PROJECT 458

Άννα Μακρίδου ΑΜ:4934

Αλέξανδρος Φουρτούνης ΑΜ:5031

Γεώργιος Ξηρουδάκης ΑΜ:5067

Παντελεήμων Τσαγκαράκης ΑΜ:5075

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.

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.

Το εργαλείο ανίχνευσε και κατηγοριοποίησε τις ευπάθειες ως εξής:

1. **ERROR** (High Severity)
2. **WARNING** (Medium Severity)
3. **INFO** (Low Severity)

<u>ERROR</u>

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.

WARNING

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.

INFO

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

Τα αποτελέσματα αυτά αποθηκεύονται στη database που φτιάξαμε. Συνολικά, η χρήση του Semgrep 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.

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 εργαλείου Semgrep από το Part 2.
3. Προσδιορισμός του επιπέδου κινδύνου κάθε ευπάθειας (ERROR, WARNING, INFO).
4. Αντικατάσταση ευπαθών αλγορίθμων με σύγχρονες επιλογές

Υλοποίηση της Μετάβασης

<u>Χρήση PQC σε μικρομεσαία επιχείρηση (SME)</u>

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 όπως το Semgrep 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.

Συμπέρασμα

Το έργο PROJECT 458 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. Συγκεκριμένα, οι MD5 και SHA-1 κρίθηκαν μη ασφαλείς λόγω επιθέσεων σύγκρουσης, οι DES και 3DES έχουν αποσυρθεί λόγω χαμηλής αντοχής σε brute-force επιθέσεις, ενώ η ασύμμετρη κρυπτογραφία, όπως οι RSA και ECC, θεωρείται ευάλωτη σε κβαντικές επιθέσεις. Επιπλέον, οι στατικές μέθοδοι Diffie-Hellman δεν παρέχουν Forward Secrecy. 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 Semgrep, 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 Semgrep 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 εργαλείων όπως το Semgrep 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.