ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Βιομετρικά κλειδιά, κρυπτογραφία και υποδομή διανομής

του φοιτητή

Παναγιώτη Ματάμη

Αρ. Μητρώου: 001582

Επιβλέπων καθηγητής

Ηλιούδης Χρήστος

Θεσσαλονίκη 2014

ΠΕΡΙΛΗΨΗ

Η βιομετρία έχει μερικά πλεονεκτήματα σε σχέση με άλλες μεθόδους αυθεντικοποίησης. Η αποθήκευση και η μετάδοση βιομετρικών δεδομένων αποτελεί όμως μεγάλο πρόβλημα, διότι τα βιομετρικά δεδομένα αν παραβιαστούν δεν μπορούν να αλλάξουν όπως συμβαίνει με τους κωδικούς. Αυτή η ανάγκη ώθησε στο να δημιουργηθούν τεχνολογίες οι οποίες μετασχηματίζουν ή κωδικοποιούν τα βιομετρικά χαρακτηριστικά και επιτρέπουν την ταύτιση τους χωρίς να χρειάζεται να επανέλθουν πρώτα στην αρχική τους κατάσταση. Σε περίπτωση παραβίασης, η αλλαγή της κωδικοποίησης, δίνει την δυνατότητα ανάκλησης και επανέκδοσης. Τεχνολογίες προστασίας βιομετρικών χαρακτηριστικών, που ανήκουν στην κατηγορία των λεγόμενων βιομετρικών κρυπτοσυστημάτων, έπειτα από επιτυχή ταύτιση απελευθερώνουν ένα κλειδί, μία πράξη η οποία είναι χρήσιμη σε πολλά κρυπτογραφικά πρωτόκολλα. Η υποστήριξη συναλλαγών με βιομετρία είναι επιθυμητή, καθώς ενισχύεται η μη-αποποίηση αλλά και η ευχρηστία παράλληλα. Στην πτυχιακή αυτή εργασία παρουσιάζεται ένα βιομετρικό κρυπτοσύστημα γνωστό ως bipartite biotoken, το οποίο υποστηρίζει επανέκδοση και απελευθέρωση κλειδιών-δεδομένων ανά συναλλαγή, με μεγάλη ασφάλεια, χωρίς μάλιστα να υπάρχει απώλεια στην απόδοση αναγνώρισης. Η τεχνολογία αυτή χρησιμοποιείται για να επιλύσει ορισμένα υπαρκτά προβλήματα στις υποδομές δημόσιου κλειδιού (PKI), όπως είναι οι επιθέσεις ενδιάμεσου ατόμου και οι επιθέσεις αλίευσης. Γίνεται μία αναλυτική περιγραφή αυτής της νέας υποδομής βιοκρυπτογραφικού κλειδιού (BKI), συμπεριλαμβάνοντας λεπτομέρειες για την σύνθεση της υποδομής και τις διαδικασίες της εγγραφής, αυθεντικοποίησης και ανάκλησης.

ABSTRACT

The use of biometrics has some advantages compared to other methods of authentication. The storage and transmission of unprotected biometric information is a big concern, because in case of compromise, biometric data cannot be changed, in contrast to passwords. As a consequence, technologies for the protection of biometric information appeared, which transform or encode the biometric characteristics in such a way that supports matching in encoded space. In case of exposure, an alteration of the transformation parameters or the encoding, allows for revocation. Biometric template technologies, which belong to the biometric cryptosystem category, support key-release after successful matching, which is very useful in various cryptographic protocols. The support of biometric transactions is something positive, as it improves non-repudiation, together with ease of use. A secure biometric template protection technology by the name bipartite biotoken is presented, which supports revocation and re-issue if needed and transactional key-release after successful matching. All of this without sacrificing matching accuracy, with evidence even suggesting the opposite. This technology is applied, in order to solve some known problems in PKIs, such as man in the middle attacks and phising attempts. A detailed explanation of this new Biocryptographic Key Infrastructure is provided, including composition, enrollment, authentication and revocation details.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τους γονείς μου για την απέραντη υπομονή που δείχνουν όλα αυτά τα χρόνια.

Θα ήθελα επίσης να ευχαριστήσω τον καθηγητή Χρήστο Ηλιούδη, διότι έδωσε λύσεις σε ότι προβλήματα προέκυψαν και το θέμα που επέλεξε, με ώθησε στο να γνωρίσω την επιστήμη της βιομετρικής αναγνώρισης και να αγαπήσω τον χώρο της κρυπτογραφίας.

Κατάλογος περιεχομένων

Ευρετήριο πινάκων

Ευρετήριο σχημάτων

ΕΙΣΑΓΩΓΗ

Σκοπός αυτής της πτυχιακής εργασίας είναι η μελέτη μίας υποδομής βιομετρικών κλειδιών, η οποία αποτελεί μία βελτιωμένη έκδοση της υποδομής δημόσιου κλειδιού (PKI). Προσθέτοντας βιομετρία και κάνοντας χρήση μίας τεχνολογίας προστασίας βιομετρικών προτύπων, βελτιώνεται η μη-αποποίηση και επιτυγχάνεται μεγαλύτερη προστασία από επιθέσεις ενδιάμεσου ατόμου και απόπειρες αλίευσης κωδικών. Η υποδομή βιομετρικών κλειδιών μπορεί να χειρίζεται όχι μόνο την διαχείριση δημόσιων κλειδιών, αλλά και την διαχείριση δημόσιων biotoken.

Η εργασία αυτή αποτελείται από τέσσερα κεφάλαια. Στο πρώτο κεφάλαιο παρουσιάζονται, οι διαφορές της χρήσης βιομετρικών στοιχείων για αυθεντικοποίηση, σε σχέση με άλλους τρόπους όπως οι κωδικοί για παράδειγμα. Έπειτα γίνεται μία εισαγωγή στα βιομετρικά συστήματα αναγνώρισης, αναφέρονται τα βασικά μέρη από τα οποία αποτελείται ένα τέτοιο σύστημα, τι ρόλο εξυπηρετεί το κάθε μέρος, ποιες λειτουργίες υποστηρίζει, τι είδους λάθη μπορεί να συμβούν και γιατί συμβαίνουν. Επίσης αναφέρονται κάποιοι βασικοί δείκτες απόδοσης. Στη συνέχεια, παρουσιάζονται οι βασικές εφαρμογές της βιομετρίας και το κεφάλαιο ολοκληρώνεται με τα ζητήματα ασφαλείας και ιδιωτικότητας που προκύπτουν από την χρήση βιομετρικών δεδομένων. Στο δεύτερο κεφάλαιο παρουσιάζονται οι διάφορες επιθέσεις που μπορούν να συμβούν σε ένα βιομετρικό σύστημα και στην συνέχεια, αναφέρονται οι βασικές κατηγορίες τεχνολογιών προστασίας προτύπων μαζί με μία σειρά από νέες επιθέσεις στις οποίες είναι ευάλωτες ορισμένες από αυτές. Το κεφάλαιο κλείνει με την παρουσίαση της τεχνολογίας προστασίας προτύπων Fuzzy Vault καθώς από αυτήν έχει δανειστεί ορισμένα στοιχεία η προστασία προτύπων που παρουσιάζεται στο τρίτο κεφάλαιο και ονομάζεται revocable biotoken ή bipartite biotoken όταν είναι στην μορφή όπου έχουν ενσωματωθεί σε αυτό δεδομένα ή κάποιο κλειδί. Στο τέταρτο κεφάλαιο ενσωματώνονται biotokens μέσα σε πιστοποιητικά, με σκοπό την υλοποίηση μίας υποδομής παρόμοιας με αυτή μίας υποδομής δημόσιου κλειδιού (PKI), η οποία ονομάζεται υποδομή βιοκρυπτογραφικού κλειδού (BKI). Αυτή η υποδομή διαχειρίζεται δημόσια κλειδιά και δημόσια biotoken ταυτόχρονα και προσφέρει καλύτερη προστασία από επιθέσεις ενδιάμεσου ατόμου και αλίευσης στοιχείων, παρέχοντας ταυτόχρονα βελτιωμένη μη-αποποίηση.

ΚΕΦΑΛΑΙΟ 1

Πρόβλημα της πιστοποίησης – Ανάπτυξη των βιομετρικών ως μέσον πιστοποίησης

ΕΙΣΑΓΩΓΗ

Οπουδήποτε έχουμε έλεγχο πρόσβασης σε εγκαταστάσεις ή σε πληροφοριακά συστήματα, απαιτείται η παρουσίαση κάποιου τύπου πιστοποιητικού για να μπορέσει να γίνει η αυθεντικοποίηση του χρήστη. Αυθεντικοποίηση ονομάζεται κάθε διαδικασία κατά την οποία επιχειρείται να διαπιστωθεί η ταυτότητα μίας οντότητας, είτε πρόκειται για εξακρίβωση της ταυτότητας ενός ατόμου, είτε για εξακρίβωση της προέλευσης κάποιου αντικειμένου ή δεδομένων. Τα πιστοποιητικά αυτά μπορεί να έχουν διάφορες μορφές. Ένα άτομο μπορεί να αναγνωριστεί σύμφωνα με α)κάτι που γνωρίζει β)κάτι που έχει στην κατοχή του γ)κάποιο μοναδικό χαρακτηριστικό του. Η πρώτη μέθοδος βασίζεται στο γεγονός ότι το άτομο έχει αποκλειστική γνώση κάποιας μυστικής πληροφορίας πχ κωδικό, προσωπικό αριθμό ταυτότητας, ή κάποιο κρυπτογραφικό κλειδί. Η δεύτερη μέθοδος βασίζεται στο γεγονός ότι το άτομο έχει στην αποκλειστική κατοχή του, ένα χειροπιαστό αποδεικτικό στοιχείο, όπως μία αστυνομική ταυτότητα, ένα δίπλωμα οδήγησης, διαβατήριο, κάποιο κλειδί ή κάποια συσκευή πρόσθετου κωδικού ασφαλείας (token) ή άλλη συσκευή, όπως ένα κινητό τηλέφωνο. Η τρίτη μέθοδος καθορίζει την ταυτότητα του ατόμου βάσει κάποιου ανατομικού χαρακτηριστικού του ή κάποιου χαρακτηριστικού στη συμπεριφορά του και είναι γνωστή ως βιομετρική αναγνώριση.

Βιομετρική αναγνώριση ή απλά βιομετρία, ονομάζεται η αναγνώριση ατόμων, με αυτόματο τρόπο, βάσει ανατομικών χαρακτηριστικών και χαρακτηριστικών που έχει η συμπεριφορά τους. Αυτά τα χαρακτηριστικά ονομάζονται βιομετρικά στοιχεία. Στην αγγλική βιβλιογραφία χρησιμοποιούνται περισσότεροι από έναν όροι, όπως, traits, indicators, identifiers, ή modalities.

Μερικά παραδείγματα βιομετρικών στοιχείων είναι το δακτυλικό αποτύπωμα, το αποτύπωμα παλάμης, η ίριδα, το πρόσωπο, η γεωμετρία χεριού, ο βηματισμός, το αυτί, η φωνή, η πληκτρολόγηση, η υπογραφή, το DNA, το θερμογράφημα υπερύθρων (του προσώπου ή του χεριού και των φλεβών του χεριού), η μυρωδιά, ο κερατοειδής κ.α. Τα πιο συνηθισμένα και δημοφιλή είναι το πρόσωπο, τα δακτυλικά αποτυπώματα και η ίριδα.

1.1 Διαφορές μεταξύ βιομετρίας, PIN και κωδικών

Οι διαφορές μεταξύ βιομετρίας και των PIN και κωδικών[28] είναι:

- Τα βιομετρικά στοιχεία μπορούν να αποκτηθούν χωρίς να το ξέρουμε. Κάποιος μπορεί να πάρει την φωτογραφία μας ή να καταγράψει ακόμα και την ίριδα μας από απόσταση με τη βοήθεια τηλεσκόπιου και υπέρυθρων ακτίνων, ή να πάρει το δακτυλικό μας αποτύπωμα από ένα ποτήρι που κρατούσαμε προηγουμένως.
- Τα βιομετρικά δείγματα δεν είναι ακριβώς ίδια κάθε φορά. Τους κωδικούς πρέπει να τους πληκτρολογούμε ακριβώς όπως είναι. Όμως κάθε φορά που λαμβάνεται το βιομετρικό δείγμα ενός ατόμου, είναι ελαφρώς διαφορετικό, ανάλογα με τις συνθήκες απόκτησης, την πάροδο του χρόνου, τον τρόπο που τοποθετήσαμε το βιομετρικό μας στοιχείο κατά την καταγραφή κτλ. Πάντα υπάρχουν μικροδιαφορές, οι οποίες αποκαλούνται ενδοατομικές διαφορές.
- Τα βιομετρικά στοιχεία παραμένουν για πάντα και μπορεί κάποιος να ανατρέξει πίσω στον χρόνο και να δει διαχρονικά τι κάναμε.
- Τα βιομετρικά στοιχεία είναι τα ίδια για όλες τις εφαρμογές. Το ίδιο βιομετρικό στοιχείο μπορεί να χρησιμοποιείται και για έλεγχο πρόσβασης στην δουλειά, αλλά και στο σπίτι ή αλλού. Ενώ με τους κωδικούς πάντα υπάρχει η παρότρυνση να χρησιμοποιούμε διαφορετικούς κωδικούς για κάθε διαφορετική εφαρμογή.
- Τα βιομετρικά στοιχεία δεν μεταδίδονται ούτε μοιράζονται, σε αντίθεση με τους κωδικούς.
- Η βιομετρία επιτρέπει τον εντοπισμό κάποιου μεταξύ πολλών συστημάτων.
- Η βιομετρία απαιτεί ειδικά μηχανήματα.
- Ένα βιομετρικό σύστημα μπορεί να αναγνωρίσει αν κάποιος είναι γνωστός στο σύστημα ή όχι.

Μερικά προβλήματα που σχετίζονται με την χρήση βιομετρίας είναι:

- Η εκτίμηση της μοναδικότητας ενός βιομετρικού στοιχείου, αλλά και της μονιμότητας, κατά πόσο δηλαδή μένουν αναλλοίωτα στο χρόνο ή όχι.

- Η ανίχνευση βιομετρικών στοιχείων σε ένα περιβάλλον χωρίς επίβλεψη και καθοδήγηση (περίπτωση παρακολούθησης, πχ δημόσιες κάμερες)
- Η ύπαρξη διαφόρων ζητημάτων ασφαλείας και ιδιωτικότητας
    - Ανάγκη προστασίας των βιομετρικών προτύπων (οι πληροφορίες που αποθηκεύονται τελικά και αναπαριστούν το βιομετρικό στοιχείο)
    - Ανάγκη ανεύρεσης αποτελεσματικών μεθόδων αναγνώρισης ψεύτικων βιομετρικών στοιχείων, αντίγραφα βιομετρικών στοιχείων (πχ δακτυλικά αποτυπώματα κατασκευασμένα από λάτεξ) ή προσπάθειες απομίμησης
- Προβλήματα στην αξιολόγηση των βιομετρικών συστημάτων.

1.2 Καταλληλότητα Βιομετρικών στοιχείων

Κάθε βιομετρικό στοιχείο (trait) έχει πλεονεκτήματα και μειονεκτήματα και έτσι η επιλογή ενός βιομετρικού στοιχείου (trait) για μία συγκεκριμένη εφαρμογή δεν εξαρτάται μόνο από την απόδοση αναγνώρισης. Σε γενικές γραμμές, επτά παράγοντες πρέπει να ληφθούν υπόψιν για να καθοριστεί η καταλληλότητα ενός ανατομικού χαρακτηριστικού ή μιας χαρακτηριστικής συμπεριφοράς που θα χρησιμοποιηθεί σε μία βιομετρική εφαρμογή και αυτοί είναι[11][16]:

1. Καθολικότητα: Κάθε άτομο που έχει πρόσβαση στην εφαρμογή θα πρέπει να είναι κάτοχος του επιλεγμένου βιομετρικού στοιχείου (trait).
2. Μοναδικότητα: Το επιλεγμένο βιομετρικό στοιχείο θα πρέπει να είναι αρκετά διαφορετικό ανάμεσα στα άτομα που αποτελούν μέρος του πληθυσμού των χρηστών.
3. Μονιμότητα: Το βιομετρικό στοιχείο ενός ατόμου θα πρέπει να παραμένει σχετικά αναλλοίωτο για κάποιο εύλογο χρονικό διάστημα ανάλογα με τον αλγόριθμο σύγκρισης.
4. Μετρησιμότητα: Η απόκτηση και ψηφιοποίηση ενός βιομετρικού στοιχείου (trait) πρέπει να μπορεί να γίνει χρησιμοποιώντας κατάλληλες συσκευές που δεν προκαλούν αδικαιολόγητη ενόχληση στο άτομο. Ακόμα, τα αποκτηθέντα ανεπεξέργαστα δεδομένα (raw data) θα πρέπει να επιδέχονται επεξεργασία έτσι ώστε να εξαχθούν διάφορα διακριτά σύνολα χαρακτηριστικών (feature sets).
5. Απόδοση: Εκτός από την ακρίβεια αναγνώρισης, η υπολογιστική δύναμη που απαιτείται για την επίτευξη αυτής της ακρίβειας και η παραγωγικότητα

(ο αριθμός των συναλλαγών που μπορούν να διεκπεραιωθούν ανά μονάδα χρόνου - throughput) του βιομετρικού συστήματος θα πρέπει να καλύπτουν τους περιορισμούς που επιβάλλονται από την εφαρμογή.

6. Αποδοχή: Άτομα που ανήκουν στην πληθυσμιακή ομάδα που θα χρησιμοποιεί την εφαρμογή θα πρέπει να αποδέχονται να παρουσιάσουν το βιομετρικό στοιχείο τους στο σύστημα.

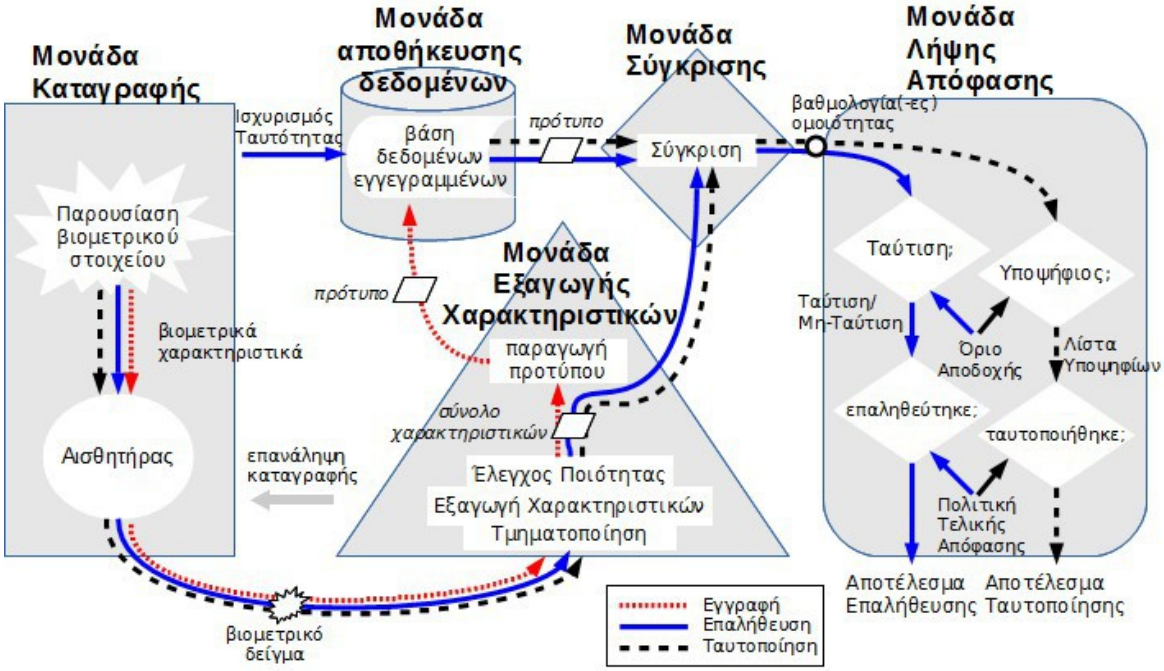
7. Παραποίηση: Αυτό αναφέρεται στην ευκολία με την οποία μπορεί να γίνει αντιγραφή του βιομετρικού στοιχείου (trait) ενός ατόμου (πχ δημιουργία ψεύτικων δακτύλων), στην περίπτωση των ανατομικών χαρακτηριστικών, ή απομίμηση, στην περίπτωση των χαρακτηριστικών συμπεριφοράς. Αναφέρεται επίσης στην περίπτωση, όπου ο χρήστης εσκεμμένα τροποποιεί το βιομετρικό στοιχείο του για να αποφύγει την αναγνώριση.

Κανένα βιομετρικό στοιχείο δεν αναμένεται να πληροί όλες τις απαιτήσεις (πχ ακρίβεια, ευχρηστία, ταχύτητα, κόστος) που απαιτούνται από όλες τις εφαρμογές (πχ σώματα ασφαλείας, έλεγχος πρόσβασης, κυβερνητικά κοινωνικά προγράμματα κτλ). Με άλλα λόγια, κανένα βιομετρικό στοιχείο δεν είναι ιδανικό αλλά ένας αριθμός από αυτά είναι αποδεκτά. Η καταλληλότητα ενός βιομετρικού στοιχείου για μία εφαρμογή εξαρτάται από τη φύση και τις απαιτήσεις της εφαρμογής και τις ιδιότητες του βιομετρικού στοιχείου. Πολλές αντιλήψεις που υπήρχαν στο παρελθόν έχουν πάψει να ισχύουν. Έχει αποδειχτεί ότι υπάρχουν δακτυλικά αποτυπώματα που μοιάζουν τόσο πολύ μεταξύ τους που θα μπορούσαν να μπερδέψουν ακόμα και το καλύτερο σύστημα αναγνώρισης ή τον καλύτερο ειδικό πάνω στα δακτυλικά αποτυπώματα. Χαρακτηριστικό παράδειγμα είναι η περίπτωση του Brandon Mayfield [9], που κρατήθηκε για δύο βδομάδες σαν ύποπτος για συμμετοχή στις βομβιστικές επιθέσεις στην Μαδρίτη. Πλέον μιλάμε για μοναδικότητα ανά πληθυσμό και για ακρίβεια ανά αριθμό χρηστών. Υπάρχουν όρια στο πόσο μπορεί να επεκταθεί ένα βιομετρικό σύστημα που κάνει χρήση κάποιου βιομετρικού στοιχείου. Πολλές φορές για να πετύχουμε την επιθυμητή ακρίβεια θα πρέπει να χρησιμοποιηθούν δύο ή περισσότερα διαφορετικά βιομετρικά στοιχεία (συστήματα πολυτροπικά, multi-modality), διότι η μοναδικότητα του ενός μόνο δεν αρκεί.

1.3 Βιομετρικό σύστημα

Ένα βιομετρικό σύστημα καταγράφει πληροφορίες από ένα ή περισσότερα ανατομικά χαρακτηριστικά ή χαρακτηριστικά στη συμπεριφορά ενός ατόμου, για να καθορίσει ή να επαληθεύσει την ταυτότητα του. Η αναγνώριση ενός χρήστη γίνεται έπειτα από μία διαδικασία αποτελούμενη από δύο βασικές φάσεις: την εγγραφή

και την αναγνώριση. Κατά την φάση της εγγραφής (enrollment), αποκτώνται τα βιομετρικά δεδομένα του χρήστη και αποθηκεύονται σε μία βάση δεδομένων μαζί με την ταυτότητα του χρήστη. Συνήθως, τα αποκτηθέντα βιομετρικά δεδομένα υφίστανται κάποια επεξεργασία και εξάγονται κάποια ιδιαίτερα και μοναδικά χαρακτηριστικά. Σε πολλές περιπτώσεις, μόνο αυτά τα χαρακτηριστικά που εξάγονται αποθηκεύονται, ενώ τα αρχικά ανεπεξέργαστα (raw) δεδομένα διαγράφονται. Κατά την φάση της αναγνώρισης, τα βιομετρικά δεδομένα αποκτώνται ξανά από το άτομο και συγκρίνονται με τα αποθηκευμένα δεδομένα για να καθοριστεί η ταυτότητα του χρήστη. Στην ουσία ένα βιομετρικό σύστημα είναι ένα σύστημα αναγνώρισης προτύπων που αποτελείται από τέσσερις βασικές μονάδες στις οποίες γίνονται α)η καταγραφή, β)η εξαγωγή χαρακτηριστικών γ)η αποθήκευση και δ)η σύγκριση.



Σχήμα 1: Περιγραφή των μονάδων ενός βιομετρικού συστήματος όπως και των λειτουργιών της εγγραφής, επαλήθευσης και ταυτοποίησης.

1.3.1 Καταγραφή

Η καταγραφή των βιομετρικών στοιχείων γίνεται από έναν αισθητήρα. Η ποιότητα των αρχικών ανεπεξέργαστων (raw) βιομετρικών δειγμάτων εξαρτάται από τα χαρακτηριστικά του αισθητήρα που χρησιμοποιείται. Για τα περισσότερα βιομετρικά στοιχεία (modalities), τα ανεπεξέργαστα βιομετρικά δεδομένα είναι στην

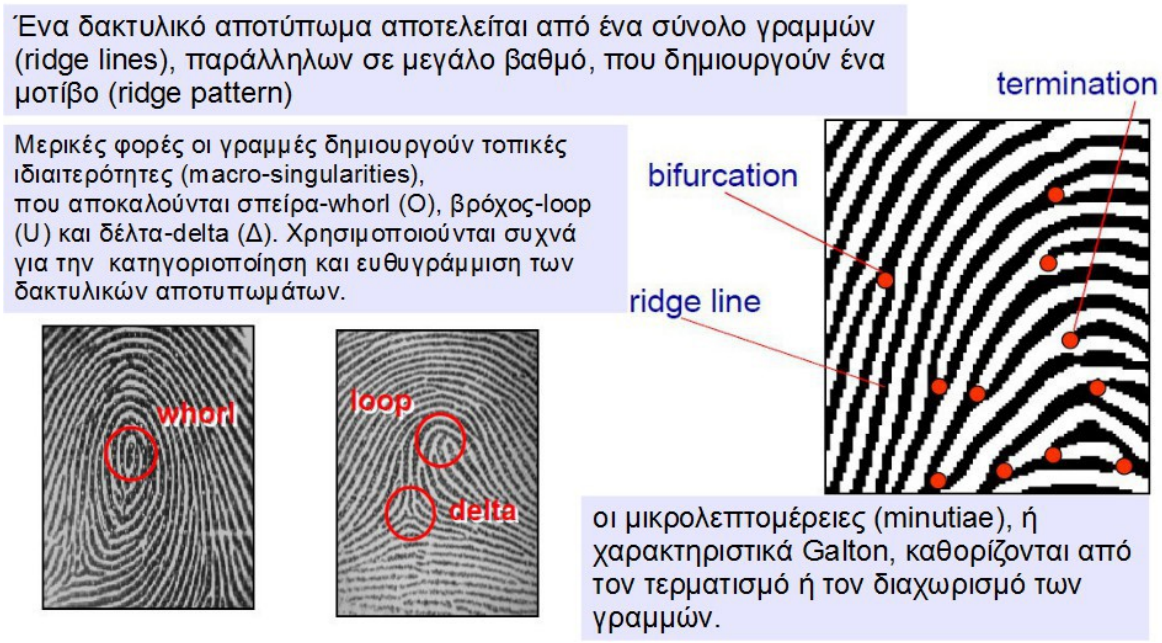
μορφή δισδιάστατων εικόνων (πχ δακτυλικά αποτυπώματα, πρόσωπο, ίριδα κτλ). Εξαιρέσεις αποτελούν η φωνή (μονοδιάστατα σήματα έντασης), online υπογραφή (πίεση στυλό, θέση και ταχύτητα), μυρωδιά και DNA (χημική ανάλυση). Για δεδομένα που βασίζονται σε εικόνες, παράγοντες όπως το μέγεθος της περιοχής σάρωσης, η ανάλυση, ο ρυθμός καρέ και η ευαισθησία της κάμερας παίζουν σημαντικό ρόλο στον καθορισμό της ποιότητας της εικόνας. Ακόμα, παράγοντες όπως το κόστος, το μέγεθος, η ανθεκτικότητα (αν θα είναι εσωτερικού ή εξωτερικού χώρου) και η ικανότητα ανίχνευσης ψεύτικων ομοιωμάτων, παίζουν σημαντικό ρόλο στην επιλογή ή στον σχεδιασμό ενός αισθητήρα.

1.3.2 Εξαγωγή χαρακτηριστικών (Feature extraction module)

Συνήθως, τα ανεπεξέργαστα βιομετρικά δεδομένα από τον αισθητήρα, υπόκεινται σε διάφορους χειρισμούς πριν από την εξαγωγή των χαρακτηριστικών από αυτά. Τα τρία συνηθέστερα βήματα που χρησιμοποιούνται πριν την επεξεργασία είναι: α)εκτίμηση ποιότητας β)τμηματοποίηση και γ)βελτιστοποίηση. Πρώτα, η ποιότητα των αποκτηθέντων βιομετρικών δειγμάτων πρέπει να αξιολογηθεί για να καθοριστεί αν είναι κατάλληλα για περαιτέρω επεξεργασία. Αν τα ανεπεξέργαστα βιομετρικά δεδομένα δεν είναι αποδεκτής ποιότητας, υπάρχουν δύο επιλογές. Κάποιος μπορεί είτε να επιχειρήσει να επαναλάβει την απόκτηση των δεδομένων από τον χρήστη ή να ενεργοποιήσει κάποια εξαίρεση (ειδοποίηση αποτυχίας) ενημερώνοντας τον διαχειριστή του συστήματος έτσι ώστε να ενεργοποιήσει εναλλακτικές διαδικασίες (συνήθως περιέχουν κάποια μορφή χειροκίνητης παρέμβασης από τον χειριστή του συστήματος). Το επόμενο βήμα προ-επεξεργασίας είναι γνωστό ως τμηματοποίηση (segmentation), όπου στόχος είναι να διαχωριστούν τα απαιτούμενα βιομετρικά δεδομένα από τον θόρυβο του φόντου (background noise). Ο εντοπισμός ενός προσώπου σε μία γεμάτη εικόνα είναι ένα καλό παράδειγμα τμηματοποίησης. Τέλος τα τμηματοποιημένα βιομετρικά δεδομένα περνούν από έναν αλγόριθμο βελτιστοποίησης ποιότητας σήματος για να βελτιωθεί η ποιότητα και να μειωθεί περαιτέρω ο θόρυβος. Στην περίπτωση δεδομένων σε μορφή εικόνας, αλγόριθμοι βελτιστοποίησης όπως smoothing ή histogram equalization μπορούν να εφαρμοστούν για να ελαττωθεί ο θόρυβος που εισάγεται από την κάμερα ή εξαιτίας του φωτισμού. Σε μερικές περιπτώσεις, τα προηγούμενα βήματα προ-επεξεργασίας μπορεί να είναι ενσωματωμένα στο βήμα εξαγωγής χαρακτηριστικών. Για παράδειγμα, η αποτίμηση της ποιότητας μπορεί να συνεπάγεται την εξαίρεση μερικών χαρακτηριστικών από τα αποκτηθέντα βιομετρικά δεδομένα.

Η εξαγωγή χαρακτηριστικών αναφέρεται στην διαδικασία παραγωγής μίας συμπαγούς αλλά εκφραστικής αναπαράστασης του επιλεγμένου βιομετρικού

στοιχείου (biometric trait), που ονομάζεται πρότυπο (template). Η εξαγωγή χαρακτηριστικών έχει σαν αποτέλεσμα ένα σύνολο χαρακτηριστικών (feature set) και από τον συνδυασμό ενός ή περισσότερων τέτοιων συνόλων χαρακτηριστικών, προκύπτει το πρότυπο (ορισμένες φορές κατά την εγγραφή απαιτείται από τον χρήστη να παρουσιάσει πολλαπλές φορές το βιομετρικό του στοιχείο για την δημιουργία του πρότυπου και επιλέγεται το καλύτερο σύνολο χαρακτηριστικών ή γίνεται ένας συνδυασμός τους). Το πρότυπο πρέπει να περιέχει μόνο τις σημαντικότερες διακριτές πληροφορίες που είναι απαραίτητες για την αναγνώριση του ατόμου. Για παράδειγμα, πιστεύεται ότι η θέση και η φορά των μικρολεπτομερειών - minutia points (περιοχές όπου οι κορυφογραμμές σε ένα δακτυλικό αποτύπωμα παρουσιάζουν κάποια ιδιομορφία, πχ σημεία όπου ξεκινάει ή τερματίζει μία γραμμή και σημεία διακλάδωσης) είναι μοναδικά για κάθε δάχτυλο. Έτσι, η ανίχνευση των μικρολεπτομερειών (minutia points) σε μία εικόνα ενός δακτυλικού αποτυπώματος αποτελεί βασικό βήμα της εξαγωγής χαρακτηριστικών στα περισσότερα βιομετρικά συστήματα που βασίζονται σε δακτυλικά αποτυπώματα.



Σχήμα 2: Μικρολεπτομέρειες (minutiae) και ιδιαιτερότητες σε ένα δακτυλικό αποτύπωμα.

Κατά την εγγραφή, το πρότυπο (template) αποθηκεύεται ανάλογα με την εφαρμογή, είτε σε μία κεντρική βάση δεδομένων του βιομετρικού συστήματος ή καταγράφεται σε ένα token (πχ smart card) που εκδίδεται για το εγγεγραμμένο άτομο.

Στην φάση της αναγνώρισης, το πρότυπο (template) ανασύρεται από την βάση δεδομένων, και συγκρίνεται με το σύνολο χαρακτηριστικών που προέκυψαν από το νέο βιομετρικό δείγμα που αποκτήθηκε από τον χρήστη. Αυτό το νέο σύνολο χαρακτηριστικών που αποκτήθηκε κατά την διάρκεια της φάσης αναγνώρισης συνήθως αποκαλείται δείγμα (query ή input στα αγγλικά). Σε πολλά βιομετρικά συστήματα που βασίζονται σε εικόνες (πχ πρόσωπο ή δακτυλικό αποτύπωμα), κατά την εγγραφή, οι αρχικές ανεπεξέργαστες βιομετρικές εικόνες μπορεί να αποθηκευθούν και αυτές στη βάση δεδομένων μαζί με τα πρότυπα (templates). Αυτές οι εικόνες είναι συχνά γνωστές ως εικόνες gallery ή εικόνες αναφοράς ή αποθηκευμένες εικόνες ή εικόνες εγγραφής (gallery images, reference images, stored images, ή enrollment images). Οι εικόνες που λαμβάνονται κατά την αναγνώριση είναι γνωστές ως εικόνες δείγματος (στα αγγλικά αποκαλούνται probe images, query images, ή input images). Στην βιβλιογραφία, η δημιουργία του προτύπου ορισμένες φορές εμφανίζεται ως ξεχωριστή μονάδα, ενώ άλλες ως μέρος της εξαγωγής χαρακτηριστικών.

1.3.3 Βάση Δεδομένων (Database module)

Η βάση δεδομένων ενός βιομετρικού συστήματος λειτουργεί σαν μία αποθήκη βιομετρικών πληροφοριών. Το σύνολο από πρότυπα που δημιουργήθηκαν κατά την διαδικασία της εγγραφής, αποθηκεύονται στην βάση δεδομένων μαζί με κάποιες προσωπικές πληροφορίες σχετικά με την ταυτότητα του χρήστη (όπως όνομα, PIN, διεύθυνση κτλ), καθώς και πληροφορίες που τον χαρακτηρίζουν. Ένα βιομετρικό σύστημα μπορεί να χρησιμοποιεί μία κεντρική βάση δεδομένων ή κάποια αποκεντρωμένη (decentralized). Η αποθήκευση όλων των προτύπων (templates) σε μία κεντρική βάση δεδομένων μπορεί να είναι ευεργετική από άποψη ασφαλείας του συστήματος, διότι τα δεδομένα μπορούν να προστατευτούν με φυσική απομόνωση και μηχανισμούς ελέγχου πρόσβασης. Από την άλλη, μία παραβίαση της κεντρικής βάσης δεδομένων θα είχε μεγαλύτερες επιπτώσεις απ' ό,τι η παραβίαση σε κάποιο από τα μέρη της αποκεντρωμένης βάσης δεδομένων. Αυτό γιατί κακόβουλα άτομα (διεφθαρμένοι διαχειριστές ή χάκερ) μπορούν να κάνουν ανεπιθύμητη χρήση των βιομετρικών πληροφοριών που είναι αποθηκευμένες στην βάση δεδομένων και να παραβιάσουν την ιδιωτικότητα αθώων χρηστών.

1.3.4 Σύγκριση (Matching module)

Ο σκοπός ενός βιομετρικού συγκριτή είναι να συγκρίνει τα χαρακτηριστικά του δείγματος (query) με τα αποθηκευμένα πρότυπα (templates) και να παράγει μία βαθμολογία ομοιότητας (match score). Η βαθμολογία ομοιότητας δείχνει πόσο ταυτίζονται μεταξύ τους το πρότυπο και το δείγμα (query). Έτσι, μεγαλύτερη

βαθμολογία σημαίνει μεγαλύτερη ομοιότητα μεταξύ του πρότυπου και του δείγματος (query). Αν ένας συγκριτής μετράει την διαφορετικότητα (αντί για την ομοιότητα) μεταξύ των δύο συνόλων χαρακτηριστικών, η βαθμολογία αναφέρεται ως βαθμολογία απόκλισης. Μικρότερη βαθμολογία απόκλισης σημαίνει μεγαλύτερη ομοιότητα. Σε βιομετρικά συστήματα βασισμένα σε δαχτυλικά αποτυπώματα, ο αριθμός των όμοιων μικρολεπτομερειών (minutiae) μεταξύ του συνόλου χαρακτηριστικών της εισόδου και του πρότυπου (template) μπορεί να θεωρηθεί σαν δείκτης ομοιότητας. Η βαθμολογία ομοιότητας μπορεί να αναθεωρηθεί (moderated) ανάλογα με την ποιότητα των βιομετρικών δεδομένων που παρουσιάστηκαν. Το κομμάτι του συγκριτή μπορεί ακόμη να εμπεριέχει κάποιον μηχανισμό λήψης αποφάσεων, ο οποίος ανάλογα με τη βαθμολογία ομοιότητας, είτε να επικυρώνει κάποια επίκληση ταυτότητας, είτε να παρέχει μία λίστα εγγεγραμμένων χρηστών, ταξινομημένη σύμφωνα με τη βαθμολογία ομοιότητας ως προς τα χαρακτηριστικά του δείγματος, προκειμένου να ταυτοποιήσει ένα άτομο. Ο μηχανισμός λήψης αποφάσεων μπορεί λοιπόν να εμφανίζεται στην βιβλιογραφία ως ξεχωριστή μονάδα, ενώ άλλοτε να θεωρείται ως μέρος της μονάδας σύγκρισης.

1.4 Λειτουργίες Βιομετρίας (Biometric functionalities)

Ένα βιομετρικό σύστημα μπορεί να παρέχει δύο ειδών λειτουργίες: επαλήθευση και ταυτοποίηση. Ο όρος αναγνώριση χρησιμοποιείται όταν δεν θέλουμε να κάνουμε κάποιον διαχωρισμό μεταξύ της επαλήθευσης και της ταυτοποίησης. Επίσης ο όρος αυθεντικοποίηση συνήθως χρησιμοποιείται σαν συνώνυμο της επαλήθευσης.

1.4.1 Επαλήθευση (Verification) (σύγκριση 1 προς 1)

Στην επαλήθευση, ο χρήστης επικαλείται μία ταυτότητα και το σύστημα επαληθεύει αυτό τον ισχυρισμό. Σε αυτό το σενάριο, λαμβάνεται μέσω ενός αισθητήρα ένα δείγμα (query) και έπειτα περνάει από τον εξαγωγέα χαρακτηριστικών και δημιουργείται ένα σύνολο χαρακτηριστικών το οποίο συγκρίνεται στη συνέχεια μόνο με το πρότυπο (template) που αντιστοιχεί στην ταυτότητα που ισχυρίζεται ο χρήστης (σύγκριση ένα προς ένα). Ο ισχυρισμός της ταυτότητας συνήθως γίνεται μέσω ενός PIN, ή του ονόματος χρήστη, ή ενός token (πχ smart card). Αν το δείγμα (input) του χρήστη και το πρότυπο της ταυτότητας που επικαλείτται έχουν μεγάλο βαθμό ομοιότητας, τότε ο ισχυρισμός γίνεται δεκτός. Αλλιώς, ο ισχυρισμός απορρίπτεται. Η επαλήθευση χρησιμοποιείται συνήθως σε εφαρμογές όπου σκοπός είναι να αποτραπεί η χρήση υπηρεσιών από μη εξουσιοδοτημένα άτομα.

1.4.2 Ταυτοποίηση (Identification)(σύγκριση ένα προς πολλά)

Η λειτουργία της ταυτοποίησης μπορεί να χωριστεί περαιτέρω σε θετική και αρνητική ταυτοποίηση. Στην θετική ταυτοποίηση, ο χρήστης προσπαθεί να ταυτοποιηθεί θετικά από το σύστημα, χωρίς να δηλώσει κάποια ταυτότητα και το σύστημα καθορίζει την ταυτότητα του χρήστη μέσα από ένα γνωστό σύνολο από ταυτότητες. Αντίθετα, σε μία εφαρμογή αρνητικής ταυτοποίησης, ένας χρήστης θεωρείται ότι αποκρύπτει την πραγματική του ταυτότητα (είτε άμεσα είτε έμμεσα) από το σύστημα. Η αρνητική ταυτοποίηση είναι επίσης γνωστή σαν προληπτικός έλεγχος (screening).

Σκοπός της αρνητικής ταυτοποίησης είναι να αποτρέψει την χρήση πολλαπλών ταυτοτήτων από ένα άτομο. Έτσι, προληπτικός έλεγχος (screening) μπορεί να χρησιμοποιηθεί για να αποτραπεί το φαινόμενο των πολλαπλών εγγράφων πιστοποίησης (πχ δίπλωμα οδήγησης, διαβατήριο) που έχουν εκδοθεί για το ίδιο άτομο ή για να αποτρέψουν κάποιο άτομο από το να διεκδικεί πολλαπλά οφέλη με την χρήση διαφορετικών ονομάτων (ένα πρόβλημα που συναντάται συχνά σε προγράμματα κοινωνικής πρόνοιας). Προληπτικός έλεγχος (screening) χρησιμοποιείται συχνά στα αεροδρόμια για να επαληθεύσουν αν η ταυτότητα κάποιου επιβάτη ταιριάζει με κάποιο άτομο στην λίστα παρακολούθησης.

Στην θετική αλλά και στην αρνητική ταυτοποίηση, το βιομετρικό δείγμα (input) του χρήστη συγκρίνεται με τα πρότυπα (templates) όλων των εγγεγραμμένων ατόμων στην βάση δεδομένων. Στη συνέχεια το σύστημα εξάγει είτε την ταυτότητα χρήστη του οποίου το πρότυπο (template) έχει τον υψηλότερο βαθμό ομοιότητας με το δείγμα (input) (η έξοδος εμφανίζεται ως μία λίστα υποψηφίων η οποία μπορεί να περιέχει μία ή περισσότερες ταυτότητες), είτε εξάγει μία απόφαση που υποδεικνύει ότι ο χρήστης που αντιστοιχεί στο δείγμα (input) αυτό δεν είναι κάποιος ήδη εγγεγραμμένος στο σύστημα (η έξοδος αποτελείται από μία κενή λίστα υποψηφίων).

Αν το σύστημα έχει τη δυνατότητα να επιστρέφει σαν αποτέλεσμα ότι ο χρήστης που παρουσίασε το δακτυλικό του αποτύπωμα δεν είναι ανάμεσα στους N εγγεγραμμένους χρήστες, (η βαθμολογία ομοιότητας δεν είναι πάνω από το κατώτερο όριο που έχει οριστεί), τότε λέμε ότι έχουμε ταυτοποίηση ανοιχτού συνόλου (open set). Όταν όμως έχει οριστεί αναγκαστικά το σύστημα να επιστρέφει μία από τις N εγγεγραμμένες ταυτότητες, άσχετα από την τιμή της βαθμολογίας ομοιότητας, μιλάμε για ταυτοποίηση κλειστού συνόλου (closed set).

Σε μερικά χρήσιμα βιομετρικά συστήματα ταυτοποίησης (πχ σύγκριση λανθανόντων δακτυλικών αποτυπωμάτων), η ταυτοποίηση είναι ημι-αυτόματη.

Ένα ημι-αυτόματο βιομετρικό σύστημα εμφανίζει σαν αποτέλεσμα τις ταυτότητες των καλύτερων ταυτίσεων t (1<t<<N) και εν συνεχεία κάποιος άνθρωπος ειδικός αποφασίζει για το ποια είναι η ταυτότητα που ταιριάζει καλύτερα στο συγκεκριμένο δείγμα (query). Η τιμή του t θα μπορούσε να καθοριστεί ανάλογα με την διαθεσιμότητα και την ικανότητα του ειδικού προσωπικού. Μία άλλη προσέγγιση είναι να επιστρέφει το βιομετρικό σύστημα όλες τις ταυτότητες που η βαθμολογία ομοιότητας τους υπερέχει μιας προκαθορισμένης τιμής (η). Καθώς ο αριθμός των εγγεγραμμένων χρηστών στη βάση δεδομένων μπορεί να είναι πολύ μεγάλος, το έργο της ταυτοποίησης είναι σημαντικά πιο απαιτητικό από την επαλήθευση.

1.5 Λάθη Βιομετρικού Συστήματος

Ένα ιδανικό βιομετρικό σύστημα, θα έπρεπε να καταγράφει το βιομετρικό στοιχείο ενός ατόμου, και βάσει αυτού να παίρνει πάντα την σωστή απόφαση. Στην πράξη, ένα βιομετρικό σύστημα είναι ένα σύστημα αναγνώρισης προτύπων (pattern recognition) που αναπόφευκτα παίρνει κάποιες λάθος αποφάσεις. Η επιστήμη της βιομετρικής αναγνώρισης βασίζεται πάνω στην μοναδικότητα και μονιμότητα (uniqueness και permanence) του εκάστοτε βιομετρικού στοιχείου. Όμως αυτές οι αξίες σπάνια αληθεύουν σε πραγματικά βιομετρικά συστήματα.

Στην πράξη, αποδεικνύεται ότι το ανατομικό χαρακτηριστικό το ίδιο μπορεί να μην είναι μοναδικό ή η ψηφιακή αναπαράσταση του να μην αποτυπώνει όλες τις πληροφορίες σχετικά με αυτό, καθιστώντας το στην πράξη μη μοναδικό. Τις τελευταίες δύο δεκαετίες, οι ισχυρισμοί ότι τα δακτυλικά αποτυπώματα είναι μοναδικά έχουν αμφισβητηθεί από την επιστημονική κοινότητα αλλά και από τη δικαστική. Το ίδιο συμβαίνει και με άλλα βιομετρικά στοιχεία, όπου δεν έχει αποδειχθεί ξεκάθαρα η μοναδικότητα τους.

Η γενετική ομοιότητα μεταξύ συγγενών (πχ δίδυμα, πατέρας και γιος) μπορεί να συνεισφέρει στην έλλειψη μοναδικότητας κάποιων βιομετρικών στοιχείων. Για παράδειγμα τα πρόσωπα των διδύμων είναι σχεδόν ίδια. Τροπικότητες (αναγνώριση βάσει κάποιου βιομετρικού στοιχείου - modalities) όπως το DNA, όπου η γενετική δομή ενός ατόμου καθορίζει σε μεγάλο βαθμό τα βιομετρικά χαρακτηριστικά του, αναφέρονται ως γονοτυπικοί παράγοντες (genotypic factors/features). Ενώ, οι τροπικότητες (modalities) όπου τα χαρακτηριστικά καθορίζονται από άλλες πηγές που είναι τυχαίες από την φύση τους (πχ δακτυλικά αποτυπώματα) αναφέρονται ως φαινοτυπικοί παράγοντες (phenotypic factors/features).

Ακόμα, η αντίληψη ότι τα βιομετρικά στοιχεία είναι μόνιμα, δεν είναι και αυτή επιστημονικά επιβεβαιωμένη. Οι επιδράσεις της σωματικής ανάπτυξης (κυρίως κατά την παιδική ηλικία και την εφηβεία) σε συνηθισμένα βιομετρικά αναγνωριστικά όπως το πρόσωπο, το δακτυλικό αποτύπωμα ή η ίριδα, δεν έχουν μελετηθεί σε βάθος. Ακόμα και αν παραμερίσουμε πιθανές φυσιολογικές αλλαγές στα ανατομικά βιομετρικά στοιχεία, τα βιομετρικά συστήματα αντιμετωπίζουν ένα ακόμη μεγαλύτερο πρόβλημα. Τα βιομετρικά συστήματα βασίζονται πάνω σε ψηφιακές μετρήσεις των χαρακτηριστικών του σώματος, και όχι στα αληθινά-πραγματικά ανατομικά βιομετρικά στοιχεία. Αυτή η διαδικασία της μέτρησης παρουσιάζει διαφορές στα δείγματα του ίδιου βιομετρικού στοιχείου ενός χρήστη έπειτα από κάποιο χρονικό διάστημα. Συνεπώς, τα σύνολα χαρακτηριστικών (feature set) που προκύπτουν από διαφορετικά δείγματα του ίδιου βιομετρικού στοιχείου ενός χρήστη είναι σπάνια ίδια.

Οι διαφορές που παρατηρούνται στο βιομετρικό σύνολο χαρακτηριστικών (feature set) ενός ατόμου είναι γνωστές ως ενδοατομικές διαφορές (στα αγγλικά αναφέρεται ως intra-user ή intra-class ή within-class variations). Αυτές οι διαφορές μπορεί να προκύπτουν για διάφορους λόγους, όπως μη ιδανικές συνθήκες καταγραφής (πχ δακτυλικό αποτύπωμα με θόρυβο εξαιτίας δυσλειτουργίας του αισθητήρα), αλλαγές στα βιομετρικά χαρακτηριστικά του χρήστη (πχ ασθένεια του αναπνευστικού που επηρεάζει την αναγνώριση φωνής), αλλαγές στις συνθήκες του περιβάλλοντος (πχ μη επαρκής φωτισμός σε εφαρμογές αναγνώρισης προσώπου), και διαφορές στον τρόπο με τον οποίο αλληλεπιδρά ο χρήστης με τον αισθητήρα (πχ μερικώς κλειστό μάτι κατά την καταγραφή της ίριδας ή μερικό δακτυλικό αποτύπωμα, ή διαφορετική πίεση του δακτύλου πάνω στον αισθητήρα).

Ενδοατομικές (intra-user) διαφορές είναι ακόμα περισσότερο εμφανείς στα χαρακτηριστικά συμπεριφοράς (behavioral traits) καθώς η διαφορετική ψυχολογική κατάσταση ενός ατόμου σε διάφορες χρονικές περιόδους, μπορεί να προκαλεί εμφανή διαφορά στη χαρακτηριστική συμπεριφορά του. Για παράδειγμα, ανάλογα με το επίπεδο άγχους ενός ατόμου, το δείγμα φωνής την ώρα της αυθεντικοποίησης μπορεί να είναι αρκετά διαφορετικό από το πρότυπο (template) εγγραφής. Παρομοίως, σε ένα μεθυσμένο άτομο, το περπάτημα και η υπογραφή μπορεί να άλλαζαν σημαντικά.

Καθώς υπάρχει αυτή η διαφορετικότητα στα αποκτηθέντα βιομετρικά στοιχεία (biometric traits), είναι παράλογο να αναμένει κανείς τέλεια ταύτιση μεταξύ οποιωνδήποτε δύο βιομετρικών συνόλων χαρακτηριστικών (feature set), ακόμα και αν προέρχονται από το ίδιο άτομο. Μάλιστα αν δύο σύνολα χαρακτηριστικών (feature sets) είναι εντελώς ίδια, μπορεί να είναι σοβαρή ένδειξη ότι τα βιομετρικά

δεδομένα προέρχονται από κάποιον που με κακό σκοπό ξαναστέλνει δεδομένα καταγεγραμμένα σε προγενέστερο χρόνο.

Ένα ιδανικό βιομετρικό σύνολο χαρακτηριστικών (feature set) πρέπει να επιδεικνύει μικρή ομοιότητα μεταξύ διαφορετικών ατόμων (εμφανείς διατομικές διαφορές - inter-user) και μικρές ενδοατομικές διαφορές (intra-user). Στην πράξη, αυτές οι δύο συνθήκες μπορεί να μην καλύπτονται πλήρως είτε εξαιτίας της έλλειψης μοναδικότητας από το χρησιμοποιούμενο βιομετρικό στοιχείο, είτε εξαιτίας περιορισμών στην αναπαράσταση (προβλήματα στην εξαγωγή των χαρακτηριστικών).

Εξαιτίας μικρών διατομικών διαφορών (μεγάλη ομοιότητα από άτομο σε άτομο) και μεγάλων ενδοατομικών διαφορών (μεγάλες διαφορές στα βιομετρικά χαρακτηριστικά του ίδιου ατόμου), ένα βιομετρικό σύστημα μπορεί να παράγει δύο τύπων σφάλματα: λανθασμένη μη-ταύτιση (false non-match) και λανθασμένη ταύτιση (false match). Όταν η διαφορά μεταξύ δειγμάτων του ίδιου χρήστη είναι μεγάλη, δύο δείγματα από το ίδιο βιομετρικό στοιχείο ενός ατόμου (mate samples) μπορεί να μην αναγνωριστούν σαν ταύτιση (match), και αυτό οδηγεί σε ένα σφάλμα λανθασμένης μη-ταύτισης (false-non-match error). Μία λανθασμένη ταύτιση (false match) συμβαίνει όταν δύο δείγματα από διαφορετικά άτομα (non-mate samples) αναγνωρίζονται λανθασμένα ότι ταυτίζονται, εξαιτίας μεγάλης διατομικής (inter-user) ομοιότητας.

1.5.1 Βασικές μετρήσεις απόδοσης

Οι παρακάτω μετρήσεις θεωρούνται θεμελιώδεις καθώς μπορούν να εφαρμοστούν στα βιομετρικά συστήματα κάθε τύπου. Ο δείκτης αποτυχίας εγγραφής (failure-to-enroll) και ο δείκτης αποτυχίας απόκτησης (failure-to-acquire) μετρούν την απόδοση της μονάδας εξαγωγής χαρακτηριστικών, ενώ ο δείκτης λανθασμένης ταύτισης (false match) και ο δείκτης λανθασμένης μη-ταύτισης (false nonmatch), μετρούν την απόδοση της μονάδας σύγκρισης.

- Δείκτης αποτυχίας εγγραφής - FTE (failure to enroll rate) είναι το ποσοστό του πληθυσμού στο οποίο το σύστημα αποτυγχάνει να ολοκληρώσει την διαδικασία της εγγραφής. Αποτυχία εγγραφής έχουμε όταν ο χρήστης δεν μπορεί να παρουσιάσει το απαιτούμενο βιομετρικό χαρακτηριστικό, ή όταν το αποκτηθέν βιομετρικό δείγμα του δεν μπορεί να γίνει αποδεκτό διότι είναι κακής ποιότητας. Αυστηρότερες απαιτήσεις όσον αφορά την ποιότητα των δειγμάτων κατά την εγγραφή θα αυξήσουν τον δείκτη αποτυχίας εγγραφής, αλλά θα βελτιώσουν την απόδοση ταύτισης διότι οι περιπτώσεις αποτυχίας

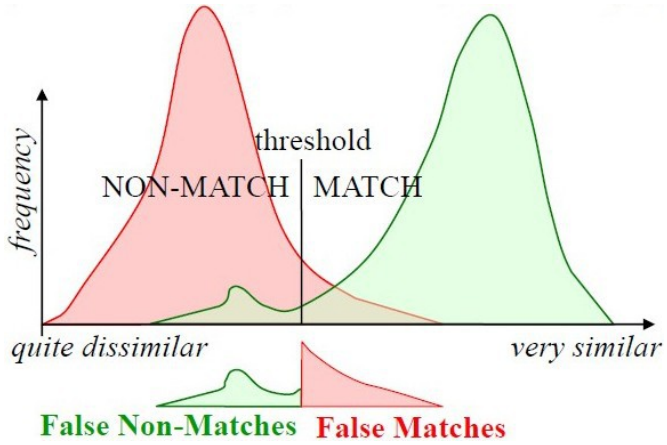
εγγραφής δεν θα συνεισφέρουν στον δείκτη αποτυχίας απόκτησης ή στους δείκτες αποτυχίας της μονάδος σύγκρισης.

- Δείκτης αποτυχίας απόκτησης – FTA (Failure to acquire rate) είναι το ποσοστό από απόπειρες επαλήθευσης ή ταυτοποίησης στις οποίες το βιομετρικό σύστημα δεν κατάφερε να καταγράψει ένα δείγμα ή να εντοπίσει μία εικόνα ή κάποιο σήμα ικανοποιητικής ποιότητας. Περίπτωση αποτυχίας απόκτησης έχουμε όταν το απαιτούμενο βιομετρικό χαρακτηριστικό δεν μπορεί να παρουσιαστεί λόγω προσωρινής ασθένειας ή τραυματισμού, ή όταν το αποκτηθέν δείγμα ή το σύνολο χαρακτηριστικών που εξήχθη δεν ικανοποιεί τις απαιτήσεις όσον αφορά την ποιότητα. Αυστηρότερες απαιτήσεις για την ποιότητα των δειγμάτων κατά την καταγραφή θα αυξήσουν τον δείκτη αποτυχίας απόκτησης, αλλά θα βελτιώσουν την απόδοση ταύτισης, διότι οι περιπτώσεις αποτυχίας απόκτησης δεν θα συμπεριλαμβάνονται στον υπολογισμό του δείκτη λανθασμένης ταύτισης και του δείκτη λανθασμένης μη-ταύτισης.

- Δείκτης λανθασμένης μη-ταύτισης – FNMR (False non match rate) είναι το ποσοστό των γνήσιων-αυθεντικών δειγμάτων που λανθασμένα δεν έγιναν αποδεκτά και θεωρήθηκε ότι δεν ταυτίζεται το δείγμα με το πρότυπο του ίδιου χρήστη (η βαθμολογία ομοιότητας ήταν κάτω από το όριο αποδοχής). Μία βαθμολογία ομοιότητας αποκαλείται γνήσια ή αυθεντική βαθμολογία (genuine or authentic score), αν υποδεικνύει την ομοιότητα μεταξύ δύο δειγμάτων του ίδιου ατόμου. Μία βαθμολογία εξαπάτησης (impostor score) μετράει την ομοιότητα μεταξύ δύο δειγμάτων που ανήκουν σε διαφορετικά άτομα.

- Δείκτης λανθασμένης ταύτισης - FMR (False match rate) είναι το ποσοστό των δειγμάτων που ενώ προέρχονται από κάποιο κακόβουλο άτομο, λανθασμένα ταυτίζονται με το πρότυπο κάποιου διαφορετικού χρήστη. Με άλλα λόγια το FMR είναι η εκτιμώμενη πιθανότητα δύο δείγματα από δύο διαφορετικά άτομα να γίνουν αποδεκτά από λάθος, να θεωρηθεί δηλαδή ότι ταυτίζονται.

Ο δείκτης λανθασμένης ταύτισης και ο δείκτης λανθασμένης μη-ταύτισης επηρεάζονται από το όριο αποδοχής (decision threshold) της βαθμολογίας ομοιότητας (similarity score). Αλλάζοντας αυτό το όριο, πάντα υπάρχει μία αντιστάθμιση μεταξύ των σφαλμάτων λανθασμένης ταύτισης και λανθασμένης μη-ταύτισης.



Σχήμα 3: Η κατανομή της βαθμολογίας ομοιότητας των κακόβουλων χρηστών (βαθμολογία εξαπάτησης) με κόκκινο χρώμα και η κατανομή της βαθμολογίας ομοιότητας των αυθεντικών χρηστών με πράσινο. [25]

1.5.2 Μετρήσεις απόδοσης ενός συστήματος επαλήθευσης

Κατά την εκτίμηση της απόδοσης των βιομετρικών συστημάτων, η μονάδα μέτρησης είναι η συναλλαγή, η οποία μπορεί να αποτελείται από μία μοναδική απόπειρα, αλλά συνήθως αποτελείται από πολλαπλές προσπάθειες. Έτσι οι βασικοί δείκτες, FMR και FNMR, δεν μπορούν να εφαρμοστούν απευθείας για την ολική εκτίμηση της απόδοσης ενός βιομετρικού συστήματος, και οι παρακάτω μέθοδοι μέτρησης είναι σχεδιασμένοι για πιο γενικές μετρήσεις.

- Δείκτης λανθασμένων απορρίψεων - False rejection rate (FRR) είναι το ποσοστό των συναλλαγών επαλήθευσης που γίνονται από αυθεντικούς χρήστες και απορρίπτονται από λάθος. Αν η συναλλαγή επαλήθευσης αποτελείται από μία μοναδική απόπειρα, το ποσοστό λανθασμένων απορρίψεων περιλαμβάνει έναν δείκτη αποτυχίας απόκτησης ή μία λανθασμένη μη-ταύτιση, και ο δείκτης λανθασμένων απορρίψεων δίνεται από τον τύπο: FRR = FTA + FNMR x (1 – FTA) (1.1)
- Δείκτης λανθασμένων αποδοχών – False acceptance rate (FAR) είναι το ποσοστό των συναλλαγών επαλήθευσης που ενώ γίνονται από κακόβουλα άτομα γίνονται αποδεκτοί από το βιομετρικό σύστημα. Αν η συναλλαγή επαλήθευσης αποτελείται από μία μοναδική απόπειρα, το ποσοστό λανθασμένων αποδοχών θα δινόταν από: FAR = FMR x (1 – FTA) (1.2)

- Ο δείκτης αυθεντικών αποδοχών – Genuine Accept Rate (GAR) ή δείκτης πραγματικών αποδοχών (True Accept Rate – TAR) μπορεί να χρησιμοποιηθεί σαν εναλλακτικό του FRR κατά την παρουσίαση της απόδοσης ενός βιομετρικού συστήματος επαλήθευσης. Ο GAR ορίζεται σαν το ποσοστό των αυθεντικών βαθμολογιών που ξεπερνούν το όριο αποδοχής.

Τα FRR και FAR δεν περιλαμβάνουν σφάλματα που έγιναν κατά την εγγραφή. Για να μπορεί να γίνει σύγκριση της απόδοσης βιομετρικών συστημάτων που έχουν διαφορετικούς δείκτες αποτυχίας εγγραφής, το FRR και το FAR χρειάζεται να γενικευτούν για να λαμβάνουν υπόψιν τους τα σφάλματα κατά την εγγραφή. Στα γενικευμένα FRR και FAR, μία αποτυχία εγγραφής παραβλέπεται (εκλαμβάνεται ότι ολοκληρώθηκε επιτυχώς η εγγραφή), αλλά όλες οι επακόλουθες συναλλαγές από ή προς το συγκεκριμένο άτομο αποτυγχάνουν.

- Γενικευμένος δείκτης λανθασμένων απορρίψεων - GFRR (generalized false reject rate) είναι το ποσοστό από αυθεντικούς χρήστες που δεν μπορούν να εγγραφούν, που το δείγμα τους παρουσιάζεται αλλά δεν μπορεί να αποκτηθεί, ή που είναι εγγεγραμμένοι (το δείγμα τους έχει αποκτηθεί παλαιότερα), αλλά απορρίπτονται λανθασμένα.

  $$GFRR = FTE + (1 – FTE) \times FRR$$

  $$= FTE + (1 – FTE) \times FTA + (1 – FTE) \times (1 – FTA) \times FMR \qquad (1.3)$$

- Γενικευμένος δείκτης λανθασμένων αποδοχών - GFAR (generalized false accept rate) είναι το ποσοστό από κακόβουλους χρήστες που είναι εγγεγραμμένοι, που έχει αποκτηθεί το δείγμα τους και ταυτίζονται λανθασμένα.

  $$GFAR = (1 – FTE) \times FAR$$

  $$= (1 – FTE) \times (1 – FTA) \times FMR \qquad (1.4)$$

Κάτι που πρέπει να σημειωθεί είναι ότι η εμφάνιση λανθασμένων αποδοχών (false accepts) και λανθασμένων απορρίψεων δεν είναι κατανεμημένη ισόποσα σε όλους τους χρήστες του βιομετρικού συστήματος. Υπάρχουν διαφορές στην “αναγνωρισιμότητα” μεταξύ των χρηστών. Μερικών τα βιομετρικά στοιχεία είναι καλής ποιότητας και είναι εύκολη η εξαγωγή του συνόλου χαρακτηριστικών, ενώ σε άλλους, πιθανόν λόγω της εργασίας την οποία κάνουν, να είναι δύσκολη η απόκτηση του συνόλου χαρακτηριστικών ή να εμφανίζουν μεγάλες ενδοατομικές

διαφορές. Επίσης είναι κάποιοι που επίτηδες προσπαθούν να παραμορφώσουν τα βιομετρικά χαρακτηριστικά τους.

1.5.3 Μετρήσεις απόδοσης ενός συστήματος ταυτοποίησης

- Δείκτης σωστής ταυτοποίησης - CIR (correct identification rate) είναι το ποσοστό των συναλλαγών ταυτοποίησης από χρήστες που είναι εγγεγραμμένοι στο σύστημα και στις οποίες η σωστή ταυτότητα του χρήστη βρίσκεται ανάμεσα σε αυτές που επιστρέφει το σύστημα. Ο δείκτης ταυτοποίησης με βαθμό r είναι η πιθανότητα σε μία συναλλαγή από έναν χρήστη εγγεγραμμένο στο σύστημα, να συμπεριλαμβάνεται η πραγματική ταυτότητα του συγκεκριμένου χρήστη εντός των r αποτελεσμάτων που επιστρέφει το σύστημα. Χρησιμοποιείται και ο όρος: δείκτης αληθώς θετικής ταυτοποίησης (true positive identification rate – TPIR).

- Δείκτης ψευδώς αρνητικής ταυτοποίησης - FNIR (false-negative identification-error rate) είναι το ποσοστό συναλλαγών ταυτοποίησης από χρήστες εγγεγραμμένους στο σύστημα, που η σωστή ταυτότητα του χρήστη δεν είναι ανάμεσα σε αυτές που επιστρέφει το σύστημα: FNIR = FTA + (1 – FTA) x FNMR (1.5)

- Δείκτης ψευδώς θετικής ταυτοποίησης - FPIR (false-positive identification-error rate) είναι το ποσοστό από συναλλαγές ταυτοποίησης από χρήστες που δεν είναι εγγεγραμμένοι στο σύστημα, όπου αντί για μία κενή λίστα, επιστρέφεται ένας αριθμός από ταυτότητες. Για μία βάση δεδομένων μεγέθους N, ο FPIR δίνεται ως εξής:

  $$FPIR = (1 - FTA) \times \{1 - (1 - FMR)^N\} \quad (1.6)$$

1.5.4 Γραφικές μετρήσεις απόδοσης

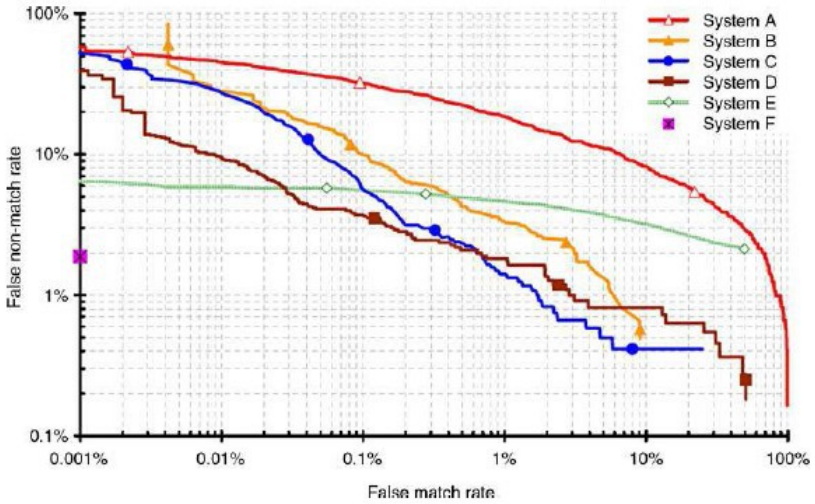
Όταν παρουσιάζονται αποτελέσματα δοκιμών, η απόδοση της μονάδας σύγκρισης ή της μονάδας λήψης αποφάσεων των βιομετρικών συστημάτων, αναπαρίστανται γραφικά χρησιμοποιώντας καμπύλες Detection Error Trade-off (DET), Receiver Operating Characteristics (ROC) ή Cumulative Match Characteristic (CMC).

Οι καμπύλες αντιστάθμισης ανίχνευσης σφαλμάτων - DET χρησιμοποιούνται για να απεικονίσουν δείκτες σφαλμάτων σύγκρισης (FNMR σε σχέση με FMR), δείκτες σφαλμάτων απόφασης (FRR σε σχέση με FAR) και δείκτες σφαλμάτων ταυτοποίησης ανοιχτού συνόλου (FNIR σε σχέση με FPIR). Η καμπύλη DET είναι μία τροποποιημένη καμπύλη ROC η οποία απεικονίζει δείκτες λαθών και στους δύο άξονες (λανθασμένη ταύτιση στον άξονα των x και λανθασμένη μη-ταύτιση

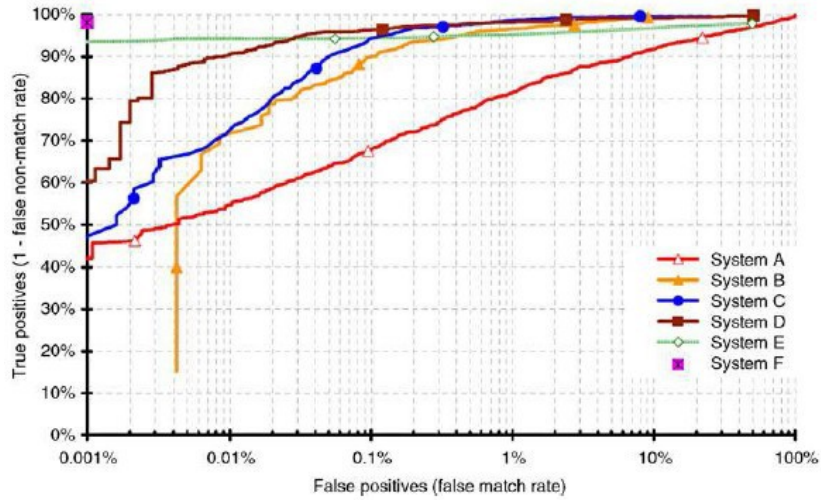
στον άξονα των y). Κάθε καμπύλη DET δημιουργείται αλλάζοντας την τιμή του ορίου αποδοχής. Αν το όριο αποδοχής οριστεί σε υψηλότερη τιμή έτσι ώστε να ελαττωθούν οι λανθασμένες αποδοχές, τότε το ποσοστό των λανθασμένων απορρίψεων θα αυξηθεί. Αντίθετα, αν το όριο αποδοχής οριστεί σε χαμηλότερη τιμή, οι λανθασμένες απορρίψεις θα μειωθούν αλλά θα αυξηθούν οι λανθασμένες αποδοχές.

Οι χαρακτηριστικές καμπύλες λειτουργίας Δέκτη - ROC είναι ανεξάρτητες του ορίου αποδοχής, επιτρέποντας την σύγκριση της απόδοσης διαφορετικών συστημάτων κάτω από παρόμοιες συνθήκες, ή ενός μοναδικού συστήματος κάτω από διαφορετικές συνθήκες. Οι καμπύλες ROC μπορούν να χρησιμοποιηθούν για να απεικονίσουν την επίδοση αλγόριθμων σύγκρισης (1-FNMR με FMR), την απόδοση συστημάτων επαλήθευσης (1-FRR με FAR), όπως και για την απόδοση συστημάτων ταυτοποίησης ανοιχτού συνόλου (CIR με FPIR). Μια καμπύλη ROC είναι μία απεικόνιση του δείκτη ψευδώς θετικών αποδοχών (οι προσπάθειες των κακόβουλων γίνονται αποδεκτές) στον άξονα των x, και τον αντίστοιχο δείκτη των αληθώς θετικών αποδοχών (αυθεντικές προσπάθειες γίνονται αποδεκτές) στον άξονα των y, που απεικονίζεται παραμετρικά συναρτήσει του ορίου αποδοχής. Ο καλύτερος τρόπος για να συγκρίνει κανείς την επίδοση δύο βιομετρικών συστημάτων είναι να εξετάσει τις ROC καμπύλες. Αν το FRR του ενός βιομετρικού συστήματος είναι συνεχώς χαμηλότερο από το FRR του άλλου συστήματος για τις αντίστοιχες τιμές του FAR, συμπεραίνουμε ότι η απόδοση ταύτισης του πρώτου συστήματος είναι καλύτερη. Αν όμως δύο ROC καμπύλες τέμνονται, τότε σημαίνει ότι το πρώτο σύστημα είναι καλύτερο από το δεύτερο σε ορισμένες περιπτώσεις (τιμές FAR), ενώ το δεύτερο σύστημα είναι καλύτερο σε άλλες.

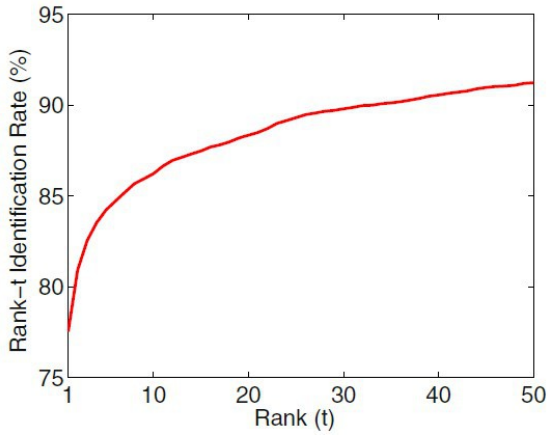
Για εφαρμογές ταυτοποίησης κλειστού συνόλου, τα αποτελέσματα των επιδόσεων συχνά παρουσιάζονται χρησιμοποιώντας μία χαρακτηριστική καμπύλη συσσωρευτικής ταύτισης - cumulative match characteristic curve (CMC curve). Η γραφική παράσταση της καμπύλης εμφανίζει το ποσοστό ένταξης της σωστής ταυτότητας ανάμεσα στις κ-καλύτερες θέσεις (rank values), για κάθε k. Στον άξονα των x είναι οι τιμές k, και στον άξονα των y, η αντίστοιχη πιθανότητα σωστής ταυτοποίησης.



Σχήμα 4: καμπύλες DET [13]



Σχήμα 5: καμπύλες ROC [13]



Σχήμα 6: καμπύλη CMC [13]

1.5.5 Άλλες μετρήσεις απόδοσης

Για την ακριβέστερη εκτίμηση της απόδοσης των βιομετρικών συστημάτων έχουν οριστεί και οι παρακάτω ενδείξεις, οι οποίες χρησιμοποιούνται σε διάφορους διαγωνισμούς σύγκρισης αλγορίθμων, όπως τους διαγωνισμούς FVC[6].

- Κατανομή Αυθεντικών βαθμολογιών (Genuine score distribution) και κατανομή Κακόβουλων βαθμολογιών (Impostor score distribution)
- Δείκτης Ισάριθμων Σφαλμάτων - EER (equal error rate), είναι το σημείο όπου ισχύει FNMR=FMR.
- EER* η τιμή που θα έπαιρνε ο EER αν τα σφάλματα σύγκρισης δεν συμπεριλαμβάνονταν στον υπολογισμό των FMR και FNMR.
- FMR100 είναι το μικρότερο FNMR για FMR < 1%
- FMR1000 είναι το μικρότερο FNMR για FMR < 0.1%
- ZeroFMR είναι το μικρότερο FNMR στο οποίο δεν συμβαίνουν λανθασμένες ταυτίσεις (false matches)
- ZeroFNMR είναι το μικρότερο FMR στο οποίο δεν συμβαίνει καμία λανθασμένη μη-ταύτιση (false nonmatches)

Εκτός από αυτούς τους δείκτες μέτρησης λαθών, υπάρχουν και άλλοι δείκτες απόδοσης που σχετίζονται με την λειτουργία των βιομετρικών συστημάτων όπως: μέσος χρόνος εγγραφής, μέσος χρόνος επαλήθευσης, μέσο και μέγιστο μέγεθος ενός προτύπου, και η μέγιστη τιμή χωρητικότητας μνήμης που απαιτείται.

1.7 Εφαρμογές Βιομετρικών Συστημάτων

Πριν την υλοποίηση ενός βιομετρικού συστήματος, θα πρέπει πρώτα να εξεταστούν όλες οι ήδη υπάρχουσες τεχνολογίες ασφαλείας. Η βιομετρία θα μπορούσε να χρησιμοποιηθεί σαν συμπληρωματική των ID cards και των κωδικών, προσθέτοντας έτσι ένα επιπλέον επίπεδο ασφαλείας. Μία τέτοια διάταξη αποκαλείται συχνά πολυπαραγοντική αυθεντικοποίηση (multifactor authentication scheme).

Ένα βιομετρικό σύστημα μπορεί να κάνει επαλήθευση ή ταυτοποίηση, αλλά υπάρχουν και περιπτώσεις όπου μπορεί να κάνει και τα δύο. Σε μερικές εφαρμογές όπως μεγάλου εύρους εθνικά ID συστήματα που έχουν μεγάλο φάσμα χρήσεων,

το σύστημα μπορεί να τρέχει σε κατάσταση επαλήθευσης για να παρέχει επιδόματα ή υπηρεσίες μόνο σε εγγεγραμμένους χρήστες. Πέρα από τον τύπο της λειτουργίας, οι βιομετρικές εφαρμογές μπορούν να καταταγούν βάσει των παρακάτω περιπτώσεων[9]:

- Συνεργάσιμοι και μη συνεργάσιμοι χρήστες (Cooperative versus non-cooperative users): Η συνεργασία αναφέρεται στην συμπεριφορά του χρήστη κατά την αλληλεπίδραση του με το σύστημα. Για παράδειγμα, σε ένα σύστημα επαλήθευσης, είναι προς το συμφέρον του χρήστη να συνεργαστεί με το σύστημα και να γίνει αποδεκτός σαν ένας έγκυρος (valid) χρήστης. Οι ηλεκτρονικές τραπεζικές συναλλαγές είναι για παράδειγμα μία εφαρμογή όπου οι εγγεγραμμένοι χρήστες αναμένεται ότι θα συνεργαστούν με το σύστημα έτσι ώστε να αναγνωριστούν σωστά. Από την άλλη, σε ένα αρνητικό σύστημα αναγνώρισης, ένας χρήστης μπορεί να μην συνεργάζεται με το σύστημα (πχ μπορεί επίτηδες να εφαρμόζει υπερβολική πίεση όταν τοποθετεί το δάκτυλο του πάνω στον αισθητήρα) για να αποφύγει την αναγνώριση. Ένας τρομοκράτης που προσπαθεί να αποκρύψει την ταυτότητα του από μία εφαρμογή ενός συστήματος προληπτικού ελέγχου (screening) σε κάποιο αεροδρόμιο, θα είναι μη συνεργάσιμος.

- Φανερή ή συγκεκαλυμμένη εφαρμογή (Overt versus covert deployment): Αν ο χρήστης γνωρίζει ότι παίρνει μέρος σε βιομετρική αναγνώριση, η εφαρμογή θεωρείται φανερή overt. Αν ο χρήστης δεν το αντιλαμβάνεται, η εφαρμογή λέγεται συγκεκαλυμμένη. Η αναγνώριση προσώπου μπορεί εύκολα να χρησιμοποιηθεί σε μία συγκεκαλυμμένη εφαρμογή (πχ παρακολούθηση), ενώ η αναγνώριση δακτυλικών αποτυπωμάτων δεν μπορεί να χρησιμοποιηθεί κατά αυτόν τον τρόπο (εκτός από αναγνώριση κάποιου κακοποιού από δακτυλικά αποτυπώματα που συλλέχθηκαν στον τόπο του εγκλήματος). Οι περισσότερες εμπορικές εφαρμογές βιομετρίας είναι φανερές.

- Εξοικειωμένοι και μη-εξοικειωμένοι χρήστες (Habituated users versus non-habituated): Αν οι εγγεγραμμένοι χρήστες αλληλεπιδρούν με το βιομετρικό σύστημα αρκετά συχνά, εξοικειώνονται με την παροχή των βιομετρικών δεδομένων τους. Για παράδειγμα, μία εφαρμογή εισόδου σε κάποιο δίκτυο υπολογιστών (computer network login application) έχει συνήθως εξοικειωμένους χρήστες (έπειτα από κάποια αρχική περίοδο εξοικείωσης) εξαιτίας της καθημερινής χρήσης του συστήματος. Όμως, η εφαρμογή σε διπλώματα οδήγησης συνήθως έχει μη-εξοικειωμένους χρήστες καθώς η άδειες οδήγησης ανανεώνονται αφού περάσουν κάποια έτη. Αυτό είναι μία

σημαντική παράμετρος στον σχεδιασμό ενός βιομετρικού συστήματος γιατί η άνεση των χρηστών με το σύστημα μπορεί να επηρεάσει την ακρίβεια της αναγνώρισης καθώς ένας εξοικειωμένος χρήστης είναι πιο πιθανό να παρέχει βιομετρικά δεδομένα καλής ποιότητας.

- Με επίβλεψη ή χωρίς επίβλεψη (Attended versus unattendend operation): Αναφέρεται στο αν η διαδικασία απόκτησης των βιομετρικών δεδομένων σε μία εφαρμογή γίνεται υπό κάποια επίβλεψη και καθοδήγηση, ή αν επιβλέπεται από κάποιον άνθρωπο (πχ προσωπικό ασφαλείας). Ακόμα, μία εφαρμογή μπορεί να έχει υπό επίβλεψη την διαδικασία της εγγραφής, αλλά χωρίς επίβλεψη την διαδικασία της αναγνώρισης. Για παράδειγμα, μία τραπεζική εφαρμογή μπορεί να έχει υπό επίβλεψη εγγραφή όταν μία κάρτα ATM εκδίδεται για κάποιον χρήστη, αλλά οι επόμενες χρήσεις του βιομετρικού συστήματος για τις συναλλαγές με το ATM να μην είναι υπό επίβλεψη.

- Ελεγχόμενο περιβάλλον και μη-ελεγχόμενο (Controlled versus uncontrolled operation): Σε ένα ελεγχόμενο περιβάλλον, συνθήκες όπως θερμοκρασία, πίεση, φωτισμός κτλ μπορούν να ελέγχονται κατά τη διάρκεια της λειτουργίας του βιομετρικού συστήματος. Συνήθως, εφαρμογές σε κλειστούς χώρους όπως computer network login λειτουργούν σε ένα ελεγχόμενο περιβάλλον, ενώ εφαρμογές σε εξωτερικούς χώρους όπως η είσοδος στο αμάξι χωρίς κλειδί, ή το σύστημα παρακολούθησης ενός χώρου στάθμευσης, λειτουργούν σε μη-ελεγχόμενο περιβάλλον. Αυτή η κατηγοριοποίηση είναι επίσης σημαντική για τον σχεδιαστή του συστήματος καθώς κάποιος πιο στιβαρός βιομετρικός αισθητήρας χρειάζεται για ένα μη ελεγχόμενο περιβάλλον.

- Ανοιχτό και κλειστό σύστημα (Open versus closed system): Αν το βιομετρικό πρότυπο (template) ενός ανθρώπου μπορεί να χρησιμοποιηθεί παράλληλα σε πολλαπλές εφαρμογές, το βιομετρικό σύστημα μπορεί να θεωρείται ανοιχτό. Για παράδειγμα, ένας χρήστης μπορεί να χρησιμοποιεί ένα σύστημα αναγνώρισης δακτυλικού αποτυπώματος για να εισέρχεται σε χώρους αυξημένης ασφάλειας, για είσοδο στο δίκτυο, electronic banking, και σε ATM τραπεζών. Όταν όλες αυτές οι εφαρμογές χρησιμοποιούν διαφορετικά πρότυπα (templates) για κάθε εφαρμογή, το σύστημα θεωρείται κλειστό. Ένα κλειστό σύστημα μπορεί να βασίζεται σε κάποιο ειδικό-εταιρικό πρότυπο ενώ ένα ανοιχτό σύστημα θα χειρίζεται συνηθισμένους τύπους αρχείων μεταξύ διαφορετικών συστημάτων (πολύ πιθανό αναπτυγμένα και από διαφορετικούς κατασκευαστές).

Οι περισσότερες εμπορικές εφαρμογές βιομετρικών, όπως η είσοδος σε εγκαταστάσεις ασφαλείας, έχουν τις παρακάτω ιδιότητες: επαλήθευση, με συνεργάσιμους χρήστες, φανερή εφαρμογή, με εξοικειωμένους χρήστες, με επίβλεψη κατά τη διάρκεια της εγγραφής και χωρίς επίβλεψη κατά την αυθεντικοποίηση και είναι κλειστά συστήματα.

Βιομετρικά συστήματα συναντάμε κυρίως σε:

1. Εμπορικές εφαρμογές όπως computer login, electronic data security, e-commerce, ATM, πιστωτικές κάρτες, έλεγχο πρόσβασης, κινητά τηλέφωνα, PDA, διαχείριση ιατρικού ιστορικού κ.α.

2. Κυβερνητικά προγράμματα όπως εθνικές ταυτότητες, διαχείριση φυλακισμένων σε μέρη επανένταξης, διπλώματα οδήγησης, κοινωνική ασφάλεια, καταβολή επιδομάτων, έλεγχος συνόρων, έλεγχος διαβατηρίων, κτλ

3. Εγκληματολογικές εφαρμογές όπως ταυτοποίηση πτωμάτων, αναζήτηση κακοποιών, αναζήτηση χαμένων παιδιών, έλεγχος πατρότητας κτλ.

1.8 Ασφάλεια και ζητήματα Ιδιωτικότητας

Υπάρχουν τέσσερις βασικές έννοιες που πρέπει να ληφθούν υπ' όψιν στην ασφάλεια πληροφοριών.

- Ακεραιότητα (Integrity) – προστασία από αθέλητη τροποποίηση ή καταστροφή των δεδομένων και διασφάλιση της μη-αποποίησης και της αυθεντικότητας των πληροφοριών.

- Εμπιστευτικότητα Δεδομένων (Data confidentiality) – αποτροπή μη επιτρεπτής πρόσβασης ή αποκάλυψης ευαίσθητων πληροφοριών.

- Διαθεσιμότητα (Availability) – εγγυημένη αδιάλειπτη και αξιόπιστη πρόσβαση στην πληροφορία.

- Αυθεντικοποίηση (Authentication) – μόνο νόμιμοι και εξουσιοδοτημένοι χρήστες θα πρέπει να είναι ικανοί να έχουν πρόσβαση στα δεδομένα και να μπορούν να εκτελέσουν ορισμένες ενέργειες.

Ένα βιομετρικό σύστημα διευθετεί μόνο το κομμάτι της αυθεντικοποίησης. Άλλες τεχνολογίες όπως η κρυπτογράφηση, οι ψηφιακές υπογραφές κτλ χρειάζονται για να επιτευχθούν οι απαιτήσεις σε μυστικότητα, ακεραιότητα και διαθεσιμότητα ολόκληρου του πληροφοριακού συστήματος.

Παρ' ότι η βιομετρική αναγνώριση μπορεί να λειτουργήσει σαν εργαλείο για την διατήρηση της ιδιωτικότητας κάποιου, περιορίζοντας την πρόσβαση στις δικές του προσωπικές πληροφορίες (πχ ιατρικό ιστορικό), την ίδια στιγμή, η χρήση βιομετρικών μπορεί από μόνη της, να δημιουργεί ζητήματα ιδιωτικότητας. Αυτό γιατί τα βιομετρικά χαρακτηριστικά που μας ξεχωρίζουν και μας ταυτοποιούν, παρέχουν έναν μόνιμο σύνδεσμο με την ταυτότητα του κάθε ατόμου.

Μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων προσωπικών πληροφοριών μπορεί να προκαλέσει αντικειμενικές (πχ οικονομική απάτη, άρνηση παροχής υπηρεσιών) και υποκειμενικές απώλειες (όπου απλά και μόνο η γνώση προσωπικών πληροφοριών από ένα δεύτερο πρόσωπο ή τρίτο πρόσωπο θεωρείται ζημία). Όταν μία παραβίαση της ασφάλειας σε ένα πληροφοριακό σύστημα έχει σαν αποτέλεσμα προσωπική και υποκειμενική ζημία για κάποιο άτομο, μπορεί να κατηγοριοποιηθεί ως απώλεια της ιδιωτικότητας (privacy). Η ιδιωτικότητα αναφέρεται στο δικαίωμα ενός ατόμου να παραμένει ανώνυμος και να ελέγχει την πρόσβαση σε δικές του προσωπικές πληροφορίες. Παρ' όλο που η ανάγκη για ιδιωτικότητα (privacy) είναι τυπικά μία προτίμηση του καθενός, υπάρχουν περιπτώσεις όπου η αποκάλυψη πληροφορίας μπορεί να απαιτείται για το δημόσιο συμφέρον (πχ εθνική ασφάλεια).

Οι κυριότερες ανησυχίες σχετικά με την χρήση της βιομετρίας είναι οι παρακάτω [3]:

- Βιομετρικά δεδομένα, μπορεί να συλλέγονται ή να μοιράζονται, χωρίς την άδεια των χρηστών, χωρίς επαρκή ενημέρωση, ή χωρίς συγκεκριμένο σκοπό.
- Βιομετρικά δεδομένα, που έχουν συλλεγεί για συγκεκριμένο σκοπό, μπορεί αργότερα να χρησιμοποιηθούν για κάποιον άλλο σκοπό, μη θεμιτό ή χωρίς εξουσιοδότηση. Αυτό είναι γνωστό σαν “function creep”.
- Όσο εξαπλώνεται η χρήση της βιομετρίας, αυξάνεται ταυτόχρονα η πιθανότητα να υποκλαπούν τα βιομετρικά μας δεδομένα, καθώς κάποια μέρη είναι πιο ευάλωτα από άλλα.
- Τα βιομετρικά δεδομένα μπορεί να χρησιμοποιηθούν για να αποκαλύψουν το φύλο και την εθνικότητα κάποιου. Ακόμα, μπορεί να αποκαλύπτουν λεπτομέρειες για το ιατρικό ιστορικό. Μπορεί να γίνει μία εκτίμηση της κατάστασης της υγείας κάποιου, συγκρίνοντας τα βιομετρικά δεδομένα που πάρθηκαν κατά την εγγραφή, με τα βιομετρικά δεδομένα κατά την διάρκεια της αναγνώρισης. Σαν αποτέλεσμα η βιομετρία μπορεί να χρησιμοποιηθεί

για κατηγοριοποίηση ανθρώπων σύμφωνα με την κατάσταση της υγείας τους.

- Η βιομετρία μπορεί να χρησιμοποιηθεί για τον εντοπισμό ή την παρακολούθηση ατόμων. Καθώς τα βιομετρικά δεδομένα θεωρούνται μοναδικά, υπάρχει η δυνατότητα εντοπισμού και παρακολούθησης ατόμου, είτε καθώς προσπαθεί να εισέλθει σε διάφορες εγκαταστάσεις, είτε με την καταγραφή του από κάποιο σύστημα παρακολούθησης. Ακόμα η συσχέτιση των βιομετρικών δεδομένων με προσωπικές πληροφορίες, όπως όνομα, διεύθυνση, αριθμό διαβατηρίου, ενέχει τον κίνδυνο κάποιος που έχει πρόσβαση, να συλλέγει και να συγκρίνει πληροφορίες για ένα άτομο ξεκινώντας από ένα βιομετρικό στοιχείο του. Επιπλέον, η χρήση της βιομετρίας μπορεί να επιτρέψει την ανίχνευση των κινήσεων ενός χρήστη που υπάρχει σε διαφορετικές βάσεις δεδομένων. Όλα αυτά μπορούν να οδηγήσουν σε μυστική παρακολούθηση, κατηγοριοποίηση και κοινωνικό έλεγχο.

- Τα βιομετρικά δεδομένα μπορεί να αποθηκεύονται ή να μεταδίδονται με ακατάλληλο τρόπο. Αυτό θέτει τα βιομετρικά δεδομένα σε κίνδυνο, από εξωτερικές επιθέσεις. Ακόμη, τα βιομετρικά δεδομένα μπορεί να είναι ευάλωτα σε κακούς χειρισμούς των διαχειριστών ή των χειριστών (κακή χρήση των δικαιωμάτων πρόσβασης στην βιομετρική βάση δεδομένων).

- Αυτή η αδιάψευστη απόδειξη εισόδου με χρήση βιομετρικών παραβιάζει το δικαίωμα κάθε ατόμου στην ανωνυμία; Για παράδειγμα, άτομα που διατηρούν νόμιμα πολλαπλά ονόματα (ας πούμε για λόγους ασφαλείας) μπορεί να ταυτοποιηθούν χρησιμοποιώντας βιομετρική αναγνώριση. Ακόμα, είναι συχνά πιθανόν να αναγνωριστεί ένας χρήστης στα κρυφά, με την απόκτηση των βιομετρικών του χαρακτηριστικών, χωρίς την δική του παρέμβαση (πχ το πρόσωπο μπορεί να καταγραφεί χρησιμοποιώντας κρυφές κάμερες παρακολούθησης). Σαν αποτέλεσμα, στα άτομα που επιθυμούν να παραμείνουν ανώνυμοι υπό όλες τις συνθήκες, ίσως να τους αφαιρεθεί αυτή η ιδιωτικότητα εξαιτίας της βιομετρικής αναγνώρισης.

- Θα πρέπει να υπάρχει κάποια ισορροπία ανάμεσα στην χρήση βιομετρίας και την ασφάλεια που απαιτείται. Δεν θα πρέπει να απαιτείται κάποιο δακτυλικό αποτύπωμα για μη πολύ σοβαρούς λόγους.

- Σε ποιον ανήκουν τα βιομετρικά δεδομένα, στο άτομο ή στους παρόχους των υπηρεσιών;

Τα παραπάνω ζητήματα ιδιωτικότητας είναι δύσκολα και δεν υπάρχουν απλές απαντήσεις. Ενώ κάποιος θα μπορούσε να ορίσει κάποια μέτρα για να προστατεύσει την ιδιωτικότητα των χρηστών, δεν υπάρχουν ικανοποιητικές πρακτικές λύσεις στον ορίζοντα για την αντιμετώπιση όλου του φάσματος των ζητημάτων ιδιωτικότητας ή το πώς ακριβώς αυτά τα θέματα πρέπει να αντισταθμιστούν με τα ζητήματα ασφαλείας. Αρχές δίκαιης χρήσης των πληροφοριών όπως διαφάνεια, συγκατάθεση, περιορισμός χρήσης, λογοδοσία και έλεγχος θα μπορούσαν να εφαρμοστούν, για να περιοριστούν οι ανησυχίες περί ιδιωτικότητας που εγείρονται από την βιομετρική αναγνώριση. Καθώς αυτά τα θέματα είναι πέρα από τις δυνατότητες της τεχνολογίας, πρέπει να δημιουργηθούν κατάλληλοι νόμοι για να ενισχυθούν αυτές οι αρχές.

ΕΠΙΛΟΓΟΣ

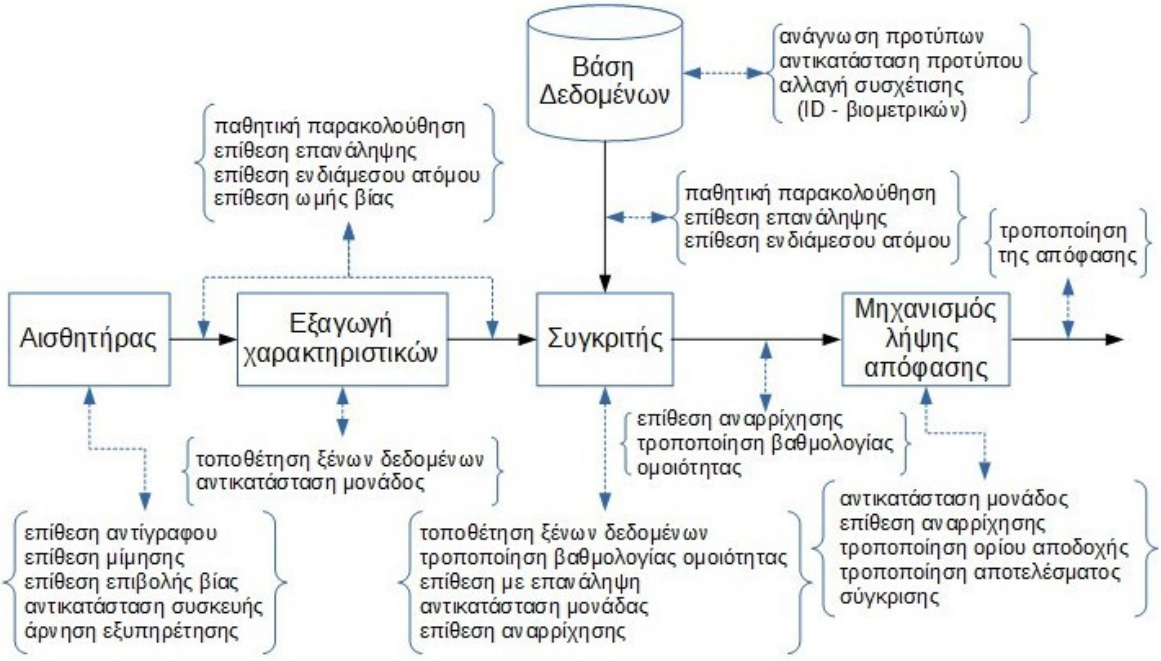
Η χρήση βιομετρίας παρέχει έναν μόνιμο σύνδεσμο με την ταυτότητα μας. Τα τελευταία χρόνια αυξάνονται όλο και περισσότερο οι εφαρμογές που κάνουν χρήση βιομετρίας, είτε για λόγους ευχρηστίας, είτε για λόγους ασφαλείας. Την συναντούμε σε ένα τεράστιο φάσμα εφαρμογών, όπου υπάρχει ανάγκη αναγνώρισης και αυθεντικοποίησης των χρηστών. Από απλά συστήματα καταγραφής της ώρας εισόδου και εξόδου του προσωπικού, μέχρι μεγάλα κυβερνητικά προγράμματα που έχουν σκοπό να εγγράψουν όλους τους πολίτες τους σε εθνικά βιομετρικά συστήματα για να τους παρέχουν υπηρεσίες χωρίς να απαιτείται η χρήση άλλων δικαιολογητικών πέραν των βιομετρικών τους στοιχείων. Πέρα από όλα αυτά που πρέπει να ληφθούν υπόψιν για την εύρυθμη λειτουργία ενός βιομετρικού συστήματος (επιλογή κατάλληλου βιομετρικού στοιχείου, συνθήκες εφαρμογής κ.α), θα πρέπει να ληφθούν και όλα εκείνα τα μέτρα τα οποία θα προστατεύουν το βιομετρικό σύστημα από διάφορες επιθέσεις. Η προστασία των προτύπων είναι ιδιαίτερα κρίσιμη καθώς η παραβίαση τους είναι μόνιμη στην περίπτωση που αποθηκεύονται χωρίς να υποστούν κάποιον μετασχηματισμό πρώτα. Στο επόμενο κεφάλαιο θα περιγραφούν διάφοροι τύποι επιθέσεων που μπορούν να συμβούν σε ένα βιομετρικό σύστημα και θα παρουσιαστούν διάφορες τεχνολογίες προστασίας των προτύπων.

ΚΕΦΑΛΑΙΟ 2

Ασφάλεια Βιομετρικών Συστημάτων

ΕΙΣΑΓΩΓΗ

Ένα βιομετρικό σύστημα μπορεί να είναι ευάλωτο λόγω επιθέσεων προς αυτό, αλλά και από κακή σχεδίαση. Ένα σύστημα που χαρακτηρίζεται από υψηλό δείκτη λανθασμένων αποδοχών (False Acceptance Rate) είναι πιθανό να παραβιαστεί έπειτα από έναν αριθμό βιομετρικών χαρακτηριστικών που θα παρουσιαστούν τυχαία στο σύστημα, καθώς θα βρεθεί κάποιο που να ταιριάζει. Αυτό μπορεί να συμβεί ακόμα και αν δεν υπάρχει κάποιος που να επιθυμεί να επιτεθεί στο σύστημα, αυτή η περίπτωση ονομάζεται επίθεση μηδενικής-προσπάθειας (zero-effort attack). Στο σχήμα 7 παρουσιάζεται το περίγραμμα ενός βιομετρικού συστήματος και αναγράφονται οι πιθανές επιθέσεις που μπορούν να συμβούν σε αυτό, ανάλογα με την τοποθεσία.



Σχήμα 7: Τρόποι επίθεσης σε ένα βιομετρικό σύστημα.

Οι περισσότερο πιθανές επιθέσεις που μπορεί να γίνουν εναντίον των διαφορετικών μονάδων ενός βιομετρικού συστήματος είναι οι παρακάτω [3]:

➔ Αισθητήρας

- Επίθεση αντίγραφου (spoofing attack) ή επίθεση μίμησης (mimicry attack): ανάλογα αν μιλάμε για ανατομικά βιομετρικά στοιχεία ή για βιομετρικά στοιχεία που βασίζονται στην συμπεριφορά. Αυτές οι επιθέσεις αντιγράφουν με διάφορα μέσα και μεθόδους, το βιομετρικό στοιχείο του εγγεγραμμένου χρήστη και το χρησιμοποιούν για να ξεγελάσουν το σύστημα.
- Επίθεση επιβολής βίας: το πραγματικό βιομετρικό παρουσιάζεται αλλά χωρίς την θέληση του χρήστη πχ ένας απατεώνας επιβάλλει σε κάποιον χρήστη κάτω από κάποιου είδους απειλή, να του δώσει πρόσβαση στο σύστημα
- Αντικατάσταση συσκευής: αντικατάσταση της αυθεντικής συσκευής καταγραφής με μία παραποιημένη ή άλλη συσκευή.
- Άρνηση εξυπηρέτησης (Denial of service): μαζικές επιθέσεις στο σύστημα που έχουν σαν συνέπεια την μη λειτουργία του συστήματος.

➔ Ο εξαγωγέας χαρακτηριστικών θα μπορούσε να είναι υπό τον έλεγχο κάποιου και να παράγει προεπιλεγμένα χαρακτηριστικά, με το να εισάγει δικά του δεδομένα.

➔ Ο συγκριτής μπορεί να είναι στόχος, έχοντας σαν σκοπό την παραγωγή ψευδών βαθμολογιών. Αυτό μπορεί να γίνει με διάφορους τρόπους:

- Τροποποίηση των βαθμολογιών ομοιότητας: αποκτώντας και αλλάζοντας την τιμή μίας βαθμολογίας ομοιότητας πριν επηρεάσει την απόφαση
- Επίθεση με επανάληψη: καταγεγραμμένα πραγματικά δεδομένα εμφυτεύονται στο κανάλι.
- Αντικατάσταση κάποιου μέρους: αλλαγή ενός από τα hardware/software μέρη με σκοπό να ελέγχεται η συμπεριφορά του.
- Επίθεση αναρρίχησης (Hill climbing attack): κλιμακούμενη επαναλαμβανόμενη επίθεση που μπορεί να επιτευχθεί όταν κάποιος έχει πρόσβαση στις βαθμολογίες ομοιότητας. Πιο συγκεκριμένα, σε ένα δείγμα επιφέρεται μία μικρή τροποποίηση και αν η βαθμολογία ομοιότητας βελτιωθεί, τότε η τροποποίηση διατηρείται, αλλιώς απορρίπτεται. Αυτή η διαδικασία επαναλαμβάνεται μέχρι η βαθμολογία ομοιότητας κάποια στιγμή να ξεπεράσει το ορισμένο όριο αποδοχής.

- ➔ Κανάλια επικοινωνίας που συνδέουν τα διάφορα μέρη ενός βιομετρικού συστήματος, όπως το κανάλι μεταξύ του αισθητήρα και του εξαγωγέα χαρακτηριστικών, μεταξύ του εξαγωγέα χαρακτηριστικών και του συγκριτή, μεταξύ της βάσης δεδομένων και του συγκριτή, και μεταξύ του συγκριτή και της εφαρμογής, μπορεί να παρακολουθούνται και να ελέγχονται από μη εξουσιοδοτημένα άτομα. Ανάμεσα στις πιθανές επιθέσεις είναι:
    - παθητική παρακολούθηση (eavesdropping attack): η κρυφή παρακολούθηση της μετάδοσης βιομετρικών δεδομένων.
    - επίθεση ενδιάμεσου ατόμου (Man-in-the-middle attack): ένας απατεώνας είναι ικανός να παραποιεί τα μηνύματα που ανταλλάσσονται μεταξύ δύο σημείων χωρίς να γνωρίζουν οι συμμετέχοντες ότι η γραμμή έχει παραβιαστεί.
    - επίθεση ωμής βίας (Brute force attack): εξαντλητική παρουσίαση ενός μεγάλου συνόλου από βιομετρικά δείγματα προς το σύστημα αναγνώρισης με σκοπό να βρεθεί ένα το οποίο να δουλεύει.
    - επίθεση επανάληψης (Replay attack)
    - επίθεση αναρρίχησης (hill climbing attack)
    - τροποποίηση της βαθμολογίας ταύτισης
    - τροποποίηση της απόφασης
- ➔ Βάση δεδομένων: ανάγνωση προτύπων, τροποποίηση ενός ή περισσότερων εγγραφών στην βάση δεδομένων, αντικατάσταση προτύπων, αλλαγή της συσχέτισης μεταξύ του ID και των βιομετρικών δεδομένων, είναι μερικές πολύ απειλητικές επιθέσεις.

Αξίζει να σημειωθεί ότι τα αυτόματα συστήματα αναγνώρισης με βιομετρία, είναι και αυτά ευάλωτα κατά την φάση της εγγραφής, σε επιθέσεις που σχετίζονται με τον έλεγχο ταυτοτήτων, καθώς πλαστές κάρτες ID μπορεί να χρησιμοποιηθούν κατά την φάση την εγγραφής.

Διαφορετικού τύπου επιθέσεις ή ευάλωτα σημεία απαιτούν και τα ανάλογα αντίμετρα. Για παράδειγμα τεχνικές ανίχνευσης ζωντανού δείγματος (liveness detection techniques), μπορούν να χρησιμοποιηθούν σαν αντίμετρο εναντίον των ψεύτικων αντιγράφων, η επίθεση αναρρίχησης (hill climbing) μπορεί να αντιμετωπιστεί χρησιμοποιώντας κρυπτογραφημένα κανάλια ή συγκρίνοντας βαθμολογίες που έχουν κβαντοποιημένες τιμές, η παθητική παρακολούθηση

αντιμετωπίζεται χρησιμοποιώντας ασφαλή κανάλια κτλ. Μερικοί κίνδυνοι μπορεί να εξαλειφθούν εξαιτίας της υλοποίησης του συστήματος. Ανάλογα με το μέρος όπου γίνεται η αποθήκευση και η σύγκριση, υπάρχουν και διαφορετικές απαιτήσεις ασφαλείας.

Η χρήση πολυτροπικών βιομετρικών συστημάτων μπορεί να βελτιώσει τον βαθμό ασφαλείας ενός βιομετρικού συστήματος αναγνώρισης. Η αύξηση του αριθμού των διαπιστευτηρίων που απαιτούνται για αναγνώριση, μπορεί να αποτρέψει μία επίθεση αντιγράφου, αυξάνοντας την ακρίβεια ταύτισης και την πληθυσμιακή κάλυψη. Από την άλλη μεριά, ένα πολυτροπικό βιομετρικό σύστημα αυξάνει το κόστος και την πολυπλοκότητα της εφαρμογής.

2.1 Προστασία βιομετρικών προτύπων – Τεχνολογίες βελτίωσης της ασφάλειας και της ιδιωτικότητας

Η μη εξουσιοδοτημένη πρόσβαση στα βιομετρικά πρότυπα είναι ανάμεσα στις πιο επικίνδυνες απειλές για την ιδιωτικότητα των χρηστών και την ασφάλεια. Παρ' ότι υπήρχε η αντίληψη ότι δεν είναι εφικτό να ανακατασκευάσει κανείς το αρχικό βιομετρικό στοιχείο από το αντίστοιχο πρότυπο, κάποια παραδείγματα που έχουν εμφανιστεί στην βιβλιογραφία, καταρρίπτουν την αντίληψη αυτή. Αποδεικνύεται ότι η γνώση ενός βιομετρικού προτύπου προσώπου μαζί με την βαθμολογία ομοιότητας, μπορεί να οδηγήσει σε ανακατασκευή προσώπου. Ακόμη προτείνεται ένας αποδοτικός αλγόριθμος για την παραγωγή δακτυλικού αποτυπώματος από τις αντίστοιχες μικρολεπτομέρειες, όπως επίσης υπάρχει παράδειγμα όπου έχει επιτευχθεί αντίγραφο ίριδας από πρότυπο.

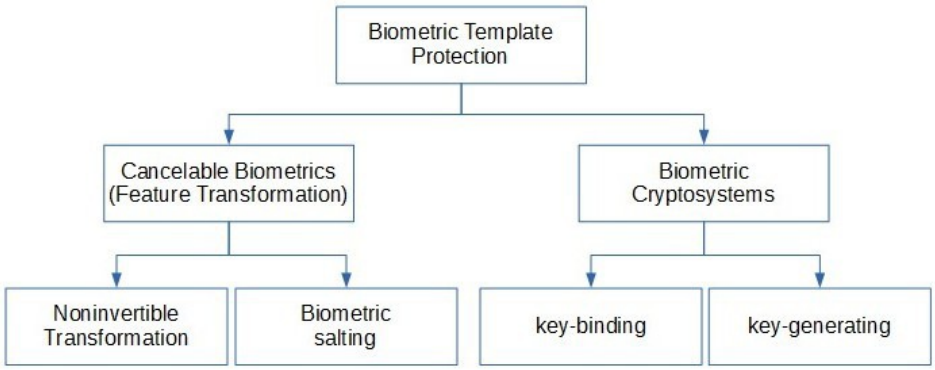
Το πρόβλημα είναι ότι οι τυπικοί αλγόριθμοι κρυπτογράφησης δεν υποστηρίζουν την σύγκριση των βιομετρικών προτύπων στον κρυπτογραφημένο χώρο. Καθώς το δείγμα είναι ελαφρώς διαφορετικό κάθε φορά που γίνεται αναγνώριση, η κρυπτογραφημένη μορφή θα είναι επίσης διαφορετική και έτσι δεν μπορεί να γίνει άμεση σύγκριση με το πρότυπο. Πρέπει να προηγηθεί αποκρυπτογράφηση του προτύπου που είναι στην βάση, για να μπορέσει να γίνει εφικτή η σύγκριση, κάτι το οποίο δεν είναι ιδιαίτερα ασφαλές.

Έτσι, η αποθήκευση βιομετρικών προτύπων δεν είναι αρκετά ασφαλής και στην περίπτωση που παραβιαστεί ένα πρότυπο, είναι επιθυμητή η ανάκληση ή η ανανέωση του. Επίσης, θα ήταν επιθυμητό να μπορεί κανείς να αποκτήσει από τα ίδια βιομετρικά χαρακτηριστικά διαφορετικά κλειδιά για να έχει πρόσβαση σε διαφορετικές τοποθεσίες, είτε φυσικές είτε λογικές, έτσι ώστε να αποφεύγεται η μη εξουσιοδοτημένη ανίχνευση των κινήσεων.

Ένας τρόπος προστασίας προτύπων θα πρέπει να εκπληρώνει τις παρακάτω ιδιότητες:

- Ανανέωση: θα πρέπει να είναι δυνατή η ανάκληση ενός παραβιασμένου πρότυπου και η επανέκδοση ενός νέου βασισμένου στα ίδια βιομετρικά δεδομένα
- Πολυμορφία: κάθε πρότυπο που παράγεται από ένα βιομετρικό στοιχείο δεν θα πρέπει να ταιριάζει με τα προγενέστερα που δημιουργήθηκαν από τα ίδια βιομετρικά δεδομένα. Αυτή η ιδιότητα απαιτείται για να προστατευθεί η ιδιωτικότητα του χρήστη (Unlinkability).
- Ασφάλεια: θα πρέπει να είναι αδύνατο ή τουλάχιστον υπολογιστικά πολύ δύσκολο να αποκτηθεί το αρχικό βιομετρικό πρότυπο (irreversibility), από αυτό που είναι αποθηκευμένο και προστατευμένο. Αυτή η ιδιότητα χρειάζεται για να αποτρέπει κάποιον κακόβουλο από το να δημιουργεί ψεύτικα βιομετρικά χαρακτηριστικά από κλεμμένα πρότυπα.
- Απόδοση: Οι δείκτες λαθών της βιομετρικής αναγνώρισης, όπως ο δείκτης λανθασμένης Απόρριψης (False Rejection Rate) ή ο δείκτης λανθασμένης Αποδοχής (False Acceptance Rate) δεν θα πρέπει να χειροτερεύουν σημαντικά με την εφαρμογή του τρόπου προστασίας προτύπων, σε σχέση με την προσέγγιση χωρίς προστασία.

Ο σχεδιασμός ενός τρόπου προστασίας προτύπων που να ικανοποιεί κάθε μία από τις προαναφερθείσες ιδιότητες δεν είναι εύκολη διαδικασία, κυρίως εξαιτίας της αναπόφευκτης ενδοατομικής μεταβλητότητας που παρουσιάζει κάθε βιομετρικό στοιχείο. Τα τελευταία χρόνια, πολλές διαφορετικές λύσεις έχουν ήδη προταθεί για την παραγωγή ασφαλών και ανανεώσιμων προτύπων, οι οποίες μπορούν να ενταχθούν σε δύο βασικές κατηγορίες: βιομετρικά κρυπτοσυστήματα και μετασχηματισμού των χαρακτηριστικών.

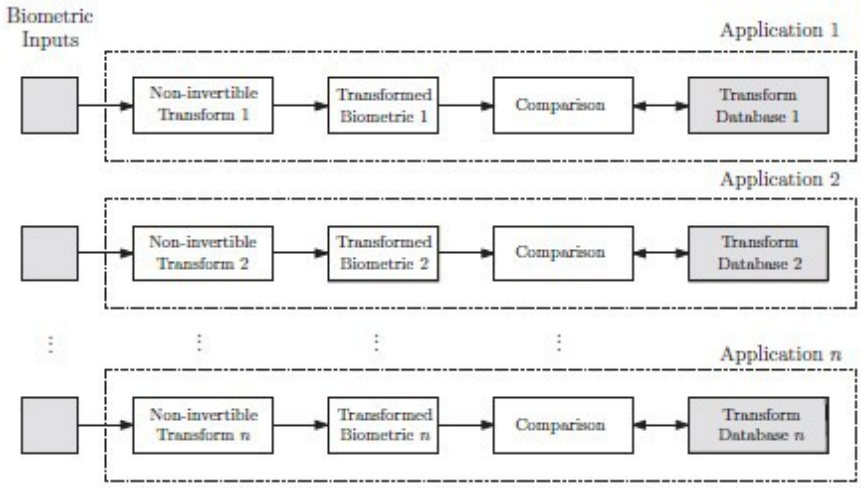


Σχήμα 8: Κατηγορίες προστασίας βιομετρικών προτύπων.

2.1.1 Μετασχηματισμοί χαρακτηριστικών για την προστασία προτύπων

Στην προσέγγιση μετασχηματισμού των χαρακτηριστικών (feature transformation), εφαρμόζεται στον αρχικό βιομετρικό χώρο (στην αρχική εικόνα δηλαδή) ή στο χώρο των χαρακτηριστικών (στο σύνολο των χαρακτηριστικών - feature set), μία συνάρτηση που βασίζεται σε κάποιες παραμέτρους, οι οποίες μπορούν να χρησιμοποιηθούν σαν κλειδί, για να παραχθεί είτε ένα μετασχηματισμένο βιομετρικό, είτε μετασχηματισμένα διανύσματα χαρακτηριστικών. Η σύγκριση έπειτα γίνεται στον μετασχηματισμένο χώρο. Η εφαρμοζόμενη συνάρτηση μπορεί να είναι αντιστρέψιμη, έχοντας σαν αποτέλεσμα μία προσέγγιση αλατισμού (salting), όπου η ασφάλεια βασίζεται στην προστασία των παραμέτρων της συνάρτησης, ή να είναι μη-αντιστρέψιμη, οπότε εφαρμόζεται μία μονόδρομη συνάρτηση στο πρότυπο και είναι υπολογιστικά δύσκολο να αντιστραφεί η συνάρτηση ακόμα και αν οι παράμετροι του μετασχηματισμού γίνουν γνωστές. Η χρήση μεθόδων που ανήκουν στην πρώτη κατηγορία συνήθως έχουν σαν αποτέλεσμα χαμηλούς δείκτες λανθασμένης αποδοχής (false acceptance rates), αλλά αν το συγκεκριμένο κλειδί ενός χρήστη παραβιαστεί, το πρότυπο του χρήστη δεν είναι πλέον ασφαλές εξαιτίας της δυνατότητας αντιστροφής του μετασχηματισμού. Αντίθετα, όταν χρησιμοποιούνται μη-αντιστρέψιμοι μετασχηματισμοί, ακόμα και αν το κλειδί γίνει γνωστό, δεν μπορεί να αποκτηθεί κάποια σημαντική πληροφορία για το πρότυπο, παρέχοντας έτσι καλύτερη ασφάλεια από αυτή που έχουμε με την προσέγγιση αλατισμού (salting). Πιο συγκεκριμένα, η ασφάλεια των επιλογών που βασίζονται σε μη-αντιστρέψιμους μετασχηματισμούς, βασίζεται στην δυσκολία αντιστροφής του μετασχηματισμού για την απόκτηση των αρχικών βιομετρικών δεδομένων. Ακόμα, σε αντίθεση με τις προσεγγίσεις κρυπτοσυστήματος, τα μετασχηματισμένα πρότυπα μπορούν να παραμείνουν στο ίδιο πεδίο τιμών - χαρακτηριστικών όπως και τα αρχικά,

επιτρέποντας έτσι την χρήση τυπικών συγκριτών για να διεκπεραιώσουν την σύγκριση στον μετασχηματισμένο χώρο. Αυτό επιτρέπει την επίτευξη παρόμοιων αποδόσεων με τις απροστάτευτες προσεγγίσεις. Επιπλέον, εκτός από τα προτερήματα στην απόδοση που υπάρχουν από την χρήση τυπικών συγκριτών στον μετασχηματισμένο χώρο, οι προσεγγίσεις μετασχηματισμού συνήθως έχουν σαν αποτέλεσμα βαθμολογίες ομοιότητας οι οποίες μπορούν να χρησιμοποιηθούν σε πολυτροπικές-βιομετρικές (multi-biometric) προσεγγίσεις. Έτσι, η χρήση προσεγγίσεων μετασχηματισμού για προστασία προτύπων σε πολυτροπικά βιομετρικά συστήματα (multi-biometric systems) επιτρέπει είτε τεχνικές ενοποίησης βαθμολογιών (score level fusion techniques) είτε τεχνικές ενοποίησης αποφάσεων (decision level fusion techniques). Οι τελευταίες είναι λιγότερο αποτελεσματικές αλλά μόνο αυτές μπορεί να εφαρμοστούν όταν έχουμε να κάνουμε με βιομετρικά κρυπτοσυστήματα.



Σχήμα 9: Η κεντρική ιδέα μη αντιστρέψιμων μετασχηματισμών [20]

Η συνάρτηση μετασχηματισμού θα πρέπει να είναι σχεδιασμένη με τέτοιο τρόπο, ώστε οι ενδοατομικές και οι διατομικές αποστάσεις στον μετασχηματισμένο χώρο να είναι παρόμοιες με τις αντίστοιχες στον αρχικό χώρο, με τέτοιο τρόπο που να παραμένει η διακριτότητα των χαρακτηριστικών. Ακόμη ο μετασχηματισμός θα πρέπει να είναι μη-αντιστρέψιμος. Δυστυχώς, είναι δύσκολο να σχεδιαστούν συναρτήσεις μετασχηματισμού που να διατηρούν ταυτόχρονα την διακριτότητα των προτύπων και τις μη αντιστρέψιμες ιδιότητες μαζί. Ακόμη, η ενδελεχής ανάλυση της ασφάλειας που παρέχει η μη αντιστρεψιμότητα της μεθόδου είναι πολύ δύσκολη, ειδικά όταν ο αλγόριθμος μετασχηματισμού και τα σχετικά κλειδιά/παράμετροι παραβιαστούν. Έτσι, μεγάλη προσοχή πρέπει να δοθεί κατά τον σχεδιασμό και την ανάλυση τέτοιων προσεγγίσεων.

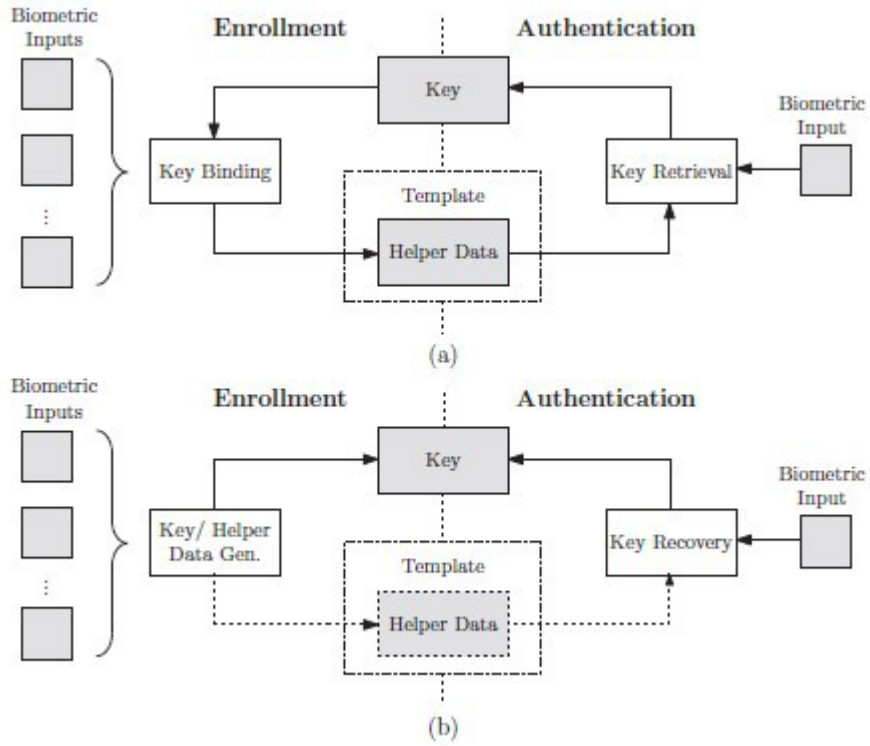
Αξίζει να σημειώσουμε ότι, όταν χρησιμοποιούμε τεχνικές παραμόρφωσης προτύπων, είτε με αντιστρέψιμους είτε με μη-αντιστρέψιμους μετασχηματισμούς, μόνο τα παραμορφωμένα δεδομένα αποθηκεύονται στην βάση δεδομένων. Αυτό συνεπάγεται ότι ακόμα και αν παραβιαστεί η βάση δεδομένων, θεωρητικά, αν τα κλειδιά δεν είναι προσβάσιμα και ο μετασχηματισμός είναι εντελώς μη αντιστρέψιμος, τα βιομετρικά δεδομένα δεν μπορούν να εξαχθούν. Ακόμα, διαφορετικά πρότυπα μπορούν να δημιουργηθούν από τα αρχικά δεδομένα, απλά αλλάζοντας τις παραμέτρους που εφαρμόζονται στους μετασχηματισμούς.

2.1.2 Βιομετρικά κρυπτοσυστήματα για την προστασία προτύπων

Τα βιομετρικά κρυπτοσυστήματα (BCSs) είναι σχεδιασμένα για να ενσωματώνουν με ασφάλεια ένα ψηφιακό κλειδί μαζί με βιομετρικά δεδομένα ή να παράγουν ένα ψηφιακό κλειδί από βιομετρικά δεδομένα, προσφέροντας έτσι λύσεις για την απελευθέρωση κλειδιού έπειτα από βιομετρική ταύτιση και προστασία βιομετρικών προτύπων. Τα κλειδιά μπορεί ακόμη να είναι κλειδιά κλασικής συμμετρικής κρυπτογραφίας, όπου η φύλαξη τους είναι προβληματική. Αντικαθιστώντας με αυτόν τον τρόπο τις λύσεις απελευθέρωσης κλειδιού βάσει κάποιου κωδικού, έχουμε σημαντικά οφέλη ως προς την ασφάλεια. Τα βιομετρικά κρυπτοσυστήματα παρέχουν τα μέσα για να υιοθετηθούν κρυπτογραφικά πρωτόκολλα με βιομετρικά δεδομένα, τα οποία είναι από την φύση τους δεδομένα με θόρυβο (noisy data). Υπάρχουν δύο κατηγορίες: 1)παραγωγής κλειδιού (key-generating) όπου δυαδικά κλειδιά δημιουργούνται από τα βιομετρικά χαρακτηριστικά και 2)ενσωμάτωσης κλειδιού (key-binding), όπου ένα τυχαίο κλειδί ενσωματώνεται με ασφάλεια στα βιομετρικά δεδομένα.

Η πλειοψηφία των βιομετρικών κρυπτοσυστημάτων απαιτεί την ύπαρξη κάποιων δημόσιων πληροφοριών ή αλλιώς βοηθητικά δεδομένα (helper data) τα οποία χρησιμοποιούνται για την απόκτηση ή την παραγωγή κλειδιών. Εξαιτίας της ενδοατομικής μεταβλητότητας που παρουσιάζουν τα περισσότερα βιομετρικά χαρακτηριστικά, δεν είναι δυνατή η απευθείας εξαγωγή κλειδιών. Τα βοηθητικά δεδομένα, τα οποία δεν θα πρέπει να αποκαλύπτουν σημαντικές πληροφορίες σχετικά με τα αρχικά βιομετρικά πρότυπα, βοηθούν στην ανακατασκευή των κλειδιών. Η βιομετρική σύγκριση γίνεται έμμεσα, με το να επαληθεύεται η εγκυρότητα των κλειδιών, οπότε το αποτέλεσμα της διαδικασίας αυθεντικοποίησης είναι είτε ένα κλειδί, είτε ένα μήνυμα λάθους. Καθώς η επαλήθευση των κλειδιών, γίνεται με βιομετρική σύγκριση στον κρυπτογραφημένο χώρο, τα βιομετρικά κρυπτοσυστήματα χρησιμοποιούνται σαν μέσο προστασίας βιομετρικών προτύπων και παράλληλα παρέχουν την δυνατότητα απελευθέρωσης κλειδιού. Ανάλογα με τον τρόπο που δημιουργούνται τα βοηθητικά δεδομένα, τα βιομετρικά

κρυπτοσυστήματα ανήκουν σε μία από τις δύο κατηγορίες: συστήματα ενσωμάτωσης κλειδιού και συστήματα παραγωγής κλειδιού.



Σχήμα 10: Βασικό σχεδιάγραμμα λειτουργίας κρυπτοσυστημάτων a)ενσωμάτωσης κλειδιού b)παραγωγής κλειδιού [20]

Ένα σύστημα ενσωμάτωσης κλειδιού (key binding system) μπορεί να χρησιμοποιηθεί για να προστατεύσει ένα βιομετρικό πρότυπο με την βοήθεια ενός δυαδικού κλειδιού, ασφαλίζοντας έτσι ένα σύστημα βιομετρικής αναγνώρισης, ή για να απελευθερώσει ένα κρυπτογραφικό κλειδί μόνο όταν ο κάτοχος του κλειδιού παρουσιάσει ένα συγκεκριμένο βιομετρικό χαρακτηριστικό. Και στις δύο αυτές περιπτώσεις ένα μυστικό κλειδί, ανεξάρτητα από το ποια βιομετρία θα χρησιμοποιηθεί, ενσωματώνεται κατά την διάρκεια της εγγραφής με ένα πρότυπο αναφοράς για να παραχθούν κάποια δεδομένα τα οποία είναι δημόσια και αποκαλούνται βοηθητικά δεδομένα (helper data). Από αυτά τα δεδομένα θα πρέπει να είναι αδύνατον ή υπολογιστικά πάρα πολύ δύσκολο να εξαχθούν πληροφορίες σχετικές με τα αρχικά βιομετρικά χαρακτηριστικά ή το κλειδί. Τα βοηθητικά δεδομένα στην συνέχεια χρησιμοποιούνται μαζί με τα βιομετρικά χαρακτηριστικά του δείγματος κατά την φάση της αναγνώρισης για να αποκτηθεί το μυστικό. Συνήθως, οι τρόποι αυτής της κατηγορίας είναι ικανοί να χειριστούν τις ενδοατομικές διαφορές, χρησιμοποιώντας κώδικες διόρθωσης λαθών (ECC).

Όμως, σε γενικές γραμμές δεν είναι εφικτό να χρησιμοποιηθούν εξελιγμένοι και αποκλειστικοί συγκριτές, με αποτέλεσμα να μειώνεται η ακρίβεια ταύτισης.

Σε ένα σύστημα παραγωγής κλειδιού, τα βοηθητικά δεδομένα προέρχονται μόνο από το βιομετρικό πρότυπο. Τα κλειδιά παράγονται απευθείας από τα βοηθητικά δεδομένα και ένα βιομετρικό δείγμα. Ενώ η αποθήκευση των βοηθητικών δεδομένων δεν είναι υποχρεωτική, η πλειοψηφία των προτεινόμενων σεναρίων παραγωγής κλειδιού τα αποθηκεύει. Αν τα σενάρια παραγωγής κλειδιού εξάγουν κλειδιά χωρίς την χρήση βοηθητικών δεδομένων, αυτά δεν μπορούν να ανανεωθούν στην περίπτωση παραβίασης. Τα βοηθητικά δεδομένα που προέρχονται από κάποιο σενάριο παραγωγής κλειδιού, αποκαλούνται επίσης “fuzzy extractors” ή “secure sketches”. Ένα fuzzy extractor εξάγει με αξιοπιστία ένα τυχαίο αλφαριθμητικό (string) από ένα βιομετρικό δείγμα που παίρνει σαν είσοδο, ενώ τα αποθηκευμένα βοηθητικά δεδομένα βοηθούν στην ανακατασκευή. Ενώ αντίθετα, σε ένα secure sketch, τα βοηθητικά δεδομένα εφαρμόζονται για να ανακτηθεί το αρχικό βιομετρικό πρότυπο.

Ορισμένες κεντρικές ιδέες για βιομετρικά κρυπτοσυστήματα μπορούν να εφαρμοστούν τόσο σε σενάρια παραγωγής κλειδιού όσο και σε σενάρια ενσωμάτωσης κλειδιού.

2.2 Επιθέσεις εναντίον των τεχνολογιών προστασίας προτύπων

Είδαμε σε προηγούμενη ενότητα, τις παραδοσιακές επιθέσεις που μπορούν να γίνουν σε ένα βιομετρικό σύστημα. Οι τεχνολογίες των βιομετρικών κρυπτοσυστημάτων και μετασχηματισμού χαρακτηριστικών, αποτρέπουν διάφορες παραδοσιακές επιθέσεις, ενώ σε ορισμένες εξακολουθούν να παραμένουν ευάλωτες. Τα πιο συνηθισμένα σημεία επίθεσης σε ένα βιομετρικό σύστημα φαίνονται στο σχήμα 7. Υπάρχουν ακόμα επιθέσεις που στοχεύουν ειδικά στην παραβίαση των τεχνολογιών προστασίας προτύπων.

Τα βιομετρικά κρυπτοσυστήματα και οι τεχνολογίες μετασχηματισμού χαρακτηριστικών, δεν αποτρέπουν τις επιθέσεις αντίγραφου (την παρουσία δηλαδή ψεύτικων αντιγράφων του βιομετρικού στοιχείου – spoofing). Όμως υπάρχουν άλλοι τρόποι για να ανιχνευτούν τυχόν ψεύτικα βιομετρικά στοιχεία (τεχνολογίες ανίχνευσης ζωντανού δείγματος - liveness detection). Το ίδιο συμβαίνει και για τις επιθέσεις επανάληψης. Οι επιθέσεις αντικατάστασης στα βιομετρικά κρυπτοσυστήματα είναι πιο δύσκολες σε σχέση με τα τυπικά βιομετρικά συστήματα, καθώς τα βιομετρικά πρότυπα είναι ενσωματωμένα με κρυπτογραφικά

κλειδιά ή έχουν χρησιμοποιηθεί για την δημιουργία βοηθητικών δεδομένων (όπου το αρχικό βιομετρικό πρότυπο έχει πλέον διαγραφεί). Οι επιθέσεις αντικατάστασης εναντίον των βιομετρικών κρυπτοσυστημάτων απαιτούν επιπρόσθετες γνώσεις (π.χ τα ενσωματωμένα κρυπτογραφικά κλειδιά στην περίπτωση των σεναρίων ενσωμάτωσης κλειδιού). Στην περίπτωση των μετασχηματισμών, οι επιθέσεις είναι εφικτές αν οι αντίπαλοι αποκτήσουν τις μυστικές παραμέτρους μετασχηματισμού ή τα μυστικά κλειδιά στις περιπτώσεις βιομετρικού αλατισμού (biometric salting). Καθώς η ανακατασκευή των αρχικών βιομετρικών προτύπων δεν πρέπει να είναι δυνατή και στις δύο ευρύτερες κατηγορίες προστασίας βιομετρικών προτύπων, αυτό κάνει την εύρεση των αρχικών βιομετρικών δεδομένων μια πολύ πολύπλοκη διαδικασία και έτσι είναι ανθεκτικά σε επιθέσεις απομίμησης (masquerade attacks). Οι δείκτες απόδοσης και στις δύο κατηγορίες προστασίας προτύπων, είναι μικρότεροι σε σύγκριση με τα τυπικά βιομετρικά συστήματα, πράγμα που κάνει τα βιομετρικά κρυπτοσυστήματα και μετασχηματισμού χαρακτηριστικών, ευάλωτα σε επιθέσεις λανθασμένης αποδοχής (false acceptance attacks). Σε αντίθεση με τις περιπτώσεις μετασχηματισμού χαρακτηριστικών, όπου σε ένα πιθανό σενάριο κάποιος μπορεί να τροποποιήσει την τελική απόφαση “ναι/όχι”, αυτό δεν είναι ιδιαίτερα εφικτό στα βιομετρικά κρυπτοσυστήματα, καθώς σε αυτά, αυτό που επιστρέφεται είναι ένα κλειδί και όχι μία δυαδική απόφαση (ενδιάμεσες επιθέσεις βαθμολογίας θα μπορούσαν όμως να υλοποιηθούν). Στον πίνακα.1 φαίνονται οι προτεινόμενες επιθέσεις ανάλογα με την τεχνολογία προστασίας προτύπων.

Στη συνέχεια παρουσιάζονται λίγο πιο παραστατικά τέσσερις τύποι επιθέσεων που μπορεί να γίνουν προς τεχνολογίες προστασίας προτύπων.

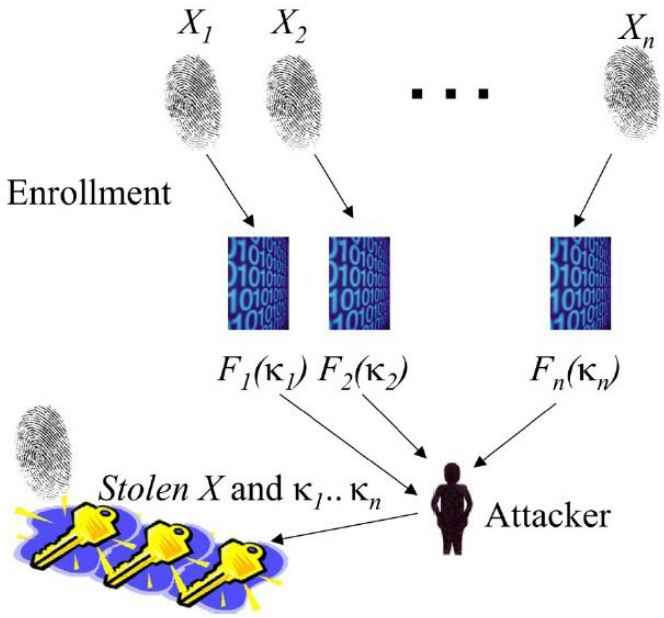
Πίνακας 1: Πιθανές επιθέσεις εναντίον τεχνολογιών προστασίας προτύπων [20]

Τεχνολογία	**Προτεινόμενη επίθεση**
Βιομετρικά κρυπτοσυστήματα	
Biometric encryption™	επίθεση ανάμιξης (blended substitution), επίθεση μέσω πολλαπλών εγγραφών (ARM), επίθεση απομίμησης (masquerade attack) μέσω hill climbing
Fuzzy commitment	επιθέσεις πάνω στους κώδικες διόρθωσης λαθών (ecc)
Shielding functions	επίθεση μέσω πολλαπλών εγγραφών (ARM)
Fuzzy vault	επίθεση ανάμιξης (blended substitution), επίθεση μέσω πολλαπλών εγγραφών (ARM), ανίχνευση σημείων chaff
Key-gen	επίθεση λανθασμένων αποδοχών, επίθεση απομίμησης (masquerade attack), επίθεση ωμής βίας (brute force)
Biometric hardened passwords	Παρατήρηση της κατανάλωσης ρεύματος
Μετασχηματισμού χαρακτηριστικών	
Non-invertible transforms	Τροποποίηση τελικής απόφασης, επίθεση μέσω πολλαπλών εγγραφών (ARM), επίθεση αντικατάστασης (έχοντας γνώση του μετασχηματισμού)
Biometric salting	Τροποποίηση τελικής απόφασης με κλεμμένο token, επίθεση λανθασμένων αποδοχών, επίθεση αντικατάστασης, επίθεση απομίμησης

2.2.1 Επίθεση μέσω Πολλαπλών Εγγραφών - Attack via record multiplicity - ARM)

Όταν κάποιος είναι εγγεγραμμένος σε πολλές διαφορετικές τοποθεσίες (όπου χρησιμοποιείται η ίδια μέθοδος προστασίας προτύπων) θα πρέπει να μην μπορεί να γίνει σύνδεση μεταξύ των προτύπων (unlinkability) και να μην είναι ευάλωτα τα πρότυπα σε συνδυασμούς. Στην περίπτωση που περιγράψαμε ο χρήστης εγγράφεται σε κάθε διαφορετική τοποθεσία και παρουσιάζει τα ίδια βιομετρικά δεδομένα X. Κάθε έγγραφή έχει το δικό της μυστικό κλειδί κ, έχοντας σαν αποτέλεσμα πολλές διαφορετικές κωδικοποιήσεις ($F_1(\kappa_1)$ έως $F_n(\kappa_n)$), οι οποίες

στην συνέχεια μεταδίδονται και αποθηκεύονται σε διάφορα συστήματα με την ίδια υλοποίηση. Σε μία Επίθεση Πολλαπλών Εγγραφών (Attack via Record Multiplicity (ARM)), ή αλλιώς επίθεση επαναχρησιμοποίησης (reusability attack) αν ένας επιτιθέμενος μπορεί να συλλέξει διάφορες από αυτές τις κωδικοποιήσεις, πιθανόν να μπορέσει να συσχετίσει τα δεδομένα που περιέχονται εντός της κωδικοποίησης για να βρει από ποια βάση προέρχονται ή σε μερικές περιπτώσεις να αποκτήσει το ίδιο το X και τα $\kappa_1 ... \kappa_n$.

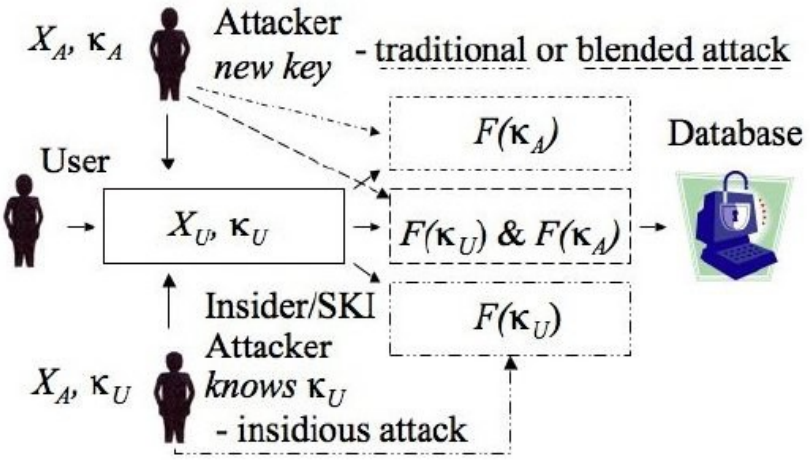


Σχήμα 11: Επίθεση πολλαπλών εγγραφών - Attack via Record Multiplicity (ARM) [22]

2.2.2 Επίθεση ανάμιξης - Blended Substitution Attacks

Σε μία επίθεση αντικατάστασης, ένας επιτιθέμενος αλλάζει τα περιεχόμενα μίας βιομετρικής εγγραφής, έχοντας κάποια γνώση ή και χωρίς, σχετικά με την εγγραφή ή τα βιομετρικά δεδομένα. Ο σκοπός της επίθεσης αυτής είναι να τοποθετηθεί μία πίσω-πόρτα (backdoor) στο πρότυπο για να χρησιμοποιηθεί από κάποιον άλλον εκτός από τον νόμιμο χρήστη του πρότυπου. Για ένα γενικό σύστημα προστασίας προτύπων, το σχήμα 12 δείχνει διάφορους τρόπους με τους οποίους μπορεί να γίνει αυτό. Ο χρήστης παρουσιάζει κατά την εγγραφή τα βιομετρικά δεδομένα X_U και ένα μυστικό κ_U. Αργότερα, ο επιτιθέμενος τοποθετεί ένα άλλο σύνολο από βιομετρικά δεδομένα X_A και ένα άλλο μυστικό κ_A (ή κ_U αν είναι γνωστό) στην θέση του πρότυπου του χρήστη. Τα δεδομένα του επιτιθέμενου μπορεί να τοποθετηθούν

απευθείας πριν από την κωδικοποίηση, είτε να είναι προ-κωδικοποιημένα και να τοποθετήθηκαν μέσα στο μήνυμα πριν (ή μετά) από την στιγμή που έγινε αποδεκτό στην βάση δεδομένων. Η βάση δεδομένων κρατάει μόνο τα δεδομένα του επιτιθέμενου. Τα πρότυπα που είναι ψηφιακά υπογεγραμμένα είναι μία μερική λύση.



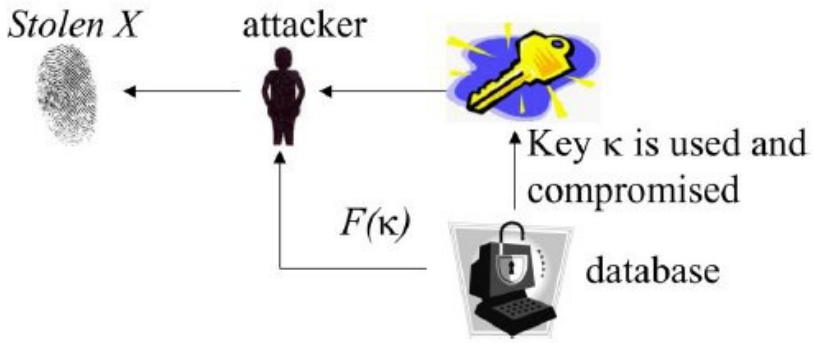
Σχήμα 12: Επίθεση αντικατάστασης και επίθεση ανάμιξης (blended substitution) [22]

Στην νέα επίθεση ανάμιξης (blended substitution), τα δεδομένα του χρήστη και του επιτιθέμενου συνδυάζονται σε ένα μοναδικό πρότυπο. Αν αναμιχθούν χρησιμοποιώντας το μυστικό κU αποκαλούμε την επίθεση αφανή ανάμιξη (insidious blending) καθώς δεν υπάρχει τρόπος να ανιχνευτεί ότι χρησιμοποιείται. Ένα αναμιγμένο πρότυπο επιτρέπει είτε στον χρήστη είτε στον επιτιθέμενο να αυθεντικοποιηθεί με την ίδια εγγραφή. Στην περίπτωση της παραδοσιακής αντικατάστασης ο επιτιθέμενος μπορεί να αυθεντικοποιηθεί αλλά ταυτόχρονα παράγει μία άρνηση εξυπηρέτησης στον πραγματικό χρήστη, που αυξάνει την πιθανότητα ανίχνευσης. Στην νέα αναμιγμένη αντικατάσταση ο επιτιθέμενος μπορεί να χρησιμοποιεί τις ίδιες εγγραφές παράλληλα με τον νόμιμο χρήστη.

Ακόμα πιο ανησυχητικό είναι ότι μία επίθεση αφανούς ανάμιξης (insidious blended attack) μπορεί να χρησιμοποιηθεί σαν πίσω-πόρτα (backdoor) στα βιομετρικά συστήματα αυθεντικοποίησης, είτε από κακά μέλη είτε από νομότυπα άτομα (για νομοταγή παρακολούθηση, ακόμα και με υπογεγραμμένα πρότυπα).

2.2.3 Επίθεση απόκρυφης αντιστροφής-κλειδιού - Surreptitious Key-Inversion Attack

Στα BFV (fuzzy vaults) και BE (biometric encryption), (δύο κεντρικές ιδέες προστασίας βιομετρικών προτύπων που ανήκουν στην κατηγορία των βιομετρικών κρυπτοσυστημάτων ενσωμάτωσης κλειδιού) ο δηλωμένος στόχος του συστήματος είναι να απελευθερώσει ένα μυστικό κλειδί. Για να είναι χρήσιμο, αυτό το κλειδί πρέπει να χρησιμοποιείται για κάτι και αν βγαίνει σε μορφή απλού κειμένου, τότε ανοίγει ο δρόμος για μία σειρά επιθέσεων (τρύπες ασφαλείας του λειτουργικού συστήματος, προγράμματα δούρειων ίππων, μη κρυπτογραφημένη μνήμη ή εικονική μνήμη, κ.α.). Ακόμα και αν απελευθερώνεται σε κρυπτογραφημένη μορφή, είναι ευάλωτο σε μία σειρά από εσωτερικές επιθέσεις, από άτομα υπεύθυνα του συστήματος. Το σχήμα 13 δείχνει αυτή την ενέργεια, με κωδικοποιημένα δεδομένα F(κ) και το μυστικό κ το οποίο υποκλάπηκε. Έπειτα, γνωρίζοντας το κ, ένας επιτιθέμενος μπορεί να αποκωδικοποιήσει τα δεδομένα του βιομετρικού πρότυπου X αναγνωρίζοντας τιμές που σχετίζονται με το κ.



Σχήμα 13: Η επίθεση Surreptitious Key-Inversion (SKI) [22]

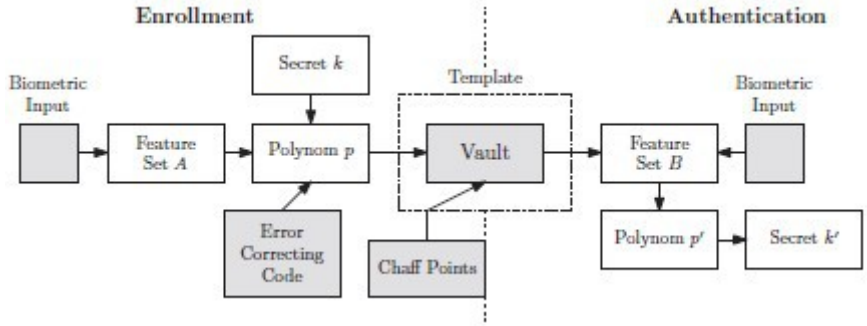
2.2.4 Αντίστροφη αναζήτηση πάνω σε ένα πρότυπο μετασχηματισμένων χαρακτηριστικών

Ακόμα και αν μία μέθοδος μετασχηματισμού χαρακτηριστικών χρησιμοποιεί έναν τεχνικά μη-αντιστρέψιμο μετασχηματισμό, ο επιτιθέμενος μπορεί να εκμεταλλευτεί το γεγονός ότι τα βιομετρικά χαρακτηριστικά έχουν έναν πεπερασμένο αριθμό από τιμές. Γνωρίζοντας αυτό το εύρος, από ένα δοκιμαστικό σύνολο βιομετρικών δεδομένων και δημιουργώντας διάφορα σύνολα χαρακτηριστικών, ο επιτιθέμενος εφαρμόζει τον μη αντιστρέψιμο μετασχηματισμό (τον οποίο με κάποιο τρόπο έμαθε) στα χαρακτηριστικά και δημιουργεί έναν πίνακα αναζήτησης (lookup table) για όλα τα μετασχηματισμένα χαρακτηριστικά. Έπειτα, κάνοντας μία αντίστροφη

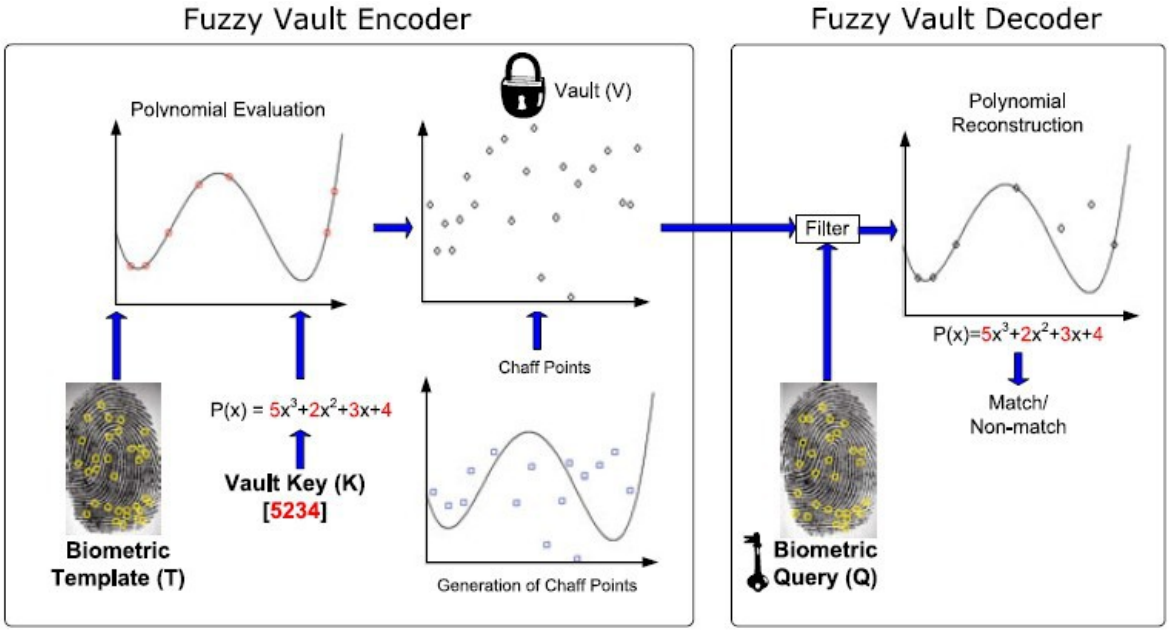
αναζήτηση, ο επιτιθέμενος μπορεί να εξάγει τα αρχικά αυθεντικά χαρακτηριστικά από ένα πρότυπο με μετασχηματισμένα χαρακτηριστικά.

2.3 Fuzzy vault

Ένα από τα πιο διαδεδομένα βιομετρικά κρυπτοσυστήματα λέγεται fuzzy vault, (“ασαφής θυρίδα ασφαλείας” θα μπορούσε να είναι η ελληνική μετάφραση), και παρουσιάστηκε από τους Juels και Sudan το 2002 [14]. Η κεντρική ιδέα του fuzzy vault, είναι να χρησιμοποιηθεί ένα μη ταξινομημένο σύνολο A για να κλειδώσει ένα μυστικό κλειδί k, και να δημιουργηθεί μία θυρίδα ασφαλείας (vault), που αναγράφεται ως V_A. Εάν κάποιο άλλο σύνολο B αλληλοεπικαλύπτει σε μεγάλο βαθμό το σύνολο A, τότε ανακατασκευάζεται το k, ξεκλειδώνει δηλαδή η θυρίδα ασφαλείας V_A. Η θυρίδα ασφαλείας (vault) δημιουργείται εφαρμόζοντας κωδικοποίηση πολυωνύμων και διόρθωση λαθών. Κατά την φάση της εγγραφής, επιλέγεται ένα πολυώνυμο p το οποίο κωδικοποιεί το κλειδί k με κάποιον τρόπο (π.χ. οι συντελεστές του πολυωνύμου παίρνουν τιμές από το k). Έπειτα, τα στοιχεία του A, μπαίνουν σαν είσοδος στο πολυώνυμο p, υπολογίζονται δηλαδή οι τιμές p(A). Στη συνέχεια, προστίθενται σημεία απόκρυψης (chaff points), έτσι ώστε να αποκρύψουν τα γνήσια σημεία του πολυωνύμου. Το σύνολο όλων των σημείων R, αποτελούν το πρότυπο. Για να επιτευχθεί επιτυχής αυθεντικοποίηση, ένα άλλο σύνολο B πρέπει να επικαλύπτεται ως έναν βαθμό με το σύνολο A, έτσι ώστε να εντοπιστεί ένας ικανοποιητικός αριθμός από σημεία εντός του συνόλου R που να ακουμπά πάνω στο p. Εφαρμόζοντας κώδικες διόρθωσης λαθών, το p μπορεί να ανακατασκευαστεί και κατά συνέπεια και το k. Η ασφάλεια όλου του εγχειρήματος βασίζεται πάνω στην αδυναμία ανακατασκευής του πολυωνύμου και το πλήθος από σημεία απόκρυψης. Το κύριο πλεονέκτημα αυτής της κεντρικής ιδέας του fuzzy vault, είναι ότι δεν απαιτεί ταξινομημένα σύνολα. Είναι ικανό να αντεπεξέρχεται στα μη ταξινομημένα σύνολα χαρακτηριστικών, όπως συμβαίνει με διάφορα βιομετρικά χαρακτηριστικά (πχ δακτυλικά αποτυπώματα). Διάφορες βελτιώσεις της αρχικής ιδέας έχουν προταθεί από τότε που παρουσιάστηκε. Κυρίως προτάσεις οι οποίες βοηθούν στην καλύτερη ευθυγράμμιση των δακτυλικών αποτυπωμάτων πριν από την σύγκριση και προτείνουν διαφορετικούς τρόπους δημιουργίας των σημείων απόκρυψης.



Σχήμα 14: Βασική λειτουργία του Fuzzy vault



Σχήμα 15: Προστασία ενός προτύπου δακτυλικών αποτυπωμάτων με μικρολεπτομέρειες χρησιμοποιώντας fuzzy vault

Εναντίον των fuzzy vaults, έχουν ανακαλυφθεί αρκετές επιθέσεις. Ο Chang et al. [7] παρουσίασαν μία παρατήρηση για το πώς να ξεχωρίζει κανείς τις μικρολεπτομέρειες (minutiae) από τα σημεία απόκρυψης (chaff) η οποία αποτελεί επίθεση για τα fuzzy vault βασισμένα σε δακτυλικά αποτυπώματα. Καθώς τα σημεία απόκρυψης δημιουργούνται ένα-ένα, αυτά που δημιουργούνται αργότερα τείνουν να εμφανίζουν μικρότερες κενές περιοχές γύρω τους (τα σημεία που είναι λύσεις του πολυωνύμου δηλαδή έχουν μεγαλύτερο κενό χώρο γύρω τους) και επαληθεύεται αυτό πειραματικά. Η ασφάλεια του fuzzy vault βασίζεται σε πολύ μεγάλο βαθμό στην μεθοδολογία δημιουργίας των σημείων απόκρυψης. Οι Scheirer και Boult [22] παρουσίασαν μία επίθεση μέσω πολλαπλών εγγραφών

(ARM). Αν αποκτηθούν πολλαπλά στιγμιότυπα ενός fuzzy vault (vault τα οποία ανήκουν στο ίδιο άτομο αλλά έχουν δημιουργηθεί από διαφορετικά κλειδιά), είναι πιθανό να επιτρέπουν την ανάκτηση των μικρολεπτομερειών. Γι' αυτό τον λόγο η αδυναμία ανίχνευσης κάποιου μεταξύ διαφορετικών βάσεων (unlinkability), χαρακτηριστικό που επιζητούμε να έχουν οι προστασίες βιομετρικών προτύπων, είναι ένα μεγάλο ζήτημα στην κατασκευή των fuzzy vaults. Μία μέθοδος για την προσθήκη σημείων απόκρυψης με μινιμαλιστική απώλεια εντροπίας προτάθηκε στο [15]. Μία επίθεση ωμής βίας (brute force) εναντίον των fuzzy vaults προτάθηκε στο [17]. Μία επίθεση παράνομης συμφωνίας (collusion attack) όπου ο επιτιθέμενος υποτίθεται ότι έχει στην κατοχή του πολλαπλές θυρίδες ασφαλείας (vaults) που είναι κλειδωμένες με το ίδιο κλειδί, παρουσιάζεται στο [18]. Παρουσιάζεται ο τρόπος με τον οποίο αναγνωρίζονται αποτελεσματικά τα σημεία απόκρυψης, που στη συνέχεια αφαιρούνται και ξεκλειδώνουν την θυρίδα ασφαλείας (vault). Σε αντίθεση με άλλα βιομετρικά κρυπτοσυστήματα (πχ το fuzzy commitment), στο fuzzy vault δεν παραμορφώνεται το αρχικό βιομετρικό πρότυπο, αλλά κρύβεται με την προσθήκη σημείων απόκρυψης (chaff), δηλαδή τα βοηθητικά δεδομένα περιέχουν τα αυθεντικά βιομετρικά χαρακτηριστικά (πχ μικρολεπτομέρειες) σε απλή μορφή. Ακόμα και αν παρέχονται πρακτικές τιμές ανάκτησης κλειδιών (κλειδιά ικανοποιητικού μεγέθους) από προτεινόμενα συστήματα, κακοποιοί ίσως να μπορούσαν να ξεκλειδώσουν θυρίδες ασφαλείας (vaults) στην περίπτωση που τα βοηθητικά δεδομένα δεν κρύβουν αποτελεσματικά τα αρχικά βιομετρικά δεδομένα, ειδικά αν οι επιτιθέμενοι έχουν στην κατοχή τους πολλά στιγμιότυπα ενός μοναδικού vault.

ΕΠΙΛΟΓΟΣ

Οι τεχνολογίες προστασίας προτύπων, δημιουργήθηκαν για να βελτιώσουν την ασφάλεια των βιομετρικών συστημάτων και για να ελαττώσουν τον κίνδυνο μόνιμης απώλειας των βιομετρικών στοιχείων των χρηστών. Οι τεχνολογίες αυτές, μετασχηματίζουν τα αρχικά πρότυπα, και επιτρέπουν την σύγκριση στον μετασχηματισμένο χώρο. Ακόμη είναι δυνατόν, σε περίπτωση που παραβιαστεί κάποιο πρότυπο, να δημιουργηθεί κάποιο άλλο, εφαρμόζοντας άλλον μετασχηματισμό. Προστέθηκε δηλαδή η δυνατότητα ανάκλησης. Επίσης, η εφαρμογή διαφορετικού μετασχηματισμού σε κάθε διαφορετική βάση ή εφαρμογή, έκανε πιο δύσκολη την ανιχνευσιμότητα ενός χρήστη μεταξύ διαφορετικών συστημάτων. Αυτός τουλάχιστον είναι ο απώτερος σκοπός, διότι όπως είδαμε, υπάρχουν επιθέσεις στις οποίες είναι ευάλωτες αυτές οι τεχνολογίες. Κάθε τεχνική προστασίας προτύπων έχει τα πλεονεκτήματα και τους περιορισμούς της, όσον

αφορά τον βαθμό προστασίας των προτύπων, το υπολογιστικό κόστος, τις απαιτήσεις σε χώρο αποθήκευσης, την εφαρμογή της σε διάφορα βιομετρικά χαρακτηριστικά και την ικανότητα να αντιμετωπίζει τις διαφορές που προκύπτουν στα βιομετρικά δεδομένα του ίδιου ατόμου (intra-class variations). Κάτι άλλο σημαντικό που συνέβη με τη χρήση των βιομετρικών κρυπτοσυστημάτων, είναι πως δόθηκε η δυνατότητα χρησιμοποίησης της βιομετρίας σε κρυπτογραφικά πρωτόκολλα, εξαιτίας της απελευθέρωσης κλειδιού, έπειτα από επιτυχή ταυτοποίηση. Στην επόμενη ενότητα θα παρουσιάσουμε μία ακόμη τεχνολογία προστασίας προτύπων για δακτυλικά αποτυπώματα, η οποία υποστηρίζει πως είναι ασφαλής, χωρίς μάλιστα να υπάρχει πτώση στην απόδοση ταύτισης.

ΚΕΦΑΛΑΙΟ 3

Ασφαλή Biotoken για δακτυλικά αποτυπώματα με δυνατότητα ανάκλησης

ΕΙΣΑΓΩΓΗ

Σε αυτό το κεφάλαιο θα παρουσιαστεί μία νέα τεχνολογία προστασίας προτύπων, η οποία συνδυάζει τις ιδέες του μετασχηματισμού των δεδομένων, την μέτρηση εύρωστων αποστάσεων και την κρυπτογραφία βιομετρικών δεδομένων. Έπειτα από κάποια μεγέθυνση, χωρίζει τα δεδομένα σε δύο μέρη, το δεκαδικό κομμάτι, το οποίο διατηρείται για τον υπολογισμό τοπικών αποστάσεων και το ακέραιο κομμάτι, το οποίο έπειτα κρυπτογραφείται.

3.1 Κρυπτογραφικά Ασφαλή Biotoken - Επισκόπηση

Ο υπολογισμός ενός Κρυπτογραφικά Ασφαλούς Biotoken χρησιμοποιεί έναν μετασχηματισμό στο σύνολο των χαρακτηριστικών και μπορεί να εφαρμοστεί σε ένα σύστημα δακτυλικών αποτυπωμάτων που βασίζεται στην εξαγωγή μικρολεπτομερειών. Οι μετασχηματισμοί μπορεί να είναι αντιστρέψιμοι, κάνοντας χρήση κρυπτογραφίας δημόσιων κλειδιών ή να είναι μη αντιστρέψιμοι στην περίπτωση που χρησιμοποιηθούν μονόδρομες συναρτήσεις (hash). Σε κάθε περίπτωση, ακόμα και αν παραβιαστούν οι παράμετροι του μετασχηματισμού, μαζί με τα μετασχηματισμένα δεδομένα, δεν υπάρχει κάποιος πρακτικός τρόπος για να αποκαλυφθούν τα αρχικά δεδομένα, αφαιρώντας έτσι τον κίνδυνο της ανακατασκευής σε περίπτωση που παραβιαστεί η κεντρική βάση δεδομένων. Οπωσδήποτε, αν χρησιμοποιηθεί μία αντιστρέψιμη έκδοση, η πρόσβαση στο ιδιωτικό κλειδί μαζί με τις παραμέτρους μετασχηματισμού και τα δεδομένα θα επέτρεπαν την αντιστροφή, αλλά αυτό το κλειδί δεν χρησιμοποιείται κατά την διαδικασία της επαλήθευσης και δεν χρειάζεται να είναι online.

Εν συντομία, τα βασικά πλεονεκτήματα της μεθόδου παρέχονται από μία προσέγγιση μετασχηματισμού η οποία παρέχει εύρωστους υπολογισμούς αποστάσεων για την υποστήριξη αξιόπιστης επαλήθευσης ενώ ταυτόχρονα υποστηρίζεται η ανάκληση, η αναγνώριση χωρίς ταυτοποίηση και μπορεί να υπάρχουν ταυτόχρονα χιλιάδες στιγμιότυπα σε χρήση χωρίς να υπάρχει η δυνατότητα σε κάποιον να συνδυάσει αυτά τα αποθηκευμένα δεδομένα και να ανακατασκευάσει τα αρχικά βιομετρικά δεδομένα. Μπορεί να εφαρμοστεί σχεδόν σε όλες τις βάσεις δεδομένων που βασίζονται σε σύνολα χαρακτηριστικών.

Μία εύρωστη μέτρηση απόστασης, είναι αυτή που εξ ορισμού, δεν επηρεάζεται έντονα από ακραίες τιμές (outliers). Αυτό σημαίνει ότι δεδομένα που δεν ταυτίζονται επειδή βρίσκονται εκτός των ορίων ενός παραθύρου, έχουν σταθερή ή μηδενική επίδραση. Πολλά συστήματα δακτυλικών αποτυπωμάτων χρησιμοποιούν εύρωστη απόσταση στην σύγκριση μικρολεπτομερειών (minutiae), αγνοώντας κάθε ταύτιση έξω από τα όρια ενός κουτιού με σταθερό μέγεθος.

Η κεντρική ιδέα παρουσιάζεται για πρώτη φορά στο [2] και γίνεται εφαρμογή σε ένα βιομετρικό σύστημα αναγνώρισης προσώπου. Η ιδέα είναι η εξής: έπειτα από έναν μετασχηματισμό που μεγεθύνει τα δεδομένα, στη συνέχεια αυτά χωρίζονται σε δεκαδικό (fraction) (r) και ακέραιο (integer) (q) μέρος. Ο ακέραιος, q, θεωρείται σταθερός και πρέπει να ταυτίζεται απόλυτα. Έτσι όταν αυτά τα πεδία q κρυπτογραφηθούν, θα εξακολουθούν να ταυτίζονται. Το άρθρο αυτό παρουσιάζει ένα θεώρημα, ότι αν η μεγέθυνση είναι σωστή, τότε η εύρωστη μέτρηση απόστασης πάνω στα αρχικά δεδομένα και η απόσταση που επήλθε μετά από την κωδικοποίηση, θα πρέπει να βελτιώνει την απόδοση σύγκρισης του συστήματος. Ο μετασχηματισμός και ο διαχωρισμός σε δύο μέρη, μπορεί επομένως να βελτιώσει την απόδοση.

Ενώ αριθμοί κινητής υποδιαστολής και δεκαδικά/ακέραιοι μπορεί να είναι κατάλληλοι για αναπαραστάσεις προσώπου, για τα δακτυλικά αποτυπώματα πρέπει να παραμείνουμε σε αναπαραστάσεις και πράξεις με ακεραίους. Πριν παρουσιαστεί ο μετασχηματισμός, θα πρέπει να γίνει συζήτηση για μία βοηθητική λειτουργία. Καθώς χωρίζουμε τα κωδικοποιημένα δεδομένα, θα γίνεται χρήση μίας πράξης τύπου modulo. Αλλά μία τέτοια πράξη μπορεί να πάρει στοιχεία που είναι κοντά μεταξύ τους και να τα χωρίσει σε μεγαλύτερες αποστάσεις. Έτσι, αναπτύχθηκε αυτό που αποκαλούμε αντικατοπτριζόμενο modulus (reflected modulus), ή rmod, έτσι ώστε κοντινά μεταξύ τους στοιχεία, να τοποθετούνται πάλι σε κοντινή απόσταση μετά από την εφαρμογή του rmod. Αυτό εφαρμόζεται μαζί με μία τεχνική αναδίπλωσης (folding technique) για να τοποθετηθούν τα αντικείμενα κοντά το ένα με το άλλο, έπειτα από την χαρτογράφηση (mapping). Έτσι, αν θέλουμε ένα παράθυρο μεγέθους E, τότε θέτουμε x = d % (E*2),

rmod(d,E) = x αν το x<E (3.1)

rmod(d,E) = (E*2) – x για όλες τις άλλες περιπτώσεις. (3.2)

Είναι εύκολο να δειχθεί ότι αν το x και y είναι τέτοια ώστε |x-y| < t τότε |rmod(x,z) – rmod(y,z)| < t. Καθώς το rmod δεν αυξάνει τις αποστάσεις μεταξύ των σημείων, όπως θα έκανε μία τυπική modulus πράξη, είναι πιο κατάλληλη για πολλούς από τους μετασχηματισμούς που απαιτούνται στα biotokens δημόσιου κλειδιού.

Πίνακας 2: Αντικατοπτριζόμενο modulo. Σύγκριση με την τυπική πράξη modulo.

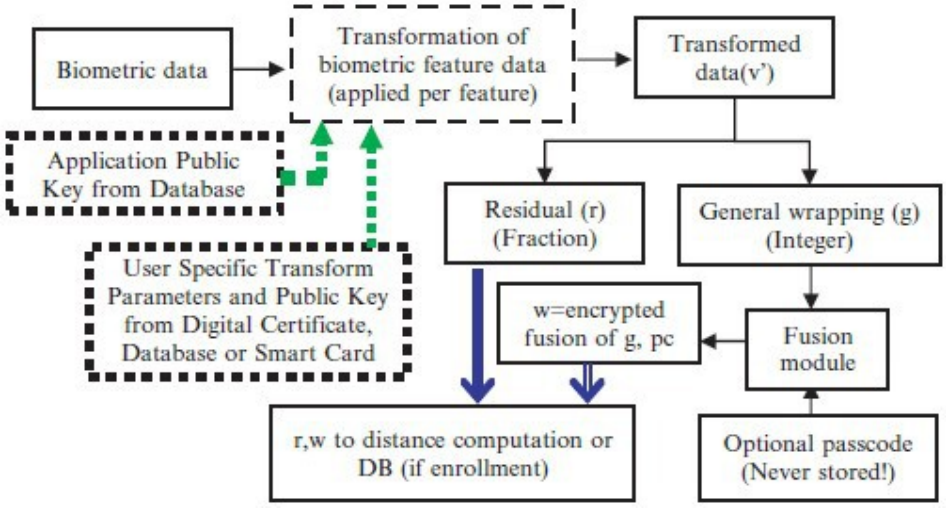
x	21	22	23	24	25	26	27	...	46	47	48	49	50	51
x mod 24	21	22	23	0	1	2	3	...	22	23	0	1	2	3
x rmod 24	21	22	23	24	23	22	21	...	2	1	0	1	2	3

Έτσι ορίστηκε ο μετασχηματισμός u' = (u – t) * s για κάθε πεδίο, με μεγέθυνση (s) και μετατόπιση (t). Έπειτα χωρίζουμε τα δεδομένα σε 2 μέρη, ένα q (πηλίκο - quotient), που πρέπει να ταιριάζει απόλυτα, ορίζοντας βασικά το “παράθυρο” για τον εύρωστο υπολογισμό, και το δεύτερο μέρος, r (αντικατοπτριζόμενο modulo - reflected modulus), που υποστηρίζει τον υπολογισμό της τοπικής απόστασης. Δοθείσης μίας παραμέτρου E, η οποία εξαρτάται από το εκτιμώμενο εύρος απόκλισης του u, ορίζουμε υπόλοιπο (residual) r = rmod(u',E), και πηλίκο (quotient) q=int(u'/E). Έπειτα μπορούμε να εφαρμόσουμε έναν μονόδρομο hash μετασχηματισμό ή έναν κρυπτογραφικό μετασχηματισμό στο q για να παράγουμε το w, το οποίο θα πρέπει να ταυτίζεται απόλυτα. Καθώς τα δεδομένα χωρίζονται σε r και q, το αποτέλεσμα αφήνει μία μη-κρυπτογραφημένη τιμή, r, εντός του “παραθύρου” στο οποίο μπορεί και υπολογίζεται η τοπική απόσταση, και έπειτα κρυπτογραφεί το μεγαλύτερο (και κατά συνέπεια πολύ σταθερό) μέρος, κρύβοντας έτσι αποτελεσματικά τα αρχικά δεδομένα με την τοποθεσία.

Για να διασφαλιστεί ότι τα βιομετρικά δεδομένα είναι προστατευμένα ακόμα και στην περίπτωση που οι παράμετροι “μετασχηματισμού” παραβιαστούν, πρέπει να διασφαλίσουμε ότι οι τιμές q είναι κρυπτογραφικά ασφαλείς. Για μεγάλα κομμάτια δεδομένων πχ doubles, η κρυπτογράφηση με δημόσιο κλειδί του q ίσως είναι αποτελεσματική. Για μικρά κομμάτια δεδομένων, όπως έχουμε στα δακτυλικά αποτυπώματα, πρέπει να γίνει επιπρόσθετη εργασία για να προστατευτούν τα δεδομένα. Για ένα μοναδικό μικρό πεδίο δεν μπορεί να γίνει τίποτα. Όπως θα δούμε στην συνέχεια, για μία συλλογή από πεδία, υπάρχει μία μίξη από κρυπτογράφηση δημόσιου κλειδιού και hashing που μπορεί να προστατεύσει πολλά μικρά πεδία και να βελτιώσει την συνολική απόδοση, επιτρέποντας ταυτόχρονα την επανέκδοση (reissue).

Υπάρχει ακόμα η δυνατότητα να προσθέσουμε μία κωδική φράση (passcode) του χρήστη. Αυτό το biotoken με τη χρήση κωδικής φράσης, παρέχει ασφάλεια δύο-παραγόντων. Οι παράγοντες μπερδεύονται μεταξύ τους και μόνο ένα biotoken αποθηκεύεται. Η συμπερίληψη της κωδικής φράσης παρέχει έναν ισχυρό τρόπο για ανάκληση, και κάνει το biotoken αυτό (με την κωδική φράση) χρήσιμο μόνο για επαλήθευση – παρέχοντας την καλύτερη προστασία από μία απειλή διπλού

εαυτού (doppelganger threat) και αυξάνει την προστασία της ιδιωτικότητας. Απειλή διπλού εαυτού, είναι η περίπτωση εκείνη όπου δύο διαφορετικά άτομα έχουν τόσο παρόμοια βιομετρικά στοιχεία που να μην μπορεί να γίνει διάκριση μεταξύ τους. Αυτή η προσέγγιση “επαλήθευσης μόνο”, είναι η μόνη πραγματική προστασία εναντίον της απειλής διπλού εαυτού (doppelganger) καθώς η χρήση μίας τεχνολογίας που υποστηρίζει ανάκληση, δεν μπορεί να σταματήσει κάποιον από το να αναζητήσει σε μία βάση δεδομένων έναν χρήστη με τον οποίο γίνεται κανονική ταύτιση. Αν τα βιομετρικά χαρακτηριστικά δύο διαφορετικών ανθρώπων ταυτίζονται στην πραγματική ζωή, τότε θα εξακολουθούν να ταυτίζονται και έπειτα από έναν μετασχηματισμό που υποστηρίζει ανάκληση. Έτσι μία τεχνολογία που δεν επιτρέπει την αναζήτηση και είναι μόνο για επαλήθευση, αποτελεί την καλύτερη άμυνα.



Σχήμα 16: Διάγραμμα με την διαδικασία παραγωγής ενός biotope, με προαιρετική χρήση κωδικολέξης [4]

Πριν παρουσιάσουμε αναλυτικά πώς υλοποιήθηκε το αρχικό biotoken βασισμένο σε δακτυλικά αποτυπώματα, θα συζητήσουμε για τον Bozorth συγκριτή πάνω στο οποίο βασίζεται.

3.1.2 Ο αλγόριθμος σύγκρισης Bozorth

Ο Bozorth συγκριτής παίρνει σαν είσοδο ένα αρχείο μικρολεπτομερειών (minutiae αρχείο) με x,y,Θ,q, όπου x,y είναι η τοποθεσία, Θ είναι η γωνία και q είναι η ποιότητα. Τέτοια αρχεία παράγει το πρόγραμμα MINDTCT, από τα εργαλεία της NIST, το οποίο παίρνει σαν είσοδο μία εικόνα ενός δακτυλικού αποτυπώματος, την

οποία επεξεργάζεται και στη συνέχεια δημιουργεί ένα αρχείο με μικρολεπτομέρειες. Δημιουργεί και άλλα βοηθητικά αρχεία (χάρτη κατεύθυνσης, χάρτη ποιότητας, χάρτη υψηλής καμπυλότητας, χάρτη αντίθεσης) τα οποία όμως δεν χρησιμοποιούνται από τον Bozorth. Ο αλγόριθμος σύγκρισης έχει τρία βασικά βήματα:

1. Κατασκευή ενδοδακτυλικών πινάκων σύγκρισης μικρολεπτομερειών (intra-fingerprint minutiae comparison tables) για το δακτυλικό αποτύπωμα του δείγματος και έναν πίνακα για κάθε gallery δακτυλικό αποτύπωμα (στη βάση), για να συγκριθούν μεταξύ τους.

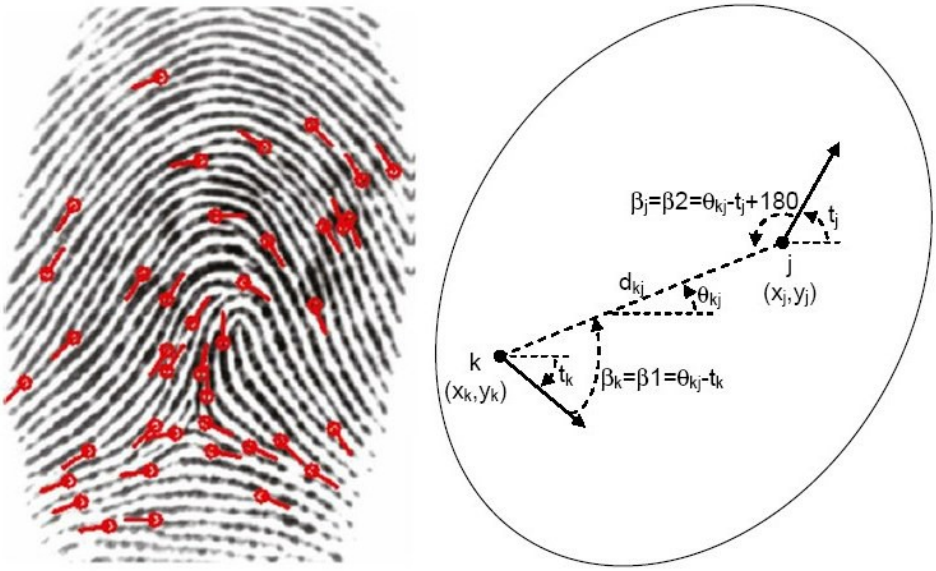
2. Κατασκευή διαδακτυλικού πίνακα συμβατότητας (inter-fingerprint pair-pair compatibility table), όπου το σύστημα συγκρίνει τον πίνακα σύγκρισης μικρολεπτομερειών του δείγματος με τον πίνακα σύγκρισης μικρολεπτομερειών της gallery και κατασκευάζει έναν νέο πίνακα συμβατότητας.

3. Σάρωση του διαδακτυλικού πίνακα συμβατότητας.

    α) Διάσχισε και σύνδεσε πεδία του πίνακα σε ένα δίκτυο/δάσος από συστάδες (clusters) που έχουν όμοιο προσανατολισμό και ίδια άκρα (endpoints) όταν συνδέονται ανά συστάδα.

    β) Ένωσε συμβατές συστάδες και υπολόγισε μία βαθμολογία ομοιότητας.

Για να κατασκευαστεί ένας ενδοδακτυλικός πίνακας σύγκρισης μικρολεπτομερειών, το σύστημα παίρνει τα ζεύγη από μικρολεπτομέρειες που είναι εντός μίας σταθερής απόστασης και παράγει μία εγγραφή στον πίνακα για αυτό το ζεύγος. Αυτή η εγγραφή του ζεύγους αποθηκεύει έξι σημαντικές πληροφορίες $\{k,j,d_{kj}, \beta_1, \beta_2, \theta_{kj}\}$. Όπου, (j,k) είναι οι δείκτες του κάθε σημείου του ζεύγους, $(d_{k,j})$ η απόσταση μεταξύ του ζεύγους, (β_1, β_2) οι γωνίες της κάθε μικρολεπτομέρειας σε σχέση με την γραμμή που τις ενώνει, και $(\theta_{k,j})$ ο συνολικός προσανατολισμός της γραμμής που ενώνει τα σημεία.



Σχήμα 17: Κατασκευή ενδοδακτυλικού πίνακα σύγκρισης μικρολεπτομερειών.

Για να κατασκευαστεί ένας διαδακτυλικός πίνακας συμβατότητας, πρέπει να καθορίσουμε ποιες γραμμές (με ζεύγη) ταυτίζονται μεταξύ του δείγματος και της gallery. Η απόσταση ανάμεσα στα ζεύγη είναι ανεξάρτητη από την περιστροφή και την μετατόπιση του αρχικού δακτυλικού αποτυπώματος και έτσι μπορεί να γίνει απευθείας σύγκριση μεταξύ του ζεύγους του δείγματος και του ζεύγους της gallery. Η διαφορά μεταξύ των αποστάσεων των ζευγαριών είναι εντός ενός σχετικού ορίου. Στον αλγόριθμό Bozorth συγκεκριμένα, θεωρείται ότι σε ένα ζεύγος υπάρχει ταύτιση αν $(d_p – d_g)^2 < (.1*(d_p+d_g))^2$, όπου d_p, d_g είναι η απόσταση μεταξύ του δείγματος/gallery ζεύγους που συγκρίνεται. Λογικά, η περιστροφή είναι πιο πολύπλοκη, καθώς η γωνία περιστροφής που χρειάζεται για να φέρει ένα ζεύγος από μικρολεπτομέρειες σε ευθυγράμμιση, δεν θα είναι η ίδια με αυτή που θα χρειάζεται σε ένα άλλο ζεύγος. Γι' αυτό το λόγο, κάθε πεδίο του πίνακα με ζεύγη, αποθηκεύει τις γωνίες μεταξύ του προσανατολισμού που έχουν στο κάθε σημείο οι μικρολεπτομέρειες, με τη γραμμή που ενώνει τις δύο μικρολεπτομέρειες μεταξύ τους. Έτσι, οι γωνίες των άκρων παραμένουν σχετικά σταθερές σε σχέση με την γραμμή σύνδεσης τους, ανεξάρτητα από την περιστροφή του δακτυλικού αποτυπώματος. Αν οι γωνίες του δείγματος και της gallery έχουν διαφορά μικρότερη από 11 μοίρες, οι γωνίες θεωρείται ότι ταυτίζονται. Αυτό το στάδιο μπορεί να συγκρίνει την απόσταση και τις τιμές των δύο γωνιών, για να καθορίσει αν υπάρχει συμβατότητα, και αν είναι συμβατά, βάζει την σχετική περιστροφή (που υπολογίζεται από την διαφορά στο θ_{kj} μεταξύ του δείγματος και της gallery) και

τους δείκτες από τις μικρολεπτομέρειες σε κάθε ζεύγος, σαν την επόμενη εγγραφή στον διαδακτυλικό πίνακα συμβατότητας.

Το τελικό στάδιο είναι να διασχίσει τον διαδακτυλικό πίνακα συμβατότητας σχηματίζοντας συστάδες και υπολογίζοντας την βαθμολογία. Ο αλγόριθμος ταξινομεί την λίστα με τα ζεύγη βάσει της γωνίας περιστροφής και έπειτα κάνει μία πολύπλοκη διέλευση (complex traversal) κατασκευάζοντας συστάδες δένδρων (forest clumps) που έχουν σχεδόν ταυτόσημες περιστροφές και τέτοιες ώστε κάθε στοιχείο της συστάδας να προέρχεται από μία κοινή μικρολεπτομέρεια (ένα κοινό σημείο) με ένα άλλο στοιχείο της συστάδας, σε κάποιο συμβατό ζεύγος. Η βαθμολογία είναι το άθροισμα του αριθμού των μικρολεπτομερειών στο καλύτερο δίκτυο ταύτισης.

3.1.3 Biotoken βασισμένο στον Bozorth αλγόριθμο

Σε αυτή την υποενότητα περιγράφεται μερικώς η υλοποίηση του βασισμένου στον Bozorth, κρυπτογραφικά ασφαλούς Biotoken [3] και η απόδοση του. Για να μετατραπεί η Bozorth αναπαράσταση σε ένα biotoken δημόσιου κλειδιού, μετασχηματίζουμε τον πίνακα-ζευγαριών, απαιτώντας μόνο μικρές αλλαγές στα βήματα 1 και 2 και 3β.

Σημαντικό ρόλο στον μετασχηματισμό παίζει η δυνατότητα να εφαρμόζεται ο μετασχηματισμός με την ίδια ακρίβεια κάθε φορά. Θα μπορούσε να χρησιμοποιηθεί ένας μοναδικός μετασχηματισμός για όλα τα δεδομένα ενός ατόμου, αλλά αυτό μειώνει την προσπάθεια που απαιτείται για μία brute force επίθεση. Στα τεστ που διενεργήθηκαν, κάθε άτομο έχει 64 διαφορετικούς μετασχηματισμούς T_i, με την επιλογή του ποιος μετασχηματισμός θα διενεργηθεί να εξαρτάται από την απόσταση d_{jk} του αρχικού ζεύγους. Κάθε μετασχηματισμός T_i καθορίζει την μετατόπιση του με την παραγωγή ενός τυχαίου αριθμού. Η μεγέθυνση είναι ντετερμινιστική έτσι ώστε κάθε “είσοδος” να χαρτογραφείται σε ένα διάστημα τουλάχιστον όσο μεγάλο είναι το ολικό εύρος των δεδομένων εισόδου (input data), για να διασφαλιστεί τυχόν επικάλυψη και αναδίπλωση, αλλά και να διασφαλιστεί μία διαφορετική ρύθμιση για κάθε μετασχηματισμό. Η μεγέθυνση εξαρτάται από το αναμενόμενο εύρος των τιμών των μικρολεπτομερειών και την ανάλυση του αισθητήρα. Για κάθε πεδίο, εφαρμόζουμε πρώτα την μετατόπιση, έπειτα την μεγέθυνση, και στη συνέχεια το χωρίζουμε σε r_{jk} και q_j.

Ο δείκτης για τον μετασχηματισμό T_n υπολογίζεται σαν συνάρτηση της απόστασης και των γωνιών της εισόδου. Επειδή μία μικρή αλλαγή στην είσοδο θα μπορούσε

να δώσει σαν αποτέλεσμα ένα διαφορετικό δείκτη, γίνεται έλεγχος αν ο δείκτης είναι κοντά σε κάποιο όριο, και αν όντως είναι, επεκτείνεται το ζεύγος εισόδου και δημιουργούνται δύο κωδικοποιημένα ζεύγη, ένα για κάθε δείκτη στον οποίο είναι κοντά. Παρομοίως, αν r_{jk} είναι κοντά στο 0 ή στο E, τότε το q μπορεί να διαφέρει κατά ένα λάθος και μία δεύτερη γραμμή μπορεί να παραχθεί με τον επόμενο δείκτη για να βελτιωθεί η ικανότητα ταύτισης. Όταν χρησιμοποιείται δεύτερη γραμμή, είναι πιθανό να ταυτίζονται και οι δύο γραμμές.

Όταν συγκρίνονται οι γραμμές, πρώτα ελέγχουμε αν τα σχετικά q πεδία ταυτίζονται απόλυτα, και μόνο αν είναι έτσι, θα γίνει έλεγχος και στις αποστάσεις για κάθε πεδίο, όπως προηγουμένως. Όταν ολοκληρωθεί η “σύγκριση γραμμών”, ο υπόλοιπος αλγόριθμος Bozorth συνεχίζει χωρίς αλλαγές. Όμως, καθώς παρουσιάσαμε το ενδεχόμενο ύπαρξης διπλών γραμμών, καθορίζουμε επίσης μία κανονικοποίηση (normalization) που προσαρμόζει ανάλογα το πλήθος των γραμμών που χρησιμοποιήθηκαν τελικά στην σύγκριση γραμμών.

Ενώ μέχρι στιγμής περιγράψαμε την διαδικασία λέγοντας “κρυπτογράφηση” ενός κωδικοποιημένου πεδίου, αυτό παρουσιάζει δύο προκλήσεις. Πρώτον, χρησιμοποιώντας κρυπτογραφία Δημόσιου Κλειδιού, το μέγεθος των κρυπτογραφημένων δεδομένων πρέπει να είναι τουλάχιστον όσο το μέγεθος του κλειδιού. Έτσι, ένα πεδίο double μήκους 64bit, όταν κρυπτογραφείται με RSA256, θα πρέπει να προστεθεί pad και να καταλήξει να είναι μήκους 256bit. Αυτό δεν θα χρειαζόταν αν ενώναμε 4 από αυτά τα πεδία πριν από την κρυπτογράφηση, αλλά με την ένωση αυτή των πεδίων, η αποτυχία ταύτισης του ενός πεδίου θα επηρέαζε την ικανότητα σύγκρισης των υπόλοιπων.

Το δεύτερο και πιο σημαντικό ζήτημα έχει να κάνει με την αντοχή της κωδικοποίησης σε brute force επίθεση. Ενώ η κρυπτογράφηση Δημόσιου Κλειδιού μπορεί να είναι υπολογιστικά πολύ δύσκολο να αντιστραφεί, αν τα δεδομένα που κωδικοποιούνται είναι μικρά πεπερασμένα πεδία, μήκους 10,16 ή ακόμα και 32 bit, θα μπορούσε κάποιος να προσπαθήσει να κωδικοποιήσει όλες τις εισόδους και να δει αν ταιριάζουν. Η λύση στην παραδοσιακή κρυπτογραφία είναι, η προσθήκη pad στα δεδομένα με επιπλέον τυχαία δεδομένα, πριν την κωδικοποίηση, τα οποία έπειτα από την αποκωδικοποίηση αγνοούνται. Όμως στην περίπτωση μας, δεν αποκωδικοποιούμε τα δεδομένα για την σύγκριση και έτσι δεν υπάρχει τρόπος να χωρίσουμε τα κωδικοποιημένα δεδομένα από τα τυχαία επιπρόσθετα δεδομένα. Το κρυπτογραφημένο τυχαίο πεδίο δεν θα μπορούσε να ταυτιστεί εκτός αν εφαρμόζαμε τα ίδια επιπρόσθετα δεδομένα και στο δείγμα και στην gallery, κάτι το οποίο θα σήμαινε, ότι αν παραβιάζονταν, θα μπορούσε να χρησιμοποιηθεί για brute force επίθεση.

Μία λύση σε αυτά τα δύο ζητήματα για τα δακτυλικά αποτυπώματα, είναι μία ενδιάμεση προσέγγιση που επιτρέπει και την αντιστροφή με χρήση δημόσιων κλειδιών και την κωδικοποίηση πολλαπλών πεδίων. Σε κάθε μία “γραμμή” στον συγκριτή Bozorth, υπάρχουν 3 πεδία των 8-bit τα οποία δεν πειράζουμε (k,j,θ_{kj}) και 3 βασικά πεδία τα οποία πρέπει να κωδικοποιήσουμε: d_{kj} (μία απόσταση η οποία είναι ένας integer μεγέθους 16bit) και δύο γωνίες β_1, β_2 (τυπικά αναπαρίστανται σαν 16bit, αλλά πρακτικά καταλαμβάνουν 9 bits). Για να προστατευτούν αυτά τα πεδία, τα μετασχηματίζουμε όπως περιγράψαμε νωρίτερα. Περιληπτικά, μετά τον μετασχηματισμό, έχουμε bytes από πεδία ελέγχου τα οποία δεν προστατεύτηκαν (ή μετασχηματίστηκαν), 4 bytes από υπόλοιπα (residuals), δηλαδή τις r τιμές και 4 bytes από q τιμές.

Καθώς και τα 3 πεδία “q” πρέπει να ταυτίζονται, θα μπορούσαμε να θεωρήσουμε αυτά τα τέσσερα προστατευμένα q bytes σαν έναν αριθμό (g) που πρέπει να προστατευτεί χωρίς να υπάρχει αλλαγή στην σύγκριση. Αλλά ακόμα, τα δεδομένα που πρέπει να προστατευτούν είναι μήκους 32 bits, πολύ μικρό μέγεθος για να προστατευτούν επαρκώς από μόνα τους. Η διαδικασία κατά την οποία μία “γραμμή” μετασχηματίζεται, χρησιμοποιεί 64 διαφορετικούς πιθανούς μετασχηματισμούς, με τον δείκτη του μετασχηματισμού να προκύπτει βάσει των αρχικών δεδομένων (τα οποία δεν είναι γνωστά σε κάποιον που επιχειρεί επίθεση brute force). Ακόμα και με την προσθήκη 64 διαφορετικών περιπτώσεων μετασχηματισμού που μπορούν να εφαρμοστούν, πάλι πρέπει να κάνουμε κάτι παραπάνω.

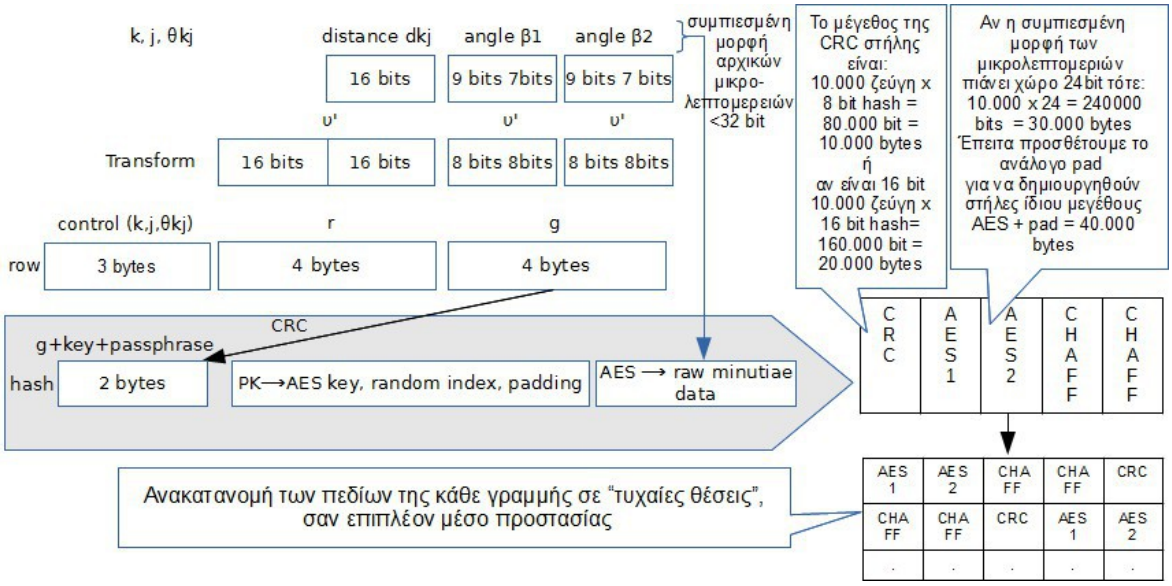
Για να υποστηρίξουμε πλήρη αντιστροφή, χρησιμοποιούμε κρυπτογραφία δημόσιου κλειδιού (PK). Χρησιμοποιούμε PK για να κρυπτογραφήσουμε ένα AES κλειδί, έναν τυχαίο δείκτη, συν συμπληρωματικά πεδία pad. Έπειτα χρησιμοποιούμε AES για να κρυπτογραφήσουμε, μία συμπιεσμένη μορφή (<32bits), των αρχικών δεδομένων μικρολεπτομερειών. Αυτά κρυπτογραφούνται όλα μαζί και προστίθεται pad ανάλογα με τον αριθμό των ζευγών. Σε μία άλλη εκδοχή, κρυπτογραφούμε με AES τα σταθερά πεδία g, αλλά επειδή η αντιστροφή του μετασχηματισμού στις αρχικές τιμές δεν είναι εμφανής και επειδή τα πεδία καταλαμβάνουν 32 bit, προτιμήθηκε η κρυπτογράφηση των αρχικών μικρολεπτομερειών. Έπειτα υπολογίζεται ένα CRC για ένα εταιρικό κλειδί, για οποιαδήποτε κωδική φράση του χρήστη, αν υπάρχει, και για τα 4-byte δεδομένων που πρέπει να προστατευτούν (g). Η χρήση CRC διπλώνει τα δεδομένα με τέτοιο τρόπο που σε μία brute force επίθεση θα υπάρχουν πολλές είσοδοι, οι οποίες θα παράγουν το ίδιο κωδικοποιημένο αποτέλεσμα με τα σωστά δεδομένα. Εξασφαλίζει επίσης ότι οποιαδήποτε αλλαγή στο κλειδί ή στην κωδική φράση θα έχει διαφορετικά αποτελέσματα. Στην περίπτωση μας, παίρνουμε 32 bit

πραγματικών δεδομένων, συν τα κλειδιά και την κωδική φράση και παίρνουμε ένα hash μήκους 8 ή 16 bit.

Μπορούμε να αυξήσουμε τον βαθμό ασάφειας, έχοντας πολλαπλές στήλες στα κωδικοποιημένα δεδομένα, μία για το CRC-αποτέλεσμα των προστατευμένων δεδομένων, δύο για τα δεδομένα που έχουν κρυπτογραφηθεί με AES (ή τέσσερις αν χρησιμοποιούμε 8 bit CRC) και αν το επιθυμούμε, επιπρόσθετες στήλες με δεδομένα απόκρυψης (τυχαία δεδομένα chaff). Στο “πρότυπο εγγραφής”, αλλάζουμε θέση στις στήλες τυχαία (ξεχωριστά για κάθε γραμμή) έτσι ώστε να μην υπάρχει συγκεκριμένη σειρά, αλλά χρησιμοποιώντας το κλειδί που ήταν στο κρυπτογραφημένο block, μπορούμε να καθορίσουμε τις “τυχαίες θέσεις” για τα κρυπτογραφημένα με AES δεδομένα (και να κάνουμε την αντιστροφή). Προφανώς το κρυπτογραφημένο με PK, AES κλειδί και ο δείκτης θα πρέπει να είναι σε μία γνωστή θέση, είτε στην επικεφαλίδα (header) ή σε κάποια άλλη γνωστή θέση που να καθορίζεται από μία μίξη του εταιρικού κλειδιού με το id του ατόμου.

Κατά την σύγκριση, θεωρούμε ότι υπάρχει ταύτιση, αν παρατηρείται ταύτιση με οποιοδήποτε πεδίο (χωρίς να αλλάζουμε τη σειρά), ενώ απαιτείται να ταυτίζονται και τα τρία υπόλοιπα (residuals). Για μία πραγματικά θετική αναγνώριση (true positive), η διαδικασία θα συγκρίνει το κωδικοποιημένο αποτέλεσμα. Η πιθανότητα ένας απατεώνας να έχει ίδιο CRC, ακόμα και αν του δοθεί η πιθανή σειρά και τα δεδομένα απόκρυψης, είναι μικρή και όταν προσθέσουμε και την απαίτηση να ταιριάζουν τα 3 υπόλοιπα (residuals), είναι αρκετά μικρή για να επηρεάσει την συνολική απόδοση σύγκρισης. Η προσθήκη περισσότερων στηλών απόκρυψης (chaff) ή έχοντας επιπλέον δεδομένα (πχ τύπος minutiae) σαν μέρος των “σταθερών δεδομένων”, αυξάνει την προστασία εκθετικά.

Καθώς τα αρχικά δεδομένα μικρολεπτομερειών είναι ανακατεμένα, προστατεύονται κατάλληλα από την κρυπτογράφηση αυτή. Τα AES κρυπτογραφημένα αρχικά δεδομένα μικρολεπτομερειών δεν χρησιμοποιούνται πουθενά στην διαδικασία της ταύτισης, αλλά αποτελούν καλά δεδομένα απόκρυψης (chaff). Καθώς τα AES κρυπτογραφημένα δεδομένα φαίνονται σαν τυχαία δεδομένα απόκρυψης στον αλγόριθμο ταύτισης, η διαφορά είναι ασήμαντη στην ολική επίδοση και κάνει απλή την αντιστροφή τους.



Σχήμα 18: Χαρτογράφηση δεδομένων που παρέχει προστασία στα πεδία μικρού αριθμού bit μίας γραμμής ζευγών.

Ένα δεύτερο πλεονέκτημα αυτής της προσέγγισης είναι ότι υποστηρίζει απλή επανέκδοση σε επίπεδο εταιρείας. Όταν κωδικοποιούνται τα δεδομένα, ο "δείκτης" (index) που επιτρέπει σε κάποιον να αναγνωρίσει τα CRC-δεδομένα ανάμεσα στα δεδομένα απόκρυψης (chaff) μπορεί να κωδικοποιηθεί με το Δημόσιο Κλειδί της εταιρείας (Master Public Key). Αν η εταιρεία αποθηκεύει αυτό σαν το κύριο-biotoken εγγραφής δημοσίου κλειδιού, μπορούν να χρησιμοποιήσουν το ιδιωτικό κλειδί για να ανακτήσουν την σειρά και να εκδώσουν ένα λειτουργικό biotoken (operational biotoken). Το λειτουργικό biotoken παράγεται χρησιμοποιώντας ένα επιπλέον κλειδί το οποίο παίζει τον ρόλο του pad (πρόσθετα δεδομένα) στον CRC-υπολογισμό των πεδίων που έχουν τα δεδομένα, πχ πάρε τα κωδικοποιημένα 16 bit CRC από τον χρήστη, πρόσθεσε τα νέα κλειδιά και υπολόγισε ένα νέο 16 bit CRC. Καθώς αυτό είναι μη-αντιστρέψιμο, μπορούν έπειτα να κρυπτογραφήσουν με PK/AES τις αρχικές CRC-τιμές, αντικαθιστώντας στήλες με δεδομένα απόκρυψης (chaff) με τα αποτελέσματα. Αν ένα λειτουργικό biotoken παραβιαστεί, ή αν σύμφωνα με την πολιτική της εταιρείας ξεπεραστεί το όριο χρήσης ενός biotoken και πρέπει να αλλάξει, η εταιρεία μπορεί να χρησιμοποιήσει το δικό της κλειδί για να ανακτήσει τις αρχικές CRC τιμές (δηλαδή να επιστρέψει πίσω στο αρχικό κύριο biotoken δημόσιου κλειδιού (master public key biotoken) και να επανεκδώσει ένα νέο λειτουργικό biotoken από το κύριο. Τα δεδομένα του χρήστη παραμένουν προστατευμένα, μόνο που η γνώση της σειράς ταξινόμησης ελαττώνει την προσπάθεια που απαιτείται για μία brute force επίθεση, αν και εξακολουθεί να απαιτεί αξιοσημείωτη προσπάθεια ακόμα και για κάποιον εντός της εταιρείας, που θα προσπαθήσει να επιχειρήσει μία brute force επίθεση. Παρέχει

πάντως ένα μοντέλο το οποίο δεν προκαλεί κάποια ενόχληση στο χρήστη (δεν απαιτείται η παρουσία του για την επανέκδοση).

Η ενσωμάτωση κλειδιών ή μία πιο γενική διαδικασία πολλαπλών σταδίων, μπορεί να χρησιμοποιηθεί για να υποστηρίξει μοναδικά ανά συναλλαγή, biotokens δημοσίου κλειδιού. Για παράδειγμα, με το CRC μοντέλο, μπορούμε να πάρουμε ένα λειτουργικό biotoken δημοσίου κλειδιού, να ενώσουμε ένα κλειδί συγκεκριμένο για κάθε συναλλαγή και να παράγουμε ένα νέο κωδικοποιημένο πεδίο. Για το επίπεδο των συναλλαγών, το σύστημα δεν χρειάζεται να καταλαβαίνει την σειρά ταξινόμησης ή να επανακωδικοποιήσει τα αρχικά CRC δεδομένα, διότι κανένας επιπρόσθετος μετασχηματισμός δεν θα εφαρμοστεί μετά την συναλλαγή. Μπορεί απλά να εφαρμόσει τον τελικό CRC υπολογισμό σε όλες τις στήλες, έτσι ώστε να μην μειωθεί η ασφάλεια σε αυτό το επίπεδο. Για την σύγκριση, τα βιομετρικά του χρήστη υποβάλλονται σε μία παρόμοια διαδικασία και τα αποτελέσματα μπορεί να συγκριθούν. Ενώ η πραγματική παραδοσιακή προσέγγιση βασισμένη σε CRC μπορεί να επαρκεί για βασικές συναλλαγές, εφαρμογές που απαιτούν υψηλότερη ασφάλεια, θα μπορούσαν να χρησιμοποιήσουν περισσότερο εξελιγμένα κρυπτογραφικά hashes, αναγνωρίζοντας ότι θα απαιτούν μεγαλύτερη χωρητικότητα και υπολογιστική ισχύ. Επίσης θα μπορούσαν να χρησιμοποιήσουν μία CRC/hash τέτοια ώστε το λειτουργικό κλειδί και το κλειδί συναλλαγής, ενώ εφαρμόζονται ξεχωριστά, να μπορούν να συνδυαστούν σε ένα μόνο κλειδί/μετασχηματισμό που θα εφαρμοστεί έτσι ώστε το μηχάνημα του χρήστη να μην λάβει ποτέ τα ξεχωριστά κλειδιά.

3.1.4 Απόδοση

Κατά την διάρκεια της εγγραφής απαιτούμε τη δημιουργία ενός RSA κλειδιού και πλήρη PK κρυπτογράφηση, που αντιπροσωπεύει το πιο ακριβό βήμα όσον αφορά τον χρόνο. Σε μία εικόνα διαστάσεων 380x380, το υπολογιστικό κόστος της εγγραφής παίρνει περίπου 750 ms ως 3000ms (δηλαδή 3 δευτερόλεπτα) σε έναν 1.6 Pentium 4 επεξεργαστή ανάλογα με το μέγεθος του επιλεγμένου RSA κλειδιού (512-2048 bits), 250ms ως 2500ms για την παραγωγή του κλειδιού και την κωδικοποίηση του AES κλειδιού, 350ms για την εξαγωγή των μικρολεπτομερειών (minutiae) και επεξεργασία της εικόνας, και άλλες παραμέτρους και 50ms για την AES κωδικοποίηση και την παραγωγή του Κρυπτογραφικά Ασφαλούς Biotoken. Η σύγκριση δεν απαιτεί τα PK βήματα, μειώνοντας δραστικά τον χρόνο σε ένα συνολικό μέσο όρο 423ms, από τα οποία 394ms είναι για την επεξεργασία της εικόνας και 29ms αντιστοιχούν στην παραγωγή του κρυπτογραφικά ασφαλούς biotoken και τη σύγκριση. Αυτό αντιπροσωπεύει μόνο 8ms περισσότερο από τον

χρόνο της τυπικής εφαρμογής του Bozorth συγκριτή από την NIST, πάνω στον οποίο βασίζεται το κρυπτογραφικά ασφαλές biotoken.

Πιο σημαντικό από την ταχύτητα όμως, είναι το πόσο επηρεάζει την ακρίβεια ταύτισης το κρυπτογραφικά ασφαλές biotoken. Η ακρίβεια ταύτισης έχει άμεση σχέση με τον αριθμό από μικρολεπτομέρειες (minutiae) ή το μέγεθος των πινάκων που διατηρούνται. Για τον Bozorth αλγόριθμο, χρησιμοποιούμε τις προ-επιλεγμένες ρυθμίσεις, που επιτρέπουν μέχρι 150 μικρολεπτομέρειες (minutiae) και 10.000 ζεύγη. Για το κρυπτογραφικά ασφαλές biotoken, περιορίσαμε το μέγεθος του πίνακα για να κρατήσουμε το μέγεθος αποθήκευσης του κρυπτογραφικά ασφαλούς biotoken κάτω από 24K, με μέσο όρο μεγέθους τα 12K. Ο περιορισμός έγινε πρώτα χρησιμοποιώντας τις προεπιλογές για κούρεμα βάσει της υπολογισμένης ποιότητας των μικρολεπτομερειών από το NIST πρόγραμμα, αλλά προσπαθώντας παράλληλα να διασφαλίσουμε ότι κάθε μικρολεπτομέρεια συμπεριλαμβανόταν σε μερικά ζεύγη, αντί να αφήσουμε τις καλύτερες μικρολεπτομέρειες να συμμετέχουν σε όλα τα ζεύγη τους. Αυτό έγινε για να διασφαλιστεί καλύτερη κάλυψη του χώρου. Ενώ μερικοί μπορεί να θεωρούν ένα 12K token πολύ μεγάλο, πιστεύουμε πως το αντίτιμο λίγης χωρητικότητας παραπάνω είναι μικρό, με αντάλλαγμα την βελτίωση της ασφάλειας και της ιδιωτικότητας που παρέχουν τα κρυπτογραφικά ασφαλή biotokens.

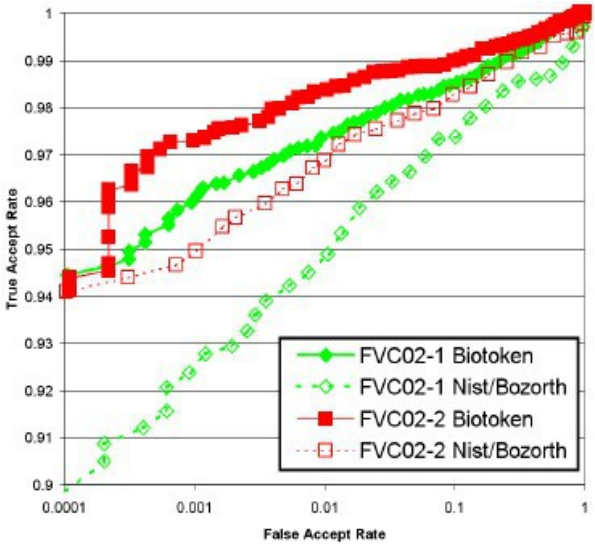
Έγιναν ελάχιστες μόνο αλλαγές στον κώδικα του συγκριτή, επεκτείνοντας τον να χειρίζεται επιπλέον στήλες και να ελέγχει τα κωδικοποιημένα πεδία συγκρίνοντας τα με τα υποσύνολα της κάθε στήλης. Επειδή η κωδικοποίηση των πινάκων και τα ζεύγη που γίνονται σύμφωνα με την ποιότητα (quality pairing) μπορεί να αλλάξουν τον αριθμό των εγγραφών, προσθέσαμε κανονικοποίηση (normalization) στην βαθμολογία βάσει του αριθμού των γραμμών που χρησιμοποιούνται.

Ο αυθεντικός Bozorth αλγόριθμος σύγκρισης και ο τροποποιημένος για σύγκριση biotokens, δοκιμάστηκαν πάνω σε βάσεις δεδομένων του γνωστού διαγωνισμού επαλήθευσης δακτυλικών αποτυπωμάτων FVC. Το σχήμα 19 εμφανίζει τις ROC καμπύλες του biotoken αλγόριθμου σε σύγκριση με τον αυθεντικό NIST/Bozorth συγκριτή, για δύο διαφορετικές βάσεις δεδομένων. Η βελτίωση στην απόδοση είναι σχετικά φανερή. Η ακρίβεια, όπως μετριέται με τον δείκτη ισάριθμων σφαλμάτων (equal-error rate) για τις τυπικές βάσεις δεδομένων του διαγωνισμού φαίνεται στον πίνακα. Συμπεριλαμβάνοντας περισσότερα χαρακτηριστικά κατά την διάρκεια της σύγκρισης (πχ αριθμό κορυφογραμμών ή τον τύπο) η απόδοση των biotoken μπορεί να βελτιωθεί περαιτέρω, αλλά δεν συμπεριλήφθηκαν επειδή δεν χρησιμοποιούνται από τον Bozorth3 και θα ήταν άδικη η σύγκριση. Ακόμα και χωρίς τα έξτρα χαρακτηριστικά, για το FVC2000, αυτές οι βαθμολογίες θα το

έφερναν στην 3η θέση των αλγόριθμων συνολικά, και στην πρώτη δεκάδα στο FVC2002. Τα δεδομένα στο FVC2004, προήλθαν από άτομα στα οποία είχε ζητηθεί να παραμορφώσουν επίτηδες τα δακτυλικά τους αποτυπώματα. Αυτό μπορεί να έφερε ορισμένες μικρολεπτομέρειες εκτός του παραθύρου που χρησιμοποιήθηκε για την σύγκριση και στην δημιουργία του δικτύου χαρακτηριστικών (feature-web) στον Bozorth αλγόριθμο και γι' αυτό επηρέασε αρνητικά την επίδοση και των δύο αλγόριθμων. Σύμφωνα με τις τελευταίες μετρήσεις στον διαγωνισμό FVC onGoing, ο αλγόριθμος σύγκρισης των biotoken κατέχει την πρώτη θέση ανάμεσα στους αλγόριθμους σύγκρισης προστατευμένων προτύπων και οι τελευταίες επίσημες επιδόσεις του φαίνονται στον πίνακα 4.

Πίνακας 3: Βελτίωση της ακρίβειας με τα biotoken[3]

Dataset	Biotoken verification EER	Improvement over EER of NIST VBT
FVC 2000 db1	.029	30%
FVC 2000 db2	.025	37%
FVC 2002 db1	.021	34%
FVC 2002 db2	.012	30%
FVC 2004 db1	.086	39%
FVC 2004 db2	.075	33%



Σχήμα 19: ROC καμπύλες του αλγόριθμου σύγκρισης Bozorth και των biotokens πάνω σε δεδομένα του διαγωνισμού FVC2002 [3]

Πίνακας 4: Επίσημα αποτελέσματα για την σύγκριση biotoken στον τελευταίο διαγωνισμό FVC OnGoing[8]

Accuracy indicators					
EER	FMR_{100}	FMR_{1000}	FMR_{10000}	$Zero_{FMR}$	$Zero_{FNMR}$
1,541% (1,540% - 1,541%)	1,753%	2,709%	3,791%	4,509%	100,000%
Efficiency indicators					

Avg Enroll Time	Avg Match Time	Avg Match Time (G)	Avg Match Time (I)
324 ms	619 ms	687 ms	597 ms

Memory indicators			
Avg Model Size	Max Model Size	Max Enroll Memory	Max Match Memory
18804 Bytes	19372 Bytes	14596 KBytes	22612 Kbytes

3.2 Ασφαλή Bipartite Biotokens με υποστήριξη ανάκλησης - Secure Revocable Bipartite Biotokens

Η έννοια του διαχωρισμού των δεδομένων για την δημιουργία δακτυλικών biotokens με υποστήριξη ανάκλησης, παρουσιάστηκε νωρίτερα. Χρησιμοποιώντας αυτή τη γνώση, και την έννοια της κρυπτογραφίας δημόσιου κλειδιού, μπορούμε να αναπτύξουμε την μεθοδολογία επανακωδικοποίησης των biotokens. Η ιδιότητα της επανακωδικοποίησης είναι βασική για την υποστήριξη ενός βιώσιμου μοντέλου συναλλαγών. Tokens με μοναδικά δεδομένα πρέπει να παράγονται γρήγορα και αυτόματα για να υποστηρίξουν κρυπτογραφικές συναλλαγές (όπως ανταλλαγή κλειδιών συναλλαγής). Η bipartite biotoken [24] μορφή ενός biotoken με δυνατότητα ανάκλησης, υποστηρίζει ενσωμάτωση δεδομένων (key-binding) σε επίπεδο συναλλαγών. Η δημιουργία ενός bipartite biotoken από ένα αποθηκευμένο biotoken επιτρέπει την απαιτούμενη απελευθέρωση δεδομένων όταν συγκρίνεται επιτυχώς με tokens που παράχθηκαν από αυθεντικά βιομετρικά χαρακτηριστικά κατά την διάρκεια της συναλλαγής.

Υποθέτοντας ότι ένα βιομετρικό παράγει μία τιμή υ η οποία μετασχηματίζεται μέσω μεγέθυνσης και μετατόπισης σε υ'=(υ-t)*s, το αποτέλεσμα υ' χωρίζεται στο σταθερό κομμάτι q, και το υπόλοιπο κομμάτι r. Η ποσότητα των σταθερών και μη-σταθερών δεδομένων είναι συνάρτηση της τροπικότητας που θα χρησιμοποιηθεί (ποιο βιομετρικό στοιχείο). Στο βασικό σενάριο, για έναν χρήστη j, το υπόλοιπο $r_j(υ')$ παραμένει χωρίς κωδικοποίηση. Για τον αρχικό μετασχηματισμό $w_{j,1}(q_j(υ'),T_1)$ εφαρμόζεται κάποια συνάρτηση μετασχηματισμού T (η οποία μπορεί να είναι μία ισχυρή μονόδρομη συνάρτηση (hash) όπως η SHA-256 που δεν επηρεάζεται από συγκρούσεις (collision attacks), ή μία ακόμη εφαρμογή κρυπτογραφίας δημόσιου κλειδιού). Για εμφωλευμένες επανακωδικοποιήσεις, το w_j επανακωδικοποιείται χρησιμοποιώντας επακόλουθους μετασχηματισμούς, δημιουργώντας μία μοναδική

νέα κωδικοποίηση για κάθε hash ή κλειδί που εφαρμόζεται: $w_{j,1}(υ', T_1)$, $w_{j,2}(w_{j,1},T_2),....,w_{j,n}(w_{j,n-1},T_n)$

Χρησιμοποιώντας κρυπτογραφία δημόσιου κλειδιού, η διαδικασία της εμφώλευσης μπορεί να είναι αντιστρέψιμη με ασφάλεια αν τα ιδιωτικά κλειδιά μέχρι την πρώτη φάση της κωδικοποίησης είναι διαθέσιμα. Μερική αντιστροφή της εμφώλευσης επιτρέπει την ανάκληση και την αυτόματη επανέκδοση του biotoken. Έχοντας την εμφώλευση κατά νου, μπορούμε να ορίσουμε τρεις ιδιότητες για ένα bipartite biotoken:

1. Αν B είναι ένα ασφαλές (secure) biotoken. Ένα bipartite biotoken B_B είναι ένας μετασχηματισμός $bb_{j,k}$ όπου το B του χρήστη j έχει μετασχηματισθεί k φορές. Αυτός ο μετασχηματισμός υποστηρίζει την σύγκριση σε κωδικοποιημένο χώρο (matching in encoded space) οποιουδήποτε στιγμιότυπου bipartite biotoken $B_{B,k}$ με κάθε στιγμιότυπο ασφαλούς biotoken B_k για τα βιομετρικά χαρακτηριστικά ενός χρήστη j και έναν κοινό αριθμό από μετασχηματισμούς $T_1, T_2, \dots, T_k$.

2. Ο μετασχηματισμός $bb_{j,k}$ πρέπει να επιτρέπει την ενσωμάτωση δεδομένων d μέσα στο B_B, και αναπαρίσταται ως: $bb_{j,k}(w_{j,k},T_k,d)$.

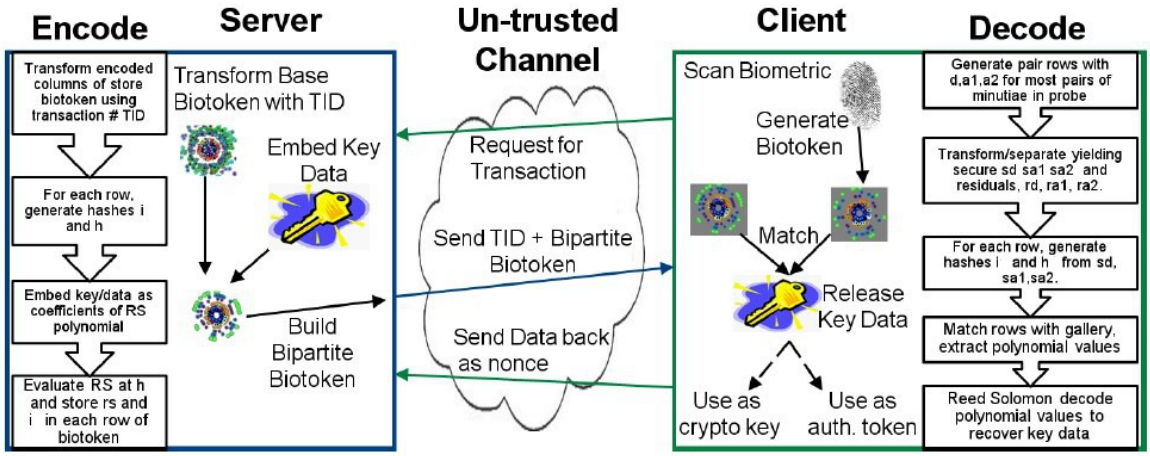
3. Αν η ταύτιση των B_k και $B_{B,k}$ είναι επιτυχής, πρέπει να απελευθερώνει το d.

Η υλοποίηση των bipartite biotoken που ικανοποιεί τις παραπάνω προϋποθέσεις, είναι μία επέκταση της έννοιας των revocable biotokens και των fuzzy vaults, όπου η ενσωμάτωση ενός πολυωνύμου κρύβει τα δεδομένα d. Η bipartite αναπαράσταση υλοποιεί κώδικα διόρθωσης λαθών Reed-Solomon και δεν αποθηκεύει τα σημεία στα οποία γίνεται ο υπολογισμός του πολυωνύμου. Επίσης, όπως θα δούμε στην συνέχεια, επιτρέπει την χρήση πολλαπλών ενσωματωμένων πολυωνύμων ταυτόχρονα. Για λόγους απόδοσης, δουλεύουμε πάνω σε πεπερασμένα σώματα Galois fields μεγέθους 2^8, όπου οι συντελεστές και τα σημεία υπολογισμού (evaluation points) είναι ποσότητες των 8 bit. Αναπαριστούμε τα δεδομένα d που πρόκειται να αποθηκευτούν σαν ένα K-byte τμήμα (block), με E bytes για διόρθωση λαθών, έτσι το συνολικό μέγεθος block είναι N = K + E. Το πολυώνυμο κωδικοποιεί τα N bytes από δεδομένα. Έπειτα υπολογίζονται οι τιμές του RS πολυωνύμου που αναπαριστά το σώμα μεγέθους N byte, σε ένα σύνολο από σημεία, με το αποτέλεσμα, την τιμή του υπολογισμένου πολυωνύμου να αποθηκεύεται εντός του προτύπου.

Για λόγους απλότητας, αν υποθέσουμε ότι ένα βιομετρικό δείγμα παράγει τρία χαρακτηριστικά a_1, a_2, a_3 που πρέπει να προστατευτούν. Ας είναι sa_1, sa_2, sa_3 τα σταθερά μέρη από αυτά τα χαρακτηριστικά και ας είναι ra_1, ra_2, ra_3 τα υπόλοιπα. Για τον υπολογισμό του πολυωνύμου, περνάμε από μία μονόδρομη συνάρτηση hash, τα 24 bits των sa_1, sa_2, sa_3 (μπορεί να καταλαμβάνουν 32 bit, αλλά εμείς παίρνουμε μόνο τα 24) και παίρνουμε το i, μία ποσότητα μεγέθους 8-bit που αποθηκεύεται στο πρότυπο. Η τιμή i έπειτα περνά από hash για δεύτερη φορά, ανά συναλλαγή, και λαμβάνουμε το h, για να καθορίσουμε το σημείο στο οποίο θα υπολογιστεί το πολυώνυμο. Για την υποστήριξη πολλαπλών “στηλών” με δεδομένα, υπολογίζουμε τις τιμές για διάφορα πολυώνυμα λαμβάνοντας τιμές rs_1 … rs_4. Σημειώστε ότι το σημείο υπολογισμού του πολυωνύμου, η τιμή hash h δεν αποθηκεύεται.

Το αποτέλεσμα είναι μία “κωδικοποιημένη bipartite γραμμή” που περιέχει τα μη προστατευμένα πεδία και έξι προστατευμένα πεδία (το κωδικοποιημένο σταθερό πεδίο w που χρησιμοποιείται στην σύγκριση, ο δείκτης i και τέσσερις στήλες από υπολογισμένα πολυώνυμα). Για δεδομένα d που είναι μικρότερα από 512 bits απλώνουμε τα δεδομένα των στηλών σε 16 γραμμές. Για δεδομένα μεγαλύτερα από 512 bits, απλώνουμε ισόποσα πάνω στις στήλες καταλαμβάνοντας όσες γραμμές απαιτούνται. Απαιτούμε τουλάχιστον 14 γραμμές, προσθέτοντας pad στα δεδομένα αν δεν απαιτούνται τέσσερις στήλες για να αναπαρασταθούν. Η τοποθεσία του w είναι τυχαία ανά γραμμή. Τα υπολογισμένα RS πολυώνυμα για τις τέσσερις στήλες rs_1 … rs_4 ακολουθούν το w ακολουθώντας κυκλική σειρά καταλαμβάνοντας τις έξι υποδοχές. Για παράδειγμα, αν ο τυχαίος δείκτης ήταν 3, τότε η σειρά θα ήταν: [rs_3, rs_4, w, rs_1, rs_2, i]

Όταν συγκρίνεται ένα δείγμα, το σύστημα δημιουργεί όλα τα πεδία για κάθε μία από τις γραμμές, συμπεριλαμβάνοντας και την hash τιμή h(που δεν αποθηκεύεται) για τον υπολογισμό του πολυωνύμου. Μία γραμμή του δείγματος πιθανώς να ταυτίζεται με μία γραμμή από την gallery αν βρεθεί ένα ταυτόσημο w ανάμεσα στα κωδικοποιημένα πεδία και τα υπόλοιπα (ra_1, ra_2, ra_3) είναι εντός των ορίων. Αυτό το τεστ είναι απαραίτητο, αλλά όχι αρκετό, για μία σωστή ταύτιση. Αφού αναγνωρίστηκε το w, ο αλγόριθμος μπορεί έπειτα να εξάγει τις τιμές των υπολογισμένων πολυωνύμων, rs_1 … rs_4. Αν το w αναγνωρίστηκε λανθασμένα, αν η γραμμή είναι μία κατά λάθος ταύτιση, ή αν η τιμή hash (h) είναι λάθος (εξαιτίας μίας τυχαίας σύγκρουσης (collision) στην παραγωγή/σύγκριση του w), θα εξαχθούν μερικές τιμές στη θέση των rs_1 … rs_4, αλλά δεν θα είναι σωστές. Εξάγουμε τις τιμές k για κάθε μία από τις j στήλες δεδομένων και παίρνουμε ένα σύνολο hash σημείων υπολογισμού h_j και τις τιμές του Reed-Solomon πολυωνύμου $rs_{j,k}$ στα αντίστοιχα σημεία.



Σχήμα 20: Κωδικοποίηση και αποκωδικοποίηση των bipartite biotoken. Καθώς τα ενσωματωμένα δεδομένα μπορεί να είναι μοναδικά ανά συναλλαγή, μία ποικιλία από κρυπτογραφικά πρωτόκολλα μπορούν να υποστηριχθούν. Τα ενσωματωμένα δεδομένα μπορεί να είναι ένα nonce, που επιστρέφεται πίσω στον server για επικύρωση. Θα μπορούσε να είναι και ένα token μίας χρήσης για αυθεντικοποίηση. Θα μπορούσε επίσης να είναι ένα συμμετρικό ή δημόσιο κρυπτογραφικό κλειδί. Τα bipartite biotokens είναι κατάλληλα για μετάδοση δεδομένων μέσα από μη-ασφαλή κανάλια επικοινωνίας.

Τώρα έρχεται μία σημαντική λεπτομέρεια της υλοποίησης, που βοηθάει και στην ασφάλεια και στην απόδοση. Κάποιος θα μπορούσε να βελτιώσει αποτελεσματικά την ευρωστία αυξάνοντας το επίπεδο της ECC, αλλά κάνοντας αυτό αυξάνεται και η ευκολία με την οποία κάποιος επιτιθέμενος μπορεί να μάθει το d. Αντί αυτού χρησιμοποιούμε hash συναρτήσεις δύο επιπέδων(two level hashing) για να βελτιώσουμε την αξιοπιστία. Η χρήση hash δύο επιπέδων, σε γενικές γραμμές, θα αντιστοιχήσει πολλαπλά sa_1, sa_2, sa_3 σύνολα στον ίδιο δείκτη. Έπειτα, ακολουθείται μία διαδικασία όπου συλλέγουμε τις πολλαπλές τιμές κατά την χαρτογράφηση, ελέγχουμε για συνέπεια και χρησιμοποιούμε αυτή την επιπλέον πληροφορία για να αντιμετωπίσουμε τυχόν ζητήματα ασυμφωνίας που προκύπτουν όταν χαρτογραφούνται δεδομένα με θόρυβο. Ο έλεγχος συνέπειας δικαιολογείται εξαιτίας του θορύβου στην διαδικασία σύγκρισης, και στην πολλά-προς-ένα χαρτογράφηση που επιτρέπει μη-μοναδικά αποτελέσματα χαρτογράφησης. Το αποτέλεσμα της χαρτογράφησης και του ελέγχου συνέπειας είναι ένα διάνυσμα μήκους N πολυωνυμικών τιμών (κάποιες από τις οποίες μπορεί να λείπουν) που περιέχει τις τιμές από τα υπολογισμένα RS πολυώνυμα για κάθε τοποθεσία. Το διάνυσμα N, με τα κενά σημαδεμένα, τροφοδοτείται σε μία RS

συνάρτηση αποκωδικοποίησης, που μας επιτρέπει να ανακτήσουμε το d με μέχρι g κενά και e λάθη, με την προϋπόθεση ότι 2g + e < E, όπου E είναι ο αριθμός από ECC bytes που χρησιμοποιούνται. Κάθε στήλη δεδομένων ανακτάται ξεχωριστά, με την ένωση πολλαπλών στηλών να επιτρέπει την ανάκτηση μεγάλου όγκου δεδομένων. Για περισσότερη ασφάλεια, υπολογίζεται ένα κρυπτογραφικό άθροισμα ελέγχου (checksum) πάνω στις έξι απροστάτευτες στήλες του biotoken εγγραφής. Τα δεδομένα d υπόκεινται σε μία πράξη XOR μαζί με το checksum πριν από την ενσωμάτωση, και πάλι μετά την αποκωδικοποίηση, και αυτό αποτρέπει οποιαδήποτε τροποποίηση του biotoken.

ΕΠΙΛΟΓΟΣ

Η υλοποίηση των bipartite biotokens παρέχει τα θεμέλια για την χρησιμοποίηση βιομετρίας σε κρυπτογραφικά πρωτόκολλα. Στο επόμενο κεφάλαιο θα δούμε πώς η προσθήκη βιομετρικών δεδομένων στα πιστοποιητικά x.509v3 μπορεί να βελτιώσει μία υποδομή δημοσίου κλειδιού (PKI), αποτρέποντας επιθέσεις αλίευσης και υποκλοπής κωδικών (phising) και επιθέσεις ενδιάμεσου ατόμου. Το μεγαλύτερο όφελος μίας υποδομής βιοκρυπτογραφικών κλειδιών (BKI) όπως ονομάζεται, είναι η ικανότητα να ανασύρουν οι χρήστες που είναι μέλη της ίδιας υποδομής, τα δημόσια biotokens άλλων χρηστών που είναι αποθηκευμένα εντός πιστοποιητικών. Έπειτα τα χρησιμοποιούν για να παράγουν ένα bipartite biotoken, με σκοπό να στείλουν κάποιο μυστικό στον ιδιοκτήτη του biotoken, με την διαβεβαίωση ότι το πιστοποιητικό που περιέχει το biotoken είναι έγκυρο.

ΚΕΦΑΛΑΙΟ 4

Επέκταση της Υποδομής Δημόσιου Κλειδιού (PKI) με βιομετρία: Υποδομή Βιοκρυπτογραφικού Κλειδιού (BKI)

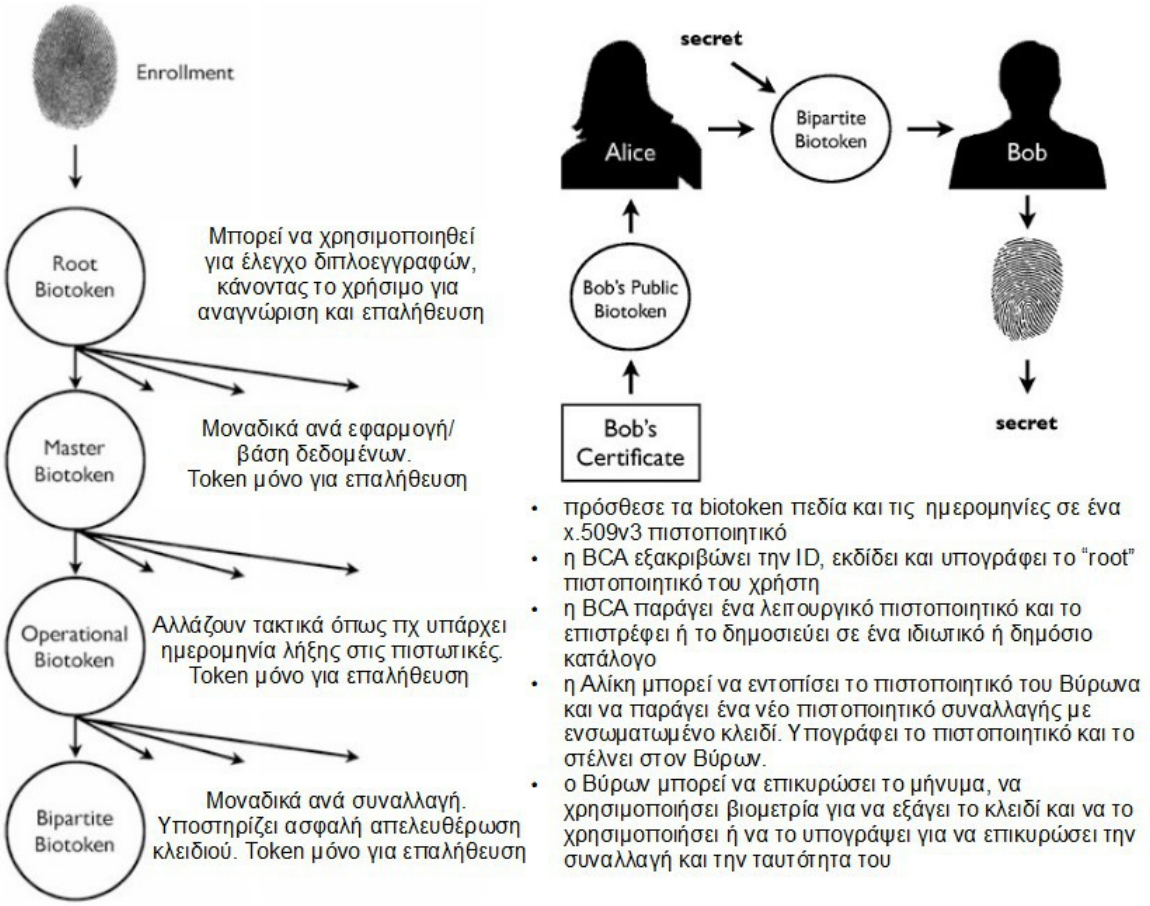
ΕΙΣΑΓΩΓΗ

Η υποδομή δημόσιου κλειδιού (public key infrastructure, PKI) είναι η υποδομή που υποστηρίζει την παραγωγή και διανομή κλειδιών. Αυτό επιτυγχάνεται με τη χρήση πιστοποιητικών, που περιέχουν κάποιο κομμάτι από έμπιστες πληροφορίες, όπως ένα όνομα και το δημόσιο κλειδί του χρήστη, οι οποίες έχουν την ψηφιακή υπογραφή μίας Αρχής Πιστοποίησης (Certificate Authority – CA). Το PKI επιχειρεί να λύσει ένα σημαντικό πρόβλημα στην διαχείριση κλειδιών: πως μπορεί η Αλίκη να επαληθεύσει ότι το δημόσιο κλειδί του Βύρωνα είναι πραγματικά του Βύρωνα; Η επίλυση αυτού του προβλήματος, όπως και των επιθέσεων ενδιάμεσου ατόμου και phishing είναι υψίστης σημασίας. Θα αναπτύξουμε μία πλήρη Υποδομή Βιομετρικών Κλειδιών, η οποία μπορεί να χειρίζεται όχι μόνο την διαχείριση δημόσιων κλειδιών, αλλά και την διαχείριση δημόσιων biotoken. Προσθέτοντας ένα βιομετρικό κομμάτι στο PKI, μπορούμε να αντιμετωπίσουμε κάποιες πολύ σημαντικές ανησυχίες περί ασφάλειας.

Με την προσθήκη βιομετρίας στο PKI, μπορούμε να προσθέσουμε μία υψηλότερου επιπέδου εμπιστοσύνη σε όλα τα μέρη της υποδομής. Αν ένας χρήστης ή μία αρχή πιστοποίησης παρουσιάσει ένα κλειδί και ένα βιομετρικό κατά την διάρκεια μίας δράσης, έχουμε περισσότερη βεβαιότητα ότι αυτή η δράση είναι νόμιμη (αλλά δεν αποδεικνύεται απόλυτα ότι ο κάτοχος του κλειδιού και του βιομετρικού εκτέλεσε πράγματι την κίνηση αυτή – κλεμμένα κλειδιά και επιθέσεις αντιγράφου (spoofing) είναι μια πραγματικότητα). Με τα βιομετρικά, έχουμε βελτίωση της μη-αποποίησης. Το πρόβλημα της εμπιστοσύνης ακολουθεί μία σειρά από σχετικές ανησυχίες. Η ασφάλεια του υπολογιστή που κάνει την επαλήθευση, η καθιέρωση μίας αρχής πιστοποίησης και γενικά θέματα με τα πιστοποιητικά. Με κατάλληλα πρωτόκολλα που συμπεριλαμβάνουν ένα βιομετρικό μέρος, μπορούμε να δώσουμε λύσεις σε κάθε ένα από αυτά τα ζητήματα.

Αλλά για να λύσουμε αυτά τα προβλήματα σωστά, δεν μπορούμε απλά να χρησιμοποιήσουμε τυπικά πρότυπα ενσωματωμένα μέσα στα x.509 πιστοποιητικά, διότι η ανάκληση ανεπεξέργαστων βιομετρικών δεδομένων (raw biometric data), μπορεί να συμβεί για έναν πολύ περιορισμένο αριθμό (1 πρόσωπο, 10 δάκτυλα). Επίσης, μη προστατευμένα βιομετρικά δεδομένα που είναι έστω κάτω από τον έλεγχο έμπιστων οντοτήτων, εξακολουθούν να είναι

ευάλωτα σε επίθεση. Τα bipartite biotokens με υποστήριξη ανάκλησης που παρουσιάστηκαν, είναι ικανά να προστατεύσουν τα βιομετρικά δεδομένα και κάνουν εφικτή την αυτόματη επανέκδοση πιστοποιητικών, ενώ παρέχουν έναν δημόσιο τρόπο αποστολής ενός μυστικού έτσι ώστε μόνο το άτομο με το σωστό βιομετρικό στοιχείο να μπορεί να το ανακτήσει.

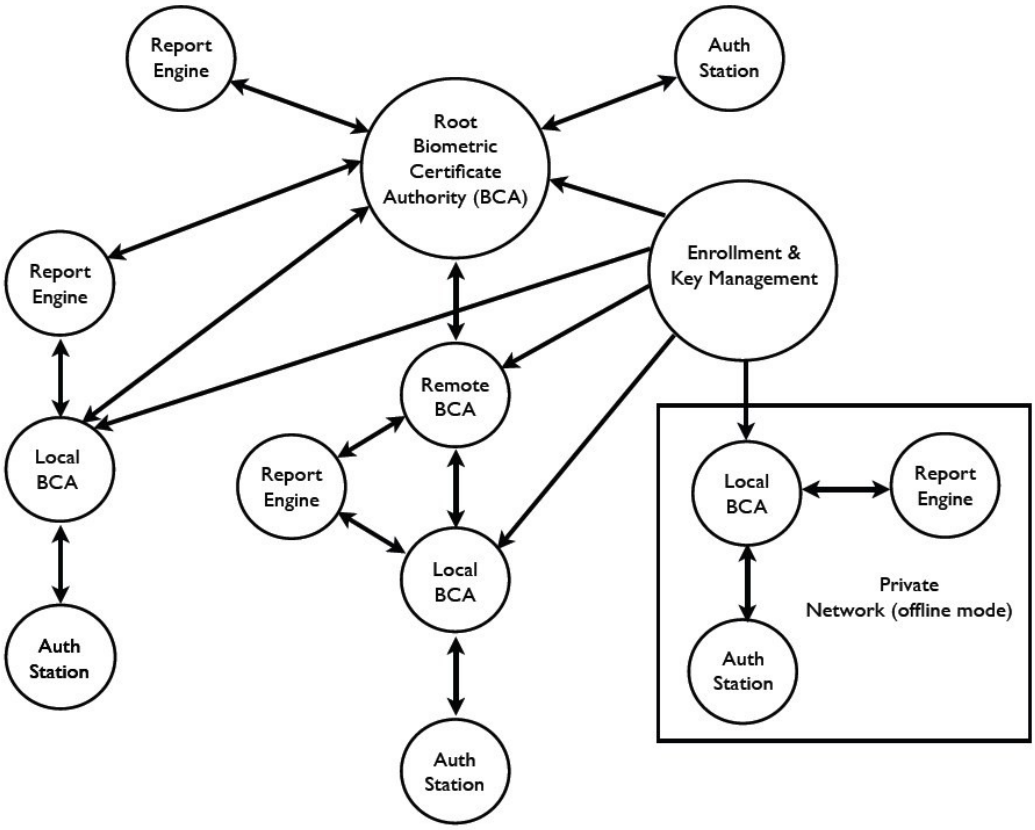


Σχήμα 21: Τυπικό δέντρο έκδοσης/επανέκδοσης biotoken. Τα biotokens μπορούν να επανακωδικοποιηθούν, ξεκινώντας από το biotoken της ρίζας που δημιουργείται κατά την εγγραφή, με επακόλουθες εφαρμογές κρυπτογραφίας δημόσιων κλειδιών (που υποστηρίζουν αυτόματη ανάκληση και επανέκδοση) ή κάποια μονόδρομη συνάρτηση hash.

Σχήμα 22: Το βασικό πλεονέκτημα της Υποδομής Βιοκρυπτογραφικών Κλειδιών: η δυνατότητα να αποθηκεύονται δημόσια biotokens μέσα σε ψηφιακά πιστοποιητικά. Μία οντότητα εντός της υποδομής μπορεί να στείλει μυστικά δεδομένα που μόνο ο ιδιοκτήτης του biotoken μπορεί να ξεκλειδώσει.

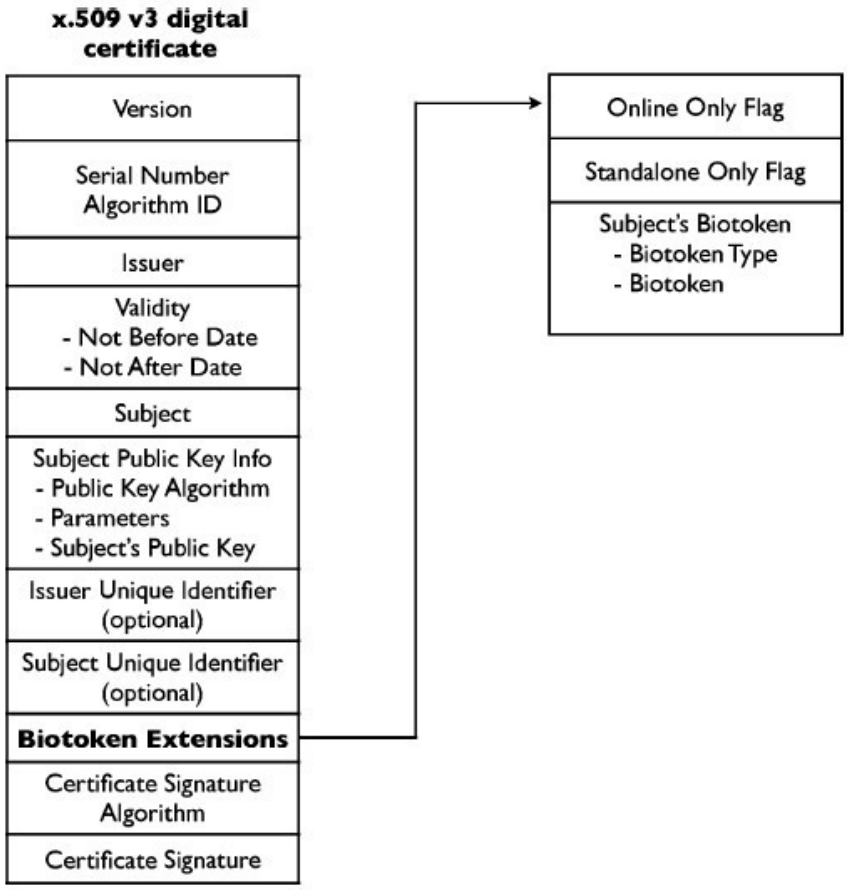
4.1 Σύσταση, Εγγραφή και Επικύρωση

Μία επισκόπηση της υποδομής βιοκρυπτογραφικών κλειδιών BKI [26] φαίνεται στο σχήμα 23. Αρκετές ξεχωριστές οντότητες διακρίνονται στο γράφημα BKI. Αρχές Βιομετρικής Πιστοποίησης - Biometric Certificate Authorities (BCA) είναι αρχές πιστοποίησης που υποστηρίζουν ταυτόχρονα δημόσια κλειδιά και biotokens με δυνατότητα ανάκλησης(revocable) και είναι βιομετρικά επικυρωμένες (verified) από υψηλότερου επιπέδου αρχές, σε μία διαδικασία που περιγράφεται με λεπτομέρεια παρακάτω. Όπως στο PKI, μία κεντρική εξουσία ρίζας (central root authority) υπάρχει για να εξουσιοδοτεί όλες τις BCA κάτω από αυτήν. Η εγγραφή και η διαχείριση κλειδιών ακολουθεί μία διαδρομή από κάθε BCA μέχρι πάνω στην ρίζα. Σταθμοί Αυθεντικοποίησης (Auth Stations) υπάρχουν στα πιο απόμακρα σημεία του γραφήματος και είναι τα μέρη όπου οι χρήστες καταχωρούν τα βιομετρικά δείγματα για να δημιουργηθούν biotokens εγγραφής (enrollment biotokens) ή biotokens για κάποια συγκεκριμένη συνεδρία. Μηχανές Αναφορών (Report Engines) μπορούν επίσης να αναπτυχθούν σε όλο το BKI γράφημα για να διαδίδουν αναφορές εγγραφής και αναφορές συναλλαγών σε άλλες αρχές.



Σχήμα 23: Σχεδιάγραμμα μίας υποδομής βιοκρυπτογραφικού κλειδιού.

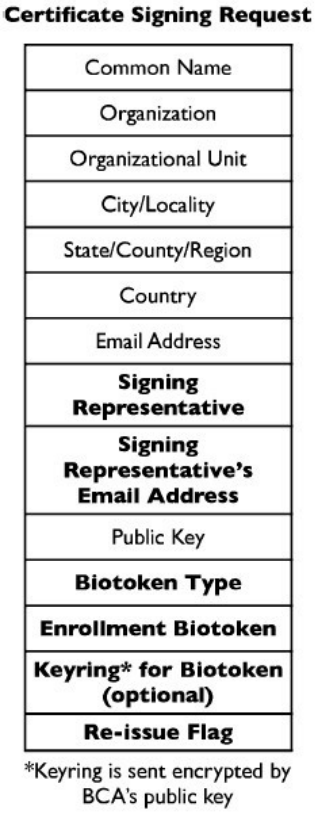
Για να υποστηριχθούν τα biotoken, προσθέτουμε μερικά επιπλέον πεδία στο βασικό x.509 v3 πιστοποιητικό. Αυτό φαίνεται στο σχήμα 24. Μπορούμε να χρησιμοποιήσουμε πιστοποιητικά και σε online αλλά και σε offline κατάσταση-περιβάλλον, όπως φαίνεται στο σχήμα 23. Αν λειτουργούμε σε offline κατάσταση, όπως σε έναν αυτόνομο υπολογιστή ή ένα ιδιωτικό δίκτυο, δεν έχουμε την ικανότητα σύνδεσης με BCAs σε εξωτερικά δίκτυα, συμπεριλαμβανομένης και της ρίζας. Για να επισημάνουμε την κατάσταση λειτουργίας στο υποκείμενο BKI λογισμικό, το πιστοποιητικό περιέχει μία “Online μόνο” και “Offline μόνο” ένδειξη (flag). Για το biotoken του υποκειμένου, πρώτα σημειώνουμε τον τύπο του biotoken που περιέχει. Υπάρχουν τριών ειδών biotokens για ένα συγκεκριμένο υποκείμενο, ένα πιστοποιητικό ενδέχεται να περιέχει ένα Biotoken Root ID, ή Biotoken Master ID ή ένα Biotoken Operational ID. Έπειτα από την ένδειξη “τύπος Biotoken”, περιέχεται το Biotoken το ίδιο.



Σχήμα 24: Ψηφιακά πιστοποιητικά που υποστηρίζουν δημόσια κλειδιά και biotokens

Χρειάζεται οι BCAs να εμπιστεύονται ο ένας τον άλλον, όπως και να μπορούμε να εμπιστευτούμε τους τελικούς χρήστες. Για να γίνει αυτό, χρειαζόμαστε μία

διαδικασία εγγραφής (enrollment process), όπου απαιτούμε από κάποιον να εγγραφεί βιομετρικά με την root BCA, η οποία μπορεί να αναζητήσει αυτό το άτομο στις υπάρχουσες εγγραφές. Η τυπική Αίτηση Υπογραφής Πιστοποιητικού (Certificate Signing Request, CSR) επεκτείνεται όπως φαίνεται στο σχήμα 23. Αυτό απαιτεί ένας εκπρόσωπος ενός οργανισμού που κάνει αίτηση, να παράγει ένα biotoken εγγραφής, το οποίο οδηγείται προς τα πάνω στην root authority για έλεγχο διπλοεγγραφής (duplicate enrollment check). Το biotoken εγγραφής (enrollment biotoken) πάντα δημιουργείται σαν ένα biotoken root ID (σχήμα 21) χρησιμοποιώντας το δημόσιο κλειδί της Αρχής Ρίζα (root authority), για να είναι ομοιογενής και σταθερή η συμπεριφορά σύγκρισης μεταξύ όλων των εγγεγραμμένων. Το token εγγραφής (enrollment token) αποθηκεύεται στην ρίζα (root) για χρήση σε όλους τους μελλοντικούς ελέγχους εγγραφής. Ενώ αυτό δεν προστατεύει την ιδιωτικότητα του εκπροσώπου του οργανισμού στο επίπεδο της βάσης δεδομένων, διατηρεί όμως την ακεραιότητα του BCA οικοδομήματος (BCA establishment), και προστατεύει τα βιομετρικά δεδομένα του εκπροσώπου.

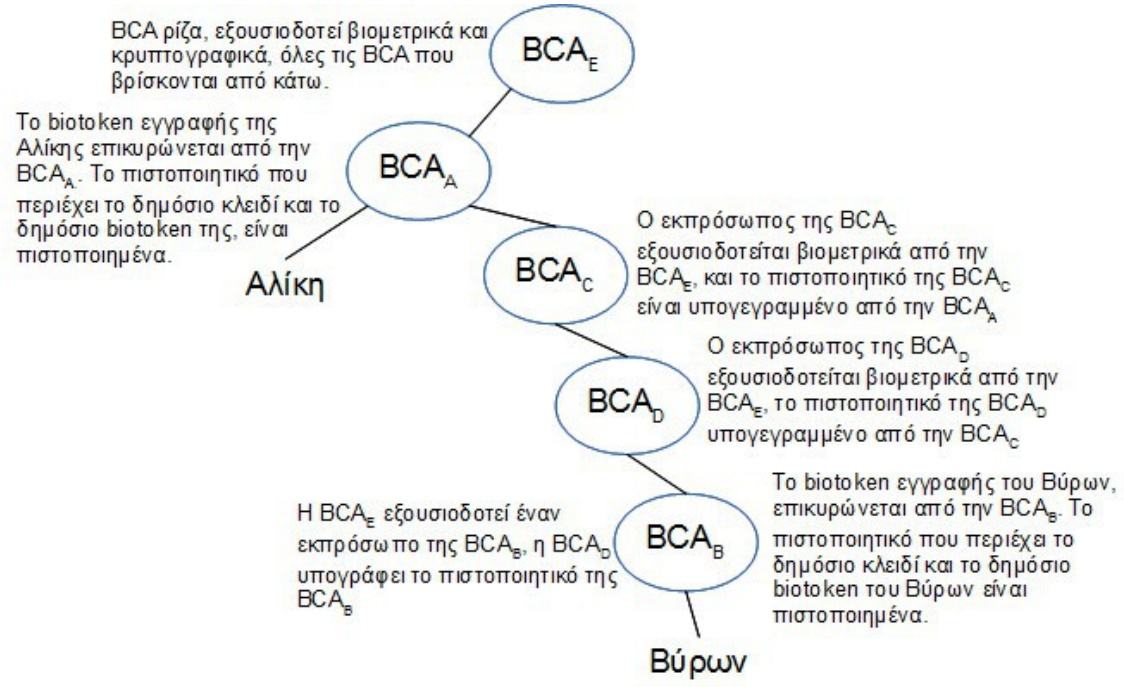


Σχήμα 25: Τροποποίηση ενός τυπικού CSR μηνύματος, που περιέχει πληροφορίες για ένα biotoken εγγραφής

Η ίδια διαδικασία ακολουθείται και για τους τελικούς χρήστες, με τη διαφορά ότι το token εγγραφής (enrollment token) δεν χρειάζεται να διανύσει ολόκληρη την διαδρομή από τον Σταθμό Αυθεντικοποίησης (Auth Station) του χρήστη μέχρι την ρίζα (root). Πιο τοπικές BCA μπορούν να το αναλάβουν. Για τα πιστοποιητικά των BCA και των χρηστών, η διαδικασία της επικύρωσης περιλαμβάνει την ανάλυση του πιστοποιητικού με μία BCA που είναι ορισμένη σαν Αρχή Επικύρωσης (VA). Αυτό είναι παρόμοιο με την τυπική διαδικασία ενός PKI, με την προσθήκη ενός ακόμη βήματος, της επικύρωσης του biotoken, για να διασφαλιστεί ότι κάποια επίθεση ενδιάμεσου ατόμου δεν αντικατέστησε το δημόσιο biotoken εντός του πιστοποιητικού, με κάποιο άλλο. Από ένα αποθηκευμένο λειτουργικό biotoken (operational biotoken) στην BCA, ένα τοπικό biotoken μπορεί να παραχθεί και να συγκριθεί με το bipartite biotoken που δημιουργήθηκε από το δημόσιο biotoken. Αν η σύγκριση είναι επιτυχής, τότε το πιστοποιητικό μπορεί να επικυρωθεί. Αυτό μειώνει τον κίνδυνο σύγκρουσης (collision attack), και για την BCA αλλά και για τους χρήστες, καθώς ένας επιτιθέμενος θα πρέπει να βρει μία σύγκρουση hash που να επικυρώνει το ψεύτικο πιστοποιητικό και να παραβιάσει βιομετρικά δεδομένα που θα ταυτίζονται επιτυχώς με το biotoken του εξουσιοδοτημένου εκπροσώπου της BCA ή του τελικού χρήστη.

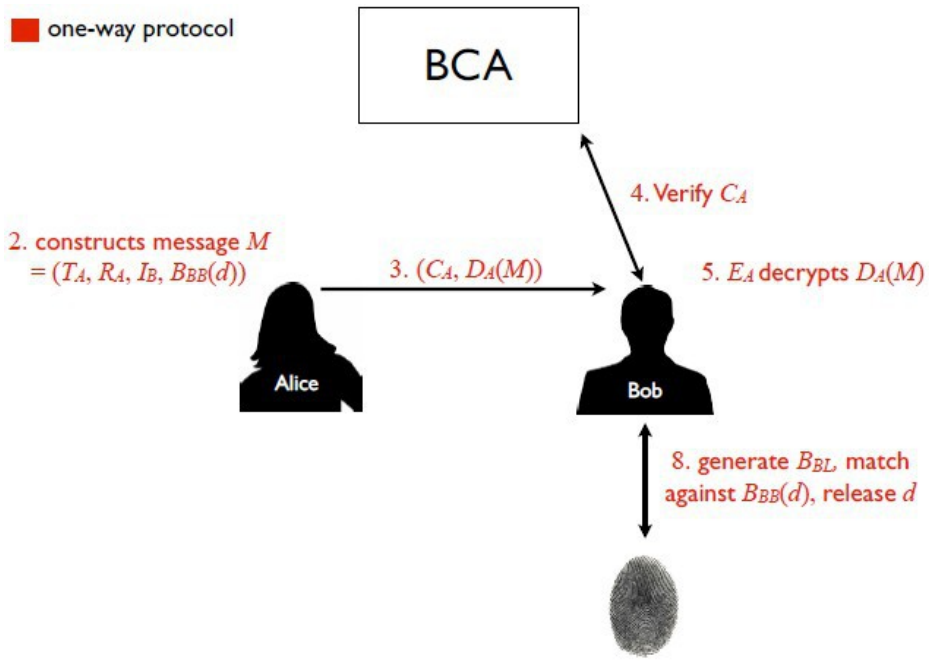
4.2 Πλαίσιο Αυθεντικοποίησης (Authentication Framework)

Για την αυθεντικοποίηση, πρέπει πρώτα να καταλάβουμε πώς παραλαμβάνονται τα πιστοποιητικά από τα μέλη που επιθυμούν να επικοινωνήσουν με κάποια σωστά πιστοποιημένη οντότητα εντός της BKI υποδομής. Στο σχήμα 26 παρουσιάζεται ένα παράδειγμα παραλαβής πιστοποιητικού, όπου ένας χρήστης, η Αλίκη, διασχίζει μία υποδομή αποτελούμενη από πέντε διαφορετικές BCA (BCA_A,...,BCA_E) για να παραλάβει το πιστοποιητικό ενός άλλου χρήστη, του Βύρωνα. Το πιστοποιητικό της Αλίκης που περιέχει το δημόσιο κλειδί της και το biotoken της, πιστοποιείται από τη BCA_A. Το πιστοποιητικό του Βύρωνα πιστοποιείται από την BCA_B. Η BCA_C, έχει ένα πιστοποιητικό υπογεγραμμένο από την BCA_A, έτσι η Αλίκη μπορεί να ξεκινήσει να ακολουθεί την διαδρομή μέσα από το γράφημα μέχρι τον Βύρωνα. Η BCA_D έχει ένα πιστοποιητικό υπογεγραμμένο από τη BCA_C, και η BCA_B έχει ένα πιστοποιητικό υπογεγραμμένο από την BCA_D. Μετακινούμενη στο γράφημα μέχρι την BCA_D, και έπειτα κάτω στον Βύρωνα, η Αλίκη μπορεί να επικυρώσει το πιστοποιητικό του Βύρωνα, και να παραλάβει το δημόσιο κλειδί του και το biotoken του για χρήση σε κάποιο πρωτόκολλο/συναλλαγή. Η BCA_E είναι η ρίζα BCA (root BCA), που υπογράφει όλα τα πιστοποιητικά των BCA κάτω από αυτήν και εξουσιοδοτεί βιομετρικά όλους τους εκπροσώπους των BCA, και έχει το πιστοποιητικό της υπογεγραμμένο από την ίδια.



Σχήμα 26: Η διαδρομή από την Αλίκη, η οποία επιθυμεί να αποκτήσει το πιστοποιητικό του Βύρωνος (Bob), μέχρι την BCAB η οποία πιστοποιεί το πιστοποιητικό του Βύρωνος, και κατά συνέπεια τον Βύρωνα, που κατέχει ένα πιστοποιητικό με το δημόσιο κλειδί του και το biotoken του

Ακολουθούν κάποια πρωτόκολλα με τα οποία μπορούμε να υποστηρίξουμε αυθεντικοποίηση με ισχυρότερη μη-αποποίηση. Για τα παρακάτω τρία πρωτόκολλα, υποθέτουμε πως η Αλίκη έχει καθιερώσει ένα μονοπάτι πιστοποίησης με τον Βύρωνα, όπως περιγράφηκε παραπάνω, και το πιστοποιητικό του Βύρωνα, περιέχει το δημόσιο κλειδί του και το biotoken. Η αρίθμηση των πρωτοκόλλων είναι διαδοχική, με κάθε πρωτόκολλο μετά το πρώτο, να βασίζεται στα προηγούμενα πρωτόκολλα.



Σχήμα 27: Η μεταφορά δεδομένων κάθε βήματος για το πρωτόκολλο μονής κατεύθυνσης

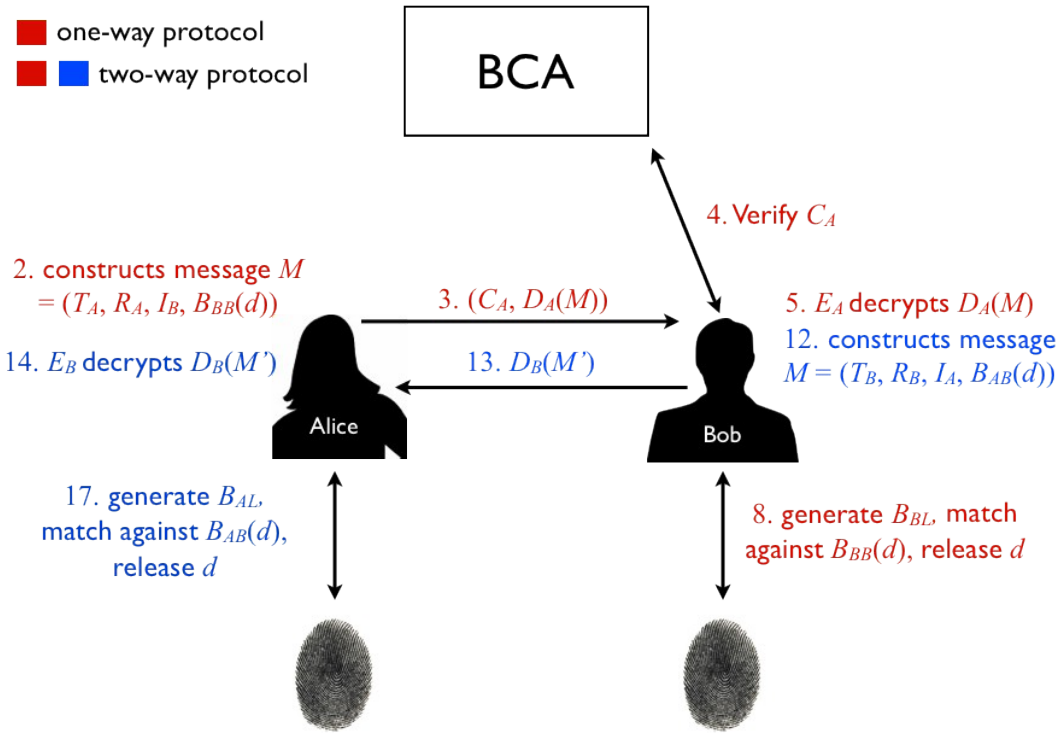
Πρωτόκολλο μονής κατεύθυνσης (The One-Way Protocol)

1. Η Αλίκη παράγει έναν τυχαίο αριθμό, R_A.
2. Η Αλίκη δημιουργεί ένα μήνυμα, M = (T_A, R_A, I_B, B_{BB}(d)), όπου T_A είναι η χρονοσφραγίδα (timestamp) της Αλίκης, I_B είναι η ταυτότητα του Βύρωνα, και d είναι ένα μικρό κομμάτι αυθαίρετων δεδομένων. Το d είναι ενσωματωμένο σε ένα bipartite biotoken B_{BB}(d) που παράγεται από το biotoken του Βύρωνα.
3. Η Αλίκη στέλνει (C_A, D_A(M)) στον Βύρωνα. (C_A είναι το πιστοποιητικό της Αλίκης, D_A είναι το ιδιωτικό κλειδί της Αλίκης).
4. Ο Βύρων επαληθεύει (verifies) το C_A και λαμβάνει το E_A. Σιγουρεύεται ότι τα κλειδιά δεν έχουν λήξει. (E_A είναι το δημόσιο κλειδί της Αλίκης).
5. Ο Βύρων χρησιμοποιεί το E_A για να αποκρυπτογραφήσει D_A(M). Αυτό επαληθεύει και την υπογραφή της Αλίκης και την ακεραιότητα της υπογεγραμμένης πληροφορίας.
6. Ο Βύρων ελέγχει το I_B στο M για ακρίβεια (accuracy).
7. Ο Βύρων ελέγχει το T_A στο M και επιβεβαιώνει ότι το μήνυμα είναι τωρινό.

8. Ο Βύρων παρέχει ένα βιομετρικό δείγμα σε έναν αισθητήρα. Ένα τοπικό biotoken B_{BL} παράγεται από το δείγμα. Το B_{BL} έπειτα συγκρίνεται με το $B_{BB}(d)$, απελευθερώνοντας το d.

9. Σαν προαιρετικό βήμα, ο Βύρων μπορεί να ελέγξει αν το R_A στο M βρίσκεται σε κάποια βάση δεδομένων παλιών τυχαίων αριθμών για να βεβαιωθεί ότι το μήνυμα δεν είναι κάποιο παλιότερο που αναμεταδόθηκε.

Αυτό το πρωτόκολλο καθιερώνει τις ταυτότητες και της Αλίκης και του Βύρωνα και την ακεραιότητα όλων των πληροφοριών που στέλνει η Αλίκη στον Βύρωνα, ειδικά αν το d είναι ένα κοινό μυστικό. Αυτό το πρωτόκολλο λειτουργεί ακόμα κι αν κρυπτογραφήσουμε το d με το δημόσιο κλειδί του Βύρωνα. Αλλά με την βιομετρική του έκδοση, ο Βύρων δεν θα χρειάζεται να έχει το ιδιωτικό του κλειδί πρόχειρο-μαζί του. Περαιτέρω ασφάλεια παρέχεται αν η Αλίκη έχει πρόσβαση σε μία ιδιωτική BCA που κατέχει το πιστοποιητικό του Βύρωνα, έτσι το biotoken του Βύρωνα θα ήταν ένα κοινό μυστικό. Κατά συνέπεια, μία επιτυχής Man-in-the-Middle επίθεση, θα έπρεπε να γνωρίζει το ιδιωτικό κλειδί της Αλίκης αλλά και το μυστικά αποθηκευμένο biotoken του Βύρωνα και το μυστικό d επίσης.



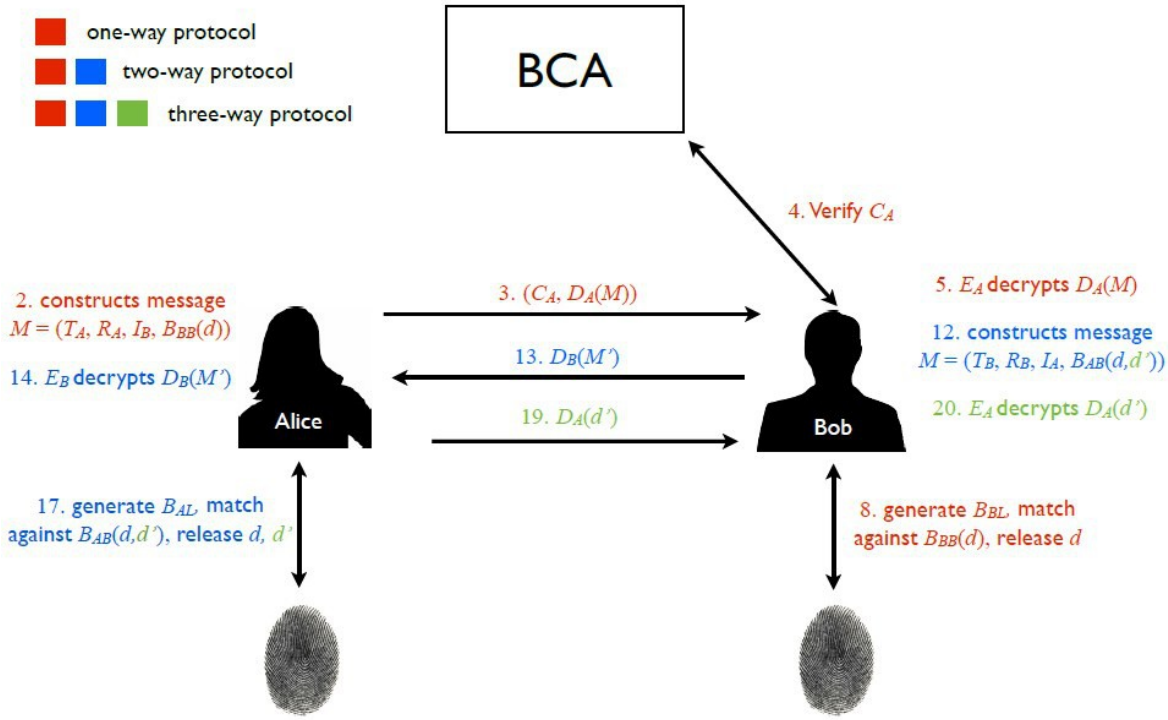
Σχήμα 28: Η μεταφορά δεδομένων κάθε βήματος για το πρωτόκολλο διπλής κατεύθυνσης

Πρωτόκολλο διπλής κατεύθυνσης (Two-Way Protocol)

10. Ο Βύρων παράγει έναν άλλο τυχαίο αριθμό, R_B.
11. Ο Βύρων δημιουργεί ένα μήνυμα M' = (T_B, R_B, I_A, B_{AB}(d)), όπου T_B είναι η χρονοσφραγίδα του Βύρωνα, I_A είναι η ταυτότητα της Αλίκης, και d είναι τα ίδια δεδομένα που ήταν και στο 2ο βήμα, το d είναι ενσωματωμένο σε ένα bipartite biotoken B_{AB}(d) που παράγεται από το biotoken της Αλίκης, που αποκτήθηκε από την C_A.
12. Ο Βύρων στέλνει D_B(M') στην Αλίκη.
13. Η Αλίκη χρησιμοποιεί το E_B για να αποκρυπτογραφήσει το D_B(M'). Αυτό επαληθεύει ταυτόχρονα, την υπογραφή του Βύρωνα και την ακεραιότητα των υπογεγραμμένων πληροφοριών.
14. Η Αλίκη ελέγχει το I_A στο M' για ακρίβεια.
15. Η Αλίκη ελέγχει το T_B στο M' και επιβεβαιώνει ότι το μήνυμα είναι τωρινό.
16. Η Αλίκη παρέχει ένα βιομετρικό δείγμα σε έναν αισθητήρα. Ένα τοπικό biotoken B_{AL} παράγεται από το δείγμα. Το B_{AL} έπειτα συγκρίνεται με το B_{AB}(d), απελευθερώνοντας το d. Αν αυτό το d συμπίπτει με το d που έστειλε κατά την πρώτη μετάδοση, η Αλίκη μπορεί να είναι βέβαιη ότι το βιομετρικό του Βύρωνα χρησιμοποιήθηκε για να ξεκλειδώσει το B_{BB}(d).
17. Σαν προαιρετικό βήμα, η Αλίκη μπορεί να ελέγξει το R_B στο M' για να βεβαιωθεί ότι το μήνυμα δεν είναι κάποιο παλιότερο που αναμεταδόθηκε.

Τώρα η Αλίκη έχει περαιτέρω διαβεβαίωση ότι ο Βύρων είναι πράγματι ο Βύρων και όχι κάποιος απατεώνας. Αλλά ο Βύρων ακόμα δεν έχει κάποια επιπλέον επιβεβαίωση για την ταυτότητα της Αλίκης, πέρα από το πιστοποιητικό της. Αυτό μπορεί να λυθεί με ένα πρωτόκολλο τριών-δρόμων, όπου επιπρόσθετα του d, ο Βύρων στέλνει ακόμα ένα d' εντός του ίδιου token (βήμα 16). Η Αλίκη μπορεί να επαληθεύσει το d (βήμα 17), και να στείλει το d' πίσω στον Βύρωνα για επαλήθευση.

18. Η Αλίκη παίρνει το ανακτημένο d' από το βήμα 16 και στέλνει το D_A(d') πίσω στον Βύρωνα.
19. Ο Βύρων χρησιμοποιεί το E_A για να αποκρυπτογραφήσει το D_A(d'), ξεκλειδώνοντας το d'. Ο Βύρων μπορεί να είναι βέβαιος ότι το βιομετρικό της Αλίκης χρησιμοποιήθηκε για να ξεκλειδώσει το B_{AB}(d) στο βήμα 17.



Σχήμα 29: Σχεδιάγραμμα των βημάτων μεταφοράς δεδομένων για τα πρωτόκολλα μονής, διπλής και τριπλής κατεύθυνσης. Υπονοείται πως η Αλίκη έχει το πιστοποιητικό του Βύρωνα C_B από την αρχή του πρωτοκόλλου μονής κατεύθυνσης

4.3 Ανάκληση και επανέκδοση (Revocation and Re-issue)

Σε αντίθεση με το τυπικό PKI, δεν μπορούμε να ανακαλέσουμε ένα πιστοποιητικό, να παράγουμε ένα νέο τυχαίο κλειδί και να κάνουμε επανέκδοση – πρέπει να επιλύσουμε και την βιομετρική επανέκδοση επίσης. Όταν μιλούμε για παραβίαση, εννοούμε μία παραβίαση του biotoken του ίδιου και όχι των αρχικών βιομετρικών χαρακτηριστικών.

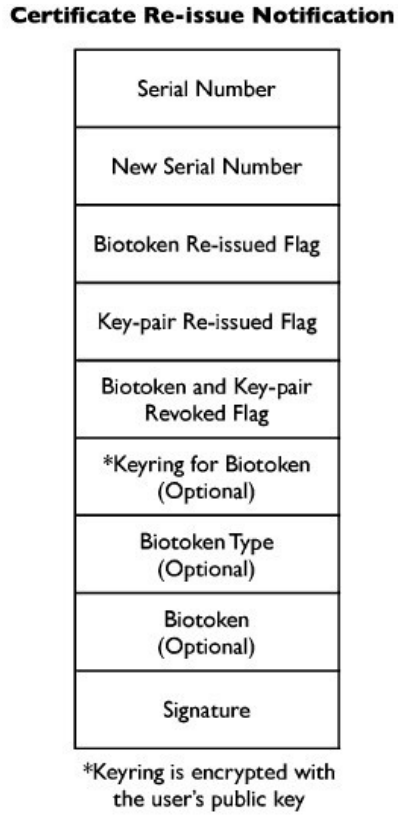
4.3.1 Σενάριο 1: Χειροκίνητη Επανέκδοση

Η BCA που εξέδωσε το πιστοποιητικό πρέπει να διατηρεί μία λίστα ανάκλησης πιστοποιητικών (certificate revocation list - CRL). Η λίστα περιέχει μόνο ανακληθέντα πιστοποιητικά, και όχι πιστοποιητικά που έληξαν. Αν παραβιάστηκε το κλειδί του χρήστη, ή αν παραβιάστηκε το biotoken του χρήστη, ή παραβιάστηκε

το κλειδί της BCA ή επειδή η BCA δεν θέλει να πιστοποιεί πλέον κάποιον χρήστη, το πιστοποιητικό του χρήστη μπορεί να ανακληθεί. Σε αυτό το σενάριο, υποτίθεται ότι η BCA δεν έχει διατηρήσει κάποια απαραίτητη πληροφορία μετασχηματισμού για να αντιστρέψει το biotoken που αποθηκεύει.

Για να ξεκινήσει η διαδικασία της ανάκλησης με επανεγγραφή, η BCA τοποθετεί το πιστοποιητικό υπό αμφισβήτηση στην CRL, και ειδοποιεί τον ιδιοκτήτη με μία Certificate Re-issue Notification (CRN) – ειδοποίηση επανέκδοσης πιστοποιητικού, μέσω των στοιχείων επικοινωνίας που παρέχονται-υπάρχουν στην αίτηση υπογραφής πιστοποιητικού CSR (Certificate Signing Request). Αν επιτραπεί στον ιδιοκτήτη η επανέκδοση, ένα νέο ζευγάρι κλειδιών δημόσιο-ιδιωτικό και ένα νέο biotoken παράγονται στον Σταθμό Αυθεντικοποίησης (Auth Station). Αυτή η πληροφορία στέλνεται πίσω στην BCA με την μορφή ενός νέου CSR. Αν αυτό το CSR γίνει αποδεκτό, εκδίδεται ένα νέο πιστοποιητικό.

Σε ένα εναλλακτικό σενάριο για χειροκίνητη επανέκδοση, δεν απαιτείται επανεγγραφή. Αν το biotoken του χρήστη, ή το biotoken και το ζεύγος κλειδιών, παραβιαστούν και η BCA κατέχει ένα αποθηκευμένο μη παραβιασμένο base biotoken που είχε χρησιμοποιηθεί για την παραγωγή του παραβιασμένου biotoken, ο ιδιοκτήτης μπορεί να επανεκδώσει το πιστοποιητικό του τροποποιώντας από την μεριά του, τους μετασχηματισμούς (transformations) που χρησιμοποιήθηκαν για την κωδικοποίηση, χωρίς την ανάγκη να υποβάλει κάποιο άλλο βιομετρικό δείγμα. Για να ξεκινήσει αυτή η διαδικασία της ανάκλησης, η BCA τοποθετεί το πιστοποιητικό υπό αμφισβήτηση στην CRL, και ειδοποιεί τον ιδιοκτήτη με μία CRN μέσω των στοιχείων επικοινωνίας που παρέχονται-υπάρχουν στην αίτηση υπογραφής πιστοποιητικού CSR (Certificate Signing Request). Αυτή η CRN περιέχει το base biotoken του ιδιοκτήτη. Ο ιδιοκτήτης θα παράγει νέα κλειδιά για την επανακωδικοποίηση του biotoken, και θα τα χρησιμοποιήσει για την παραγωγή ενός νέου biotoken. Αυτό το νέο biotoken και προαιρετικά ένα νέο δημόσιο κλειδί, στέλνονται πίσω στην BCA με ένα νέο CSR.



Σχήμα 30: Το νέο CRN μήνυμα για την ανάκληση και επανέκδοση πιστοποιητικού

Ενώ δύο σενάρια για αυτόματη επανέκδοση συζητούνται πιο κάτω, αν ένα δημόσιο κλειδί και ένα biotoken παραβιαστούν για ένα συγκεκριμένο πιστοποιητικό, τότε θα επιβάλλεται πάντα η χειροκίνητη επανέκδοση με επανεγγραφή. Χειροκίνητη επανέκδοση με επανεγγραφή επιβάλλεται επίσης αν το κλειδί της BCA παραβιαστεί, οπότε δεν μπορεί να υπάρχει πλέον εμπιστοσύνη στα υπάρχοντα δεδομένα που βρίσκονται αποθηκευμένα στην BCA.

4.3.2 Σενάριο 2: Αυτόματη Επανέκδοση Biotoken

Σε περιπτώσεις όπου η BCA ανιχνεύσει κάποια παραβίαση (ειδικά στην δική της υποδομή) ενός αποθηκευμένου biotoken, είναι πολύ θεμιτό να γίνεται ανάκληση και επανέκδοση πιστοποιητικών με κάποιο αυτόματο τρόπο. Για να υποστηριχθεί αυτό, η BCA πρέπει να έχει στην κατοχή της τα απαραίτητα κλειδιά για να αντιστρέψει το token, και ακολούθως να παράγει ένα νέο token βασισμένο σε αποθηκευμένες πληροφορίες. Αυτή η αποθηκευμένη πληροφορία δεν πρέπει να είναι τα αρχικά βιομετρικά χαρακτηριστικά. Ανακαλώντας το δέντρο έκδοσης/επανέκδοσης biotoken του σχήματος 21, token κάθε επιπέδου μπορούν

να παραχθούν από έναν Σταθμό Αυθεντικοποίησης (Auth Station), και να μεταδοθούν στην BCA. Έτσι, αν το biotoken είναι κωδικοποίησης δευτέρου ή μεγαλύτερου επιπέδου, κάθε BCA (εκτός ίσως από την ρίζα), που εκτελεί την αντιστροφή δεν θα είναι ικανή να ανακτήσει τα αρχικά βιομετρικά χαρακτηριστικά.

Η αρχική διαδικασία εγγραφής τροποποιείται σε αυτό το σενάριο για να μεταβιβάσει τις πληροφορίες μετασχηματισμού του κλειδιού, που χρησιμοποιήθηκαν για να δημιουργηθεί το biotoken εγγραφής, προς την BCA. Το CSR περιέχει ένα προαιρετικό πεδίο για να συμπεριλαμβάνεται ένας κρίκος κλειδιών (keyring) με όλα τα απαραίτητα κλειδιά/κωδικούς/προσδιοριστές-identifiers που χρησιμοποιήθηκαν για την κρυπτογράφηση του σταθερού μέρους του biotoken (κάποια κωδικοποίηση $w_{j,n}(w_{j,n-1},T_n)$, όπου n > 1, αν τα αρχικά βιομετρικά χαρακτηριστικά θέλουμε να είναι προστατευμένα), κατά τη διάρκεια του μετασχηματισμού. Η αιτούμενη οντότητα (που ζητάει την έκδοση πιστοποιητικού) θα συμπεριλάβει αυτόν τον κρίκο κλειδιών (keyring), κρυπτογραφημένο με το δημόσιο κλειδί της BCA, μέσα στην CSR. Η BCA θα αποθηκεύσει αυτό το κρυπτογραφημένο keyring σε περίπτωση που είναι απαραίτητο να γίνει ανάκληση και επανέκδοση.

Αν το biotoken του χρήστη έχει παραβιαστεί, το πιστοποιητικό του χρήστη μπορεί να ανακληθεί και να επανεκδοθεί αυτόματα. Για να ξεκινήσει η διαδικασία της ανάκλησης, η BCA τοποθετεί το πιστοποιητικό υπό αμφισβήτηση στην CRL, και ειδοποιεί τον ιδιοκτήτη με ένα CRN μέσω των στοιχείων επικοινωνίας που παρέχονται-υπάρχουν στην αίτηση υπογραφής πιστοποιητικού CSR (Certificate Signing Request). Αν επιτρέπεται στον ιδιοκτήτη η επανέκδοση, η BCA θα αναλάβει η ίδια την αντιστροφή του biotoken κατά ένα επίπεδο πίσω (στο $w_{j,n-1}$, όπου n > 1), να παράγει ένα νέο σετ από πληροφορίες μετασχηματισμού κλειδιού, και να επανεκδώσει το biotoken (παράγοντας $w'_{j,n}$). Ένα νέο πιστοποιητικό δημιουργείται με το νέο biotoken και το αρχικό δημόσιο κλειδί. Η BCA έπειτα στέλνει στον ιδιοκτήτη του πιστοποιητικού ένα CRN, το οποίο υποδεικνύει τον σειριακό αριθμό του ανακληθέντος πιστοποιητικού, τον σειριακό αριθμό του πιστοποιητικού που επανεκδόθηκε, και το νέο keyring για το νέο biotoken (κρυπτογραφημένο με το δημόσιο κλειδί του χρήστη). Αυτό το μήνυμα είναι υπογεγραμμένο από την BCA.

Η αυτόματη επανέκδοση μπορεί να συμβεί χωρίς να το αντιληφθεί ο χρήστης, με το BKI λογισμικό να παρατηρεί τη CRN, και ανανεώνοντας τις πληροφορίες μετασχηματισμού κλειδιού για την παραγωγή ενός biotoken στον Σταθμό Αυθεντικοποίησης (Auth Station) του χρήστη.

4.3.3 Σενάριο 3: Αυτόματη Επανέκδοση του Ζεύγους-Κλειδιών

Παρόμοια με το σενάριο 2, είναι ιδιαίτερα επιθυμητή η ανάκληση και επανέκδοση των πιστοποιητικών με κάποιο αυτόματο τρόπο, όταν το ζεύγος δημόσιο/ιδιωτικό κλειδί παραβιαστεί. Για να υποστηριχθεί αυτό, η BCA μπορεί να χρησιμοποιήσει ένα bipartite biotoken που έχει παραχθεί από ένα μη παραβιασμένο biotoken αποθηκευμένο στο πιστοποιητικό του χρήστη για να μεταφέρει ένα μυστικό πίσω στον χρήστη.

Αν το ζεύγος-κλειδιών του χρήστη έχει παραβιαστεί, το πιστοποιητικό του χρήστη μπορεί να ανακληθεί και να επανεκδοθεί αυτόματα. Για να ξεκινήσει η διαδικασία ανάκλησης, η BCA τοποθετεί το πιστοποιητικό υπό αμφισβήτηση στην CRL, και ειδοποιεί τον ιδιοκτήτη με ένα CRN μέσω των στοιχείων επικοινωνίας που παρέχονται-υπάρχουν στην αίτηση υπογραφής πιστοποιητικού CSR (Certificate Signing Request). Αν επιτρέπεται στον ιδιοκτήτη η επανέκδοση, η BCA θα αναλάβει η ίδια την παραγωγή ενός νέου ζεύγους κλειδιών. Έπειτα ένα νέο πιστοποιητικό δημιουργείται με το νέο δημόσιο κλειδί, και το αρχικό biotoken. Η BCA έπειτα ενσωματώνει το νέο ιδιωτικό κλειδί σε ένα bipartite biotoken που παράχθηκε από το biotoken του χρήστη. Η BCA τότε στέλνει στον ιδιοκτήτη του πιστοποιητικού μία ειδοποίηση επανέκδοσης πιστοποιητικού - Certificate Re-issue Notification (CRN), που υποδεικνύει τον σειριακό αριθμό του ανακληθέντος πιστοποιητικού, τον σειριακό αριθμό του πιστοποιητικού που επανεκδόθηκε, και το bipartite biotoken που περιέχει το ενσωματωμένο ιδιωτικό κλειδί. Αυτό το μήνυμα είναι υπογεγραμμένο από την BCA.

Η αυτόματη διαδικασία επανέκδοσης, θα απαιτήσει κάποια μεσολάβηση-παρέμβαση του χρήστη. Για την ακρίβεια, ο χρήστης πρέπει να υποβάλλει το βιομετρικό του δείγμα στον Σταθμό Αυθεντικοποίησης (Auth Station) για να απελευθερώσει το νέο ιδιωτικό κλειδί από το bipartite biotoken εντός του CRN.

4.4 Πιστοποιητικά με βιομετρικές πληροφορίες

Καθώς περιγράφαμε την υποδομή βιοκρυπτογραφικών κλειδιών (BKI), αναφέρθηκε η ανάγκη ύπαρξης πιστοποιητικών στα οποία εκτός από το δημόσιο κλειδί του κάθε χρήστη πρέπει να περιέχεται και το δημόσιο biotoken του. Υπάρχουν τρεις διαφορετικοί τρόποι για να εισάγουμε βιομετρικές πληροφορίες σε ένα πιστοποιητικό. Καμία από αυτές δεν έχει κάποιο ξεκάθαρο πλεονέκτημα σε σχέση με τις υπόλοιπες, για να μπορεί να προταθεί σαν μία γενική λύση, κι έτσι η επιλογή θα πρέπει να γίνεται ανάλογα με τις απαιτήσεις του εκάστοτε συστήματος.

4.4.1 X.509 v3 Extensions

Η έκδοση 3 του X.509 παρουσίασε έναν μηχανισμό επεκτάσεων. Ο μηχανισμός αυτός επιτρέπει σε οποιονδήποτε να δημιουργήσει μία νέα επέκταση, αρκεί να έρθει σε συνεννόηση με τις κατάλληλες αρχές πιστοποίησης (ITU ή ISO). Κάθε επέκταση περιέχει τις ακόλουθες πληροφορίες: Τύπος, Κρισιμότητα, Τιμή (Type, Criticality, Value).

Ο Τύπος χρησιμοποιείται σαν αναγνωριστικό της επέκτασης. Η Κρισιμότητα είναι μία ένδειξη (flag) ενός bit, που χρησιμοποιείται για να περιγράψει αν αυτή η πληροφορία στην επέκταση αυτή, μπορεί να αγνοηθεί ή όχι. Αν ενεργοποιηθεί και η εφαρμογή δεν μπορεί να διαχειριστεί τον τύπο της επέκτασης αυτής, τότε η εφαρμογή απορρίπτει το πιστοποιητικό. Μία εφαρμογή μπορεί να απαιτεί την παρουσία μίας επέκτασης για επεξεργασία άσχετα αν είναι δηλωμένη ως μη-κρίσιμη. Η ένδειξη κρισιμότητας υπάρχει για να διαβεβαιώνει ότι όλες οι εφαρμογές θα λάβουν υπόψιν τους αυτή την επέκταση διότι είναι μεγάλης σημασίας. Οι περισσότερες επεκτάσεις θα είναι μη-κρίσιμες. Η Τιμή περιέχει τα δεδομένα της επέκτασης.

Οι επεκτάσεις μπορούν να κατηγοριοποιηθούν σε τέσσερις ομάδες. Επεκτάσεις που αφορούν πληροφορίες για το κλειδί και την πολιτική που ακολουθείται, επεκτάσεις για περιορισμούς στην διαδρομή των πιστοποιητικών, επεκτάσεις για το υποκείμενο του πιστοποιητικού και τις ιδιότητες του εκδότη του πιστοποιητικού, και επεκτάσεις που αφορούν τις λίστες ανάκλησης πιστοποιητικών (CRL).

Ενώ θα μπορούσαμε να περιμένουμε να προταθεί και να εγκριθεί μία επέκταση για την προσθήκη πληροφοριών αυθεντικοποίησης, όπως είναι τα βιομετρικά πρότυπα, θα μπορούσαμε να δούμε αν υπάρχει κάποια ήδη εγκεκριμένη επέκταση που να μπορεί να διαχειριστεί τέτοιου είδους πληροφορίες. Από τις βασικές κατηγορίες των επεκτάσεων, μόνο η κατηγορία για επεκτάσεις που αφορούν το υποκείμενο του πιστοποιητικού και τις ιδιότητες του εκδότη του πιστοποιητικού, είναι κατάλληλη για την προσθήκη περισσότερων πληροφοριών σχετικά με το υποκείμενο. Οι απαιτήσεις για την συγκεκριμένη κατηγορία περιλαμβάνουν και την παρακάτω διατύπωση:

> Ένας χρήστης ενός πιστοποιητικού πιθανόν να χρειάζεται να μάθει με σιγουριά ορισμένες αναγνωριστικές πληροφορίες σχετικά με ένα υποκείμενο, έτσι ώστε να έχει μεγαλύτερη εμπιστοσύνη ότι το υποκείμενο είναι στην πραγματικότητα το άτομο ή η οντότητα που επιζητούσε.

Το μόνο πεδίο που αναφέρεται σε αυτή την ενότητα, που παρέχει τη δυνατότητα να τοποθετηθεί ένα γενικό χαρακτηριστικό, είναι το πεδίο subjectDirectoryAttributes. Το πεδίο αυτό (όπως ορίζεται από την ITU-T X.509), εκχωρεί οποιεσδήποτε επιθυμητές τιμές από ιδιότητες καταλόγου για το υποκείμενο του πιστοποιητικού. Ο παρακάτω ASN.1 τύπος ορίζεται για το πεδίο αυτό:

subjectDirectoryAttributes EXTENSION::={

SYNTAX AttributeSyntax

IDENTIFIED BY {id-ce subjectDirectory Attributes}}

AttributeSyntax::=SEQUENCE SIZE (1...MAX) OF Attribute

Αυτή η επέκταση είναι πάντα μη-κρίσιμη. Αυτό σημαίνει ότι μία εφαρμογή θα μπορεί να αγνοήσει αυτή την επέκταση αν δεν έχει την δυνατότητα να την διαχειριστεί. Αν υπάρχει μία ορισμένη ιδιότητα καταλόγου που θα μπορούσε να κρατήσει πληροφορίες αυθεντικοποίησης, τότε αυτή η επέκταση, θα ήταν η πιο κατάλληλη.

Τα πλεονεκτήματα, αν χρησιμοποιήσουμε αυτό το πεδίο είναι:

1. Η χρήση μίας ήδη καθορισμένης επέκτασης για την υλοποίηση πληροφοριών αυθεντικοποίησης και επαλήθευσης δεν απαιτεί κάποιο μεγάλο διάστημα αναμονής μέχρι να γίνει αποδεκτή.
2. Καθώς η επέκταση είναι μη-κρίσιμη, αυτές οι πληροφορίες μπορούν να αγνοούνται από εφαρμογές που δεν τις χρειάζονται.
3. Το πεδίο υλοποιεί μία εγκεκριμένη επέκταση σε ένα παγκόσμιο πρότυπο.

Τα μειονεκτήματα, είναι:

1. Οι πληροφορίες σε ένα x.509 πιστοποιητικό είναι δημόσιες. Μία ιδιότητα εντός ενός πιστοποιητικού δεν μπορεί να είναι απόρρητη.
2. Η πληροφορία εντός ενός πιστοποιητικού είναι άμεσα συνυφασμένη με τη διάρκεια ζωής του πιστοποιητικού.

4.4.2 PKCS #6 Extended Certificate Syntax Standard

Η RSA Data Security Inc. παρουσίασε ένα επεκτεταμένο X.509 πιστοποιητικό. Η επέκταση επιτρέπει σε ένα υπάρχον X.509 πιστοποιητικό να ενσωματωθεί εντός μίας δομής που προσθέτει επιπλέον πληροφορίες. Αυτό επιτρέπει την εξαγωγή ενός X.509 πιστοποιητικού από το επεκτεταμένο πιστοποιητικό για προς τα πίσω συμβατότητα.

Το PCKS#6 περιέχει ένα ExtendedCertificateInfo πεδίο το οποίο έχει την ακόλουθη ASN.1 σύνταξη:

ExtendedCertificateInfo::=SEQUENCE{

version Version

certificate Certificate

attribute Attributes}

Το PCKS#6 χρησιμοποιεί τα πρότυπα από το X.509 και ιδιότητες για να δημιουργήσει έναν “φάκελο” γύρω από το πιστοποιητικό. Αυτός ο φάκελος μπορεί να έχει χρήσιμες πληροφορίες αυθεντικοποίησης, όπως βιομετρικές πληροφορίες, χωρίς να κάνει κάποιες αλλαγές στο υπάρχον πρότυπο.

Καθώς η αυθεντικοποίηση του υποκειμένου θα χρειαστεί σε λίγες ενέργειες (όπως logon, μεγάλες συναλλαγές οικονομικής φύσης κτλ) αυτή η μέθοδος έχει ένα μεγάλο πλεονέκτημα, καθώς υπάρχει η δυνατότητα να αφαιρεθούν τα επιπλέον δεδομένα που χρειάζονται για την αυθεντικοποίηση και να κρατηθεί το x.509 πιστοποιητικό.

Πλεονεκτήματα:

1. Το επεκτεταμένο πιστοποιητικό αφήνει ακέραιο το αρχικό x.509 πιστοποιητικό και το επικαλύπτει με επιπρόσθετες υπογεγραμμένες πληροφορίες. Μπορεί λοιπόν να γίνει απόσπαση του x.509 πιστοποιητικού, για λόγους συμβατότητας με άλλα πρότυπα ή προϋπάρχουσες εφαρμογές. Εφαρμογές στις οποίες η ταχύτητα είναι σημαντική, και δεν απαιτούν τις πληροφορίες που βρίσκονται στο επεκτεταμένο πιστοποιητικό, δεν χρειάζεται να διαχειριστούν τις επιπλέον πληροφορίες.
2. Το X.509 πιστοποιητικό και το επεκτεταμένο πιστοποιητικό μπορούν να επικυρωθούν σε ένα βήμα, καθώς είναι υπογεγραμμένα από τον ίδιο εκδότη πιστοποιητικών.

3. Μόνο οι επιπρόσθετες πληροφορίες που απαιτούνται θα τοποθετηθούν στο επεκτεταμένο πιστοποιητικό. Οι εφαρμογές που χρησιμοποιούν το επεκτεταμένο πιστοποιητικό θα έχουν πρόσβαση σε όλες τις πληροφορίες εντός του X.509 πιστοποιητικού.
4. Διαφορετικές Αρχές Πιστοποίησης (CA) θα μπορούσαν να χρησιμοποιηθούν για την δημιουργία πιστοποιητικών και επεκτεταμένων πιστοποιητικών. Αυτά θα απαιτούσε την χρήση δύο διαφορετικών υπογραφών, αλλά, θα επέτρεπε η λειτουργία της εγγραφής να μεταφερθεί σε άλλες CA.

Μειονεκτήματα:

1. Το PCKS δεν είναι κάποιο παγκόσμιο πρότυπο.
2. Δύο υπογραφές θα πρέπει να δημιουργηθούν από την CA: μία για το X.509 πιστοποιητικό και μία για το επεκτεταμένο πιστοποιητικό. Αυτό ίσως ελαττώσει την αποτελεσματικότητα της CA.
3. Προσθέτοντας το επεκτεταμένο πιστοποιητικό, το σύστημα γίνεται πιο πολύπλοκο και η επίλυση ζητημάτων που σχετίζονται με την διαχείριση των κλειδιών γίνεται πιο πολύπλοκη εργασία.
4. Αν χρησιμοποιηθούν δύο διαφορετικές υπογραφές, η επαλήθευση δύο διαφορετικών υπογραφών θα απαιτεί περισσότερο υπολογιστικό χρόνο και πόρους.

4.4.3 Πιστοποιητικά Ιδιοτήτων - Attribute Certificates

Τα πιστοποιητικά Ιδιοτήτων είναι στην ουσία X.509 πιστοποιητικά χωρίς τις πληροφορίες που αφορούν το δημόσιο κλειδί. Μπορεί να τα δει κανείς και ως επεκτεταμένα πιστοποιητικά, χωρίς το X.509 πιστοποιητικό ενσωματωμένο μέσα τους. Χρησιμοποιούνται για να μεταφέρουν ένα σύνολο από ιδιότητες μαζί με το αναγνωριστικό του πιστοποιητικού δημόσιου κλειδιού (δηλαδή το serial number και το όνομα του εκδότη, issuer name, ενός πιστοποιητικού δημόσιου κλειδιού) ή το όνομα της οντότητας. Οι ιδιότητες τοποθετούνται σε μία ξεχωριστή δομή για να διατηρηθεί η συμβατότητα με τα υπάρχοντα διεθνή στάνταρντ (X.509). Μία οντότητα μπορεί να έχει πολλά πιστοποιητικά ιδιοτήτων που να σχετίζονται με κάθε ένα από τα πιστοποιητικά δημόσιου κλειδιού που έχει. Δεν υπάρχει η απαίτηση ότι η ίδια αρχή θα πρέπει να δημιουργήσει το πιστοποιητικό δημόσιου κλειδιού και το

πιστοποιητικό ιδιοτήτων. Οι προδιαγραφές του X9.57 καθορίζουν μία ιδιότητα, σαν εκείνες τις πληροφορίες (εκτός από το δημόσιο κλειδί), που βρίσκονται εντός ενός πιστοποιητικού ιδιοτήτων και παρέχονται από μία οντότητα ή μία αρχή ιδιοτήτων και πιστοποιούνται από την αρχή ιδιοτήτων. Οι ιδιότητες προσάπτονται σε ένα πιστοποιητικό δημόσιου κλειδιού ή το όνομα μίας οντότητας, με την υπογραφή της αρχής ιδιοτήτων στο πιστοποιητικό ιδιοτήτων.

Πλεονεκτήματα:

1. Μπορεί να γίνει αμοιβαία επαλήθευση, με πρόκληση-απόκριση μεταξύ του κατόχου του πιστοποιητικού ιδιοτήτων και της οντότητας που κάνει την αυθεντικοποίηση, πριν από την αποστολή των πληροφοριών με τις ιδιότητες.
2. Οι πληροφορίες με τις ιδιότητες μπορεί να είναι κρυπτογραφημένες, παρέχοντας πρόσβαση στις απόρρητες πληροφορίες μόνο σε επικυρωμένες οντότητες που διενεργούν την αυθεντικοποίηση.
3. Οι πληροφορίες μπορούν να είναι χωρισμένες σε πολλά πιστοποιητικά ιδιοτήτων, αν απαιτείται από το σύστημα.
4. Ανωνυμία μπορεί να παρέχεται αν το Distinguished Name (DN) του χρήστη σε ένα X.509 πιστοποιητικό είναι μία αναφορά, και όχι κάποια πραγματική ταυτότητα. Το DN μπορεί να χρησιμοποιηθεί για να συγκρίνονται πιστοποιητικά ιδιοτήτων με X.509 πιστοποιητικά.
5. Τα πιστοποιητικά ιδιοτήτων είναι παγκόσμιο πρότυπο (όπως το X.509)

Μειονεκτήματα:

1. Η παρουσία πολλών αρχών ιδιοτήτων στην αρχιτεκτονική δομή ενός συστήματος, κάνει το σύστημα πιο πολύπλοκο.
2. Ο χρόνος για την αυθεντικοποίηση των χρηστών ίσως είναι ένα ζήτημα αν δύο υπογραφές πρέπει να επαληθευτούν και αν το πιστοποιητικό ιδιοτήτων χρειάζεται να αποκρυπτογραφηθεί.

4.5 Εφαρμογές

Τώρα που είδαμε την υποδομή και τα πρωτόκολλα, μπορούμε να ξεκινήσουμε να σκεφτόμαστε για την χρησιμότητα του BKI σε διάφορες εφαρμογές. Εργαλεία του διαδικτύου είναι πρωταρχικού ενδιαφέροντος. Η επιβολή της επικύρωσης των

εξυπηρετητών (servers) είναι σημαντική, αν θέλουμε να υπερνικήσουμε Phishing και Man-in-the-Middle επιθέσεις. Το πρωτόκολλο μονής κατεύθυνσης που παρουσιάστηκε, είναι κατάλληλο για επικύρωση εξυπηρετητών, και επιβάλλει στον χρήστη να δράσει παρουσιάζοντας ένα βιομετρικό δείγμα όταν λαμβάνει ένα πιστοποιητικό. Για επικύρωση εξυπηρετητών, το d μπορεί να είναι ένα “μήνυμα καλωσορίσματος” που βάζει ο Βύρων κατά τη διάρκεια της εγγραφής. Το βιομετρικό μέρος αυτού του σχήματος επιβάλλει στον Βύρωνα να επικυρώσει την ακεραιότητα του εξυπηρετητή, ακόμα και αν ο έλεγχος του πιστοποιητικού έγινε και αγνοήθηκε. Αν ο Βύρων μπορεί να ξεκλειδώσει το $B_{BB}(d)$ και να πάρει το “μήνυμα καλωσορίσματος” πίσω, τότε ο εξυπηρετητής είναι πράγματι νόμιμος. Αυτό το πρωτόκολλο μπορεί να ενσωματωθεί σε κοινά διαδικτυακά εργαλεία, όπως web browsers, email clients και instant messaging clients που ήδη υποστηρίζουν PKI. Η μόνη διαφορά για τους χρήστες είναι ότι θα απαιτείται από αυτούς να υποβάλλουν ένα βιομετρικό δείγμα κατά την παραλαβή ενός πιστοποιητικού από κάποιον εξυπηρετητή.

Όσον αφορά τις δικτυακές υπηρεσίες, BKI συμβατές υπηρεσίες, παρέχουν ισχυρότερη αυθεντικοποίηση, δίνοντας στον χρήστη περισσότερη εμπιστοσύνη για τον εξυπηρετητή και στον εξυπηρετητή περισσότερη εμπιστοσύνη ότι έχει να κάνει με νόμιμο χρήστη. Η εργασία [23] πρότεινε την χρήση bipartite biotokens σε ένα πρωτόκολλο Kerveros, αλλά σε μία αυτόνομη διαμόρφωση χωρίς πιστοποιητικά που πιστοποιούν biotokens. Κάποιος μπορεί επίσης να οραματιστεί ένα σχήμα παρόμοιο με το s/Key[10] χρησιμοποιώντας bipartite biotokens. Σε αυτό το σχήμα, από τη στιγμή που λαμβάνεις την αίτηση, ο εξυπηρετητής αυθεντικοποίησης παράγει έναν κωδικό μίας χρήσης και δημιουργεί ένα bipartite biotoken που περιέχει αυτό τον κωδικό. Αν ο πελάτης (client) ταιριάξει με το bipartite biotoken που έστειλε ο εξυπηρετητής αυθεντικοποίησης, θα απελευθερώσει τον κωδικό και θα ολοκληρωθεί η αυθεντικοποίηση. Για να λυθεί το πρόβλημα της διανομής των biotoken για δικτυακή αυθεντικοποίηση, ένα PKI-συμβατό LDAP μπορεί να χρησιμοποιηθεί με παρόμοιο τρόπο για BKI εφαρμογές. Έτσι, μια μεγάλη ποικιλία σχημάτων αυθεντικοποίησης μπορούν να εκμεταλλευτούν ένα κοινό αποθετήριο πιστοποιητικών, συμπεριλαμβάνοντας εγγραφές χρήστη, κλειδιά και biotokens.

Τα ψηφιακά έγγραφα αποτελούν ένα ακόμα σημαντικό πεδίο εφαρμογής για το BKI. Πολλά ευαίσθητα έγγραφα, συμπεριλαμβανομένων ιατρικών αρχείων, οικονομικών αρχείων και κυβερνητικών εγγράφων, προστατεύονται χρησιμοποιώντας PKI και ψηφιακές υπογραφές. Χρησιμοποιώντας bipartite biotokens, το κλειδί που χρησιμοποιείται για να κρυπτογραφήσει ένα έγγραφο που ανήκει στον Βύρωνα μπορεί να ενσωματωθεί στο bipartite biotoken του Βύρωνα. Έτσι, μόνο ο Βύρων θα μπορεί να απελευθερώσει το κλειδί, και να έχει πρόσβαση

στο έγγραφο. Για ψηφιακές υπογραφές, ένα πρωτόκολλο εξυπηρετητή υπογραφών (signature server protocol) μπορεί να προσθέσει ένα μέρος βιομετρικής εξουσιοδότησης στην τυπική διαδικασία υπογραφών. Με το BKI να παρέχει έναν μηχανισμό διανομής πιστοποιητικών, μία ολοκληρωμένη λύση ασφαλείας για τη διαχείριση εγγράφων γίνεται πραγματικότητα.

Σε όλες αυτές τις εφαρμογές, η ευχρηστία είναι φυσικά μία λογική ανησυχία. Προσθέτοντας ένα δεύτερο φυσικό παράγοντα, προσθέτουμε περισσότερη δουλειά στον χρήστη και υπάρχει ένα μικρό κόστος για τον επιπρόσθετο αισθητήρα. Όμως, δεν απαιτείται πολλή δουλειά για να υποβληθεί ένα βιομετρικό δείγμα και τα τελευταία χρόνια αισθητήρες συναντάμε σε όλο και περισσότερες συσκευές. Θα λέγαμε ακόμη ότι χάρη στην εξάπλωση των βιομετρικών συστημάτων τα τελευταία χρόνια, πολλοί χρήστες είναι ήδη εξοικειωμένοι με την χρήση τους. Πολλά laptops είναι ήδη εξοπλισμένα με φθηνούς αισθητήρες δακτυλικών αποτυπωμάτων. Θα μπορούσε ακόμη ένας χρήστης να βρει μία χρυσή τομή, και να κάνει επιλεκτική χρήση βιομετρίας, ανάλογα με την περίσταση. Αν ένας χρήστης είναι πολύ προβληματισμένος για την ασφάλεια των οικονομικών συναλλαγών του, μπορεί να επιλέξει να χρησιμοποιεί BKI μόνο για συγκεκριμένες ιστοσελίδες που έχουν σχέση με οικονομικές υπηρεσίες και να παίρνει κάποιο ρίσκο χρησιμοποιώντας συμβατικές PKI διατάξεις σε όλες τις υπόλοιπες περιπτώσεις.

ΕΠΙΛΟΓΟΣ

Στο κεφάλαιο αυτό είδαμε πώς με την προσθήκη μίας τεχνολογίας προστασίας προτύπων, όπως είναι τα biotoken με υποστήριξη ανάκλησης, μέσα στις αιτήσεις για ψηφιακή υπογραφή πιστοποιητικού (digital certificate signing requests), επιτυγχάνεται βελτίωση της μη-αποποίησης και κατά συνέπεια μεγαλώνει η εμπιστοσύνη μεταξύ των χρηστών και των αρχών πιστοποίησης. Ακόμη με την προσθήκη ενός δεύτερου παράγοντα που επιτρέπει την ασφαλή αποστολή ενσωματωμένων δεδομένων, μπορεί να υποστηριχθεί αυτόματη ανάκληση πιστοποιητικού και επανέκδοση. Ο απώτερος στόχος είναι να αποτραπούν επιθέσεις phishing και ενδιάμεσου ατόμου, και αυτό επιτυγχάνεται χρησιμοποιώντας τα πρωτόκολλα που περιγράφηκαν για ασφαλή αυθεντικοποίηση μεταξύ δύο μελών που χρησιμοποιούν κλειδιά και biotokens. Κάνοντας χρήση των πρωτοκόλλων που περιγράφηκαν, δίνεται η δυνατότητα να βελτιωθούν γνωστές εφαρμογές όπως το LDAP, διαδικτυακά προγράμματα (όπως οι browsers, το email και προγράμματα συνομιλίας IM) και η ψηφιακή υπογραφή εγγράφων.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Στο [20] εκφράζεται η άποψη ότι ενώ η ιδέα των revocable biotokens είναι πολλά υποσχόμενη, αφήνει κάποιες ερωτήσεις αναπάντητες. Ο σχεδιασμός της βοηθητικής συνάρτησης, η οποία χωρίζει τα βιομετρικά χαρακτηριστικά στο σταθερό μέρος και το μέρος με τα υπόλοιπα, δεν εξηγείται λεπτομερώς και δεν υπάρχουν στοιχεία για το πόσο αποτελεσματική είναι αυτή η μέθοδος με άλλα βιομετρικά στοιχεία, πέρα από τα δακτυλικά αποτυπώματα.

Στο [6] αναφέρεται ότι τα biotokens είναι ευάλωτα σε επίθεση αντίστροφης αναζήτησης. Μαθαίνοντας τις παραμέτρους μετασχηματισμού t και s και τον αλγόριθμο κρυπτογράφησης (το δημόσιο κλειδί ή την συνάρτηση hash), ο επιτιθέμενος θα μπορούσε να αποκτήσει το g από το w, χρησιμοποιώντας αντίστροφη αναζήτηση. Τρέχοντας μία μικρή δοκιμαστική βιομετρική βάση δεδομένων, ο επιτιθέμενος μπορεί να καθορίσει το εύρος του u' και κατά συνέπεια, όλους τους πιθανούς αριθμούς του g. Αυτό το εύρος δεν είναι πολύ μεγάλο, ειδάλλως, η ακρίβεια του συστήματος θα έπεφτε λόγω υπερβολικής κβαντοποίησης. Ο πίνακας αναζήτησης δημιουργείται εφαρμόζοντας τον αλγόριθμο κρυπτογράφησης σε όλες τις πιθανές τιμές του g. Τέλος πιστεύεται ότι η επίθεση αντίστροφης αναζήτησης θα ανακατασκευάσει το ακριβές βιομετρικό πρότυπο από τα αποθηκευμένα δεδομένα, πράγμα που σημαίνει ότι το σύστημα δεν είναι ιδιαίτερα ασφαλέστερο από πλευράς προστασίας της ασφάλειας και ιδιωτικότητας απ' ό,τι άλλα συστήματα μετασχηματισμού των χαρακτηριστικών με αντιστρέψιμους μετασχηματισμούς. Δεν αναφέρεται όμως κάποιο ενδεικτικό νούμερο της προσπάθειας που απαιτείται για να γίνει κάτι τέτοιο και έτσι δεν μπορώ προσωπικά να αξιολογήσω το μέγεθος του κινδύνου. Ακόμα όμως και αν παραδεχτούμε ότι είναι αξιοσημείωτος ο κίνδυνος, θα μπορούσαμε να πούμε πως η επίθεση αυτή εφαρμόζεται μόνο στα root biotokens, καθώς για να εφαρμοστεί σε κάποιο master ή operational biotoken, ο επιτιθέμενος θα πρέπει να έχει στην κατοχή του περισσότερα κλειδιά (και αυτή τη φορά θα χρειάζεται τα ιδιωτικά κλειδιά).

Τα biotokens με υποστήριξη ανάκλησης (revocable biotokens) και κατά προέκταση τα bipartite biotokens, όπως περιγράφηκε σε αυτή την πτυχιακή εργασία, κατέχουν μερικές μοναδικές ιδιότητες που άλλες τεχνολογίες προστασίας προτύπων δεν διαθέτουν. Αν εξαιρέσουμε την επίθεση που περιγράφηκε προηγουμένως, που μένει να μελετηθεί κατά πόσο είναι εφικτή, η συγκεκριμένη τεχνολογία προστασίας προτύπων παρέχει ικανοποιητική προστασία, υποστηρίζει ανάκληση και επανέκδοση, υποστηρίζει την δημιουργία ιεραρχίας προτύπων για διαφορετικές χρήσεις, επιτρέπει την απελευθέρωση κλειδιών/δεδομένων έπειτα από επιτυχή

ταύτιση και τέλος υποστηρίζει δημόσια πρότυπα τα οποία μπορεί να χρησιμοποιήσει κανείς για να στείλει κάποιο μήνυμα στο κάτοχο του προτύπου. Επίσης δεν θα πρέπει να ξεχνάμε πως όλα αυτά τα καταφέρνει χωρίς να υπάρχει μείωση στην απόδοση σύγκρισης. Κατέχει άλλωστε την πρώτη θέση ανάμεσα σε όλους τους αλγόριθμους προστασίας προτύπων που έχουν πάρει μέρος στον διαγωνισμό FVC Ongoing και επέλεξαν να δημοσιευτούν τα αποτελέσματα τους.

Η υποδομή BKI που περιγράφηκε, βελτιώνει την μη-αποποίηση και προστατεύει από επιθέσεις phishing και ενδιάμεσου ατόμου, αλλά ίσως το κόστος υλοποίησης και συντήρησης να αποδειχτεί μεγάλο. Το πρότυπο x.509 είναι αρκετά πολύπλοκο και ασαφές σε ορισμένα σημεία, με αποτέλεσμα να εμφανίζονται συχνά προβλήματα στην ομαλή λειτουργία μεταξύ συστημάτων, όταν χρησιμοποιούνται διαφορετικές βιβλιοθήκες και λειτουργικά συστήματα. Το να ενσωματώσεις βιομετρικές πληροφορίες εντός ενός πιστοποιητικού x.509 δεν είναι απλή υπόθεση. Όπως είδαμε, υπάρχουν περισσότεροι από ένας τρόποι, ο καθένας με τα δικά του πλεονεκτήματα και μειονεκτήματα. Επίσης δεν έχει βρεθεί κάποιος αποτελεσματικός και εύκολος τρόπος για την διαχείριση των λιστών ανάκλησης πιστοποιητικών. Εφόσον στο BKI οι λόγοι για ανάκληση ενός πιστοποιητικού είναι περισσότεροι: παραβίαση του ιδιωτικού κλειδιού και παραβίαση του biotoken ενός χρήστη, ίσως είναι εύλογο να υποθέσουμε ότι οι περιπτώσεις όπου θα χρειαστεί να γίνει κάποια ανάκληση πιστοποιητικού, θα είναι περισσότερες. Μπορεί η διαδικασία τις περισσότερες φορές να γίνεται αυτόματα για τον χρήστη, αλλά δεν παύει το διαχειριστικό κόστος να αυξάνεται. Αρκεί κανείς να αναλογιστεί την διαφορά στο πλήθος των κλειδιών που έχει να διαχειριστεί μία υποδομή βιοκρυπτογραφικού κλειδιού σε σχέση με μία τυπική υποδομή δημόσιου κλειδιού, για να αντιληφθεί ότι το διαχειριστικό κόστος θα είναι αρκετά αυξημένο.

Στο [1] προτείνεται μία βελτιωμένη εκδοχή της BKI, η οποία αποκαλείται Έμπιστες Βιομετρικές Διαδικτυακές Ταυτότητες, Trusted Biometric Web Identities (Trusted-BWI). Η νέα γενιά βιομετρικών αισθητήρων ασφαλείας, είναι εφοδιασμένη με επιπλέον υλικό (hardware), το οποίο αποκαλείται Υπομονάδα Έμπιστης Πλατφόρμας – Trusted Platform Module (TPM) και στην ουσία αποτελείται από έναν μικροελεγκτή ασφαλείας κατάλληλο για κρυπτογραφικές πράξεις, μαζί με κάποιον ασφαλή χώρο αποθήκευσης. Η βιομετρική σύγκριση γίνεται εντός του αισθητήρα και αν η ταύτιση είναι επιτυχής, ο βιομετρικός αισθητήρας απελευθερώνει τον κωδικό του χρήστη ή γίνεται χρήση ενός ιδιωτικού κλειδιού που είναι αποθηκευμένο στον ασφαλή χώρο αποθήκευσης. Αυτού του είδους οι βιομετρικοί αισθητήρες, που δεν αποκαλύπτουν βιομετρικά δεδομένα, δεν είναι συμβατοί με την BKI υλοποίηση. Οι συγγραφείς της παραπάνω εργασίας παρουσιάζουν μία βελτιωμένη έκδοση που επιτρέπει την χρήση τέτοιων

αισθητήρων. Εκτός από το δημόσιο κλειδί σε ένα πιστοποιητικό και το biotoken, προστίθεται προαιρετικά και ένα βιομετρικό δημόσιο κλειδί. Στη συνέχεια παρουσιάζεται η έννοια ενός Ασύμμετρου Βιοκρυπτογραφικού Υποσυστήματος (Asymmetric Bio-Cryptographic Subsystem (ABCS), το οποίο υλοποιείται στο firmware ή μέσω hardware κατά προτίμηση και παρέχει λειτουργίες ασύμμετρης κρυπτογραφίας (όπως κρυπτογράφηση δημόσιου κλειδιού), και πρόσβαση ή χρήση του βιομετρικού ιδιωτικού κλειδιού μόνο έπειτα από βιομετρική αυθεντικοποίηση. Το βιομετρικό ιδιωτικό κλειδί θα πρέπει να χρησιμοποιείται ή να έχει κάποιος πρόσβαση σε αυτό, μόνο έπειτα από βιομετρική αυθεντικοποίηση του κατόχου του κλειδιού. Για να επιτευχθεί αυτό, προτείνονται τέσσερις περιπτώσεις με διαφορετικό βαθμό ασφαλείας. Στην πρώτη περίπτωση, το βιομετρικό ιδιωτικό κλειδί θα μπορούσε να φυλάσσεται σε μία υπομονάδα έμπιστης πλατφόρμας (TPM), εντός του βιομετρικού αισθητήρα. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον μικροελεγκτή για να υπογράφει ή να αποκρυπτογραφεί δεδομένα έπειτα από επιτυχή βιομετρική ταύτιση. Η δεύτερη περίπτωση, λιγότερο ασφαλής, είναι το βιομετρικό ιδιωτικό κλειδί να κρυπτογραφηθεί με ένα κλειδί που φυλάσσεται εντός του αισθητήρα όπως στην προηγούμενη περίπτωση, και να απελευθερώνεται μόνο έπειτα από επιτυχή βιομετρική ταύτιση. Τρίτη περίπτωση, η χρήση κάποιου εικονικού virtual TPM[19] και κάποιου Firmware TPM[27], μειώνοντας το κόστος και παρέχοντας ένα περιβάλλον έμπιστης εκτέλεσης (Trusted Execution Environment – TEE). Τέλος η εναλλακτική λύση είναι ένα μοντέλο με χρήση λογισμικού για την προστασία του βιομετρικού ιδιωτικού κλειδιού. Σε αυτή την περίπτωση το βιομετρικό ιδιωτικό κλειδί, ενσωματώνεται σε ένα bipartite biotoken, ή ενσωματώνεται ένα κλειδί το οποίο κρυπτογραφεί το βιομετρικό ιδιωτικό κλειδί. Το βιομετρικό ιδιωτικό κλειδί, ή το κλειδί για την αποκρυπτογράφηση του, απελευθερώνονται από το bipartite biotoken μόνο έπειτα από επιτυχή ταύτιση του χρήστη. Στην ιδανικότερη περίπτωση, το λογισμικό ή το firmware για το ABCS θα πρέπει να είναι αποκομμένο από το λειτουργικό σύστημα. Με την παρουσίαση του ABCS και κάνοντας χρήση του βιομετρικού ιδιωτικού κλειδιού, δίδεται πλέον η δυνατότητα στη BKI να υποστηρίξει όλα τα είδη βιομετρικών αισθητήρων, με ή χωρίς TPM.

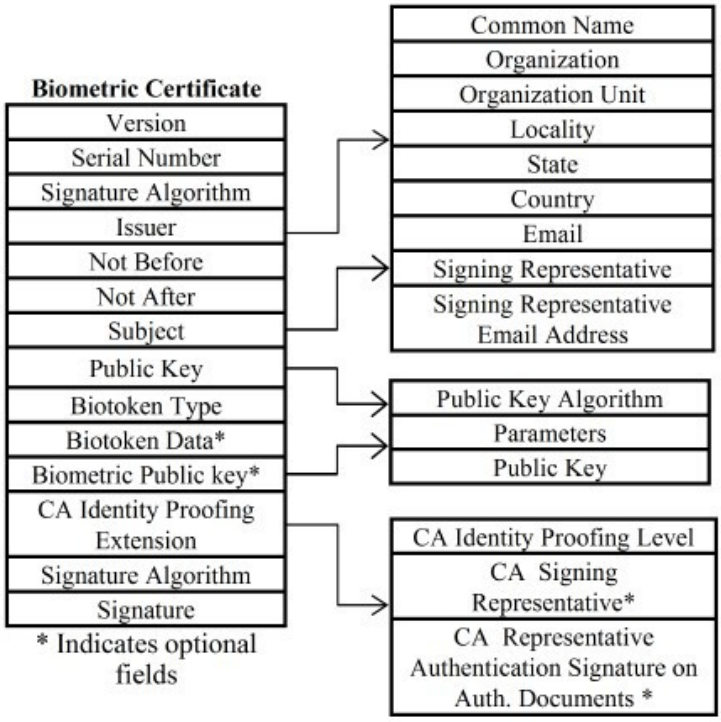
Στην ίδια εργασία [1], θεωρούν πως για να βελτιωθεί η εμπιστοσύνη στις συναλλαγές που γίνονται με απομακρυσμένη βιομετρική αναγνώριση, θα πρέπει τα πιστοποιητικά να εμπεριέχουν σαν πληροφορία και την διαδικασία που ακολούθησε η Αρχή Πιστοποίησης (CA) έτσι ώστε να πιστοποιήσει τον χρήστη. Μία CA μπορεί να ελέγξει έγραφα του χρήστη, να κάνει χρήση βιομετρίας ή και τα δύο. Ακόμη θα μπορούσε να πιστοποιεί τους χρήστες από απόσταση ή να απαιτεί οι χρήστες να παρευρεθούν αυτοπροσώπως για την αυθεντικοποίηση. Η CA θα

μπορούσε επίσης να απαιτεί οι χρήστες που έχουν ασφαλείς βιομετρικούς αισθητήρες που εκπονούν την σύγκριση τοπικά με κάποιον δικό τους μικροελεγκτή, να τους φέρουν για έλεγχο, για να διαπιστωθεί ότι το βιομετρικό ιδιωτικό κλειδί υπάρχει πράγματι εντός του βιομετρικού αισθητήρα. Ακόμη, τα βιομετρικά δεδομένα (όπως biotoken και βιομετρικό δημόσιο κλειδί) που είναι σε ένα βιομετρικό πιστοποιητικό μπορούν να αυθεντικοποιηθούν από απόσταση, χρησιμοποιώντας πρωτόκολλα αυθεντικοποίησης πρόκλησης-απόκρισης. Το βιομετρικό πιστοποιητικό θα πρέπει να αναφέρει τα μέτρα με τα οποία έγινε ο έλεγχος της ταυτότητας του πιστοποιημένου χρήστη. Αυτή η πληροφορία βοηθάει άλλες οντότητες στο να καθορίσουν τον βαθμό εμπιστοσύνης τους προς ένα πιστοποιητικό. Το πεδίο που θα εμφανίζει τα μέτρα εξακρίβωσης της ταυτότητας από την CA (CA identity proofing level), αποτελείται από τρία νούμερα που αναπαριστούν τα μέτρα βιομετρικής αυθεντικοποίησης από την CA, τα μέτρα αυθεντικοποίησης εγγράφων, και τα μέτρα αυθεντικοποίησης κατά την επανέκδοση (CA biometric authentication level, document authentication level, and reissue authentication level). Ο πίνακας 5 καθορίζει τις τιμές οι οποίες τοποθετούνται στο πεδίο “μέτρα για την εξακρίβωση της ταυτότητας από την CA” (CA identity proofing level) ενός βιομετρικού πιστοποιητικού. Υπάρχουν επίτηδες κενά στην αρίθμηση για τυχόν μελλοντικές προσθήκες επιπρόσθετων, πιο ειδικών μέτρων, όπως για παράδειγμα στην περίπτωση που θα θέλαμε στα μέτρα για τα έγγραφα να χειριζόμαστε διαφορετικά τα διπλώματα οδήγησης, απ' ό,τι τα διαβατήρια.

Πίνακας 5: Μέτρα αυθεντικοποίησης βιομετρίας και εγγράφων από την CA.

No.	Μέτρα βιομετρικής αυθεντικοποίησης από την CA
00	Καμία χρήση βιομετρικής αυθεντικοποίησης δεν χρησιμοποιείται.
10	Η CA αυθεντικοποιεί από απόσταση το biotoken του χρήστη χρησιμοποιώντας κάποιο πρωτόκολλο απομακρυσμένης αυθεντικοποίησης.
20	Η CA αυθεντικοποιεί από απόσταση το δημόσιο βιομετρικό κλειδί του χρήστη χρησιμοποιώντας κάποιο πρωτόκολλο απομακρυσμένης αυθεντικοποίησης.
30	Η CA αυθεντικοποιεί αυτοπροσώπως το biotoken του χρήστη και το βιομετρικό δημόσιο κλειδί του (χρησιμοποιώντας κάποιο τοπικό πρωτόκολλο πρόκλησης-απόκρισης)
40	Η CA αυθεντικοποιεί, αυτοπροσώπως, το περιβάλλον έμπιστης εκτέλεσης (TEE) με το βιομετρικό δημόσιο κλειδί, του χρήστη (απαιτώντας από τον χρήστη να φέρει την συσκευή με το TEE.
50	Η CA αυθεντικοποιεί, αυτοπροσώπως, το δημόσιο βιομετρικό κλειδί μίας συσκευής του χρήστη (απαιτώντας από τον χρήστη να φέρει τον ασφαλή βιομετρικό αισθητήρα που περιέχει TPM).
No.	Μέτρα αυθεντικοποίησης εγγράφων από την CA

00	Δεν γίνεται κάποια αυθεντικοποίηση εγγράφου
10	Η CA αυθεντικοποιεί από απόσταση τα έγγραφα του χρήστη
20	Η CA αυθεντικοποιεί, αυτοπροσώπως, τα έγγραφα του χρήστη



Σχήμα 31: Η μορφή ενός βιομετρικού πιστοποιητικού

Η BKI και η βελτιωμένη της έκδοση, οι Έμπιστες Βιομετρικές Διαδικτυακές Ταυτότητες, βελτιώνουν την μη-αποποίηση και προστατεύουν από επιθέσεις ενδιάμεσου ατόμου και επιθέσεις αλίευσης, αλλά παρ' όλα αυτά υπάρχει κάποιο επιπλέον κόστος για τον εξοπλισμό και την συντήρηση της όλης υποδομής. Αυτό που μένει να μελετηθεί είναι πώς συγκρίνεται η υποδομή αυτή σε σχέση με άλλες λύσεις που συνδυάζουν μία υποδομή pki μαζί με αυθεντικοποίηση 2-παραγόντων. Αν υπάρχουν ευκολότερες λύσεις για να προστατευθεί κανείς από επιθέσεις ενδιάμεσου ατόμου και επιθέσεις αλίευσης, αξίζει κανείς να υλοποιήσει ένα bki, μόνο και μόνο για την αύξηση της μη-αποποίησης που προσφέρει;

ΑΝΑΦΟΡΕΣ

[1] Albahdal A., Alzahrani H., Jain L., Boult T. (2013) Trusted BWI: Privacy and trust enchanced biometric web identities, in Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on IEEE 2013, pages 1-8

[2] Boult T. (2006) Robust distance measures for face-recognition supporting revocable biometric tokens. In Automatic Face and Gesture Recognition, 2006. Int. Conf. on, pages 560-566. IEEE

[3] Boult T., Scheirer W., Woodworth R. (2007) Secure revocable finger biotokens In Proceedings of the IEEE conference on computer vision and pattern recognition (CVPR 2007)

[4] Boult T., Woodworth R. (2008) Privacy and Security Enhancements in Biometrics In Ratha N., Govindaraju V. (eds) *Advances in Biometrics: Sensors, Algorithms and Systems* page 423-445 Springer

[5] Campisi P. (2013) Security and Privacy in Biometrics: Towards a Holistic Approach In Campisi P. (Eds) *Security and Privacy In Biometrics.* pages 6-9 Springer

[6] Cavoukian A., Stoianov A. (2010) Biometric Encryption: The New Breed of Untraceable Biometrics. In Boulgouris N., Plataniotis K., Micheli-Tzanakou E. (Eds) *Biometrics Theory, Methods, and Applications* (Chapter 26) Piscataway, NJ: IEEE Press

[7] Chang E-C, Shen R, Teo FW (2006) Finding the original point set hidden among chaff. ASIACCS '06: Proc of the 2006 ACM Symposium on Information, Computer and Communications Security 2006, pages 182-188

[8] FVC-onGoing: on-line evaluation of fingerprint recognition algorithms Retrieved from: https://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx https://biolab.csr.unibo.it/FvcOnGoing/UI/Form/AlgResult.aspx?algId=2960

[9] Fine, G.E (2006) A review of FBI's handling of the Brandon Mayfield case. Office of the Inspector General. U.S Department of Justice

[10] Haller N.(1995) The S/KEY One-Time Password System. RFC 1760 (Proposed Standard) http://www.ietf.org/rfc/rfc1760.txt

[11] Jain A., Ross A., Nandakumar K. (2011) *Introduction to Biometrics*. pages 28-30 Springer

[12] Jain K. Nandakumar K., Nagar A. (2013) Fingerprint template protection: From theory to practice. In Campisi P. (Eds) *Security and Privacy In Biometrics.* pages 187-214 Springer

[13] Jang J., Kim H. (2009) Perfomance Measures In Stan Z. Li (Eds) *Encyclopedia of Biometrics,* pages 1062-1068 Springer

[14] Juels A, Sudan M (2002) A fuzzy vault scheme. Proc 2002 IEEE Int Symp on Information Theory 2002, 408.

[15] Li Q, Chang E-C (2006) Hiding secret points amidst chaff. Proc of the Eurocrypt '2006, 59-72, (LNCS 4004).

[16] Maltoni D., Maio D., Jain A., Prabhakar S. (2009) *Handbook of Fingerprint Recognition.* page 8 Springer

[17] Mihailescu P (2007) The fuzzy vault for fingerprints is vulnerable to brute force attack. CoRR 2007, abs/0708.2974.

[18] Miri A, Poon HT (2009) A collusion attack on the fuzzy vault scheme. ISC Int J Inf Secur 2009, 1(1):27-34.

[19] Perez R., Sailer R., van Doorn L. (2006) vtpm: virtualizing the trusted platform module. In Proc. 15th Conf. on USENIX Security Symposium, pages 306-320.

[20] Rathgeb and Uhl (2011) A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security 2011:3

[21] Reinert L., Luther S (1997) User authentication techniques using public key certificates Retrieved from http://www.biometrics.org/html/x.509.html

[22] Scheirer W, Boult T. (2007) Cracking fuzzy vaults and biometricencryption. Biomet Symp 2007, 2007:1-6.

[23] Schreirer W., Bout T. (2008) Bio-cryptographic protocols with bipartite biotokens. Proceedings of the IEEE 2008 biometrics Symposium, held in conjunction with the Biometrics Consortium Conference.

[24] Scheirer W., Boult T. (2009) Bipartite biotokens: definition, implementation, and analysis. Advances in Biometrics, pages 775-785

[25] Schreirer W., Bishop W.,Boult T. (2010) Beyond PKI: The Biocryptographic Key Infrastructure. In Proceedings of the IEEE International Workshop on Information Foensics and Security (WIFS), pages 1-6

[26] Schreirer W., Bishop W., Boult T.E (2013) Beyond PKI: The Biocryptographic Key Infrastructure Patrizio Campisi in *Security and Privacy In Biometrics* Springer pages 44-68

[27] Thom S., Cox J., Linsley D., Nystrom M., Raj H., Robinson D., Saroiu S., Spiger R., Wolman A. (2003) Firmware-based trusted platform module for arm processor architectures and trustzone security extensions.

[28] Wayman J. (2012) Biometrics: Best Practices and Applications. Proceedings from International Conference on Biometrics, New Delhi. Retrieved from http://icb12.iiitd.ac.in/BestPractices- ICB2012.pdf

ΒΙΒΛΙΟΓΡΑΦΙΑ

Adams C, Farrell S. (1999) Internet X.509 Public Key Infrastructure Certificate Management Protocols

Boult T., Scheirer W., Woodworth R. (2007) Secure revocable finger biotokens In Proceedings of the IEEE conference on computer vision and pattern recognition (CVPR 2007)

Boult T., Woodworth R. (2008) Privacy and Security Enhancements in Biometrics In Ratha N., Govindaraju V. (eds) *Advances in Biometrics: Sensors, Algorithms and Systems* page 423-445 Springer

Cappelli R., Lumini A., Maio D., Maltoni D. (2007) Fingerprint Image Reconstruction from Standard Templates IEEE TRANSACTION ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE 29

Cavoukian A., Stoianov A. (2010) Biometric Encryption: The New Breed of Untraceable Biometrics. In Boulgouris N., Plataniotis K., Micheli-Tzanakou E. (Eds) *Biometrics Theory, Methods, and Applications* (Chapter 26) Piscataway, NJ: IEEE Press

Ellison C., Schneier B. (2000) Ten Risks of PKI: what you're not being told about public key infrastructure, IEEE Computer, vol 16, pages 1-7

Gutmann P. (2002) PKI: It's not dead, just resting, IEEE Computer, vol. 35, 8, 2002, pages 41-49

Jain A., Ross A., Nandakumar K. (2011) *Introduction to Biometrics*. pages 1-48 Springer

Jain A. (2013) 50 Years of biometric research: Almost Solved, the unsolved and the unexplored. Proceedings from International Conference on Biometrics, Madrid.

Jain K. Nandakumar K., Nagar A. (2013) Fingerprint template protection: From theory to practice. In Campisi P. (Eds) *Security and Privacy In Biometrics.* (chapter 8) Springer

Jihyeon Jang, Hale Kim (2009) Perfomance Measures In Stan Z. Li (Eds) *Encyclopedia of Biometrics* (pages 1062-1068) Springer

Maltoni D., Maio D., Jain A., Prabhakar S. (2009) *Handbook of Fingerprint Recognition.* Springer

Maltoni D. (2012) Fingerprint Recognition. Proceedings from International Conference on Biometrics, New Delhi.

Martinez-Silva G., Henriquez F., Cortes N., Ertaul L.(2007) On the Generation of X.509v3 Certificates with Biometric Information. In: Proc. of the 2007 International Conference on Security and Management (SAM ’07)

Reinert L., Luther S (1997) User authentication techniques using public key certificates Retrieved from http://www.biometrics.org/html/x.509.html

Scheirer W., Boult T. (2009) Bipartite biotokens: definition, implementation, and analysis. Advances in Biometrics, pages 775-785

Schreirer W., Bishop W.,Boult T. (2010) Beyond PKI: The Biocryptographic Key Infrastructure. In Proceedings of the IEEE International Workshop on Information Foensics and Security (WIFS), pages 1-6

Schreirer W., Bishop W., Boult T.E (2013) Beyond PKI: The Biocryptographic Key Infrastructure Patrizio Campisi in *Security and Privacy In Biometrics* Springer 44-68

Watson C., Garris M., Tabassi E., Wilson C., McCabe R., Janet S., Ko K. (2007) User's Guide to NIST Biometric Image Software NIST

ΠΑΡΑΡΤΗΜΑ Α – Αρχείο minutiae

Δείγμα αρχείου με minutiae g001t2u_nist.xyt

20 600 79 8

111 507 225 6

133 518 214 7

138 494 45 7

158 378 67 16

161 508 45 33

169 366 247 37

178 273 225 35

181 180 214 15

186 81 34 42

190 161 214 7

199 565 56 37

199 318 225 75

202 177 202 35

203 572 236 39

203 461 247 81

203 148 34 37

213 15 56 9

214 384 247 81

216 526 56 85

216 290 214 78

217 436 247 81

ΠΑΡΑΡΤΗΜΑ Β – Πιστοποιητικά και βιομετρικές πληροφορίες

X.509 Certificate ASN.1 Syntax

```
Certificate ::=SIGNED {SEQUENCE {
        version [0]Version DEFAULT v1,
        serialNumber CertificateSerialNumber,
        signature AlgorithmIdentifier,
        issuer Name,
        validity Validity,
        subject Name,
        subjectPublicKeyInfoSubjectPublicKeyInfo,
        issuerUniqueIdentifier[1]IMPLICIT UniqueIdentifier OPTIONAL,
                -- if present, version must be v2 or v3
        subjectUniqueIdentifier[2]IMPLICIT UniqueIdentifier OPTIONAL
                -- if present, version must be v2 or v3
        extensions    [3]Extensions OPTIONAL -- If present, version must be v3 -- }}
Version                 ::=INTEGER { v1(0), v2(1), v3(2) }
CertificateSerialNumber::=INTEGER
AlgorithmIdentifier ::=SEQUENCE {
        algorithm ALGORITHM.&id ({SupportedAlgorithms}),
        parameters ALGORITHM.&Type ({SupportedAlgorithms}{ @algorithm})
OPTIONAL }
-- Definition of the following information object set is deferred, perhaps to
-- standardized profiles or to protocol implementation conformance statements.
-- The set is required to specify a table constraint on the parameters component of
```

```
-- AlgorithmIdentifier. SupportedAlgorithmsALGORITHM::={ ... }
Validity        ::=SEQUENCE {
        notBeforeTime,
        notAfterTime }
SubjectPublicKeyInfo::=SEQUENCE {
        algorithm AlgorithmIdentifier,
        subjectPublicKeyBIT STRING }
Time   ::= CHOICE {
        utcTime UTCTime,
        generalizedTimeGeneralizedTime }
Extensions ::= SEQUENCE OF Extension
Extension ::= SEQUENCE {
        extnId EXTENSION.&id ({ExtensionSet}),
        critical BOOLEAN DEFAULT FALSE,
        extnValue OCTET STRING
                -- contains a DER encoding of a value of type &ExtnType
                -- for the extension object identified by extnId -- }
ExtensionSetEXTENSION::={ ... }
EXTENSION ::= CLASS {
        &id OBJECT IDENTIFIER UNIQUE,
        &ExtnType }
WITH SYNTAX {
        SYNTAX &ExtnType
        IDENTIFIED BY&id }
```

X509 Attribute Certificate ASN.1 Syntax

```
AttributeCertificate ::= SIGNED {AttributeCertificateInfo}
AttributeCertificateInfo ::= SEQUENCE {
        versionVersion DEFAULT v1,
        subject CHOICE {
                baseCertificateID[0]IssuerSerial, -- associated with a Public Key
                                                                Certificate
                subjectName [1] GeneralNames }, -- associated with a name
        issuer GeneralNames, -- CA issuing the attribute certificate
        signature AlgorithmIdentifier,
        serialNumberCertificateSerialNumber,
        attrCertValidityPeriodAttCertValidityPeriod,
        attributes SEQUENCE OF Attribute,
        issuerUniqueIDUniqueIdentifier OPTIONAL,
        extensions Extensions OPTIONAL }
IssuerSerial ::= SEQUENCE {
        issuer GeneralNames,
        serial CertificateSerialNumber,
        issuerUID UniqueIdentifier OPTIONAL}
AttCertValidityPeriod ::= SEQUENCE {
        notBeforeTimeGeneralizedTime,
        notAfterTimeGeneralized Time }
```

Παράρτημα Γ – Τροποποιημένος κώδικας του Bozorth

Είδαμε ότι για να δημιουργηθεί ένα revocable biotoken, σε κάθε γραμμή του ενδοδακτυλικού πίνακα που δημιουργεί ο Bozorth, εφαρμόζεται ένας από συνολικά 64 μετασχηματισμούς ανάλογα με την απόσταση και τις γωνίες της γραμμής και έπειτα παίρνουμε το πηλίκο και το υπόλοιπο. Αυτός ο κώδικας είναι μία απλουστευμένη μορφή, όπου απλά εφαρμόζεται ο ίδιος μετασχηματισμός σε όλες τις γραμμές. Οι τιμές του παραθύρου, της μετατόπισης και της μεγέθυνσης, περνιούνται σαν παράμετροι. πχ αν t=20 s=70 και E=800 τότε θα τρέχαμε το πρόγραμμα ως εξής: bozorth3.exe minutiae.xyt 70 20 800 και σαν έξοδο θα μας δώσει δύο αρχεία txt, ένα με τον ενδοδακτυλικό πίνακα που φτιάχνει ο Bozorth, και ένα αρχείο με έναν πίνακα που περιέχει τα r και g των μετασχηματισμένων τιμών. Ο πίνακας αυτός έχει την μορφή {k,j, g(d),r(d),g(b1),r(b1),g(b2),r(b2),th(jk)}

/**

License:
This software and/or related materials was developed at the National Institute
of Standards and Technology (NIST) by employees of the Federal Government
in the course of their official duties. Pursuant to title 17 Section 105
of the United States Code, this software is not subject to copyright
protection and is in the public domain.

This software and/or related materials have been determined to be not subject
to the EAR (see Part 734.3 of the EAR for exact details) because it is
a publicly available technology and software, and is freely distributed
to any interested party with no licensing requirements. Therefore, it is
permissible to distribute this software as a free download from the internet.

Disclaimer:
This software and/or related materials was developed to promote biometric
standards and biometric technology testing for the Federal Government
in accordance with the USA PATRIOT Act and the Enhanced Border Security
and Visa Entry Reform Act. Specific hardware and software products identified
in this software were used in order to perform the software development.
In no case does such identification imply recommendation or endorsement
by the National Institute of Standards and Technology, nor does it imply that
the products and equipment identified are necessarily the best available
for the purpose.

This software and/or related materials are provided "AS-IS" without warranty

of any kind including NO WARRANTY OF PERFORMANCE, MERCHANTABILITY,
NO WARRANTY OF NON-INFRINGEMENT OF ANY 3RD PARTY INTELLECTUAL PROPERTY
or FITNESS FOR A PARTICULAR PURPOSE or for any purpose whatsoever, for the
licensed product, however used. In no event shall NIST be liable for any
damages and/or costs, including but not limited to incidental or consequential
damages of any kind, including economic damage or injury to property and lost
profits, regardless of whether NIST shall be advised, have reason to know,
or in fact shall know of the possibility.

By using this software, you agree to bear all risk relating to quality,
use and performance of the software and/or related materials. You agree
to hold the Government harmless from any claim arising from your use
of the software.

**********/

/**********

LIBRARY: FING - NIST Fingerprint Systems Utilities

FILE: BOZORTH3.C
ALGORITHM: Allan S. Bozorth (FBI)
MODIFICATIONS: Michael D. Garris (NIST)
Stan Janet (NIST)
DATE: 09/21/2004

Contains the "core" routines responsible for supporting the
Bozorth3 fingerprint matching algorithm.

****

ROUTINES:
#cat: bz_comp - takes a set of minutiae (probe or gallery) and
#cat: compares/measures each minutia's {x,y,t} with every
#cat: other minutia's {x,y,t} in the set creating a table
#cat: of pairwise comparison entries
#cat: bz_find - trims sorted table of pairwise minutia comparisons to
#cat: a max distance of 75^2
#cat: bz_match - takes the two pairwise minutia comparison tables (a probe
#cat: table and a gallery table) and compiles a list of
#cat: all relatively "compatible" entries between the two

```
#cat:          tables generating a match table
#cat: bz_match_score - takes a match table and traverses it looking for
#cat:          a sufficiently long path (or a cluster of compatible paths)
#cat:          of "linked" match table entries
#cat:          the accumulation of which results in a match "score"
#cat: bz_sift -  main routine handling the path linking and match table
#cat:          traversal
#cat: bz_final_loop - (declared static) a final postprocess after
#cat:          the main match table traversal which looks to combine
#cat:          clusters of compatible paths

*****************************************************************/

#include <stdio.h>
#include "bozorth.h"

#include <string.h>

#include <stdlib.h>


int main(int argc, char *argv[])

{

   int s=atoi(argv[2]);          // scaling value

   int t=atoi(argv[3]);          // translation value

   int E=atoi(argv[4]);          // window value


   printf("s=%d t=%d E=%d\n",s,t,E);


   int x[MAX_BOZORTH_MINUTIAE];

   int y[MAX_BOZORTH_MINUTIAE];

   int th[MAX_BOZORTH_MINUTIAE];

   int comp_table[MAX_BOZORTH_MINUTIAE*MAX_BOZORTH_MINUTIAE][COLS_SIZE_2];
```

```
int no_of_points=0;

int no_of_comparisons=0;

int * col_pointers[MAX_BOZORTH_MINUTIAE*MAX_BOZORTH_MINUTIAE];

FILE * f = fopen(argv[1],"r");                  //input file : the first argument of the program call

FILE * output1 = fopen("bozorth_table.txt","w");    // bozorth intra-fingerprint comparison table output file

FILE * output2 = fopen("q_and_r_table.txt","w");    // file containing a q and an r value for each of d,th1,th2

int crap;

int i=0;

while(!feof(f) && (i<MAX_BOZORTH_MINUTIAE))     //read input file

{

fscanf(f,"%d",&x[i]);

fscanf(f,"%d",&y[i]);

fscanf(f,"%d",&th[i]);

fscanf(f,"%d",&crap);

i++;

}
```

```
   no_of_points=i;
   int j;



   bz_comp(no_of_points,x,y,th,&no_of_comparisons,comp_table,col_pointers);    // bozorth
bz_comp() function call


   printf("np = %d nc = %d \n",no_of_points,no_of_comparisons);


   for(i=0;i<no_of_comparisons-1;i++)                  // write the comparison table in the output file
   {
      for(j=0;j<COLS_SIZE_2;j++)
      {
         fprintf(output1,"%d ",comp_table[i][j]);
      }
      fprintf(output1,"\n");
   }


   int new_table[10000][9];                  // the 9 columns correspond to i,j,q(d),r(d),q(b1),r(b1),
                                    // q(b2),r(b2) and th(ij)


   int d_new,b1_new,b2_new,qd,rd,qb1,rb1,qb2,rb2;


   for(i=0;i<no_of_comparisons;i++)               // loop for computing the q and r values
   {
```

```
new_table[i][0]=comp_table[i][3];

new_table[i][1]=comp_table[i][4];


d_new =(comp_table[i][0]-t)*s;     // new distance (translated and scaled)


qd = d_new/E;

rd = d_new%(E*2);


if (rd>=E)

   rd = (E*2)-rd;


new_table[i][2]=qd;

new_table[i][3]=rd;



b1_new=(comp_table[i][1]-t)*s;      // new b1 (translated and scaled)


qb1 = b1_new/E;

rb1 = b1_new%(E*2);


if (rb1>=E)

   rb1 = (E*2)-rb1;


new_table[i][4]=qb1;

new_table[i][5]=rb1;
```

```
        b2_new=(comp_table[i][2]-t)*s;      // new b2 (translated and scaled)


        qb2 = b2_new/E;

        rb2 = b2_new%(E*2);


        if (rb2>=E)

           rb2 = (E*2)-rb2;


        new_table[i][6]=qb2;

        new_table[i][7]=rb2;


        new_table[i][8]=comp_table[i][5];

   }


   for(i=0;i<no_of_comparisons-1;i++)              //write the q and r values of d,b1,b2 in the output
file

   {

      for(j=0;j<9;j++)

      {

         fprintf(output2,"%d ",new_table[i][j]);

      }

      fprintf(output2,"\n");

   }
```

```
fclose(f);

fclose(output1);

fclose(output2);


return 0;


}

/*********************************************************************/
void bz_comp(
        int npoints,                            /* INPUT: # of points */
        int xcol[    MAX_BOZORTH_MINUTIAE ], /* INPUT: x cordinates */
        int ycol[    MAX_BOZORTH_MINUTIAE ], /* INPUT: y cordinates */
        int thetacol[ MAX_BOZORTH_MINUTIAE ],       /* INPUT: theta values */

        int * ncomparisons,                     /* OUTPUT: number of pointwise comparisons */
        int cols[][ COLS_SIZE_2 ],              /* OUTPUT: pointwise comparison table */
        int * colptrs[]                         /* INPUT and OUTPUT: sorted list of pointers to
rows in cols[] */
        )
{
int i, j, k;

int b;
int t;
int n;
int l;

int table_index;

int dx;
int dy;
int distance;
```

```
int theta_kj;
int beta_j;
int beta_k;

int * c;

int m1_xyt = 0;          //copied from bozorth.c

int verbose_bozorth = 0;    //copied from bozorth.c


c = &cols[0][0];

table_index = 0;
for ( k = 0; k < npoints - 1; k++ ) {
        for ( j = k + 1; j < npoints; j++ ) {


                if ( thetacol[j] > 0 ) {

                        if ( thetacol[k] == thetacol[j] - 180 )
                                continue;
                } else {

                        if ( thetacol[k] == thetacol[j] + 180 )
                                continue;
                }


                dx = xcol[j] - xcol[k];
                dy = ycol[j] - ycol[k];
                distance = SQUARED(dx) + SQUARED(dy);
                if ( distance > SQUARED(DM) ) {
                        if ( dx > DM )
                                break;
                        else
                                continue;

                }
```

```
                        /* The distance is in the range [ 0, 125^2 ] */
if ( dx == 0 )
        theta_kj = 90;
else {
        double dz;

        if ( m1_xyt )
                dz = ( 180.0F / PI_SINGLE ) * atanf( (float) -dy / (float) dx );
        else
                dz = ( 180.0F / PI_SINGLE ) * atanf( (float) dy / (float) dx );
        if ( dz < 0.0F )
                dz -= 0.5F;
        else
                dz += 0.5F;
        theta_kj = (int) dz;
}


beta_k = theta_kj - thetacol[k];
beta_k = IANGLE180(beta_k);

beta_j = theta_kj - thetacol[j] + 180;
beta_j = IANGLE180(beta_j);


if ( beta_k < beta_j ) {
        *c++ = distance;
        *c++ = beta_k;
        *c++ = beta_j;
        *c++ = k+1;
        *c++ = j+1;
        *c++ = theta_kj;
} else {
        *c++ = distance;
        *c++ = beta_j;
        *c++ = beta_k;
        *c++ = k+1;
        *c++ = j+1;
        *c++ = theta_kj + 400;
```

```
}


b = 0;
t = table_index + 1;
l = 1;
n = -1;                         /* Init binary search state ... */



while ( t - b > 1 ) {
        int * midpoint;

        l = ( b + t ) / 2;
        midpoint = colptrs[l-1];




        for ( i=0; i < 3; i++ ) {
                int dd, ff;

                dd = cols[table_index][i];

                ff = midpoint[i];


                n = SENSE(dd,ff);


                if ( n < 0 ) {
                        t = l;
                        break;
                }
                if ( n > 0 ) {
                        b = l;
                        break;
                }
        }
```

```
                        if ( n == 0 ) {
                                n = 1;
                                b = l;
                        }
                } /* END while */

                if ( n == 1 )
                        ++l;




                for ( i = table_index; i >= l; --i )
                        colptrs[i] = colptrs[i-1];


                colptrs[l-1] = &cols[table_index][0];
                ++table_index;


                if ( table_index == 19999 ) {
#ifndef NOVERBOSE
                        if ( verbose_bozorth )
                                printf( "bz_comp(): breaking loop to avoid table overflow\n" );
#endif
                        goto COMP_END;
                }

        } /* END for j */

} /* END for k */

COMP_END:
        *ncomparisons = table_index;

}
```