. Ο αλγόριθμος DSA παρουσιάζει περιορισμένη αντοχή σε κβαντικούς υπολογιστές, ενώ το Static Diffie-Hellman δεν παρέχει forward secrecy, αυξάνοντας την πιθανότητα υποκλοπών. Το Blowfish, λόγω του μικρού μεγέθους μπλοκ και άλλων γνωστών αδυναμιών, παραμένει λιγότερο ασφαλές για μεγάλες ποσότητες δεδομένων. Η κατηγοριοποίηση αυτή αποδίδεται σε περιπτώσεις όπου οι επιπτώσεις μπορούν να περιοριστούν μέσω υφιστάμενων αντιμέτρων.

LOW

Η κατηγορία INFO αφορά μακροπρόθεσμες συστάσεις για την υιοθέτηση σύγχρονων πρακτικών. Το SHA-256, αν και ασφαλές για κλασικούς υπολογιστές, έχει μειωμένο περιθώριο ασφάλειας υπό τον αλγόριθμο Grover. Ο αλγόριθμος IDEA, αν και παρωχημένος, εξακολουθεί να χρησιμοποιείται σε legacy εφαρμογές. Οι ευπάθειες αυτές δεν απαιτούν άμεση παρέμβαση, αλλά ενδείκνυται η σταδιακή μετάβαση σε εναλλακτικές, όπως το AES-GCM.

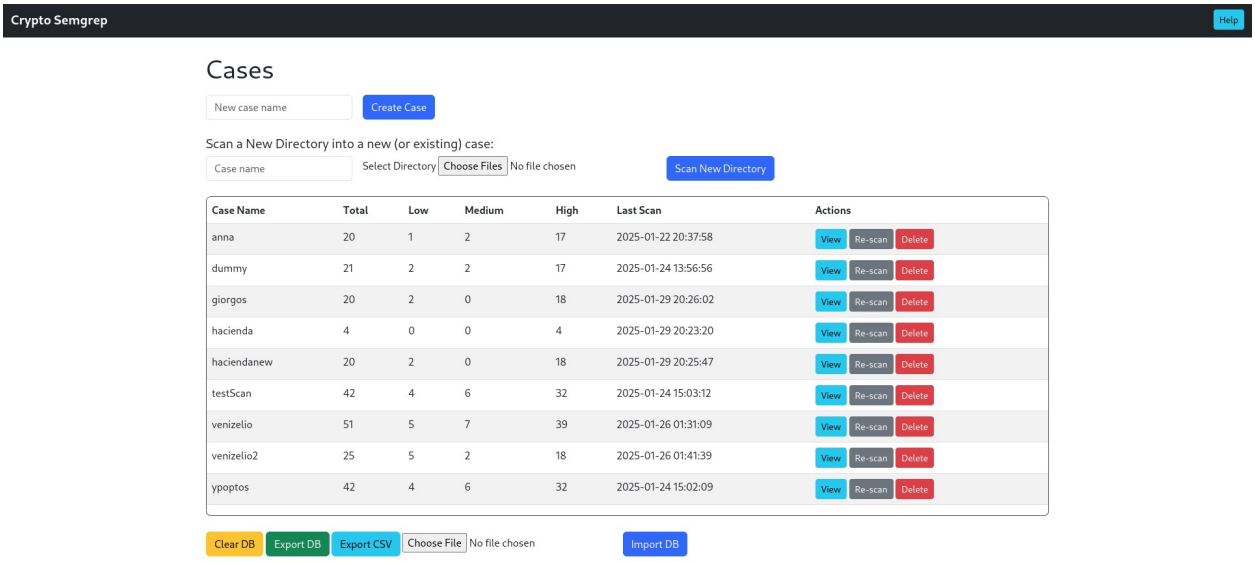
Στη συνέχεια φτιάξαμε ένα dummy node με 14 αρχεία, 4 Java, 5 Python, 5 C. Τρέξαμε το εργαλείο σε αυτά τα αρχεία και καταλήξαμε στα εξής αποτελέσματα:

1. **Java**: 4 vulnerable files out of 4 scanned
2. **C**: 5 vulnerable files out of 5 scanned
3. **Python**: 5 vulnerable files out of 5 scanned

Επίσης δοκιμάσαμε το εργαλείο μας σε κώδικα άλλης ομάδας. Τα αποτελέσματα αυτά αποθηκεύονται στη database που φτιάξαμε. Συνολικά, η χρήση του εργαλείου μας επέτρεψε την ανίχνευση ευπαθειών με ακρίβεια και τη διαβάθμισή τους σύμφωνα με την κρισιμότητα. Τα αποτελέσματα έδειξαν ότι η πλειοψηφία των σφαλμάτων ανήκει στην κατηγορία ERROR, υποδεικνύοντας την ανάγκη για άμεσες παρεμβάσεις.

DATABASE

Για τη διαχείριση των αποτελεσμάτων της ανάλυσης κρυπτογραφικών ευπαθειών, αναπτύξαμε ένα γραφικό περιβάλλον χρήστη σε συνδυασμό με μία βάση δεδομένων για την αποθήκευση και οργάνωση των σαρώσεων. Το GUI επιτρέπει στους χρήστες να εκτελούν σαρώσεις σε αρχεία και φακέλους, να προβάλλουν τα αποτελέσματα σε πίνακες και να φιλτράρουν τα δεδομένα με βάση το



επίπεδο σοβαρότητας της ευπάθειας (**HIGH, MEDIUM, LOW**).

Το γραφικό περιβάλλον χρήστη επιτρέπει την εύκολη διαχείριση των σαρώσεων και των αποτελεσμάτων τους.

Στην κεντρική σελίδα εμφανίζεται ένας πίνακας με όλες τις καταγεγραμμένες περιπτώσεις ανάλυσης κρυπτογραφικών ευπαθειών, περιλαμβάνοντας πληροφορίες όπως το όνομα της περίπτωσης, τον συνολικό αριθμό ευπαθειών, την κατηγοριοποίησή τους σε επίπεδα σοβαρότητας και την ημερομηνία της τελευταίας σάρωσης.

Ο χρήστης μπορεί να δημιουργήσει νέα περίπτωση ελέγχου, να εκτελέσει σάρωση νέων αρχείων και φακέλων, να προβάλει λεπτομερή αποτελέσματα, να επαναλάβει μια σάρωση ή να διαγράψει μία εγγραφή.

Παράλληλα, έχουν ενσωματωθεί λειτουργίες επιτρέποντας την εισαγωγή και εξαγωγή δεδομένων, τη διαγραφή όλου του αποθηκευμένου ιστορικού και την εξαγωγή των αποτελεσμάτων σε μορφή CSV, ώστε να διευκολύνεται η περαιτέρω ανάλυση.

Τέλος, έχει προστεθεί ένα κουμπί βοήθειας Help που παρέχει καθοδήγηση στον χρήστη σχετικά με τη χρήση του εργαλείου, καθοδηγώντας τον σε αυτήν την αναφορά.

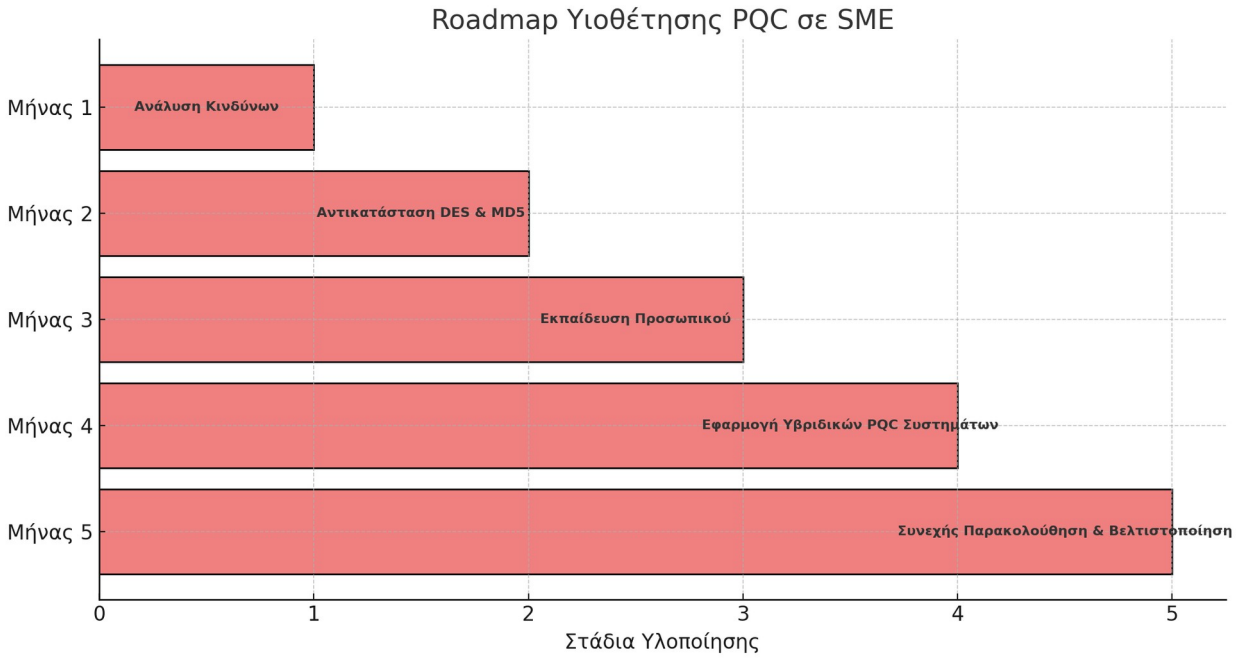
Part 3

Η μετάβαση από αδύναμους ή ξεπερασμένους κρυπτογραφικούς αλγόριθμους σε ισχυρότερους αποτελεί κρίσιμο βήμα για τη διασφάλιση της ασφάλειας συστημάτων, ειδικά ενόψει της απειλής από κβαντικούς υπολογιστές. Στόχος του Part 3 είναι ο σχεδιασμός ενός δομημένου πλάνου μετάβασης, λαμβάνοντας υπόψη επιχειρησιακές και τεχνικές ανάγκες.

Βήματα Μετάβασης

1. Καταγραφή των υπαρχόντων κρυπτογραφικών μηχανισμών, βιβλιοθηκών και κλειδιών.
2. Ανίχνευση ευπαθειών μέσω του parser μας από το Part 2.
3. Προσδιορισμός του επιπέδου κινδύνου κάθε ευπάθειας (ERROR, WARNING, INFO).
4. Αντικατάσταση ευπαθών αλγορίθμων με σύγχρονες επιλογές

Visual Roadmap



Υλοποίηση της Μετάβασης

Οι αλλαγές που εφαρμόσαμε αφορούν την ενίσχυση της ασφάλειας κρυπτογραφίας στον κώδικα, σύμφωνα με τις οδηγίες των NIST SP 800-57 και NIST SP 800-131A. Συγκεκριμένα, αντικαταστήσαμε μη ασφαλείς αλγορίθμους όπως MD5, SHA-1, DES, 3DES, RC4, Blowfish και IDEA με ασφαλέστερες επιλογές όπως SHA-256, SHA-3, AES-GCM και ισχυρότερα RSA/ECC κλειδιά. Επιπλέον, επιβάλαμε ελάχιστο μήκος κλειδιού 2048 bits για RSA και ενθαρρύναμε τη χρήση OAEP padding, που είναι απαραίτητο για την ασφάλεια της RSA κρυπτογράφησης. Εξαλείψαμε τη χρήση hardcoded κλειδιών και στατικών IVs, αντικαθιστώντας τα με δυναμικά παραγόμενες τιμές μέσω ασφαλών τυχαίων γεννητριών. Καταργήσαμε τη χρήση AES σε ECB mode λόγω των γνωστών αδυναμιών του και ενσωματώσαμε προειδοποιήσεις για CBC mode χωρίς integrity checks, προτείνοντας τη χρήση GCM ως πιο ασφαλή εναλλακτική. Παράλληλα, προσθέσαμε έλεγχο για την ανίχνευση DSA και στατικών Diffie-Hellman κλειδιών, προτείνοντας ECDSA με secp256r1 και ephemeral Diffie-Hellman για καλύτερη ασφάλεια.

Για την προστασία από μελλοντικές απειλές κβαντικών υπολογιστών, προσθέσαμε προειδοποίηση για SHA-256, προτείνοντας εναλλακτικά SHA-3 για μεγαλύτερη ανθεκτικότητα. Όλες αυτές οι αλλαγές βελτιώνουν την ασφάλεια του κώδικα και συμμορφώνονται με τις προδιαγραφές των NIST SP 800-57 και NIST SP 800-131A, ενισχύοντας τη θωράκιση έναντι σύγχρονων κρυπτογραφικών επιθέσεων.

Python Files

Στα Python αρχεία, πραγματοποιήσαμε σημαντικές αλλαγές για τη βελτίωση της ασφάλειας της κρυπτογραφίας, αντικαθιστώντας παρωχημένους και ευάλωτους αλγορίθμους με πιο ασφαλείς επιλογές, σύμφωνα με τις οδηγίες των NIST SP 800-57 και NIST SP 800-131A.

Συγκεκριμένα, αντικαταστήσαμε τη χρήση των MD5 και SHA-1, που είναι επιρρεπείς σε collision attacks, με SHA-256 και SHA-3, ενώ εξαλείψαμε τους αλγόριθμους DES, 3DES, RC4, Blowfish και IDEA, αντικαθιστώντας τους με AES-GCM που παρέχει καλύτερη ασφάλεια και ακεραιότητα δεδομένων.

Εντοπίσαμε και αποτρέψαμε τη χρήση του ECB mode στην AES κρυπτογράφηση, το οποίο διαρρέει πρότυπα δεδομένων, προτείνοντας εναλλακτικά το CBC ή το GCM mode με σωστή διαχείριση της ακεραιότητας των δεδομένων.

Για τη διαχείριση κλειδιών, επιβάλαμε την απαίτηση ελάχιστου μήκους 2048 bits για RSA κλειδιά, απαγορεύσαμε τη χρήση RSA χωρίς OAEP padding, και ενθαρρύναμε τη μετάβαση από DSA σε ECDSA με καμπύλες secp256r1.

Μετά εξαλείψαμε τη χρήση στατικών IVs, ενθαρρύνοντας τη χρήση τυχαίων IVs μέσω ασφαλών RNGs και αποτρέψαμε τη χρήση hardcoded κρυπτογραφικών κλειδιών και μυστικών προτείνοντας τη φόρτωσή τους από ασφαλή key management συστήματα.

Τέλος, βελτιώσαμε την ασφάλεια των τυχαίων αριθμών απορρίπτοντας τη χρήση του random.random() για κρυπτογραφικές λειτουργίες και προτείναμε τη χρήση secrets.token_bytes ή os.urandom, ενώ προειδοποιήσαμε για τη χρήση SHA-256, προτείνοντας το SHA-3 για μακροχρόνια ανθεκτικότητα σε επιθέσεις κβαντικής κρυπτογραφίας.

Java Files

Στα αρχεία Java, πραγματοποιήσαμε σημαντικές αλλαγές για την ενίσχυση της κρυπτογραφικής ασφάλειας, σύμφωνα με τις οδηγίες των NIST SP 800-57 και NIST SP 800-131A.

Αντικαταστήσαμε τη χρήση του MD5 και SHA-1, που είναι επιρρεπείς σε collision attacks, με SHA-256 ή SHA-3 για ισχυρότερη ακεραιότητα δεδομένων.

Αποτρέψαμε τη χρήση του DES με ECB mode, ο οποίος είναι πλέον ξεπερασμένος και ευάλωτος σε επιθέσεις, αντικαθιστώντας τον με AES-256 σε GCM mode που παρέχει αυξημένη ασφάλεια και προστασία από επιθέσεις padding oracle.

Επιβάλαμε την αποφυγή hardcoded keys, προτείνοντας αντ' αυτού τη χρήση Key Management Systems (KMS) για ασφαλή αποθήκευση και διαχείριση κλειδιών.

Για την ασφάλεια της ασύμμετρης κρυπτογράφησης, εξαλείψαμε τη χρήση RSA κλειδιών μικρότερων των 2048 bits, ώστε να πληρούνται οι ελάχιστες προδιαγραφές του NIST και να αποτρέπονται brute-force επιθέσεις.

Αντικαταστήσαμε τη χρήση RSA χωρίς padding, η οποία εκθέτει τον αλγόριθμο σε επιθέσεις, με OAEP padding με SHA-256 και MGF1, διασφαλίζοντας ότι η κρυπτογράφηση δεν είναι ευάλωτη σε επιθέσεις κειμένου-επιλέκτη (chosen-plaintext attacks).

Όλες αυτές οι αλλαγές εξασφαλίζουν ότι ο κώδικας συμμορφώνεται με τις βέλτιστες πρακτικές κρυπτογράφησης του NIST και ενισχύει την προστασία των δεδομένων από σύγχρονες κρυπτογραφικές απειλές.

C Files

Στα αρχεία C, πραγματοποιήσαμε σημαντικές αλλαγές για την ενίσχυση της κρυπτογραφικής ασφάλειας, εναρμονίζοντας τον κώδικα με τις οδηγίες των NIST SP 800-57 και NIST SP 800-131A.

Αντικαταστήσαμε τη χρήση των MD5 και SHA-1, οι οποίοι είναι πλέον ξεπερασμένοι λόγω ευπάθειας σε collision attacks, με SHA-256 ή SHA-3 για ισχυρότερη προστασία της ακεραιότητας των δεδομένων.

Επιπλέον, αποτρέψαμε τη χρήση του DES, ο οποίος θεωρείται ανασφαλής λόγω μικρού μήκους κλειδιού και επιθέσεων brute-force, αντικαθιστώντας τον με AES-256, ο οποίος προσφέρει αυξημένη ασφάλεια και μεγαλύτερη ανθεκτικότητα σε σύγχρονες κρυπτογραφικές απειλές.

Ανιχνεύσαμε και εξαλείψαμε τη χρήση hardcoded keys, καθώς η αποθήκευσή τους στον πηγαίο κώδικα αποτελεί σοβαρή ευπάθεια, προτείνοντας τη φόρτωσή τους από ασφαλή key management συστήματα.

Για την ασύμμετρη κρυπτογράφηση, αντικαταστήσαμε τη δημιουργία RSA κλειδιών μικρότερων των 2048 bits, διασφαλίζοντας ότι πληρούνται τα ελάχιστα πρότυπα ασφαλείας και μειώνοντας τον κίνδυνο αποκρυπτογράφησης μέσω brute-force επιθέσεων.

Επίσης, βελτιώσαμε την ασφάλεια του AES encryption, αποτρέποντας τη χρήση κλειδιών μικρότερων των 256 bits, ώστε να ενισχύσουμε την ανθεκτικότητα της κρυπτογράφησης ενάντια σε κβαντικές απειλές.

Όλες αυτές οι αλλαγές διασφαλίζουν ότι ο κώδικας συμμορφώνεται με τα σύγχρονα κρυπτογραφικά πρότυπα του NIST και ενισχύουν την προστασία των δεδομένων από επιθέσεις.

Χρήση PQC σε μικρομεσαία επιχείρηση (SME)

Ας εξετάσουμε το παράδειγμα μιας μικρομεσαίας επιχείρησης, έστω μιας εταιρείας με 50 υπαλλήλους. Η επιχείρηση αυτή διαχειρίζεται ευαίσθητα δεδομένα όπως στοιχεία πληρωμών, χρηστών κτλ. Ωστόσο η χρήση παλαιών συστημάτων και οι περιορισμένοι πόροι δημιουργούν προκλήσεις για την υιοθέτηση ισχυρότερων κρυπτογραφικών προτύπων και τη μετάβαση σε τεχνολογίες Post Quantum Cryptography.

Η έλλειψη επαρκούς προϋπολογισμού είναι μία από τις κύριες δυσκολίες. Καθιστά δύσκολη την πλήρη αναβάθμιση των υποδομών ή την πρόσληψη εξειδικευμένων ειδικών στην κρυπτογραφία. Παράλληλα, τα legacy συστήματα που χρησιμοποιούν ξεπερασμένους αλγορίθμους, όπως MD5 για αποθήκευση κωδικών και DES για κρυπτογράφηση δεδομένων, απαιτούν εκτεταμένες αλλαγές. Επιπλέον, η ανάγκη για συνεχή λειτουργία της επιχείρησης περιορίζει τη δυνατότητα διακοπών λειτουργίας κατά τη διάρκεια της μετάβασης, καθώς ακόμη και μικρές καθυστερήσεις μπορούν να επηρεάσουν την εμπιστοσύνη των πελατών και τα έσοδα.

Οι περιορισμοί αυτοί επηρεάζουν την υιοθέτηση ισχυρότερων συστημάτων με διάφορους τρόπους. Αρχικά, η επιχείρηση επικεντρώνεται στην αντικατάσταση του MD5 και του DES που παρουσιάζουν άμεσους κινδύνους ασφάλειας. Η μετάβαση γίνεται σταδιακά εξοικονομώντας πόρους και μειώνοντας τον κίνδυνο λειτουργικών διαταραχών. Επιπλέον επιλέγονται εργαλεία για την ανάλυση και εντοπισμό ευπαθειών, καθώς και υβριδικά μοντέλα που διευκολύνουν τη σταδιακή ενσωμάτωση των PQC τεχνολογιών.

Παράλληλα, πρέπει να παρέχεται εκπαίδευση στο προσωπικό για την κατανόηση και τη χρήση των νέων τεχνολογιών, μειώνοντας έτσι τα πιθανά λάθη κατά την εφαρμογή. Οι παραπάνω παράγοντες οδηγούν σε μια σταδιακή, αλλά αποτελεσματική προσέγγιση, η οποία εξισορροπεί την ανάγκη για αυξημένη ασφάλεια με τους περιορισμούς της επιχείρησης. Με αυτόν τον τρόπο, η μικρομεσαία επιχείρηση θέτει τις βάσεις για την επιτυχή ενσωμάτωση των τεχνολογιών PQC, προετοιμαζόμενη για τις μελλοντικές απειλές από τους κβαντικούς υπολογιστές.

Part4

Η κρυπτογραφική ευελιξία (Crypto Agility) είναι η ικανότητα ενός συστήματος να αλλάζει και να προσαρμόζεται σε νέους κρυπτογραφικούς αλγορίθμους χωρίς την ανάγκη σημαντικών αλλαγών στην υποδομή του. Με την ανάπτυξη των κβαντικών υπολογιστών, οι σημερινοί αλγόριθμοι κρυπτογράφησης γίνονται ολοένα και πιο ευάλωτοι. Ο προσομοιωτής κρυπτογραφικής ευελιξίας που αναπτύξαμε επιτρέπει την αναγνώριση αδύναμων κρυπτογραφικών μηχανισμών και την προσομοίωση της μετάβασης σε πιο ασφαλείς αλγορίθμους, λαμβάνοντας υπόψη τα διεθνή πρότυπα, όπως τα NIST SP 800-57 και NIST SP 800-131A.

Ο προσομοιωτής αποτελεί συνέχεια του Cryptographic Inventory Tool που αναπτύχθηκε στο Part 2 και της στρατηγικής μετάβασης που σχεδιάστηκε στο Part 3.

Ο προσομοιωτής βασίζεται στις εξής βασικές λειτουργίες:

1. Ανίχνευση αδύναμων κρυπτογραφικών μηχανισμών μέσω της βάσης δεδομένων του Cryptographic Inventory Tool.
2. Αυτόματη πρόταση ισχυρότερων αλγορίθμων για κάθε ευπαθή μηχανισμό.
3. Δυναμική αντικατάσταση αλγορίθμων σε προσομοιωμένο περιβάλλον, χωρίς να επηρεάζονται οι υπόλοιπες λειτουργίες του συστήματος.
4. Παρακολούθηση συμμόρφωσης με διεθνή κρυπτογραφικά πρότυπα.
5. Στατιστική ανάλυση των αλλαγών και του επιπέδου ασφαλείας μετά την αντικατάσταση.

Bonus

Στο πλαίσιο της εργασίας, υλοποιήσαμε και τις bonus απαιτήσεις που προβλέπονται στην εκφώνηση.

Συγκεκριμένα, επεκτείναμε το εργαλείο σάρωσης ώστε να πραγματοποιεί αναδρομική ανάλυση φακέλων και υποφακέλων (*recursive scanning*), διασφαλίζοντας ότι όλα τα αρχεία ενός συστήματος εξετάζονται για ευπάθειες.

Επιπλέον, ενσωματώσαμε λειτουργίες *case management*, επιτρέποντας στους χρήστες να δημιουργούν, αποθηκεύουν και φορτώνουν διαφορετικές σαρώσεις ως ξεχωριστές περιπτώσεις με δική τους βάση δεδομένων.

Στον τομέα της διαχείρισης βάσεων δεδομένων, προσθέσαμε δυνατότητες εισαγωγής, εξαγωγής και διαγραφής δεδομένων, διασφαλίζοντας ευελιξία και μεταφερσιμότητα των αποτελεσμάτων.

Επίσης έγινε stress test στη βάση δεδομένων.

Τέλος, ενσωματώσαμε οπτικοποιήσεις στατιστικών στοιχείων, προσφέροντας στους χρήστες έναν πιο διαδραστικό τρόπο παρουσίασης των ευρημάτων της σάρωσης.

Συμπέρασμα & Στατιστικά

Το έργο επικεντρώθηκε στην ανάλυση και την αντιμετώπιση ευπαθειών που σχετίζονται με την κρυπτογραφία, με ιδιαίτερη έμφαση στην απειλή που θέτουν οι κβαντικοί υπολογιστές.

Αρχικά, πραγματοποιήθηκε μελέτη των σύγχρονων και παρωχημένων κρυπτογραφικών αλγορίθμων, η οποία αποκάλυψε ότι πολλοί από αυτούς είναι πλέον ευάλωτοι.

Από αυτή την έρευνα προέκυψε η σημασία της κρυπτογραφικής ευελιξίας, δηλαδή της δυνατότητας αλλαγής αλγορίθμων χωρίς μεγάλες τροποποιήσεις στις υποδομές.

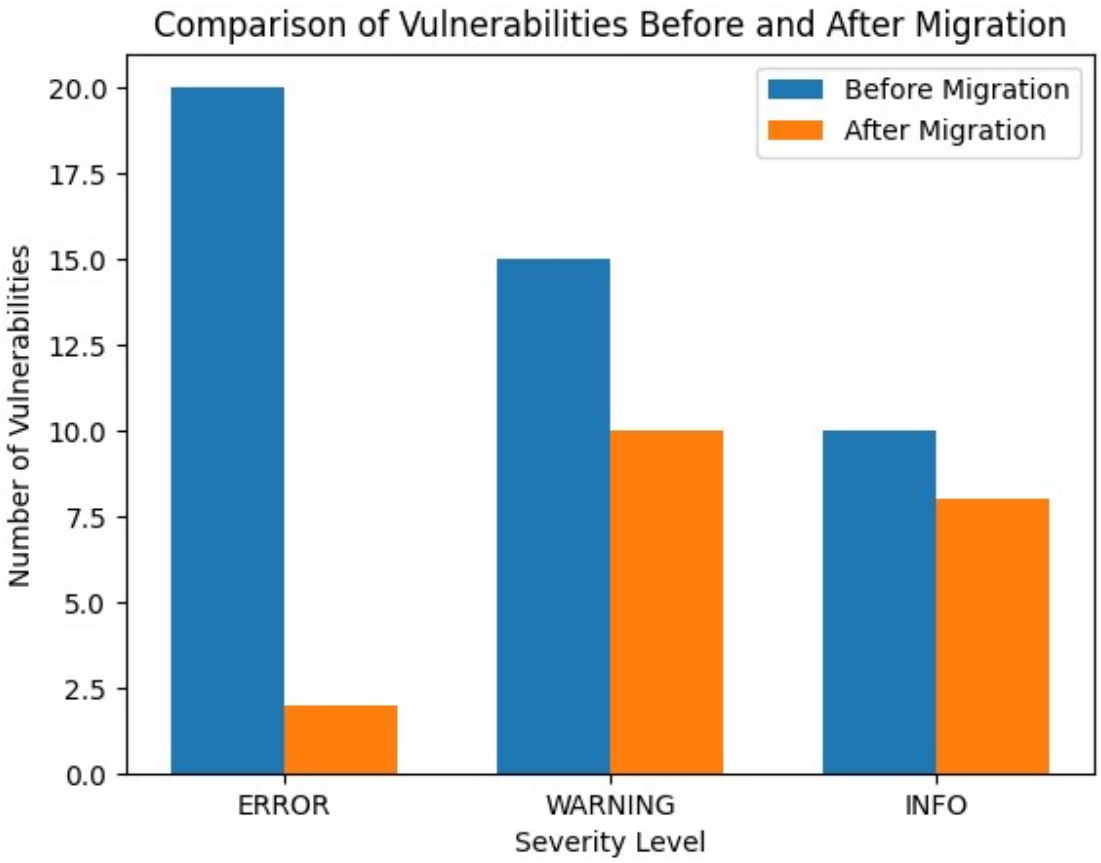
Στη συνέχεια, για την ανίχνευση κρυπτογραφικών αδυναμιών, χρησιμοποιήθηκε το εργαλείο custom parser, το οποίο επέτρεψε την ανίχνευση deprecated αλγορίθμων σε κώδικα Java, Python και C, την κατηγοριοποίηση των ευπαθειών σε ERROR (σοβαρές), WARNING (μέτριας σοβαρότητας) και INFO (μακροπρόθεσμες προτάσεις) και την αξιολόγηση των αποτελεσμάτων, τα οποία έδειξαν ότι όλα τα αρχεία που αναλύθηκαν είχαν τουλάχιστον μία σοβαρή αδυναμία.

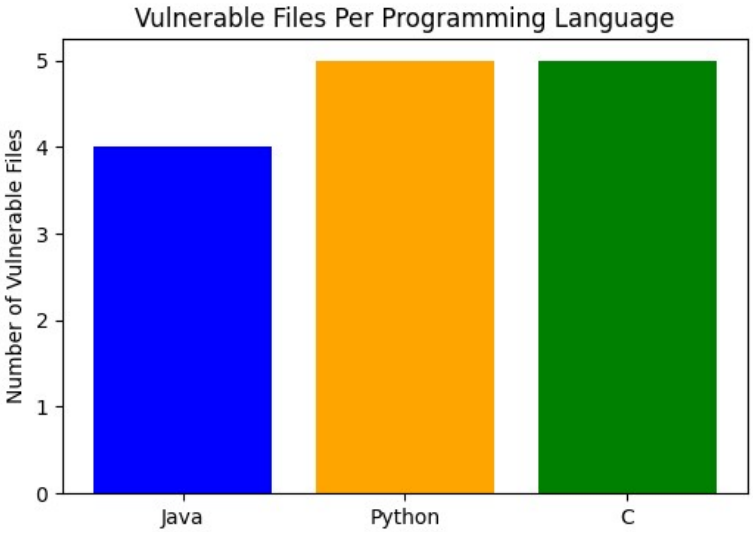
Η χρήση του parser παρείχε μια αυτοματοποιημένη και επαναλαμβανόμενη διαδικασία ανάλυσης κώδικα, προετοιμάζοντας το έδαφος για διορθώσεις.

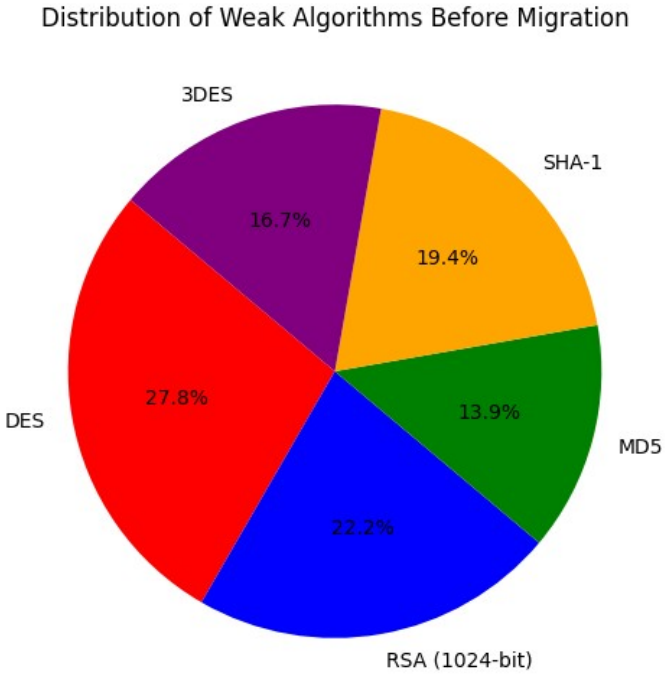
Στη συνέχεια, αναπτύχθηκε ένα δομημένο πλάνο μετάβασης, το οποίο περιλαμβάνει την καταγραφή των υπαρχόντων συστημάτων και κρυπτογραφικών μηχανισμών, την ανίχνευση ευπαθειών με αυτοματοποιημένα εργαλεία, την αντικατάσταση των ξεπερασμένων αλγορίθμων με σύγχρονες επιλογές, όπως AES-GCM αντί για DES και SHA-256 αντί για MD5, καθώς και την ενσωμάτωση Post-Quantum αλγορίθμων, διατηρώντας παράλληλα υβριδικά μοντέλα ασφαλείας.

Ιδιαίτερη έμφαση δόθηκε στις προκλήσεις που αντιμετωπίζουν οι μικρομεσαίες επιχειρήσεις λόγω περιορισμένων πόρων και τεχνογνωσίας, προτείνοντας μια σταδιακή μετάβαση που επιτρέπει τη βελτίωση της ασφάλειας χωρίς να διαταράσσει τη λειτουργία τους.

Συνολικά, το έργο παρείχε μια πρακτική προσέγγιση στη μετάβαση από παραδοσιακά κρυπτογραφικά συστήματα σε πιο ανθεκτικές τεχνολογίες. Η χρήση του custom parser κατέδειξε τη διαδεδομένη παρουσία ευπαθειών, ενώ η ανάλυση των κινδύνων ανέδειξε τη σημασία της προληπτικής ασφάλειας. Οι προτάσεις για Post-Quantum Cryptography θέτουν τις βάσεις για ένα μελλοντικά ασφαλές κρυπτογραφικό περιβάλλον.




Vulnerable Files Per Programming Language
Number of Vulnerable Files
0
1
2
3
4
5
Java
Python
C


Distribution of Weak Algorithms Before Migration
3DES
16.7%
SHA-1
19.4%
DES
27.8%
13.9%
MD5
22.2%
RSA (1024-bit)