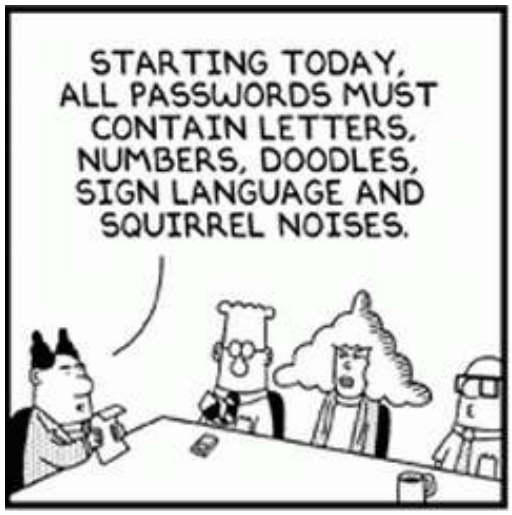
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ (M.I.S.)



Διπλωματική Εργασία

Θέμα: "Συγκριτική και πειραματική μελέτη των Proof by Knowledge τεχνικών πιστοποίησης χρηστών"

Συγγραφέας: Γκαραφλή Σταματή (9/05)

Επιβλέπων Καθηγητής: Οικονομίδης Αναστάσιος

Εξεταστική Επιτροπή:
Οικονομίδης Αναστάσιος (Αναπληρωτής Καθηγητής)
Πρωτόγερος Νικόλαος (Λέκτορας)

Θεσσαλονίκη Φεβρουάριος 2007

*Η έγκριση της διπλωματικής εργασίας από το Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών στα Πληροφοριακά Συστήματα (M.I.S.) του Πανεπιστημίου Μακεδονίας δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους τους.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον καθηγητή μου και επιβλέποντα αυτής της διπλωματικής εργασίας, κ. Αναστάσιο Οικονομίδη, για την πολύτιμη βοήθειά του, την υπομονή και επιμονή του και την πολύ σωστή καθοδήγησή του, ώστε να μπορέσει να διεκπεραιωθεί σωστά η παρούσα έρευνα. Επιπλέον, θα ήθελα να μεταφέρω τις ευχαριστίες μου στον καθηγητή κ. Νικόλαο Πρωτόγερο για τα ιδιαίτερα και πολύ ενθαρρυντικά σχόλια του. Επίσης, θα ήθελα να ευχαριστήσω τον καλό μου φίλο και συνάδελφο Κωνσταντίνο Χαλκιά για την υποστήριξη και τη βοήθεια που μου προσέφερε κατά τη διάρκεια της παρούσας εργασίας. Τέλος θα ήθελα να αφιερώσω τη δουλειά αυτή στους αγαπημένους μου γονείς Δημήτρη και Ελένη και στα αδέρφια μου Αποστόλη και Αιμιλία, για τη βοήθειά τους και για όλα όσα μου έχουν προσφέρει κατά τη διάρκεια των προπτυχιακών και μεταπτυχιακών σπουδών μου.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία παρουσιάζει μία συγκριτική μελέτη και έρευνα των proof by knowledge τεχνικών πιστοποίησης που μπορούν να χρησιμοποιήσουν οι χρήστες για την είσοδό τους σε ένα σύστημα. Πιο συγκεκριμένα, συγκρίνουμε την παραδοσιακή μέθοδο πιστοποίησης, τα text passwords, με δύο καινούργιες εναλλακτικές μεθόδους: τα visual passwords και τα graphical passwords. Οι δύο αυτές μέθοδοι είναι πολύ πιο εύκολες στην απομνημόνευση, καθώς οι χρήστες ασχολούνται με εικόνες και όχι με αλφαριθμητικούς χαρακτήρες, ενώ ιδιαίτερα για την περίπτωση των γραφικών δημιουργούνται passwords πολύ πιο ασφαλή. Στην έρευνά μας συμμετείχαν 100 χρήστες, οι οποίοι αφού ενημερώθηκαν για τις νέες μεθόδους πιστοποίησης, δημιούργησαν τα δικά τους text, visual και graphical passwords, τα επιβεβαίωσαν και τέλος απάντησαν και στο ερωτηματολόγιο που είχαμε ετοιμάσει, που περιείχε ερωτήσεις πάνω στους αλφαριθμητικούς κωδικούς που χρησιμοποιούν οι χρήστες σήμερα, αλλά και στις νέες μεθόδους πιστοποίησης. Βασισμένοι λοιπόν σε όλα αυτά, διαπιστώσαμε ότι σχεδόν όλοι οι χρήστες χρησιμοποιούν πολύ συχνά τους προσωπικούς τους κωδικούς σε διάφορες εφαρμογές, και ότι τα text passwords που τελικά δημιουργούν είναι προβλέψιμα και άρα πολύ ευαίσθητα σε κακόβουλες επιθέσεις. Τα visual passwords από την άλλη, εντυπωσίασαν πολύ τους χρήστες, ιδιαίτερα των μεγαλύτερων ηλικιών, αλλά τελικά τα passwords που δημιουργούσαν δεν ήταν καθόλου δύσκολα και πραγματικά πολύ εύκολα στο να σπάσουν. Τέλος τα graphical passwords, παρά το γεγονός ότι δεν εντυπωσίασαν ιδιαίτερα ένα ποσοστό των χρηστών που στην πλειοψηφία τους ήταν άνδρες, είναι πολύ εύκολα στην απομνημόνευσή τους και θεωρήθηκαν, ιδιαίτερα από τις γυναίκες, μια πολύ εύχρηστη μέθοδος, αλλά και ασφαλής, καθώς οι χρήστες με ελάχιστη προσπάθεια δημιουργούν δύσκολούς γραφικούς κωδικούς. Για το λόγο αυτό, στο τέλος της εργασίας παραθέτουμε και μια σειρά κανόνων, τους οποίους εάν ακολουθήσουν οι χρήστες, θα μπορέσουν να αποφύγουν τη δημιουργία σχετικά εύκολων γραφικών passwords.

ABSTRACT

This thesis presents a comparative survey of proof by knowledge authentication techniques that people can use to enter in a system. More precisely, we compare the traditional text passwords with the new alternative authentication methods: visual passwords and graphical passwords. These passwords are more memorable, as users have to deal with images instead of alphanumeric characters, while graphical passwords are also more secure. A total of 100 users participated in our survey, who after getting informed about the new authentication methods, they created their own text, visual and graphical passwords, they tried to confirm them correctly and finally they answered in the questionnaire we have prepared. Based on all these, we found out that users use many passwords everyday and the text passwords that they create are predictable and very vulnerable to attacks. Visual passwords attracted them very much, especially users over 45 years old, but the passwords that they made are really easy to be cracked. Graphical passwords from the other hand, even if they did not impressed a lot many of the participants, mostly men, were characterized as a very friendly method especially from women, as the passwords that are created are difficult, memorable and above all very safe. For this reason, in the end of the thesis, we present a set of rules and advices that users should follow, in order to avoid the creation of rather easy graphical passwords.

1. ΕΙΣΑΓΩΓΗ

Στη σημερινή εποχή, με την τόσο μεγάλη ανάπτυξη των ηλεκτρονικών υπολογιστών και την ευρεία χρήση του Internet, η κοινωνία μας έχει αυτοματοποιήσει όλο και περισσότερες δραστηριότητες, με σκοπό την μεγαλύτερη ευκολία και καλύτερη εξυπηρέτηση του κάθε ατόμου. Για παράδειγμα, η χρήση μηχανημάτων ATM, η διεκπεραίωση ηλεκτρονικών συναλλαγών μέσω Internet, η χρήση πιστωτικών καρτών, η είσοδος σε συγκεκριμένες ιστοσελίδες για την πληροφόρησή μας, η χρησιμοποίηση e-mail, είναι φαινόμενα, με τα οποία όλο και περισσότεροι άνθρωποι έρχονται καθημερινά αντιμέτωποι.

Μέσα σε μια τέτοια κατάσταση, μια έννοια που έχει κεντρίσει το ενδιαφέρον πολλών ερευνητών, αλλά και απλών ανθρώπων, είναι αυτή του *"computer security"*. Τεράστια ποσά απόρρητων ή προσωπικών δεδομένων, αποθηκεύονται και μεταδίδονται ηλεκτρονικά, μετατρέποντας το θέμα της ασφάλειας σε ένα μείζον θέμα που αφορά τον κάθε άνθρωπο. Για το λόγο αυτό η πρώτη μέθοδος που απέτρεψε την πρόσβαση μη εξουσιοδοτημένων χρηστών σε ευαίσθητα δεδομένα, είναι η χρησιμοποίηση των προσωπικών κωδικών ή password. Όπως είναι λοιπόν γνωστό, για την είσοδο κάποιου χρήστη σε ένα σύστημα (authentication), είναι απαραίτητο ο χρήστης να παραχωρήσει στο σύστημα το προσωπικό του password και εάν αυτό είναι σωστό να του επιτραπεί η είσοδος, ενώ σε αντίθετη περίπτωση να απαγορευτεί.

Μέχρι πριν λίγα χρόνια ο μόνος τρόπος για την είσοδο των χρηστών σε ένα σύστημα ήταν αυτός των password, και πιο συγκεκριμένα των PINs και text passwords. Όταν μιλάμε για PIN εννοούμε 4 αριθμούς με συγκεκριμένη σειρά, τους οποίους ο χρήστης θα πρέπει να θυμάται και να πληκτρολογήσει, ώστε να κάνει είσοδο σε ένα σύστημα. Στην περίπτωση των text passwords, αναφερόμαστε σε μια συγκεκριμένη σειρά χαρακτήρων (συνήθως πάνω από 4), που θα πρέπει να εισάγει ο χρήστης στο σύστημα για την είσοδό του. Οι χαρακτήρες αυτοί μπορεί να είναι αριθμοί, γράμματα κεφαλαία ή μικρά, αλλά και οποιοδήποτε από τα αλφαριθμητικά σύμβολα.

Παρόλα αυτά, με την τεράστια ανάπτυξη της τεχνολογίας σήμερα έχουν αναπτυχθεί διάφοροι τρόποι με τους οποίους κάποιος χρήστης μπορεί να κάνει login σε ένα

σύστημα. Για το σκοπό αυτό με βάση τα χαρακτηριστικά τους, χωρίζονται σε τρεις διαφορετικές κατηγορίες [14] οι οποίες αναφέρονται παρακάτω:

- **Proof by knowledge techniques:** τεχνικές οι οποίες βασίζονται σε μια συγκεκριμένη πληροφορία που έχει ένα άτομο και θα πρέπει να θυμάται. Όταν δώσει την πληροφορία αυτή ο συγκεκριμένος χρήστης, θα αποκτήσει το δικαίωμα να κάνει είσοδο στο σύστημα. Παραδείγματα των τεχνικών αυτών είναι τα PINs και text passwords που προαναφέραμε και στα οποία εάν ο χρήστης θυμάται την καθορισμένη σειρά των ψηφίων ή χαρακτήρων, θα αποκτήσει πρόσβαση στο σύστημα με το οποίο αλληλεπιδρά.
- **Proof by property techniques:** τεχνικές οι οποίες βασίζονται σε μια συγκεκριμένη ιδιότητα που έχει ένας χρήστης και η οποία επιβεβαιώνει την ταυτότητα του. Τεχνικές που ανήκουν σε αυτή την κατηγορία είναι:
  - ✓ *Fingerprint verification:* πιστοποίηση με το δακτυλικό αποτύπωμα του χρήστη, μια ιδιότητα που είναι ξεχωριστή και μοναδική σε κάθε άτομο.
  - ✓ *Voice verification:* πιστοποίηση μέσω της φωνής, όπου ο χρήστης καλείται να πει και να επαναλάβει για κάποιες φορές, συγκεκριμένες λέξεις σε ένα μικρόφωνο. Από την είσοδο που έχουμε, γίνονται μετρήσεις και παίρνουμε αποτελέσματα για συγκεκριμένα χαρακτηριστικά της φωνής. Τα αποτελέσματα αυτά συγκρίνονται με τα ήδη αποθηκευμένα και εάν συμπίπτουν επιτρέπεται η είσοδος του χρήστη στο σύστημα.
  - ✓ *Iris scanning:* πιστοποίηση με εξέταση (scan) της ίριδας του ματιού του χρήστη, η οποία έχει χαρακτηριστικά διαφορετικά σε κάθε άτομο
- **Proof by procession techniques:** τεχνικές που βασίζονται στην κατοχή ενός συγκεκριμένου αντικειμένου που έχει ένας χρήστης. Όταν θέλει να αποκτήσει πρόσβαση σε ένα σύστημα, απλά πρέπει να δώσει το αντικείμενο αυτό που επιβεβαιώνει την ταυτότητα του. Τεχνικές της συγκειμένης κατηγορίας είναι:
  - ✓ *Smart cards:* πλαστικές κάρτες, στο μέγεθος των πιστωτικών καρτών, που διαθέτουν όμως έναν ενσωματωμένο μικροεπεξεργαστή και μνήμη διαφόρων μεγεθών, όπου αποθηκεύονται διάφορες πληροφορίες για τον κάτοχό της
  - ✓ *Digital certificates:* είναι ένα ηλεκτρονικό "διαβατήριο" που εκδίδεται από μια αρχή πιστοποίησης όπως είναι η Entrust και η Verisign. Περιέχει, μεταξύ

των άλλων, το όνομα, έναν αύξοντα αριθμό, την ημερομηνία λήξης της κάρτας και την ψηφιακή υπογραφή της αρχής πιστοποίησης, έτσι ώστε ένας παραλήπτης να μπορεί να ελέγξει ότι το πιστοποιητικό είναι γνήσιο.

Όπως έχουμε ήδη προαναφέρει, οι πιο διαδεδομένες από αυτές τις τεχνικές είναι τα PINs και τα text passwords, δηλαδή οι proof by knowledge τεχνικές, ενώ οι υπόλοιπες έχουν αρχίσει να αναπτύσσονται τα τελευταία χρόνια και έχουν γίνει γνωστές, κατά κύριο λόγω, μέσω του κινηματογράφου και όχι από προσωπική χρήση και εμπειρία. Με βάση όμως διάφορες έρευνες, όπως για παράδειγμα την έρευνα του Davies [8], οι χρήστες πολύ σπάνια διαλέγουν password που να είναι ταυτόχρονα δύσκολο να το μαντέψει κάποιος, αλλά και εύκολο να το απομνημονεύει ο ίδιος. Έτσι τα password που επιλέγονται συνήθως έχουν ένα από τα δύο αυτά χαρακτηριστικά:

- είναι πολύ εύκολα, με αποτέλεσμα κάποιος που επιτίθεται στο σύστημα να είναι πολύ εύκολο να τα μαντέψει ή να τα βρει με αυτοματοποιημένες μεθόδους
- είναι τόσο δύσκολα που είτε ξεχνιούνται εύκολα, είτε για να αποφευχθεί μια τέτοια κατάσταση, οι χρήστες καταφεύγουν σε άλλες μεθόδους, όπως να τα γράφουν κάπου, να τα μοιράζονται με άλλους, να μην τα αλλάζουνε ποτέ ή να έχουν ένα μόνο για διάφορα συστήματα.

Και στις δύο περιπτώσεις βέβαια, αυτό που έχουμε ως αποτέλεσμα είναι τα password που τελικά επιλέγονται να μην είναι καθόλου ασφαλή, αλλά αντίθετα ένας πολύ εύκολος στόχος για κάποιον που επιτίθεται στο σύστημά μας.

Βασιζόμενοι σε αυτές τις παρατηρήσεις, και διαβάζοντας το άρθρο του Computerworld [11] με βάση το οποίο μια ομάδα σε μια μεγάλη εταιρία, έσπασε και κατάφερε να βρει περίπου το 80% των passwords, μπορούμε εύκολα να κατανοήσουμε ότι παρά τη δημοτικότητα τους, τα PIN και τα text passwords είναι ιδιαίτερα ανασφαλή και μπορούν να δημιουργήσουν πολλά προβλήματα στους χρήστες, τα οποία συνοψίζονται παρακάτω:

- Οι χρήστες επιλέγουν passwords που είναι μικρά σε μήκος ή ιδιαιτέρως ευκολομνημόνευτα
- Πολλές φορές καταγράφουν κάπου τα password που έχουν, ή τα μοιράζονται με άλλους, με σκοπό να μην τα ξεχάσουν

- Χρησιμοποιούν ίδια ή παρόμοια passwords σε διαφορετικές εφαρμογές
- Τα text passwords είναι πολύ ευαίσθητα στις επιθέσεις μέσω λεξικού ή αλλιώς *"dictionary attacks"*. Επειδή υπάρχει μια ιδιαίτερη δυσκολία στο να θυμούνται οι χρήστες μία σειρά τυχαίων χαρακτήρων, ώστε το password που θα δημιουργήσουν να είναι ασφαλές, συχνά πολλοί από αυτούς επιλέγουν μια συνηθισμένη λέξη, ένα όνομα ή μια ημερομηνία που σημαίνει κάτι γι' αυτούς και θα είναι δύσκολο να την ξεχάσουν. Δυστυχώς όμως, με τον τρόπο αυτό δημιουργούνται προβλέψιμα passwords, που μπορούν πολύ εύκολα να σπάσουν, μέσα από dictionaries – λεξικά, που έχουν κατασκευαστεί. Τα λεξικά αυτά είναι ουσιαστικά εργαλεία, που έχουν τη δυνατότητα να σπάνε αυτόματα τα προβλέψιμα αυτά passwords, τσεκάροντας όλες τις λέξεις που χρησιμοποιούνται συχνά και άρα είναι στο dictionary.

  Η κατάσταση αυτή επιβεβαιώνεται και από το case study του Klein [19], το οποίο αναφέρει ότι χρησιμοποιώντας ένα λεξικό των 3 εκ. λέξεων μόνο, μπόρεσαν να σπάσουν το 25% από 14000 passwords, γεγονός που δείχνει ότι στις μέρες μας αυτές οι μέθοδοι έχουν γίνει ανασφαλείς εντελώς.

2. VISUAL και GRAPHICAL PASSWORDS

Βασισμένοι στα προβλήματα των text passwords που έχουμε αναφέρει, πολλοί ερευνητές προσπάθησαν να βρούνε άλλους τρόπους, πιο ασφαλείς, για την είσοδο των χρηστών σε κάποιο σύστημα, με αποτέλεσμα να επινοηθούν τα **visual** (οπτικά) και τα **graphical** (γραφικά) passwords. Και οι δύο μέθοδοι, ανήκουν στις proof by knowledge τεχνικές και έχουν πολλά πλεονεκτήματα, που μας βοηθάνε να ξεπεράσουμε τα προβλήματα των text passwords, τα οποία αναφέρονται παρακάτω [1, 6, 28]:

- Μετά από έρευνες, έχει αποδειχθεί, ότι είναι πιο εύκολο για κάποιον να θυμάται εικόνες, παρά μια σειρά από χαρακτήρες
- Οι εικόνες είναι ανεξάρτητες από τη γλώσσα του κάθε χρήστη
- Ειδικά όσον αφορά τα γραφικά passwords, το συνολικό μέγεθος του password (password space), είναι πολύ μεγάλο
- Οι επιθέσεις με βάση κάποιο λεξικό (dictionary attacks), είναι ανέφικτες, καθώς δεν υπάρχουν ακόμη αντίστοιχα λεξικά, αλλά ταυτόχρονα είναι πολύ δύσκολο να δημιουργηθούν, εάν λάβουμε υπόψιν μας ότι το password space, όπως έχουμε ήδη αναφέρει, είναι πολύ μεγάλο
- Εφόσον δεν έχουν κατασκευαστεί ακόμη λεξικά για τα visual και τα graphical passwords, είναι πολύ δύσκολο να γίνουν αυτοματοποιημένες επιθέσεις.

Όπως μπορούμε εύκολα να καταλάβουμε τα πλεονεκτήματα των οπτικών και γραφικών passwords, είναι πολλά και ιδιαιτέρως σημαντικά, με αποτέλεσμα οι κωδικοί που δημιουργούνται να είναι πολύ πιο ασφαλείς. Εκτός από όλα αυτά τα πλεονεκτήματα όμως, υπάρχει και ένα πολύ βασικό μειονέκτημα το οποίο ανέφεραν οι Renaud και De Angeli [26], και είναι το πρόβλημα του ***"shoulder surfing"***. Το πρόβλημα του shoulder surfing είναι η κατάσταση κατά την οποία όταν ένας χρήστης προσπαθεί να κάνει login σε ένα σύστημα, κάποιος που θέλει να "κλέψει" τον κωδικό του, κοιτάει πάνω από τον ώμο του (shoulder) [28]. Για παράδειγμα, εάν κάποιος παρακολουθεί το πληκτρολόγιο όταν ένας χρήστης εισάγει το PIN του σε ένα μηχάνημα ATM, μπορεί να κλέψει την προσωπική αυτή πληροφορία. Άρα, ακόμη και αν είναι πολύ δύσκολο να μαντέψει κάποιος τα οπτικά και γραφικά passwords, εάν ένα άτομο παρακολουθεί μια διαδικασία εισόδου σε ένα σύστημα, μπορεί να ανακαλύψει τον προσωπικό κωδικό του συγκεκριμένου χρήστη και να χρησιμοποιήσει την πληροφορία αυτή εναντίον του.

2.1. VISUAL PASSWORDS

Τα visual passwords (οπτικά) είναι τα passwords που δημιουργούνται με την επιλογή μιας αλληλουχίας εικόνων. Έτσι οι χρήστες, αντί να θυμούνται μια σειρά από αριθμούς, χαρακτήρες ή ακόμη και σύμβολα, θα πρέπει να θυμούνται μια σειρά από εικόνες [14, 23]. Αυτό είναι πολύ σημαντικό εάν το συσχετίσουμε με διάφορες ψυχολογικές έρευνες που έχουνε γίνει και που αποδεικνύουν ότι οι άνθρωποι μπορούνε πολύ πιο εύκολα να θυμούνται μια σειρά από εικόνες, παρά μια σειρά από χαρακτήρες. Με βάση την ιδέα αυτή, έχουν αναπτυχθεί διάφορα εμπορικά προϊόντα, τα οποία παρουσιάζονται ξεχωριστά στο κείμενο που ακολουθεί.

2.1.1. Passfaces

Η Real User Corporation ανέπτυξε ένα προϊόν το οποίο ονομάζεται "Passfaces" [24, 25]. Με βάση την τεχνική αυτή, ο χρήστης αρχικά καλείται να επιλέξει τέσσερις εικόνες ανθρώπων από μία τεράστια βάση δεδομένων, οι οποίες θα αποτελούν το μελλοντικό του password. Όταν ο χρήστης θελήσει να κάνει login, αυτό που θα δει είναι ένα πλέγμα με εννέα εικόνες, αντίστοιχο με αυτό της Εικόνας 1, το οποίο αποτελείται από ένα πρόσωπο που έχει επιλεχθεί προηγουμένως, και από οκτώ παραπλανητικά πρόσωπα (decoy faces). Ο χρήστης αναγνωρίζει και κάνει κλικ στο ένα και μοναδικό πρόσωπο που υπάρχει μέσα στο password που είχε δημιουργήσει, ενώ η συγκεκριμένη διαδικασία επαναλαμβάνεται, μέχρι να αναγνωρίσει και να κάνει κλικ και τα τέσσερα πρόσωπα που είχε επιλέξει. Εάν κάνει όλη αυτή τη διαδικασία σωστά, το σύστημα του επιτρέπει πλέον την είσοδό του.

Εικόνα 1: Passfaces.

Η όλη ιδέα βασίζεται στο γεγονός ότι οι άνθρωποι μπορούνε πολύ πιο εύκολα να θυμούνται εικόνες άλλων ανθρώπων, παρά εικόνες με οποιαδήποτε άλλη αναπαράσταση. Μια επέκταση της ιδέας αυτής, που κάνει ακόμη πιο δελεαστική τη συγκεκριμένη τεχνική, είναι ο κάθε χρήστης να δημιουργεί τη δικιά του βάση δεδομένων, με τις προσωπικές του εικόνες. Το γεγονός αυτό κάνει τα συγκεκριμένα password πιο ασφαλή, καθώς για την περίπτωση των τυχαίων εικόνων έχουν

ανακαλυφθεί ορισμένα patters (πρότυπα) που ακολουθούν οι χρήστες και που έχουν ως αποτέλεσμα τα passwords που επιλέγουν, να είναι τελικά προβλέψιμα (π.χ. φυλή, φύλο, ηλικία, κλπ).

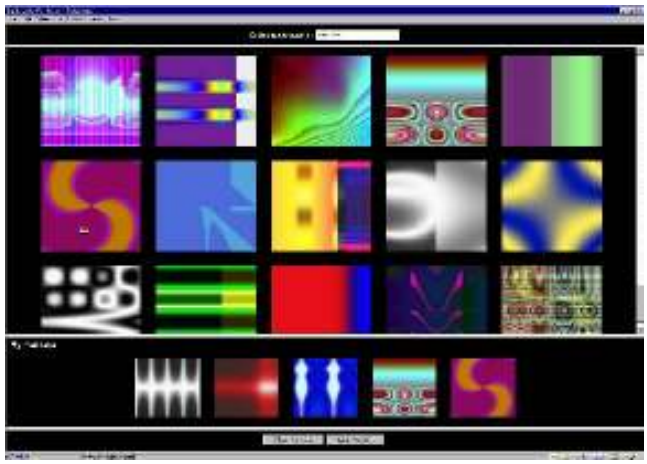
2.1.2. Story Scheme

Το Story Scheme, είναι μια άλλη εφαρμογή, παρόμοια με το Passfaces, που έχουμε ήδη αναλύσει. Η βασική διαφορά είναι ότι εικόνες δεν απεικονίζουν μόνο ανθρώπινα πρόσωπα. Αντίθετα, οι εικόνες εδώ, χωρίζονται σε συγκεκριμένες κατηγορίες, ορισμένες από τις οποίες είναι ζώα, φαγητά, αθλήματα, καθημερινά αντικείμενα, αυτοκίνητα, φύση, παιδιά, ή ακόμη και πρόσωπα. Στην περίπτωση αυτή λοιπόν, ο χρήστης για να δημιουργήσει το προσωπικό του password, το οποίο βέβαια να μπορεί να θυμάται και εύκολα, θα πρέπει να επινοήσει μια ιστορία η οποία να απεικονίζεται με μια σειρά εικόνων της βάσης δεδομένων. Από εκεί και πέρα, έχοντας δημιουργήσει τον προσωπικό του κωδικό, η διαδικασία που ακολουθείται για να γίνει αποδεκτή η είσοδός του στο σύστημα, είναι παρόμοια με αύτη του Passfaces, που έχουμε ήδη αναπτύξει: εάν δηλαδή επιλέξει τις σωστές εικόνες, που αντιστοιχούν στο password που έχει ήδη δημιουργήσει, η είσοδός του στο σύστημα θα είναι επιτυχής [9].

Εικόνα 2: Story Scheme.

2.1.3. Déjà vu

Δύο άλλοι ερευνητές, οι Dhamija και Perrig ανέπτυξαν ένα άλλο σύστημα για την πιστοποίηση χρήστη, το οποίο ονομάσανε "Déjà vu" [10]. Με βάση το σύστημα αυτό ο χρήστης αρχικά δημιουργεί το δικό του *"image portfolio"*, διαλέγοντας ένα σύνολο από *p* εικόνες, ανάμεσα



Εικόνα 3: Déjà Vu.

από ένα πολύ ευρύτερο.

Όταν ο χρήστης επιχειρήσει να κάνει login στο συγκεκριμένο σύστημα, η εφαρμογή αυτή παρουσιάζει ένα σύνολο από *n* εικόνες, που αποτελούνται από:

- *x* εικόνες που ανήκουν στο image portfolio που έχει δημιουργήσει ο χρήστης, και
- *y* εικόνες, για παραπλάνηση του χρήστη, οι οποίες ονομάζονται *"decoy images"*.

Στο σημείο αυτό ο χρήστης πρέπει να επιλέξει και να κάνει κλικ, σε όσες από τις εικόνες αναγνωρίζει και έχει τοποθετήσει στο δικό του image portfolio που έχει δημιουργήσει στην αρχή. Εάν μπορέσει να φέρει σε πέρας τη συγκεκριμένη διαδικασία, μπορεί πλέον να έχει πρόσβαση στο σύστημα, αφού έχει γίνει με επιτυχία η είσοδός του.

Το πιο σημαντικό πράγμα στη συγκεκριμένη μέθοδο, και κάτι το οποίο θα πρέπει να αναφέρουμε και να τονίσουμε ιδιαίτερα, είναι ο τύπος των εικόνων που χρησιμοποιούνται. Οι εικόνες λοιπόν, βασίζονται στο ***"Random Art"***, μια ιδέα του Andrej Bauer, με βάση την οποία δημιουργούνται τυχαίες, αφηρημένες εικόνες [3]. Όταν ο χρήστης δημιουργεί σε πρώτη φάση το προσωπικό του image portfolio, το σύστημα δίνει στη συγκεκριμένη διαδικασία ένα αρχικό seed. Με βάση αυτό το seed, η τεχνική Random Art δημιουργεί ένα τυχαίο μαθηματικό τύπο, ο οποίος καθορίζει το χρώμα του κάθε pixel της εικόνας. Με τον τρόπο αυτό λοιπόν, ο κάθε χρήστης για να δημιουργήσει το image portfolio, έχει να επιλέξει ανάμεσα από δικές του τυχαίες εικόνες, που έχουν δημιουργηθεί από το δικό του αρχικό seed.

Με βάση όλα όσα αναφέραμε παραπάνω, οδηγούμαστε στο συμπέρασμα ότι ο τύπος των εικόνων που χρησιμοποιεί η μέθοδος déjà vu, κάνει το όλο σύστημα πολύ πιο ασφαλές, καθώς είναι πολύ δύσκολο σε κάποιον που παρατηρεί τη διαδικασία εισόδου, να θυμάται τις εικόνες που έχουν επιλεγεί. Επιπλέον, το σύστημα δεν χρειάζεται να αποθηκεύει κάθε εικόνα ξεχωριστά, αλλά να αποθηκεύει μόνο το αρχικό seed, και κάθε φορά να γίνεται με βάση αυτό ο υπολογισμός των εικόνων.

2.1.4. Picture Password

Το Picture Password, είναι ένας άλλος μηχανισμός πιστοποίησης χρήστη, ο οποίος βασίζεται στα visual passwords, και ο οποίος επινοήθηκε από τον W. Jansen [14, 16].

Οι εικόνες στην περίπτωση αυτή χωρίζονται σε πολλές διαφορετικές κατηγορίες, με βάση το θέμα που αναπαριστούν. Τέτοια θέματα υπάρχουν πολλά όπως Αθλήματα, Θάλασσα, Τοπία, Γάτες, Σκυλιά, Πρόσωπα, Μέσα Μεταφοράς κλπ. Για να δημιουργήσει λοιπόν ο χρήστης ένα password, πρέπει πρώτον να διαλέξει ένα από τα θέματα που είναι διαθέσιμα και στη συνέχεια να επιλέξει μια σειρά από εικόνες του συγκεκριμένου θέματος.

Εικόνα 4: Picture Password.

Το Picture Password είναι μια μέθοδος πιστοποίησης όπου η κάθε εικόνα αντιστοιχεί σε ένα στοιχείο ενός αλφαβήτου. Παρόλα αυτά, ο χρήστης δεν θα πρέπει να θυμάται μια σειρά από τυχαίους χαρακτήρες του αλφάβητου αυτού, αλλά μια σειρά από εικόνες, κάτι που όπως έχουμε ήδη αναφέρει, είναι πολύ πιο εύκολο για ένα άτομο.

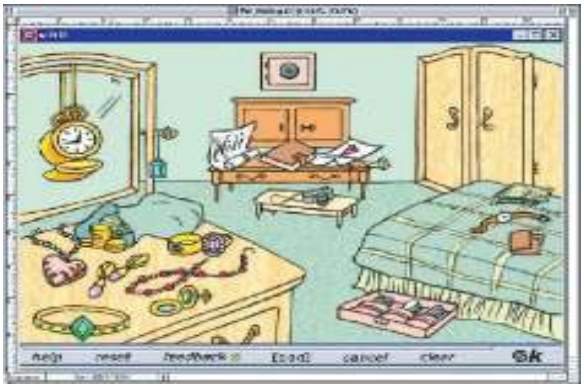
Υπάρχουν δύο διαφορετικοί τρόποι με τους οποίους μπορούμε να επιλέξουμε μια σειρά από εικόνες, και είναι αυτοί που αναφέρονται παρακάτω:

- *Individual Selection:* στην περίπτωση αυτή κάθε εικόνα αναπαριστά ένα μόνο στοιχείο του αλφαβήτου
- *Paired Selection:* εδώ μπορεί να υπάρξει συνδυασμός δύο εικόνων. Αρχικά γίνεται η επιλογή των δύο εικόνων που θα συνδυαστούν. Στη συνέχεια, συνήθως με τη μέθοδο του drag and drop, ο χρήστης παίρνει τη μία εικόνα και την βάζει πάνω στην άλλη. Το "ζευγάρωμα" αυτό έχει ως αποτέλεσμα ο συνδυασμός των δύο εικόνων να αναπαριστά ένα στοιχείο του αλφάβητου, ένα γεγονός που προσθέτει εν τέλει ασφάλεια στην όλη διαδικασία.

2.1.5. Passlogix - Passpoints

Η Passlogix από τη μεριά της, μελέτησε το θέμα των οπτικών (visual) passwords και πιο συγκεκριμένα την ιδέα του Blonder [5], με βάση την οποία κάποιος χρήστης για να πιστοποιήσει την ταυτότητά του σε ένα σύστημα, θα πρέπει να κάνει κλικ σε συγκεκριμένα σημεία της οθόνης. Έτσι δημιούργησε το δικό της σύστημα πιστοποίησης, το οποίο κιόλας ονόμασε Passlogix. Στη συγκεκριμένη εφαρμογή, ο

χρήστης για να κάνει ένα επιτυχημένο login, θα πρέπει να κάνει κλικ σε μια σειρά από αντικείμενα που βρίσκονται στην εικόνα που προβάλλεται. Το μόνο πρόβλημα εδώ είναι: πως θα γίνεται αντιληπτό κατά την επιβεβαίωση, ανάλογα με το σημείο που έχει κάνει κλικ ο χρήστης, εάν το σημείο έχει επιλεχθεί ή όχι; Για την επίλυση της κατάστασης αυτής, έχουν δημιουργηθεί αόρατα σύνορα. Με βάση λοιπόν τα σύνορα αυτά, ακόμη και αν κάποιος χρήστης κάνεις κλικ σε ακριανό σημείο ενός αντικειμένου, μπορούμε να ξέρουμε εάν είναι αποδεκτό ή όχι, ελέγχοντας εάν είναι εντός ή εκτός των συνόρων.



Εικόνα 5: Passlogix.

Μια επέκταση της ιδέας αυτής έχει αναπτυχθεί από τους Wiedenbeck, Waters, Birget, Brodskiy και Memon [32, 33, 34], και ονομάζεται Passpoints. Αυτοί βασίστηκαν επίσης στην ιδέα του Blonder, αλλά μείωσαν τα προκαθορισμένα σύνορα και προσέθεσαν μια ανοχή (tolerance) γύρω από κάθε pixel. Με τον τρόπο αυτό, το μόνο πράγμα που είχε να κάνει κάποιος χρήστης για να κάνει είσοδο σε ένα σύστημα, είναι να κάνει κλικ, μέσα στο όριο ανοχής των pixels που είχε επιλέξει, αλλά και τη σωστή σειρά.

Εικόνα 6: Passpoints.

Αυτό που θα πρέπει σίγουρα να αναφέρουμε εδώ, είναι ότι οι πιο πολύπλοκες εικόνες έχουν εκατοντάδες ευκολομνημόνευτα σημεία. Έτσι με 5 ή 6 κλικ σε μια εικόνα, ένας χρήστης μπορεί να δημιουργήσει περισσότερα passwords από τα text passwords που δημιουργούνται με 8 χαρακτήρες σήμερα. Με βάση λοιπόν όλα αυτά, είναι πολύ εύκολο να καταλάβουμε ότι το πιθανό password space με τη μέθοδο αυτή είναι πολύ μεγάλο, γεγονός που έχει ως αποτέλεσμα, το όλο σύστημα των Passpoints να αποδεικνύεται ως ένα πολύ έγκυρο και ασφαλές σύστημα.

2.2. ΕΠΙΛΥΟΝΤΑΣ ΤΟ ΠΡΟΒΛΗΜΑ ΤΟΥ SHOULDER SURFING

Το shoulder surfing είναι όταν κοιτάει κάποιος πάνω από τον ώμο ενός χρήστη που προσπαθεί να εισάγει τις προσωπικές του πληροφορίες σε ένα σύστημα και να κάνει login. Λόγω της γραφικής τους φύσης όλα τα visual passwords, αλλά και τα γραφικά που θα εξετάσουμε αμέσως μετά, είναι πολύ ευαίσθητα στο φαινόμενο αυτό. Στο κομμάτι που ακολουθεί αμέσως μετά, παρουσιάζονται τρεις τρόποι που έχουν αναπτυχθεί από τους Sobrado και Birget και που έχουν ως σκοπό την επίλυση του προβλήματος αυτού.

2.2.1. Triangle Scheme

Την κεντρική ιδέα του Triangle Scheme, μπορούμε να την δούμε στην Εικόνα 7. Με βάση την εικόνα αυτή, σε μια τέτοια περίπτωση, αυτό που βλέπει ο χρήστης στην οθόνη του, είναι ένα σύνολο από *N* αντικείμενα, σε τυχαία θέση. Σε πρώτη φάση ο χρήστης θα πρέπει να δημιουργήσει το προσωπικό του password. Για το σκοπό αυτό, θα πρέπει να επιλέξει *K* αντικείμενα από αυτά που βλέπει στην οθόνη του, τα οποία ονομάζονται *pass-objects* και θα αποτελούν από δω και πέρα το portfolio του.

Εικόνα 7: Triangle Scheme.

Όταν ο χρήστης θα πρέπει να κάνει είσοδο στο σύστημα, στην οθόνη του θα δει ένα σύνολο από *L* εικόνες, για το οποίο θα ισχύει $L<N$. Τη στιγμή αυτή λοιπόν, ο χρήστης θα πρέπει να αναγνωρίσει 3 από τα pass-objects που είχε προεπιλέξει και να κάνει κλικ μέσα στο αόρατο τρίγωνο που δημιουργείται από αυτά. Η διαδικασία αυτή βέβαια, δεν γίνεται μόνο μία φορά, καθώς θα ήταν πολύ εύκολο για κάποιο κακόβουλο άτομο, να κάνει κλικ στο συγκεκριμένο τρίγωνο καθαρά από τύχη. Για να αποφευχθεί κάτι τέτοιο λοιπόν, η όλη διαδικασία επαναλαμβάνεται 8 – 10 φορές σε κάθε διαδικασία εισόδου, ώστε να μειωθεί όσο γίνεται περισσότερο η πιθανότητα ενός τυχαίου κλικ, στη σωστή περιοχή.

2.2.2. Movable Frame

Εικόνα 8: Movable Frame Scheme.

Έχοντας ως βάση την ίδια ιδέα που έχει και το Triangle Scheme που αναλύσαμε προηγουμένως, δημιουργήθηκε και το Movable Frame Scheme, που θα αναλύσουμε τώρα. Στην περίπτωση αυτή λοιπόν, χρήστης θα πρέπει να αναγνωρίσει και πάλι 3 από τα pass-objects που έχει ήδη επιλέξει. Η διαφορά είναι ότι τώρα θα μετακινήσει το κινητό πλαίσιο που υπάρχει γύρω-γύρω, όπως βλέπουμε στην Εικόνα 8, μέχρι τα τρία pass-objects (δύο μέσα και ένα στο πλαίσιο) να ευθυγραμμιστούν.

Όπως είναι φυσικό βέβαια, η συγκεκριμένη διαδικασία, επαναλαμβάνεται και πάλι για αρκετές φορές, καθώς όπως έχει ήδη αναφερθεί πιο πάνω, θα πρέπει να αποφευχθεί η πιθανότητα να ευθυγραμμιστούν τα σωστά αντικείμενα, εντελώς τυχαία.

2.2.3. Other Geometric Configurations

Εικόνα 9: Other Geometric Configurations.

Η τρίτη και τελευταία μέθοδος των Sobrado και Birget, για την επίλυση του προβλήματος του shoulder surfing, παρουσιάζεται παρακάτω και ακολουθεί τους ίδιους βασικούς κανόνες με τις προηγούμενες δύο. Η διαφορά εδώ είναι ότι ο χρήστης θα πρέπει να αναγνωρίσει 4 pass-objects από αυτά που έχει επιλέξει και που έχει στο προσωπικό του portfolio, και να κάνει κλικ στο σημείο που τέμνονται οι αόρατες γραμμές που δημιουργούνται από τα αντικείμενα. Βέβαια, όπως είναι φυσικό, υπάρχει μία ανοχή γύρω από pixel που κάνει κλικ ο χρήστης, ώστε να μην υπάρχουν διαφωνίες για το ακριβές σημείο που επιλέγει ο χρήστης, ενώ θα πρέπει να αναφέρουμε ακόμη ότι η διαδικασία επαναλαμβάνεται, ώστε να μην έχουμε τυχαία επιλογή του σωστού σημείου.

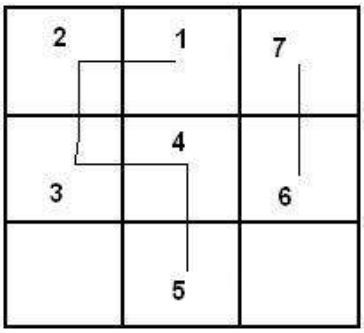
2.3. GRAPHICAL PASSWORDS

Στο κομμάτι που ακολουθεί, θα αναλύσουμε τα γραφικά passwords, την άλλη τεχνική που ανήκει στην κατηγορία των proof by knowledge τεχνικών, που βοηθά τους χρήστες στην ασφαλέστερη πιστοποίηση της ταυτότητάς τους. Με τα γραφικά passwords ο κάθε χρήστης πρέπει να ζωγραφίζει ένα προσωπικό σχέδιο, το οποίο θα αποτελεί από δω και πέρα τον μυστικό του κωδικό για την είσοδό του στο σύστημα. Πιο συγκεκριμένα, θα εξετάσουμε την τεχνική DAS (Draw-a-Secret) και μια πολύ καινούργια επέκταση, τα Multi-grid passwords.

2.3.1. Draw-a-Secret (DAS) Scheme

Η τεχνική DAS ή Draw-a-Secret, έχει προταθεί από τους Jermyn, Mayer, Monrose, Reiter, και Rubin [17] και όπως μπορούμε εύκολα να καταλάβουμε και από το όνομά της, βασίζεται στο σχεδιασμό του μυστικού κωδικού. Όταν ο χρήστης θελήσει να δημιουργήσει το προσωπικό του password, αυτό που θα δει στην οθόνη του είναι ένα ορθογώνιο πλέγμα $G \times G$. Πάνω σε αυτό το πλέγμα, θα πρέπει να ζωγραφίσει μια σειρά από γραμμές, οι οποίες από εδώ και πέρα θα αντιπροσωπεύουν τον μυστικό του κωδικό.

Στην Εικόνα 10 παρουσιάζουμε ένα παράδειγμα της τεχνικής DAS. Στη συγκεκριμένη περίπτωση το πλέγμα έχει μέγεθος 3×3, και μέσα σε αυτό έχουν ζωγραφιστεί μια σειρά από γραμμές. Όπως βλέπουμε λοιπόν, για να δημιουργήσει ο χρήστης τον κωδικό του, θα πρέπει να σχεδιάσει μία ή περισσότερες γραμμές, ενώ κατά τη διαδικασία εισόδου θα πρέπει να σχεδιάσει τις ίδιες γραμμές, με την ίδια φορά, αλλά και με την ίδια σειρά. Για το λόγο αυτό, το τελικό σχέδιο χαρτογραφείται σε μια ακολουθία ισότιμων ζευγαριών, φτιάχνοντας μια λίστα των κελιών από τα οποία κάθε γραμμή περνάει, με τη σωστή σειρά, συμπεριλαμβάνοντας και pen-up events κάθε φορά που ο χρήστης σηκώνει το μολύβι του και συνεχίζει από ένα άλλο σημείο. Στη συνέχεια παραθέτουμε τη λίστα με τα κελιά και τα pen-up events που αντιστοιχεί στο σχέδιο της Εικόνας 10:

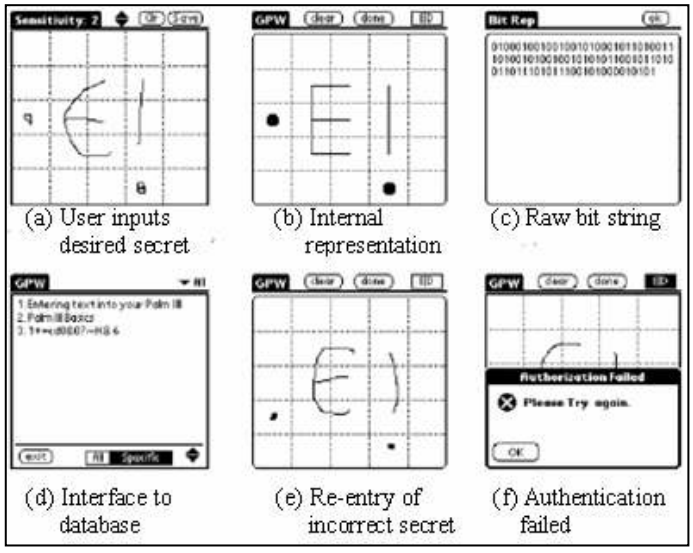


Εικόνα 10: DAS Scheme.

(1,2), (1,1), (2,1), (2,2), (3,2), pen-up, (2,3), (1,3).

Με βάση τη συγκεκριμένη λίστα θα πρέπει να τονίσουμε ένα πολύ σημαντικό θέμα που αφορά το DAS Scheme. Για να μπορέσει ένας χρήστης να πιστοποιήσει την ταυτότητά του και να κάνει επιτυχημένο login σε ένα σύστημα, αυτό που έχει σημασία δεν είναι να ζωγραφίσει το ακριβές σχήμα που έχει φτιάξει (να περάσει δηλαδή από τα ίδια ακριβώς pixel στην οθόνη). Αντίθετα, αυτό που έχει πραγματική σημασία είναι η σειρά των κελιών από τα οποία περνάει το μολύβι του χρήστη, σε συνδυασμό με τα Pen-up events.

Στην Εικόνα 11 μπορούμε να δούμε ένα άλλο παράδειγμα του DAS Scheme, την εσωτερική του αναπαράσταση, το bit string που δημιουργείται και μια αποτυχημένη απόπειρα login εξαιτίας ενός shift error.



Εικόνα 11: DAS Scheme. Εσωτερική αναπαράσταση του σχεδίου, και ένα αποτυχημένο login εξαιτίας ενός shift error [17].

Αυτό που είναι πολύ σημαντικό εδώ και θα πρέπει να αναφέρουμε είναι ότι το bit string που δημιουργείται δεν αποθηκεύεται. Αντίθετα, εφαρμόζεται σ' αυτό μια μονόδρομη hash συνάρτηση και το αποτέλεσμα αυτής αποθηκεύεται τελικά στον server. Έτσι όταν ένας χρήστης προσπαθήσει να κάνει είσοδο στο σύστημα, το πρώτο πράγμα που θα πρέπει να κάνει είναι να σχεδιάσει το password που είχε επιλέξει. Στη συνέχεια, η ίδια hash συνάρτηση εφαρμόζεται στο καινούργιο σχέδιο και το αποτέλεσμα που θα έχουμε συγκρίνεται τελικά με αυτό που είχαμε αποθηκευμένο. Εάν τα δύο αυτά είναι ίδια ο

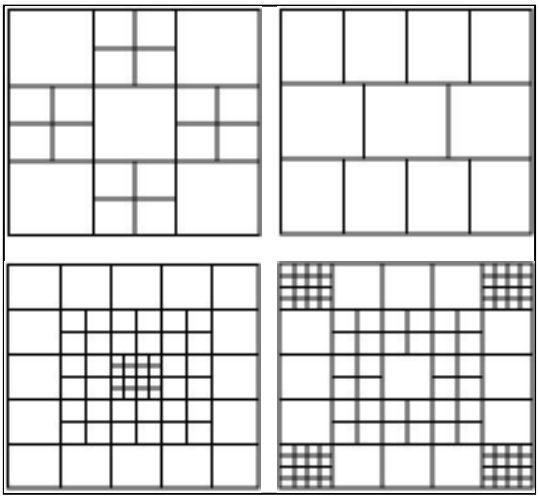
χρήστης έχει πιστοποιήσει με επιτυχία την ταυτότητά του και έχει κάνει είσοδο στο σύστημα, ενώ σε αντίθετη περίπτωση δεν αποκτά το δικαίωμα εισόδου. Όπως μπορούμε να καταλάβουμε η όλη διαδικασία γίνεται πολύ ασφαλής και αυτό γιατί το σύστημα δεν γνωρίζει το password του κάθε χρήστη. Αυτό συμβαίνει εξαιτίας της hash συνάρτησης που εφαρμόζεται, από την οποία καθώς είναι μονόδρομη, δεν μπορούμε να υπολογίσουμε το αρχικό σχέδιο από το αποτέλεσμα που είναι αποθηκευμένο στον server.

2.3.2. Multi-grid Passwords

Το DAS Scheme ήταν η πρώτη εφαρμογή που βασίστηκε στην ιδέα του σχεδιασμού ενός password, με σκοπό να ξεφύγουμε από τα text passwords και όλα τα προβλήματα που δημιουργούν σε θέματα ασφάλειας. Όμως ακόμη και τα DAS passwords έχουν τα δικά τους προβλήματα. Οι Nali και Thorpe [20], έκαναν μια έρευνα με σκοπό να ανακαλύψουνε τα προβλήματα αυτά, ή μάλλον πιο συγκεκριμένα τις αιτίες που μπορούν να κάνουν τα DAS passwords προβλέψιμα. Με βάση λοιπόν τα αποτελέσματά τους αποδεικνύεται ότι όντως υπάρχουν κάποιοι λόγοι που αν συντελέσουν θα δημιουργήσουν πρόβλημα και θα κάνουν τα passwords ευαίσθητα σε επιθέσεις. Τα όλα προβλήματα βέβαια βασίζονται στη συμπεριφορά των χρηστών όταν θέλουν να επιλέξουν ένα password, καθώς σχεδιάζουν passwords με προβλεπόμενα χαρακτηριστικά. Για να είναι ένα password λοιπόν προβλεπόμενο, θα πρέπει ή να είναι συμμετρικό ή να έχει ζωγραφιστεί στο κέντρο, μειώνοντας με τον τρόπο αυτό κατά πολύ το password space και βοηθώντας άτομα που θέλουν να επιτεθούν στο σύστημα στη δημιουργία αυτοματοποιημένων λεξικών με σκοπό να κάνουν dictionary attacks [21, 30]. Βασιζόμενοι στη συγκεκριμένη δουλειά, οι Birget, Hong και Memon [4] την επεκτείνανε, καθώς αναφέρανε και προβλήματα των DAS passwords εξαιτίας της αβεβαιότητας που υπάρχει στις περιοχές που κάνει κλικ και από τις οποίες περνάει ο χρήστης κατά τη δημιουργία του password, ιδιαίτερα όταν έχουμε να ζωγραφίσουμε μέσα σε ένα πολύ μεγάλο grid

Οι Chalkias, Alexiadis και Stephanides [2, 7] δημιουργήσανε μια επέκταση του DAS με σκοπό να μειώσουνε όσο γίνεται περισσότερο τις καταστάσεις που αναφέραμε παραπάνω και τα προβλήματα που αυτές μπορεί να δημιουργήσουν. Προτείνανε λοιπόν

τα Multi-grid passwords, τα οποία υλοποιούνται με αλλαγή του πλέγματος πάνω στο οποίο ο χρήστης θα πρέπει να σχεδιάσει τον κωδικό του. Πιο συγκεκριμένα, αυτό που κάνανε ουσιαστικά είναι ότι φτιάξανε εμφωλευμένα πλέγματα (nested grids) πάνω στο αρχικό πλέγμα του DAS (Εικόνα 12).



Εικόνα 12: Multi-grid passwords [2].

Η ιδέα αυτή βασίστηκε στους βασικούς λόγους για τους οποίους οι χρήστες αποτυγχάνουν στην επιβεβαίωση των προσωπικών τους DAS κωδικών, και οι οποίοι είναι οι παρακάτω:

- ξεχνάνε την σειρά με την οποία σχεδιάσανε τις γραμμές
- περνάνε από γειτονικά κελιά αντί για τα σωστά (shift errors)

Με την τεχνική DAS των multi-grid passwords οι χρήστες μπορούν να αποφύγουν τις καταστάσεις που προαναφέραμε, καθώς με τον τρόπο αυτό όπως παρατηρούμε και στην Εικόνα 12, δημιουργούνται περισσότερα σημεία εστίασης. Έτσι δεν είναι αναγκασμένοι να σχεδιάζουν στο κέντρο ή συμμετρικά για να θυμούνται πιο εύκολα, αλλά αντίθετα έχουν στη διάθεσή τους περισσότερα σημεία που μπορούν να επικεντρωθούν, δημιουργώντας με τον τρόπο αυτό πιο πολύπλοκα passwords, καθόλου προβλέψιμα και ταυτόχρονα ιδιαίτερα εύκολα στην απομνημόνευσή τους.

3. ΑΛΛΕΣ ΣΧΕΤΙΚΕΣ ΕΡΓΑΣΙΕΣ

Επειδή η ασφάλεια είναι ένα θέμα πολύ σημαντικό στις μέρες, που χρειάζεται συνεχή παρακολούθηση και συνεχείς βελτιώσεις για να έχουμε τελικά ένα καλό αποτέλεσμα, αρκετοί είναι οι ερευνητές αυτοί που ασχολήθηκαν με τις νέες μεθόδους πιστοποίησης των χρηστών. Σκοπός τους ήταν να συγκρίνουν συνήθως την κάθε καινούργια μέθοδο με τα text passwords που χρησιμοποιούνται ευρέως σήμερα, να βρούνε πιθανά μειονεκτήματα που μπορεί να δημιουργήσουν προβλήματα και εξετάζοντας όλα αυτά να μπορέσουν να συμπεράνουν κατά πόσο οι νέες αυτές μέθοδοι μπορούν να γίνουν αποδεκτοί από την ευρύτερη κοινωνία μας.

Οι Irakleous, Furnell, Dowland και Papadaki [13] με την έρευνά τους αποδείξανε ότι στις μέρες μας, με την τόση μεγάλη ανάπτυξη των υπολογιστών και γενικότερα όλων των νέων τεχνολογιών, σχεδόν όλοι άνθρωποι χρησιμοποιούν μυστικά passwords, έστω ένα κάθε μέρα, για να καλύψουν προσωπικές τους ανάγκες όπως συναλλαγές χρημάτων μέσω ATM, χρήση κινητού τηλεφώνου, χρήση e-mail κλπ. 59% των ατόμων που συμμετείχαν στην έρευνά τους, διαθέτουν 2 – 5 passwords για χρήση σε διάφορες εφαρμογές, ενώ το 15% έχει πάνω από 10. Συνδυάζοντας λοιπόν τα αποτελέσματα αυτά με το γεγονός ότι το 65% των ατόμων αυτών χρησιμοποιεί καθημερινά τουλάχιστον ένα από τα passwords που διαθέτει, καταλαβαίνουμε πόσο σημαντικό ρόλο παίζει η ασφάλεια των προσωπικών μας κωδικών. Επίσης, μετρώντας τον αριθμό των επιτυχημένων προσπαθειών για login που έκαναν οι χρήστες της συγκεκριμένης έρευνας, βρέθηκε ότι το μόνο το 70% αυτών επιβεβαίωσε σωστά τον προσωπικό του κωδικό, κάτι που δίνει ακόμη μεγαλύτερη ώθηση στην έρευνα για τη δημιουργία καινούργιων μεθόδων για την πιστοποίηση χρηστών.

Ο Tribelhorn [31] μέσα από δική του έρευνα, απέδειξε ότι η ασφάλεια είναι ένα θέμα που δεν είναι αδιάφορο ακόμη και στους πιο απλούς χρήστες που δεν έχουν καμία σχέση με τις νέες τεχνολογίες. Αρχικά εξέτασε ποιοι χαρακτήρες είναι οι πιο συνηθισμένοι στα text passwords που χρησιμοποιούμε σήμερα. Έτσι αποδείχτηκε ότι το 58% των συμμετεχόντων στην έρευνα, έχει passwords που αποτελούνται μόνο από αριθμούς, ενώ μόνο το 15% χρησιμοποιεί στους κωδικούς του εκτός από αριθμούς και γράμματα, και άλλα σύμβολα. Το ενθαρρυντικό εδώ είναι ότι το 27% των χρηστών

έχουν passwords που αποτελούνται από 8 και πάνω χαρακτήρες, κάτι που αποδεικνύει ότι πολλοί άνθρωποι προσπαθούν να έχουν τουλάχιστον ένα password μεγαλύτερο, πιο δύσκολο και άρα πιο ασφαλές, έστω για την πιο σημαντική εφαρμογή που χρησιμοποιούνε. Παρόλα αυτά όμως, ακόμη και αν οι χρήστες πραγματικά πιστεύουν ότι η ασφάλεια των κωδικών είναι ένα θέμα πολύ μεγάλης σημασίας, το 65% αυτών δημιουργεί ένα password στη αρχή και δεν το αλλάζει ποτέ ξανά για τη συγκεκριμένη εφαρμογή, με αποτέλεσμα όσο ο καιρός περνάει να γίνεται όλο και πιο ευάλωτο στις επιθέσεις.

Όλα όσα έχουμε αναφέρει οδηγούν στο γεγονός ότι ήταν επιτακτική ανάγκη η δημιουργία καινούργιων μεθόδων πιστοποίησης των χρηστών, που θα είναι πολύ πιο ασφαλείς από τις ήδη υπάρχουσες. Έτσι δημιουργήθηκαν τα visual και τα graphical passwords. Με βάση τον Jansen [15] τα visual passwords δεν είναι πραγματικά μια ασφαλής μέθοδος, επειδή οι χρήστες συνήθως διαλέγουν ένα μικρό αριθμό εικόνων (4 ή 5). Για παράδειγμα, εάν βασιστούμε στη δουλειά του, και συγκρίνουμε τα visual με τα text passwords, μπορούμε να αποδείξουμε ότι τα άτομα που έχουν 4 – 6 χαρακτήρες στο προσωπικό τους text password, επιλέγουν 4 εικόνες, δημιουργώντας ένα password πολύ εύκολα να σπάσει. Εξετάζοντας τώρα τα άτομα που στο text password έχουν 8 – 9 χαρακτήρες, δηλαδή έχουν ένα αρκετά ασφαλή κωδικό, επιλέγουν 6 εικόνες, δημιουργώντας με τον τρόπο αυτό ένα visual password πολύ εύκολο και άρα πολύ ευαίσθητο σε κακόβουλες επιθέσεις.

Πολλές εφαρμογές πιστοποίησης χρήστη, που βασίζονται στα visual passwords και στην επιλογή εικόνων έχουν δημιουργηθεί, ενώ την ίδια στιγμή γίνονται πολλές έρευνες με σκοπό την εξέταση των τεχνικών αυτών και την εύρεση των πλεονεκτημάτων και μειονεκτημάτων τους. Μερικές από τις έρευνες αυτές αναφέρονται και αναλύονται στο κείμενο που ακολουθεί:

- Οι Kim και Kwon [18] εξέτασαν πόσο εύκολα στην απομνημόνευση είναι τα visual passwords ανάλογα με το θέμα που έχουν οι εικόνες. Η έρευνά τους έδειξε ότι τα καλύτερα αποτελέσματα τα είχαν οι εικόνες με γνωστά στον κάθε χρήστη πρόσωπα. Αυτά τα passwords μπορούν να απομνημονευθούν πολύ πιο εύκολα απ’ ότι τα passwords που απεικονίζουν τυχαία πρόσωπα ή τοπία. Αυτό που θα

πρέπει να τονίσουμε εδώ, καθώς είναι ιδιαίτερα περίεργο και αξιοθαύμαστο, είναι ότι οι χρήστες που συμμετείχαν και επέλεξαν 15 εικόνες γνωστών προσώπων (ένας αριθμός πολύ μεγάλος για την περίπτωση των visual passwords), είχε τη δυνατότητα να τις θυμάται και να κάνει μια επιτυχημένη είσοδο στο σύστημα που χρησιμοποιούσε, ακόμη και μία εβδομάδα μετά τη δημιουργίας τους, που οι συμμετέχοντας υποβλήθηκαν ξανά στο test. Αυτό είναι πολύ σημαντικό καθώς για την περίπτωση των τυχαίων προσώπων ή των τοπίων τα αντίστοιχα ποσοστά είναι πολύ μικρά ακόμη και όταν αναφερόμαστε σε password που αποτελούνται από 5 – 8 εικόνες.

- Οι Davis, Monrose και Reiter [9] ασχολήθηκαν με το είδος των εικόνων που επιλέγουν οι γυναίκες σε σχέση με τους άντρες στο Story Scheme, ανάλογα με το τι απεικονίζει η κάθε μια. Η δουλειά τους αποδεικνύει ότι οι γυναίκες επιλέγουν ζώα σε ποσοστό διπλάσιο απ' ότι οι άντρες, ενώ οι άντρες επιλέγουν γυναικεία πρόσωπα, σε ποσοστό διπλάσιο από αυτό των γυναικών. Επίσης το θέμα που οι γυναίκες προτιμούν περισσότερο από τα άλλα και συνήθως επιλέγουν είναι το φαγητό, σε αντίθεση με τους άντρες προτιμούν να διαλέγουν εικόνες που έχουν ως θέμα τη φύση ή διάφορα αθλήματα.
- Οι Dhamija και Perrig [10] τέλος ασχολήθηκαν με τη μέθοδο πιστοποίησης Déjà vu. Μέσα από την έρευνά τους απέδειξαν ότι οι χρήστες ξοδεύουν πολύ χρόνο για τη δημιουργία του image portfolio καθώς και για να κάνουνε login και να μπούνε στο σύστημα που θέλουν να χρησιμοποιήσουνε. Εντονότερο γίνεται το πρόβλημα εάν χρησιμοποιείται η τεχνική του Random Art που έχουμε προαναφέρει, η οποία όπως φαίνεται μπορεί να κάνει το σύστημα ασφαλέστερο, αλλά μπερδεύει λίγο περισσότερο τον χρήστη. Βέβαια, η περίπτωση αυτή έχει και ένα θετικό αποτέλεσμα που είναι πολύ σημαντικό και που θα πρέπει να αναφέρουμε. Μία εβδομάδα μετά τη δημιουργία των προσωπικών κωδικών, έγινε επανάληψη της διαδικασίας πιστοποίησης των χρηστών που συμμετείχαν στην έρευνα. Μετά από αυτό το χρονικό διάστημα λοιπόν, πολλά άτομα έκαναν λάθος και δεν μπόρεσαν να κάνουν ένα επιτυχημένο login χρησιμοποιώντας PINs ή text passwords. Αντίθετα, οι χρήστες που δεν θυμόταν καλά το visual password που είχαν δημιουργήσει και έκαναν λάθος στην επιβεβαίωσή του, ήταν πολύ λιγότεροι, όχι μόνο για την περίπτωση των απλών εικόνων, αλλά ακόμα και χρησιμοποιώντας

εικόνες που στηρίζονται στην τεχνική Random Art. Βασιζόμενοι λοιπόν στο τελευταίο αυτό αποτέλεσμα, μπορούμε πλέον με σιγουριά να πούμε ότι είναι πολύ πιο εύκολο σε κάποιον χρήστη να θυμάται εικόνες, ακόμη και αν αυτές είναι αφηρημένες, απ' το να θυμάται μια σειρά από χαρακτήρες για τους text κωδικούς του.

Εξετάζοντας τα μειονεκτήματα των visual passwords, που απέδειξαν ότι δεν είναι καθόλου ασφαλή, ήταν απαραίτητο να βρεθούν και άλλου τρόποι για την πιστοποίηση των χρηστών. Έτσι επινοήθηκαν τα γραφικά passwords. Οι Wiedenbeck, Waters, Birget, Brodskiy και Memon [32] μετά από έρευνά τους που εξέταζε τη λειτουργία των γραφικών passwords, κατέληξαν στο συμπέρασμα ότι είναι πιο χρονοβόρα από τα αλφαριθμητικά passwords και ότι στο ξεκίνημα της χρήσης τους, το ποσοστό των μη επιτυχημένων login είναι κατά πολύ μεγαλύτερο. Υπάρχει βέβαια και το γεγονός που επιβεβαιώνει ότι τα γραφικά passwords είναι μια πάρα πολύ καλή και πάνω απ' όλα ασφαλής μέθοδος πιστοποίησης χρήσης. Αυτό που συμπεραίνουν λοιπόν οι συγγραφείς μετά τη διεξαγωγή της έρευνάς τους, είναι ότι τα ποσοστά που αναφέρονται πιο πάνω αντιστρέφονται, όταν οι χρήστες που συμμετέχουν περάσουν από μια περίοδο εξάσκησης. Αυτό σημαίνει ότι εάν χρησιμοποιηθούν τα γραφικά passwords για ένα δοκιμαστικό χρονικό διάστημα, όχι πολύ μεγάλο, οι συγκεκριμένοι χρήστες θα έχουν τη δυνατότητα να δημιουργήσουν πολύ δύσκολα passwords και άρα πολύ ασφαλή, και καθόλου ευαίσθητα σε κακόβουλες επιθέσεις.

Μια καλύτερη και μεγαλύτερη έρευνα πάνω στα γραφικά passwords έγινε από τους Goldberg et al. [12], οι οποίοι απέδειξαν ότι πολλοί χρήστες ζωγραφίζουν σχέδια που μοιάζουν ακριβώς με τα πρωτότυπα, αλλά δεν είναι πανομοιότυπα αφού οι χρήστες έχουν σχεδιάσει λάθος τον αριθμό των γραμμών, τη σειρά ή τη κατεύθυνσή τους. Το ενθαρρυντικό αποτέλεσμα που παρατηρείται εδώ είναι ότι μετά από ένα μικρό χρονικό διάστημα πρακτικής εξάσκησης, πολλοί από τους χρήστες μπορούν να επιβεβαιώσουν πλέον σωστά τον προσωπικό τους κωδικό και να κάνουν εισαγωγή στο σύστημα που χρησιμοποιούν. Το αποτέλεσμα αυτό γίνεται πιο συγκεκριμένο εάν τονίσουμε ότι το 72% των ατόμων που συμμετείχαν στην έρευνα, μετά από εξάσκηση, συμφώνησε ότι

τα είναι πολύ πιο εύκολο για κάποιον να θυμάται το γραφικό password που έχει δημιουργήσει, από το να θυμάται το PIN του ή κάποιον αλφαριθμητικό κωδικό.

Οι Nali και Thrope [20], διεξήγαγαν μία έρευνα στην οποία ο βασικός της στόχος είναι η εύρεση των μειονεκτημάτων που παρατηρούνται στα γραφικά passwords. Με βάση λοιπόν την έρευνα αυτή, αποδείχτηκε ότι το 86% των χρηστών σχεδιάζουν κεντραρισμένα ή σχεδόν κεντραρισμένα password, το 45% των passwords που δημιουργούνται είναι συμμετρικά και το 29% είναι άκυρα επειδή δεν ακολουθούν τους συγκεκριμένους κανόνες που έχουν οριστεί.

Οι Chalkias et al. [7], βασιζόμενοι σε όλα τα παραπάνω αποτελέσματα προτείνανε τα multi-grid passwords και κάνανε μια έρευνα στην οποία συγκρίνανε τα αποτελέσματα ανάμεσα σε άτομα που χρησιμοποιούν τις νέες τεχνολογίες (technical users) και σε αυτά που δεν είναι πληροφορημένοι πάνω σε αντίστοιχα τεχνικά θέματα (non-technical users). Αποδείχτηκε λοιπόν ότι το 66% των χρηστών που δεν έχουν σχέση με τις νέες τεχνολογίες και το 80% αυτών που έχουν, επιβεβαίωσαν με επιτυχία τα text passwords που είχανε δημιουργήσει. Τα αντίστοιχα ποσοστά με τη μέθοδο DAS είναι μικρότερα και φτάνουν το 47% και 60%, ενώ επίσης η έρευνα έδειξε ότι το 80% των μη ενημερωμένων χρηστών και το 67% των ενημερωμένων σχεδίασαν κεντραρισμένα passwords. Λαμβάνοντας λοιπόν υπόψιν τα αποτελέσματα αυτά, προτάθηκαν τα multi-grid passwords, τα οποία δημιουργούν μια διαφορετική κατάσταση. Στην περίπτωση αυτή, θα πρέπει να τονίσουμε ότι ο αριθμός των κεντραρισμένων passwords είναι πολύ μικρότερος (46% για τους μη ενημερωμένους χρήστες και 33% για τους τεχνολογικά ενημερωμένους). Με βάση αυτό μπορούμε να καταλάβουμε ότι με τα multi-grid passwords, οι χρήστες δημιουργούν πολύ πιο δύσκολα και μη προβλέψιμα passwords και άρα λιγότερο ευαίσθητα σε κάθε είδους επιθέσεις.

Οι έρευνες που αναφέραμε και αναλύσαμε μέχρι τώρα, έχουν δύο βασικά χαρακτηριστικά τα οποία θα πρέπει να τονίσουμε απαραιτήτως, ώστε να μπορέσουμε να προσδιορίσουμε καλύτερα το σκοπό της δικής μας εργασίας. Πρώτον, η κάθε έρευνα προτείνει μια καινούργια μέθοδο πιστοποίησης και βασίζεται στη μέθοδο αυτή. Έτσι σε κάθε περίπτωση, οι συγγραφείς κάνουν μια σύγκριση του visual ή graphical password

που προτείνεται, με τα text passwords που χρησιμοποιούνται σήμερα. Δεύτερον, θα πρέπει να τονίσουμε ότι ο αριθμός των ατόμων που συμμετείχαν στις έρευνες είναι πολύ μικρός (η μεγαλύτερη έρευνα έγινε σε περίπου 40 άτομα, ενώ οι περισσότερες έγιναν σε 20 περίπου άτομα) και ότι όλοι οι χρήστες είχαν ηλικία μέχρι 25 ετών, αφού οι έρευνες διεξήχθηκαν σε σχολεία, πανεπιστήμια και κολέγια. Οι τελευταίες δύο παρατηρήσεις που κάναμε, είναι πολύ σημαντικές και μπορούν να θεωρηθούν ακόμη και σοβαρά μειονεκτήματα των ερευνών, αφού το δείγμα είναι μικρό και όχι σωστά κατανεμημένο, με αποτέλεσμα να υπάρχει περίπτωση να οδηγήσει σε αποτελέσματα μη στατιστικά σημαντικά.

Η δική μας έρευνα είναι η πρώτη ολοκληρωμένη έρευνα που κάνει μια πολύ αναλυτική και εκτενέστατη σύγκριση ανάμεσα στα visual και graphical passwords και στα text που ήδη χρησιμοποιούνται. Έτσι, συμπεριλάβαμε ένα ερωτηματολόγιο αλλά και μια εφαρμογή όπου οι χρήστες είχαν τη δυνατότητα να δημιουργήσουν τα δικά τους passwords. Με τον τρόπο αυτό εξετάσαμε τα βασικά χαρακτηριστικά και των τριών μεθόδων και ανακαλύψαμε τα πλεονεκτήματα που μπορεί να προσφέρει η κάθε μία. Επιπλέον, στη δική μας έρευνα προσπαθήσαμε να είμαστε πιο αντικειμενικοί, με απώτερο στόχο να έχουμε καλύτερα και πιο έγκυρα αποτελέσματα. Για το λόγο αυτό, στην έρευνά μας συμμετείχαν 100 άτομα (ένα δείγμα αρκετά μεγάλο), ηλικίας από 18 έως 60 ετών. Αρχικά ενημερώσαμε τους χρήστες για τις νέες μεθόδους πιστοποίησης (visual και graphical passwords) και κάναμε μια σύγκρισή τους μεταξύ τους, αλλά και με τα PINs και τα text passwords που χρησιμοποιούνται σήμερα. Έτσι μπορέσαμε να βρούμε και να εξετάσουμε τα πλεονεκτήματα τους που τα κάνουν πιο ασφαλή από τις παραδοσιακές μεθόδους και τελικά να δούμε σε τι ποσοστό είναι διατεθειμένη η κοινωνία μας να διαφοροποιήσει τις συνήθειές της και να δεχτεί μια τόσο καινούργια και καινοτομική ιδέα.

4. ΜΕΘΟΔΟΛΟΓΙΑ

4.1. ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ – ΕΦΑΡΜΟΓΕΣ

Για τη διεξαγωγή της έρευνάς μας δημιουργήσαμε ένα ερωτηματολόγιο, με σκοπό μέσα από τις απαντήσεις των χρηστών να εξετάσουμε την προσωπική τους γνώμη. Επίσης πριν επιχειρήσουν να το απαντήσουν, δημιούργησαν τα προσωπικά τους passwords, ώστε να έχουν μια καλύτερη και πιο εμπεριστατωμένη γνώμη για το όλο θέμα της ασφάλειας των κωδικών και των νέων μεθόδων που έχουν προταθεί.

Το ερωτηματολόγιο μας είναι ένα εντελώς καινούργιο ερωτηματολόγιο, το οποίο αποτελείται από 23 ερωτήσεις κλειστού τύπου και πολλαπλών επιλογών και μία ερώτηση ανοικτού τύπου στο τέλος, όπου οι χρήστες μπορούν να εκφράσουν την προσωπική τους γνώμη ή οποιαδήποτε άλλη παρατήρηση ή προβληματισμό τους πάνω στο όλο θέμα. Πιο συγκεκριμένα, αμέσως παρακάτω αναφέρουμε σύντομα τα βασικά στοιχεία και πληροφορίες που περιλαμβάνουν οι ερωτήσεις. Αυτά είναι:

- Πόσα passwords χρησιμοποιούν οι χρήστες, για ποιους λόγους και πόσο συχνά τα χρησιμοποιούνε
- Τι τρόπους χρησιμοποιούν για να θυμούνται καλύτερα τους προσωπικούς τους κωδικούς
- Εάν αλλάζουν τους κωδικούς τους για λόγους ασφαλείας ή χρησιμοποιούν τους ίδιους κωδικούς σε πολλαπλές εφαρμογές
- Τι είδους passwords χρησιμοποιούν (τι χαρακτηριστικά έχουν)
- Εάν είχαν ακούσει πιο πριν για visual και graphical passwords ή για οποιαδήποτε άλλη καινούργια μέθοδο πιστοποίησης
- Εάν έχουν θετική στάση απέναντι στα visual και graphical passwords
- Ποια είναι η γνώμη τους για τα visual και graphical passwords όσον αφορά την ασφάλειά τους, την ευκολία στην απομνημόνευσή τους, τη φιλικότητα προς τον χρήστη, το χρόνο που απαιτούν και τη συνολική ομορφιά τους αισθητικά.

Επίσης, για να μπορέσουν οι χρήστες να δημιουργήσουν τα δικά τους text, visual και graphical passwords, προσομοιώσαμε την όλη αυτή διαδικασία που κανονικά γίνεται σε υπολογιστή, στο χαρτί. Αυτό το κάναμε με σκοπό να ελέγχουμε πιο εύκολα τη

συγκεκριμένη διαδικασία και να την κάνουμε λιγότερο χρονοβόρα, καθώς ο αριθμός των ατόμων που συμμετέχουν στην έρευνα είναι πολύ μεγάλος. Έτσι για να βγάλουμε τα τελικά αποτελέσματα της έρευνάς μας, συνδυάσαμε τις απαντήσεις των χρηστών στο ερωτηματολόγιο, με τα προσωπικά passwords που δημιούργησαν και τις επιτυχημένες ή μη επιβεβαιώσεις τους. Με τον τρόπο αυτό διαπιστώσαμε εάν οι χρήστες στη χώρα μας μπορούν να απομακρυνθούν από τα text passwords που χρησιμοποιούνται σήμερα και να αποδεχτούν τις νέες και ασφαλέστερες μεθόδους πιστοποίησης που παρουσιάσαμε.

4.2. ΣΥΜΜΕΤΕΧΟΝΤΕΣ

Όπως έχουμε ήδη αναφέρει, στην έρευνά μας συμμετείχαν 100 άτομα που γνωρίζουν τη χρήση των PINs και text passwords από την προσωπική τους καθημερινή εμπειρία. Τα άτομα αυτά ήταν άνδρες και γυναίκες, ηλικίας από 18 έως 60 ετών.

Πιο συγκεκριμένα, το δείγμα αποτελείται από 49 άνδρες και 51 γυναίκες και χωρίζονταν σε 3 κατηγορίες με βάση την ηλικία τους: 59 χρήστες ηλικίας 18 έως 30 ετών, 20 χρήστες μέχρι 45 ετών και 21 χρήστες ηλικίας από 46 έως 60 ετών. Οι νεότεροι σε ηλικία συμμετέχοντες, είναι φοιτητές ή μεταπτυχιακοί φοιτητές στο Πανεπιστήμιο Μακεδονίας Θεσσαλονίκης, στο Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης και στο ΤΕΙ Λάρισας. Όσον αφορά τους μεγαλύτερους συμμετέχοντες τους απασχολήσαμε στον τόπο εργασίας τους και ήταν καθηγητές σε σχολεία και Πανεπιστήμια, άτομα που δουλεύουν σε δημόσιες υπηρεσίες και στον ιδιωτικό τομέα και τέλος κάποια άτομα που δουλεύουν σε άλλες βιομηχανίες και εργοστάσια στις περιφέρειες Θεσσαλονίκης και Λάρισας.

Αυτό που μας ενθάρρυνε πολύ από την αρχή της έρευνάς μας, αλλά και σε όλη τη διάρκειά της, είναι ότι όλοι τα άτομα που συμμετείχαν ήταν πολύ πρόθυμοι να αφιερώσουν ένα μέρος από το χρόνο τους και να μας βοηθήσουν. Σε αυτό βέβαια βοήθησε και η σύντομη εισαγωγή και επεξήγηση του θέματός μας που έγινε από την πρώτη κιόλας στιγμή. Με τον τρόπο αυτό έγινε κατανοητό ότι τα text passwords που χρησιμοποιούνται σήμερα δεν είναι πραγματικά καθόλου ασφαλής μέθοδος πιστοποίησης και ότι ήταν πλέον επιτακτική ανάγκη η εύρεση καινούργιων τεχνικών που θα μπορούν να ξεπεράσουν το πρόβλημα αυτό.

Αυτό που θα πρέπει να τονίσουμε εδώ είναι ότι ήταν πολύ δύσκολη και ιδιαίτερα χρονοβόρα η όλη διαδικασία εξεύρεσης των ατόμων που θα συμμετείχαν στην έρευνα, και περισσότερο όσον αφορά τις ηλικίες άνω των 35 ετών τους οποίους δεν μπορούμε να βρούμε σε μια τάξη και να τους απασχολήσουμε όλους μαζί για όσο χρονικό διάστημα χρειάζεται. Έτσι η όλη διαδικασία διήρκησε περίπου τρεις μήνες και εκτός από επισκέψεις σε σχολεία και Πανεπιστήμια, ήταν απαραίτητες και οι επισκέψεις στον τόπο εργασίας των χρηστών. Στις περιπτώσεις αυτές απασχολούνται ξεχωριστά 3 - 4 άτομα, καθώς ήταν πολύ δύσκολο μια ομάδα περισσότερων ατόμων να έχει ταυτόχρονα κάποιο χρόνο ελεύθερο για να μας διαθέσει.

4.3. ΔΙΑΔΙΚΑΣΙΑ

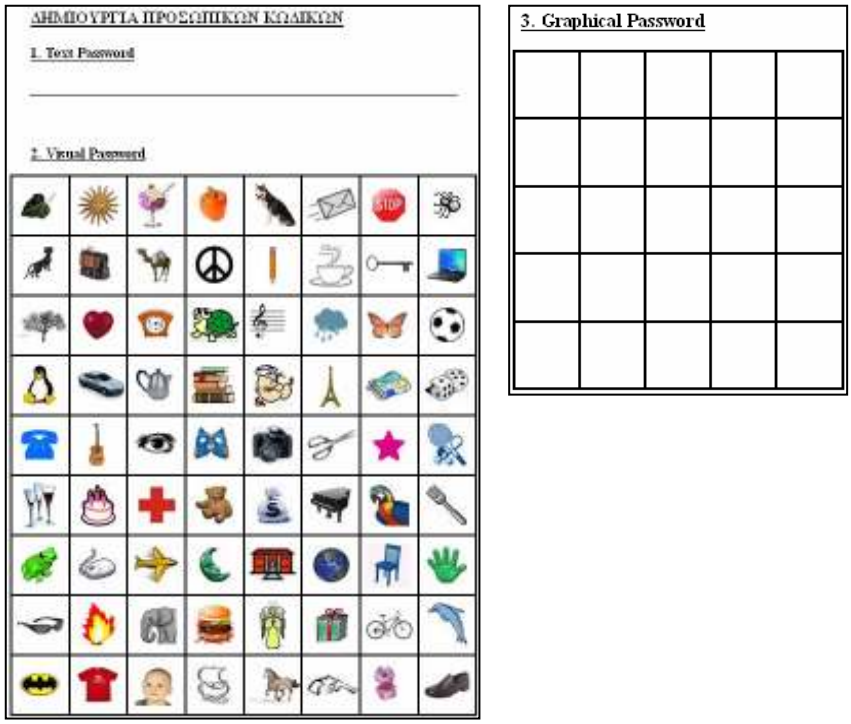
Η συνολική διαδικασία για τη διεξαγωγή της έρευνάς μας, χωρίζεται σε εφτά διαφορετικά βήματα τα οποία είναι: 1) σύντομο σεμινάριο πάνω στα οπτικά και γραφικά passwords, 2) δημιουργία οπτικών και γραφικών passwords, 3) προβληματισμός των συμμετεχόντων και συζήτηση, 4) επιβεβαίωση οπτικών και γραφικών passwords, 5) συμπλήρωση του ερωτηματολογίου, 6) ανάλυση των passwords και της επιβεβαίωσής τους, και 7) ανάλυση των απαντήσεων του ερωτηματολογίου.

Στο πρώτο στάδιο οργανώσαμε ένα σεμινάριο για όλους τους συμμετέχοντες στην έρευνά μας. Το σεμινάριο ήταν σχετικά μικρό σε μέγεθος, καθώς συναντήσαμε πολλούς από τους χρήστες στον τόπο εργασίας τους και προσπαθήσαμε να τους απασχολήσουμε όσο λιγότερη ώρα μπορούσαμε. Μέσα από το σεμινάριο αυτό, ενημερώσαμε τους συμμετέχοντες για τα visual και graphical passwords, για τα προβλήματα που μπορούν να επιλύσουν σε σχέση με τα text, τα πλεονεκτήματα και μειονεκτήματά τους και τέλος για τον τρόπο με τον οποίο ένας χρήστης μπορεί να δημιουργήσει τους προσωπικούς του οπτικούς και γραφικούς κωδικούς και να κάνει μια επιτυχημένη είσοδο στο σύστημα που χρησιμοποιεί.

Αφού κατανόησαν οι χρήστες όλα αυτά τα βασικά σημεία που σχετίζονται με την έρευνά μας, δημιούργησαν τα δικά τους text, visual και graphical passwords. Για το

σκοπό αυτό, σε κάθε έναν δόθηκε ένα φύλλο χαρτί όπως αυτό που παρουσιάζεται στην Εικόνα 13. Εδώ οι χρήστες θα έπρεπε να δημιουργήσουν:

- Ένα text password με αριθμό χαρακτήρων πάνω από 4
- Ένα visual password, επιλέγοντας 4 ή περισσότερες εικόνες με μια συγκεκριμένη σειρά (η σειρά των εικόνων θα καθορίζεται τοποθετώντας τα αντίστοιχα νούμερα σε κάθε εικόνα), και
- Ένα graphical password, ζωγραφίζοντας ένα σχέδιο σε ένα πλέγμα 5 × 5, περνώντας από 4 κελιά τουλάχιστον.



Εικόνα 13: Η φόρμα όπου οι χρήστες δημιούργησαν τα text, visual και graphical passwords.

Αφού οι χρήστες δημιούργησαν τους προσωπικούς τους κωδικούς, περάσαμε περίπου δύο ώρες συζητώντας με τους χρήστες για οποιονδήποτε προβληματισμό τους πάνω στις καινούργιες μεθόδους πιστοποίησης, την ασφάλεια των συστημάτων σήμερα και τον σκοπό της έρευνας που προσπαθούμε να φέρουμε σε πέρας ή αφήνοντας τους να συνεχίσουν με τη δουλειά τους ένα βρισκόμασταν στο χώρο εργασίας τους. Παρεμβάλαμε το τρίτο αυτό στάδιο για δύο λόγους. Πρώτον για να μπορέσουν οι χρήστες να θέσουν όλες τις απορίες τους πάνω στα οπτικά και γραφικά passwords και εμείς από τη μεριά μας να τους απαντήσουμε, ώστε να κατανοήσουν τη χρησιμότητά τους και τα πλεονεκτήματα που έχουν σε σχέση με τα παραδοσιακά, αλφαριθμητικά

passwords. Δεύτερον, για να τους απασχολήσουμε για ένα χρονικό διάστημα πριν προχωρήσουμε στην επιβεβαίωση των προσωπικών τους passwords.

Στο τέταρτο λοιπόν αυτό στάδιο, οι χρήστες θα έπρεπε να επιβεβαιώσουν σωστά τα τρία passwords που είχαν δημιουργήσει. Για το σκοπό αυτό, τους δόθηκε άλλο ένα φύλλο χαρτί, παρόμοιο με το προηγούμενο, με τη διαφορά ότι όσον αφορά τα visual passwords, οι εικόνες τοποθετήθηκαν σε μια τυχαία, διαφορετική θέση (Εικόνα 14).

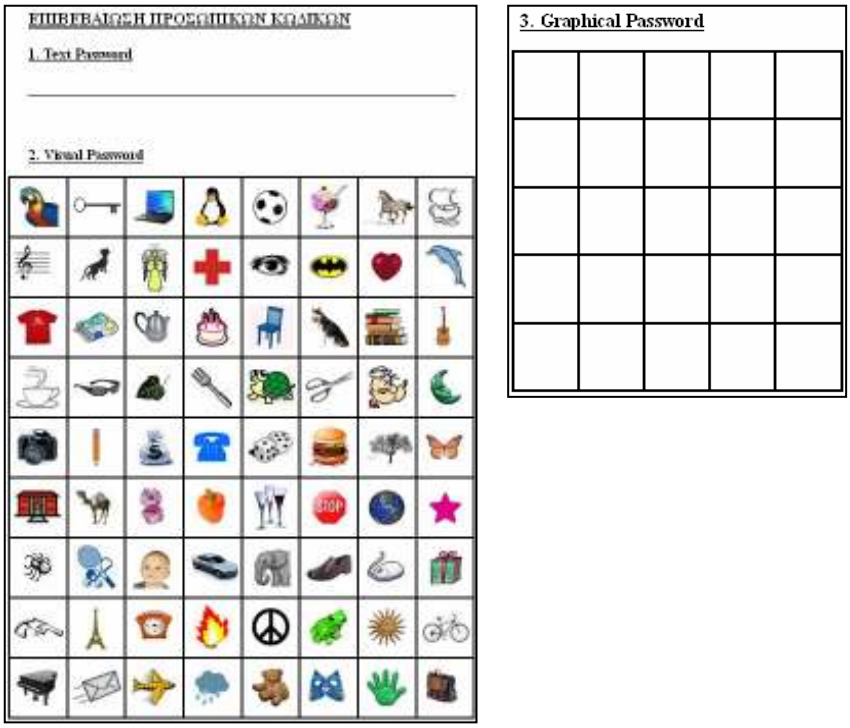


Figure 14: Η φόρμα όπου οι χρήστες επιβεβαίωσαν τα μυστικά passwords που είχαν δημιουργήσει.

Μετά την προσπάθεια των χρηστών να επιβεβαιώσουν σωστά τους προσωπικούς τους κωδικούς, περάσαμε στο πέμπτο στάδιο της διαδικασίας μας. Σε αυτό το σημείο όλοι οι συμμετέχοντες συμπλήρωσαν το ερωτηματολόγιο που τους δόθηκε, ώστε να ανακαλύψουμε και τη δική τους γνώμη πάνω στο θέμα που του παρουσιάσαμε και το οποίο εξετάζουμε.

Τελειώνοντας περάσαμε στην ανάλυση των passwords που δημιούργησαν οι χρήστες, της σωστής ή λανθασμένης επιβεβαίωσής τους και των απαντήσεων στο ερωτηματολόγιο. Συνδυάζοντας όλα αυτά, καταλήξαμε σε κάποια αποτελέσματα, τα οποία παρουσιάζουμε στην επόμενη ενότητα με κάθε λεπτομέρεια.

5. ΑΠΟΤΕΛΕΣΜΑΤΑ

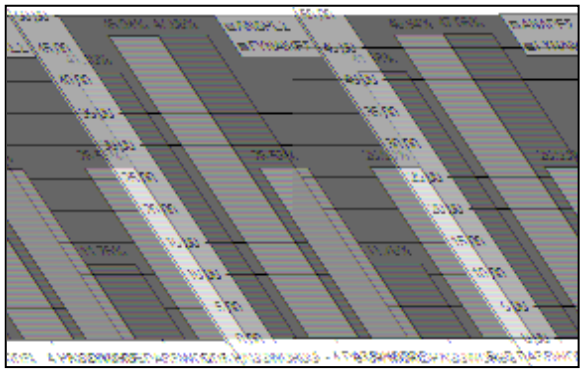
Στο κομμάτι αυτό παρουσιάζουμε τα αποτελέσματα της έρευνάς μας, λαμβάνοντας υπόψιν τη διαδικασία δημιουργίας και επιβεβαίωσης των text, visual και graphical passwords, αλλά και τις απαντήσεις των συμμετεχόντων στο ερωτηματολόγιο. Χωρίσαμε τα αποτελέσματα σε έξι κατηγορίες, με σκοπό να είναι πιο ευανάγνωστα και να μην προκαλούν σύγχυση στον αναγνώστη εξαιτίας του μεγάλου πλήθους τους. Οι κατηγορίες αυτές είναι: 1) σημαντικότητα των password στην καθημερινή ζωή των χρηστών, 2) προβλήματα με τα PINs και text passwords, 3) εναλλακτικές τεχνικές πιστοποίησης χρηστών, 4) σύγκριση των τριών μεθόδων πιστοποίησης, 5) επιτυχημένη επιβεβαίωση των passwords που δημιούργησαν οι χρήστες, and 6) δυσκολία και ασφάλεια των passwords που δημιούργησαν οι χρήστες.

5.1. ΣΗΜΑΝΤΙΚΟΤΗΤΑ ΤΩΝ PASSWORDS ΣΤΗΝ ΚΑΘΗΜΕΡΙΝΗ ΖΩΗ

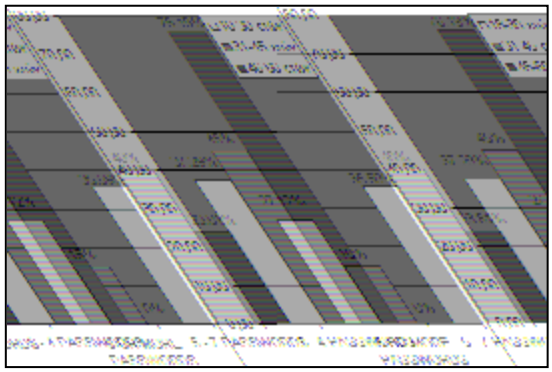
Το πρώτο πράγμα για το οποίο ενδιαφερόμαστε είναι το πόσο σημαντική είναι η μυστικότητα και ασφάλεια των προσωπικών κωδικών στην καθημερινή ζωή του κάθε ανθρώπου. Έτσι ρωτήσαμε τα άτομα που συμμετείχαν στην έρευνά μας για τον αριθμό των passwords που χρησιμοποιούν στις καθημερινές τους δραστηριότητες. Το 47% των ατόμων αυτών έχει 1- 4 passwords, το 34% έχει 5 έως 7 passwords και το 19% έχει από 8 passwords και πάνω.

Στην Εικόνα 15, παρουσιάζουμε τα ποσοστά των δύο φύλων ανάλογα με τον αριθμό των passwords που κατέχουν. Παρατηρούμε λοιπόν, ότι τα ποσοστά των ανδρών και γυναικών που έχουν 1-4 passwords είναι σχεδόν ίδια, ενώ αντίθετα πολύ περισσότερες γυναίκες (41.18%) σε σχέση με τους άνδρες (26.53%) έχουν 5-7 passwords. Η ακριβώς αντίθετη κατάσταση επικρατεί για την περίπτωση των 8 και πάνω προσωπικών κωδικών, καθώς το ποσοστό των γυναικών εδώ μειώνεται πάρα πολύ, ενώ των ανδρών παραμένει το ίδιο (26.53% για τους άνδρες και 11,78% για τις γυναίκες). Παρατηρούμε λοιπόν μια πολύ σημαντική διαφορά ανάμεσα στους άνδρες και τις γυναίκες που χρησιμοποιούν πάνω από 4 προσωπικούς κωδικούς.

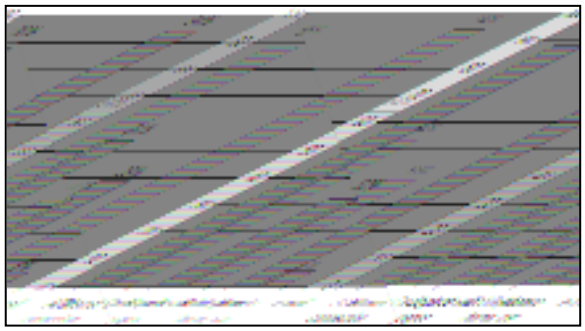
Λαμβάνοντας υπόψιν τώρα την ηλικία των ατόμων που συμμετείχαν στην έρευνά μας, παρατηρούμε ότι η πλειοψηφία των χρηστών ηλικίας 46 έως 60 ετών (76.19%) έχουν 1-4 passwords, ενώ οι νεότεροι σε ηλικίας έχουν συνήθως πολύ περισσότερα (Εικόνα 16). Πέντε έως εφτά passwords κατέχει το 35.59% των ατόμων ηλικίας 18 έως 30 ετών και το 40% των ατόμων ηλικίας 31 έως 45 ετών. Τέλος, περισσότερα από 8 passwords χρησιμοποιούνται από το 27.12% των χρηστών ηλικίας 18 έως 30 ετών και από το 15% των χρηστών ηλικίας 31 έως 45 ετών.



Εικόνα 15: Αριθμός των passwords που χρησιμοποιούν τα δύο φύλλα.



Εικόνα 16: Αριθμός των passwords που χρησιμοποιούν οι χρήστες με βάση την ηλικία τους.



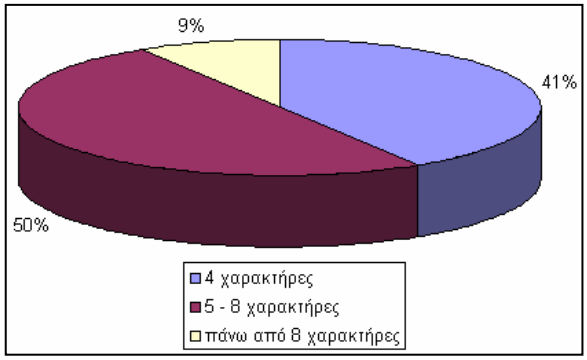
Εικόνα 17: Οι εφαρμογές στις οποίες οι χρήστες χρησιμοποιούν τους προσωπικούς τους κωδικούς.

Είναι επίσης πολύ σημαντικό να εξετάσουμε τις εφαρμογές στις οποίες οι χρήστες χρησιμοποιούν αυτά τα passwords και πόσο συχνά τα χρησιμοποιούνε στη ζωή τους. Σχεδόν όλοι οι χρήστες έχουν κινητό τηλέφωνο (94%) για την επικοινωνία τους με άλλους ανθρώπους και κάρτες ATM (88%) για τις συναλλαγές τους με τις τράπεζες, όπου χρησιμοποιούνε μυστικά passwords για να επικυρώσουν την ταυτότητά τους (Εικόνα 17). Επίσης, εάν σκεφτούμε τη μεγάλη ανάπτυξη των νέων τεχνολογιών και την όλο και μεγαλύτερη χρησιμοποίηση του διαδικτύου, μπορούμε να κατανοήσουμε το λόγο για τον οποίο ένας τόσο μεγάλος αριθμός ατόμων κατέχει password για το προσωπικό του e-mail (64%), για τη σύνδεσή του στο Internet (54%) ή για να κάνει login σε διάφορες ιστοσελίδες (39%).

Τελειώνοντας ανακαλύψαμε ότι το 69% των ατόμων που συμμετείχαν στην έρευνά μας, χρησιμοποιούν τουλάχιστον ένα password κάθε μέρα και σίγουρα κάποιο μία ή δύο φορές το μήνα. Από το γεγονός αυτό μπορούμε να καταλάβουμε πόσο σημαντικό είναι σε κάθε άνθρωπο να έχει προσωπικούς κωδικούς που εκτός από ασφαλείς, να είναι και εύκολοι στην απομνημόνευσή τους.

5.2. ΠΡΟΒΛΗΜΑΤΑ ΤΩΝ PINs ΚΑΙ TEXT PASSWORDS

Στην ενότητα αυτή εξετάζουμε τα προβλήματα που δημιουργούνται από τη σημερινή χρησιμοποίηση των PINs και των text passwords. Το πρώτο θέμα με το οποίο ασχοληθήκαμε είναι ο αριθμός των χαρακτήρων που έχουν οι χρήστες στους προσωπικούς τους κωδικούς. Το 50% των συμμετεχόντων δήλωσαν ότι τα passwords που έχουν αποτελούνται από 5-8 χαρακτήρες, το 41% από 4 χαρακτήρες και μόνο το 9% από 8 χαρακτήρες και πάνω, δημιουργώντας ένα password που μπορεί να θεωρηθεί ασφαλές και δύσκολο να σπάσει (Εικόνα 18). Τα αποτελέσματα αυτά θα μπορούσαμε να τα χαρακτηρίσουμε σχετικά ικανοποιητικά εάν τα στοιχεία που αποτελούν το password δεν είναι μόνο αριθμοί. Δυστυχώς το 49% όλων των κωδικών αποτελούνται μόνο από αριθμούς (Εικόνα 19), ένα γεγονός που κάνει αυτόματα τα passwords πολύ ευαίσθητα σε κάθε είδους επιθέσεις.



Εικόνα 18: Αριθμός των χαρακτήρων σε ένα text password.

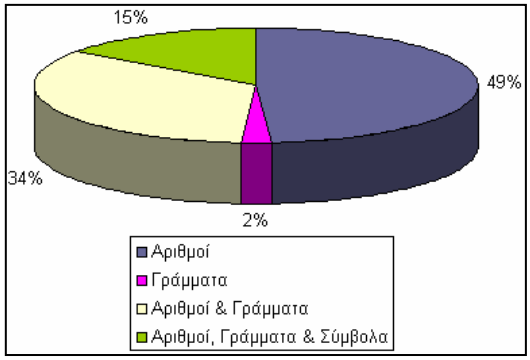
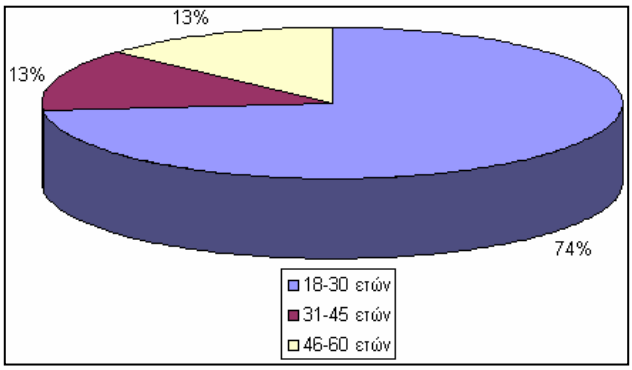


Figure 19: Το είδος των χαρακτήρων από τους οποίους αποτελούνται τα text passwords are consisted of.

Αυτό που είναι κάπως ενθαρρυντικό στο σύνολο των παραπάνω αποτελεσμάτων, είναι το γεγονός ότι το 15% των χρηστών που συμμετείχαν στην έρευνα, δεν χρησιμοποιούν μόνο αριθμούς στους κωδικούς τους, αλλά επίσης γράμματα και σύμβολα. Από αυτούς τους χρήστες, που προσέχουν ιδιαίτερα τα passwords που δημιουργούν, το 74% έχει

ηλικία μέχρι 30 ετών. Από αυτό καταλαβαίνουμε ότι όλο και περισσότεροι νέοι άνθρωποι κατανοούν πόσο σημαντικό είναι όχι απλά να έχουν έναν κωδικό, αλλά πολύ περισσότερο να έχουν έναν ασφαλή κωδικό, καθόλου ευαίσθητο στις κακόβουλες επιθέσεις (Εικόνα 20).

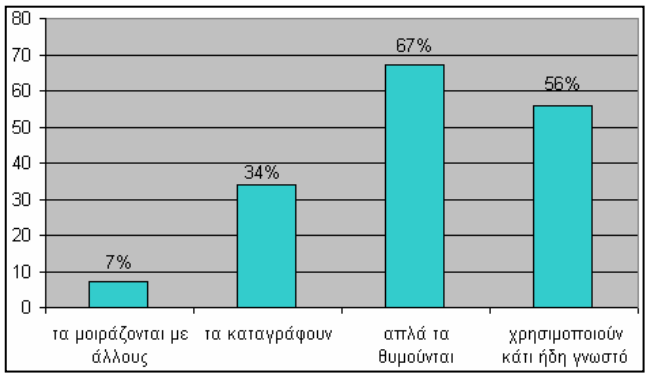


Εικόνα 20: Χρήστες που δημιουργούν passwords που αποτελούνται από αριθμούς, γράμματα και σύμβολα, με βάση την ηλικία τους.

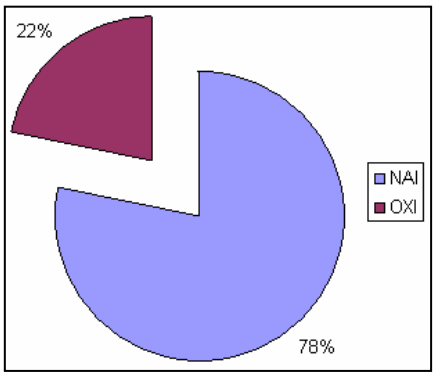
Στη συνέχεια εξετάσαμε την ανασφάλεια που αισθάνονται οι χρήστες, φοβούμενοι μήπως ξεχάσουν τους κωδικούς τους και δεν έχουν κανένα τρόπο για να τους θυμηθούνε ξανά. Για το σκοπό αυτό οι χρήστες προσπάθησαν να βρούνε άλλους τρόπους, οι οποίοι θα τους βοηθάνε να αντιμετωπίσουν την κατάσταση αυτή. Εκτός λοιπόν από το να προσπαθούνε να θυμηθούν απέξω τους κωδικούς τους, τους μοιράζονται με άλλους ανθρώπους (7%), τους γράφουνε κάπου (34%), ή χρησιμοποιούν κάτι ήδη γνωστό σε αυτούς π.χ. ημερομηνίες ή ονόματα (33%), ώστε να μην τους ξεχάσουν ποτέ (Εικόνα 21). Επίσης το 78% των συμμετεχόντων χρησιμοποιούν συνήθως τον ίδιο ή παρόμοιο password σε διαφορετικές εφαρμογές (Εικόνα 22). Με βάση λοιπόν τα ποσοστά αυτά, καταλαβαίνουμε πόσο δύσκολο είναι για τους χρήστες να θυμούνται όλους τους κωδικούς που έχουν και να μπορέσουν να τα βγάλουν πέρα χωρίς προβλήματα.

Έχοντας ως στόχο λοιπόν να μην ξεχνάνε ή να μπερδεύουν τα passwords που χρησιμοποιούν, οι χρήστες δημιουργούν ένα password για μια εφαρμογή και το 81% αυτών δεν το αλλάζει ποτέ. Παρόλα αυτά, δημιουργώντας ένα password που παραμένει στάσιμο, όσο δύσκολο και να είναι καθώς περνάει ο καιρός, γίνεται όλο και πιο ευαίσθητο σε επιθέσεις. Για το λόγο αυτό, οι ερευνητές προσπάθησαν να δημιουργήσουν καινούργιες, ασφαλέστερες και πιο εύκολες στην απομνημόνευσή τους

μεθόδους για την πιστοποίηση της ταυτότητας των χρηστών. Τις μεθόδους αυτές αναλύουμε στην επόμενη ενότητα.

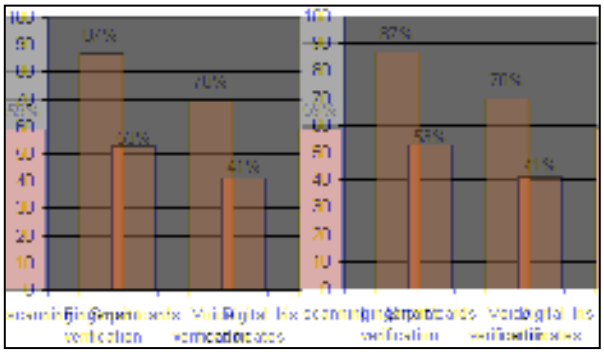


Εικόνα 21: Τρόποι με τους οποίους οι χρήστες δεν ξεχνάν τα προσωπικά τους passwords



Εικόνα 22: Οι χρήστες συνήθως χρησιμοποιούν ίδια ή παρόμοια passwords σε διαφορετικές εφαρμογές

5.3. ΕΝΑΛΛΑΚΤΙΚΕΣ ΜΕΘΟΔΟΙ ΠΙΣΤΟΠΟΙΗΣΗΣ



Εικόνα 23: Γνώση εναλλακτικών μεθόδων πιστοποίησης.

Εάν αναλογιστούμε όλα τα προβλήματα των text passwords που παρουσιάσαμε παραπάνω, μπορούμε να κατανοήσουμε ότι πλέον ήταν επιτακτική ανάγκη η εύρεση καινούργιων εναλλακτικών μεθόδων πιστοποίησης. Στη συνέχεια παρουσιάζουμε πέντε βασικές τέτοιες μεθόδους, τις οποίες αναφέραμε ξανά, και οι οποίες όπως αποδεικνύεται, δεν είναι καθόλου άγνωστες στους χρήστες που συμμετείχαν στην έρευνά μας (Εικόνα 23):

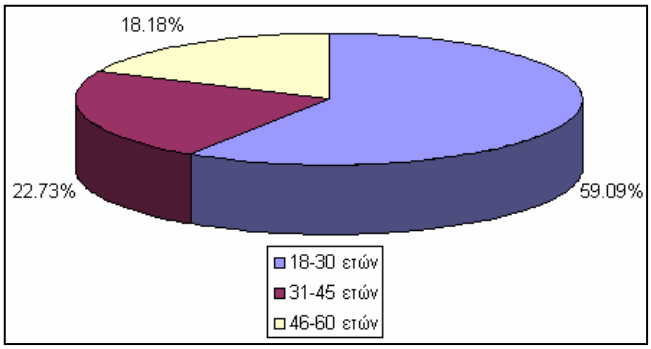
- **Fingerprint verification:** τεχνική πιστοποίησης που ανήκει στις βιομετρικές (biometric) τεχνικές και που αυτόματα αναγνωρίζει ηλεκτρονικά, το δακτυλικό αποτύπωμα του χρήστη.

- **Voice verification:** τεχνική πιστοποίησης που ανήκει στις βιομετρικές (biometric) τεχνικές και που αυτόματα αναγνωρίζει τη φωνή του χρήστη.
- **Iris scanning:** τεχνική πιστοποίησης που ανήκει στις βιομετρικές (biometric) τεχνικές και που σκανάρει την ίριδα του ματιού του χρήστη, καθώς σε κάθε άτομο τα χαρακτηριστικά της είναι διαφορετικά
- **Smart cards:** είναι πλαστικές κάρτες παρόμοιες με τις πιστωτικές, αλλά διαθέτουν έναν ενσωματωμένο μικροεπεξεργαστή που κρατάει όλες τις πληροφορίες που αφορούν τον κάτοχο της κάρτας.
- **Digital certificates:** είναι ηλεκτρονικά "διαβατήρια", τα οποία εκδίδονται από μια αρχή πιστοποίησης όπως η Entrust και η Verisign. Περιλαμβάνουν, εκτός των άλλων, το όνομα, έναν σειριακό αριθμό, την ημερομηνία λήξης και μια ψηφιακή υπογραφή της αρχής πιστοποίησης, ώστε ο παραλήπτης να είναι σίγουρος ότι το πιστοποιητικό είναι γνήσιο.

Αυτές οι μέθοδοι είναι γνωστές στους περισσότερους χρήστες από ταινίες στον κινηματογράφο, καθώς δεν χρησιμοποιούνται ακόμη ευρέως. Η πιστοποίηση μέσω του δακτυλικού αποτυπώματος (fingerprint verification) είναι η πιο γνωστή μέθοδος, σε ποσοστό 87% και ακολουθείται κατά σειρά από την πιστοποίηση μέσω φωνής (voice verification) σε ποσοστό 70% και το σκανάρισμα της ίριδας του ματιού (iris scanning) σε ποσοστό 59%. Αυτό που παρατηρείται εδώ και μας φαίνεται λίγο παράξενο, είναι ότι οι άλλες δύο μέθοδοι (smart cards και ψηφιακά πιστοποιητικά), δεν είναι τόσο γνωστές παρά το γεγονός ότι μαζί με τη μέθοδο fingerprint verification είναι αυτές που ήδη χρησιμοποιούνται περισσότερο σήμερα.

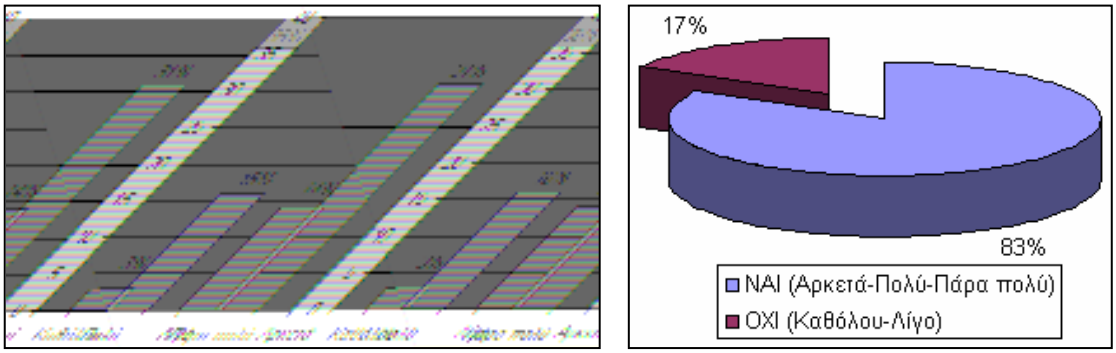
Τα visual και graphical passwords είναι μια πολύ καινούργια ιδέα, που αναπτύχθηκε με σκοπό να δημιουργούν οι χρήστες ασφαλέστερα passwords και πιο εύκολα στην απομνημόνευσή τους. Το τελευταίο αυτό χαρακτηριστικό βασίζεται στο γεγονός ότι μετά από έρευνες έχει αποδειχτεί ότι οι άνθρωποι μπορούν να θυμούνται πιο εύκολα μια σειρά από εικόνες, απ' ότι μια σειρά χαρακτήρων. Αφού αυτές οι μέθοδοι αναπτύχθηκαν τα τελευταία χρόνια, είναι φυσικό μόνο το 22% των συμμετεχόντων να γνωρίζουν την ύπαρξή τους και το 78% αυτών να μην έχουν ακούσει ποτέ πριν τις συγκεκριμένες έννοιες.

Ενδιαφέρον επίσης παρουσιάζει το γεγονός ότι ανάμεσα στους χρήστες που είχαν προηγούμενη γνώση των δύο νέων μεθόδων, σχεδόν το 60% είναι ηλικίας 18 έως 30 ετών και μόνο το 18% είναι ηλικίας 46 έως 60 ετών (Εικόνα 24).



Εικόνα 24: Η ηλικία των χρηστών που είχαν προηγούμενη γνώση των Visual και Graphical passwords.

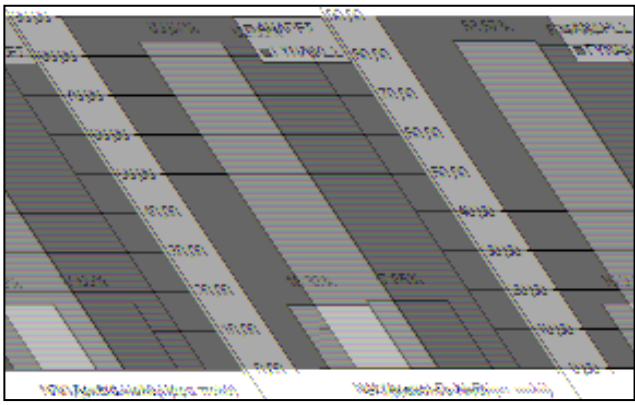
Στη συνέχεια εξετάζουμε σε τι βαθμό οι σημερινοί χρήστες είναι θετικοί στην περεταίρω ενημέρωσή τους και αργότερα και χρησιμοποίηση των visual και graphical passwords. Οι απαντήσεις τους χωρίζονται σε πέντε κατηγορίες (Εικόνα 25). Έχοντας ως σκοπό να παρουσιάσουμε τα συγκεκριμένα αποτελέσματα σε μια άλλη κλίμακα θετικής και αρνητικής ανταπόκρισης, ώστε να είναι πιο κατανοητά, αθροίσαμε τις απαντήσεις "αρκετά", "πολύ" και "πάρα πολύ " σε ΝΑΙ και τις "καθόλου" και "λίγο" σε ΟΧΙ (Εικόνα 26). Έτσι παρατηρούμε ότι το 83% των συμμετεχόντων είναι θετικοί στη χρησιμοποίηση των νέων μεθόδων και μόνο το 17% είναι αρνητικοί ή καθόλου περίεργοι να δουν τις θετικές επιδράσεις που αυτές έχουν.



Εικόνα 25: Η προσωπική γνώμη των χρηστών για την αποδοχή των visual και graphical passwords.

Εικόνα 26: Θετική και αρνητική αντιμετώπιση των visual και graphical passwords.

Τέλος, η Εικόνα 27 αποδεικνύει για άλλη μια φορά ότι ανάμεσα στα δύο φύλλα δεν υπάρχουν διαφορές. Πιο συγκεκριμένα εδώ, το 83% και των δύο φύλλων κρατάνε θετική στάση απέναντι στα οπτικά και γραφικά passwords, ενώ μόνο το 17% είναι αρνητικοί.

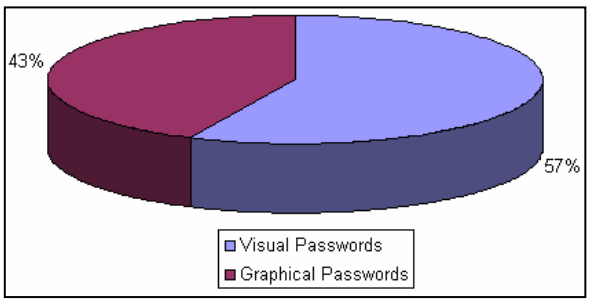


Εικόνα 27: Συγκριτική αποδοχή των οπτικών και γραφικών passwords με βάση το φύλο.

5.4. ΑΝΑΛΥΟΝΤΑΣ ΤΑ TEXT, VISUAL και GRAPHICAL PASSWORDS

Στην ενότητα αυτή εξετάζουμε τις προτιμήσεις των χρηστών για διάφορες παραμέτρους των τριών μεθόδων πιστοποίησης (αλφαριθμητικών, οπτικών και γραφικών passwords). Ρωτήσαμε λοιπόν τους συμμετέχοντες για την προσωπική τους γνώμη πάνω στις τρεις αυτές μεθόδους όσον αφορά τα ακόλουθα έξι κριτήρια: 1) ευκολία στην απομνημόνευση των passwords, 2) ασφάλεια των passwords, 3) ευκολία στην κατανόηση και εκμάθηση του τρόπου λειτουργίας τους, 4) φιλικότητα προς τον χρήστη, 5) κατανάλωση χρόνου, and 6) συνολική αισθητική.

Αρχίζουμε λοιπόν εξετάζοντας τις μεθόδους ως προς την ευκολία απομνημόνευσής τους. Εφόσον οι χρήστες χρησιμοποιούν τα PINs και τα text passwords καθημερινά, είναι



Εικόνα 28:Ευκολία στην απομνημόνευση των δύο μεθόδων.

φυσικό να θεωρούν αυτούς τους κωδικούς ως τους πιο εύκολους στην απομνημόνευσή τους. Συγκρίνοντας τώρα τις δύο καινούργιες μεθόδους (visual passwords and graphical passwords) μεταξύ τους, το 57% των χρηστών θεωρεί τα visual passwords ευκολότερα στην απομνημόνευσή τους, ενώ το υπόλοιπο 43% τα graphical passwords (Εικόνα 28). Επίσης εάν κάνουμε μια διάκριση ανάμεσα στα δύο φύλλα (Εικόνα 29), και οι άντρες αλλά και γυναίκες πιστεύουν ότι τα visual passwords είναι ευκολότερα στην απομνημόνευσή τους. Παρόλα αυτά, το ποσοστό των γυναικών που προτιμούν τα graphical passwords είναι μεγαλύτερο (45.1%), σε σχέση με αυτό των αντρών (38.78%).

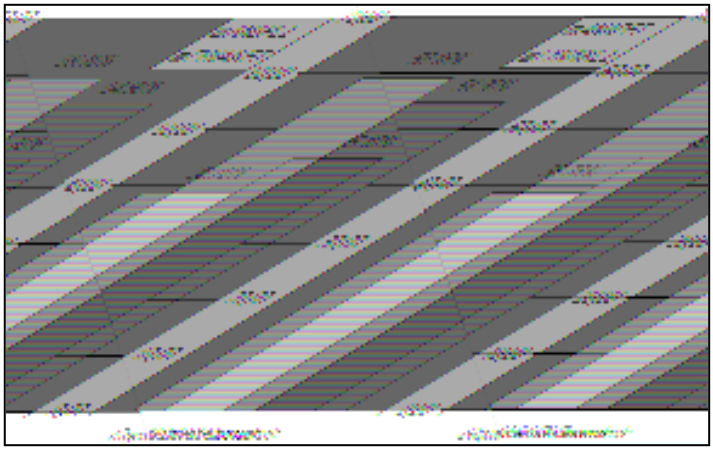
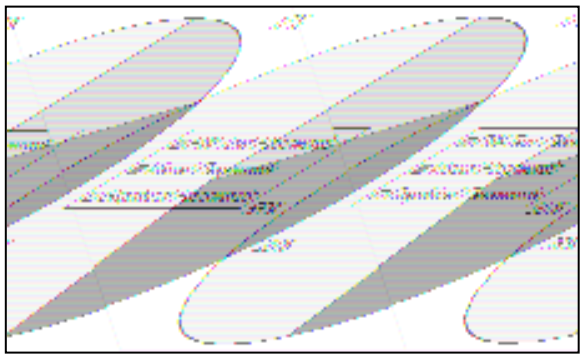


Figure 29: Σύγκριση των δύο φύλλων όσον αφορά την ευκολότερη μέθοδο απομνημόνευσης

Στη συνέχεια θα εξετάσουμε ποια από τις τρεις μεθόδους πιστοποίησης θεωρείται από τους χρήστες η ασφαλέστερη. Αφού εξηγήσαμε με λεπτομέρειες στα άτομα που συμμετείχαν στην έρευνά μας τις δύο καινούργιες μεθόδους, στο αρχικό μας σεμινάριο, το 55% αυτών κατανόησε τα πλεονεκτήματα των graphical passwords και πλέον πιστεύουν ότι είναι η ασφαλέστερη μέθοδος (Εικόνα 30). Παρόλα αυτά, ένα αρκετά σημαντικό ποσοστό των συμμετεχόντων (28%) πιστεύει ότι τα visual passwords είναι ασφαλέστερα, ενώ το 17% επιμένει ότι ο πατροπαράδοτος τρόπος των text



Εικόνα 30: Ασφαλέστερη μέθοδος πιστοποίησης.

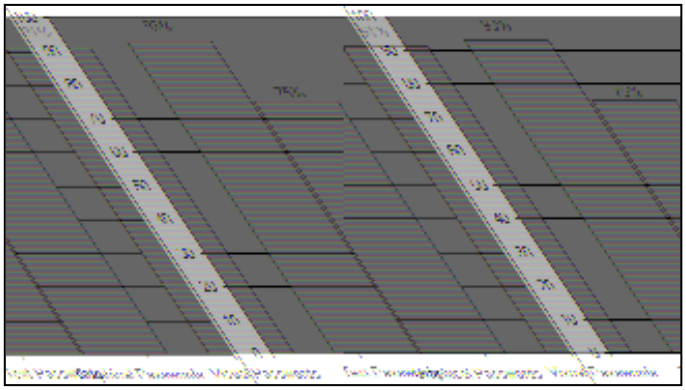
passwords δεν κρύβει κανένα κίνδυνο και είναι ο ασφαλέστερος, ακόμη κι αν εμείς υποστηρίζουμε κάτι αντίθετο.

Μια κατάσταση η οποία θα πρέπει να μας ανησυχεί στο σημείο αυτό, είναι ότι το 64.7% των χρηστών που πιστεύουν ότι η ασφαλέστερη μέθοδος είναι τα text passwords, είναι νέοι άνθρωποι, ηλικίας κάτω των 30 ετών. Αυτό βέβαια ίσως συμβαίνει επειδή τόσο νεαρά σε ηλικία άτομα δημιουργούν συνήθως δύσκολα passwords, που αποτελούνται δηλαδή όχι μόνο από αριθμούς, αλλά και από γράμματα ή σύμβολα, κάτι που όμως δεν συμβαίνει στη γενικότερη πλειοψηφία των χρηστών.

Η επόμενη παράμετρος που θα εξετάσουμε, είναι η ευκολία στην εκμάθηση του τρόπου λειτουργίας των τριών μεθόδων πιστοποίησης (Εικόνα 31). Για να δούμε πιο εύκολα την αρνητική η θετική γνώμη των χρηστών, ομαδοποιήσαμε τις απαντήσεις τους σε δύο κατηγορίες:

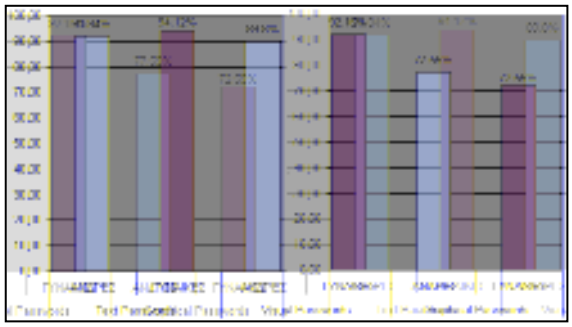
- ΟΧΙ όπου αντιστοιχούν οι απαντήσεις "καθόλου" και "λίγο", δηλαδή ότι οι χρήστες είχαν δυσκολίες στην κατανόηση και εκμάθηση του τρόπου λειτουργίας των μεθόδων πιστοποίησης
- ΝΑΙ όπου αντιστοιχούν οι απαντήσεις "αρκετά" "πολύ" και "πάρα πολύ", δηλαδή ότι οι χρήστες κατανόησαν και έμαθαν με ευκολία τον τρόπο λειτουργίας των τριών μεθόδων πιστοποίησης

Ένα μεγάλο ποσοστό λοιπόν των συμμετεχόντων θεώρησαν πολύ εύκολη την εκμάθηση του τρόπου λειτουργίας των text passwords (93%), αφού ήταν και ήδη γνωστά, αλλά και των visual passwords (91%). Το αντίστοιχο ποσοστό για τα graphical passwords είναι μικρότερο (75%), πολύ πιθανόν επειδή περιλαμβάνουν πολύ περισσότερους κανόνες σε σχέση με τις δύο προηγούμενες μεθόδους.

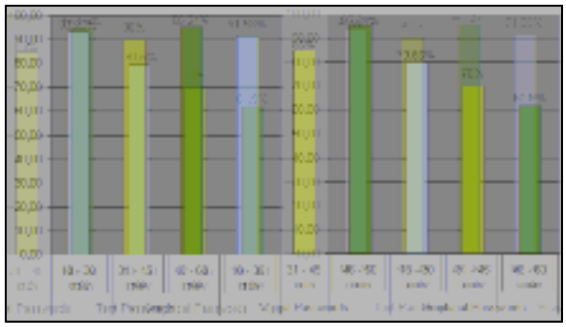


Εικόνα 31: Ευκολία στην εκμάθηση του τρόπου λειτουργίας κάθε μεθόδου

Ανάμεσα στα δύο φύλλα ή κατάσταση που υπάρχει παρουσιάζει ιδιαίτερο ενδιαφέρον. Όσον αφορά τα text και visual passwords το ποσοστό των γυναικών που δεν δυσκολεύτηκαν στην εκμάθηση του τρόπου λειτουργίας τους είναι μεγαλύτερο από αυτό των ανδρών. Αντίθετα, όπως παρατηρούμε και στην Εικόνα 32, στην περίπτωση των graphical passwords οι γυναίκες συνάντησαν περισσότερες δυσκολίες, αφού το ποσοστό των ανδρών (77.55%) είναι μεγαλύτερο κατά 5 μονάδες από το αντίστοιχο των γυναικών (72.55%). Επίσης στηριζόμενοι στην Εικόνα 33, που κάνει σύγκριση των διαφόρων ηλικιών, αφού που θα πρέπει να τονίσουμε είναι ότι οι χρήστες ηλικίας πάνω από 45 ετών δεν είχαν κανένα πρόβλημα στην εκμάθηση λειτουργίας των text και visual passwords, ενώ όσον αφορά τα γραφικά είναι η ομάδα που σε μεγαλύτερο ποσοστό σε σχέση με τις άλλες δύο παρουσίασε δυσκολίες.

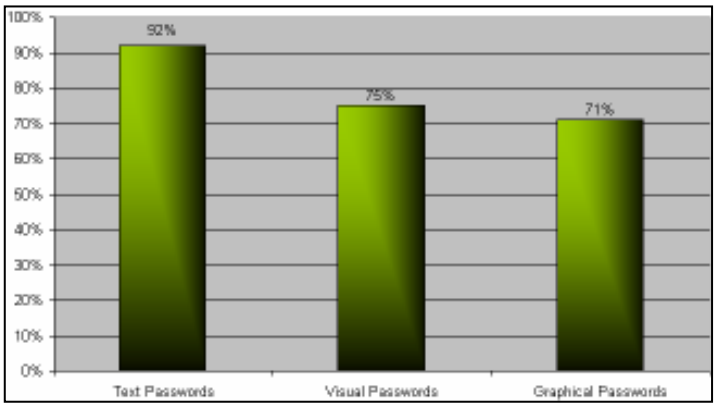


Εικόνα 32: Ευκολία στην εκμάθηση του τρόπου λειτουργίας κάθε μεθόδου, ανάλογα με το φύλο



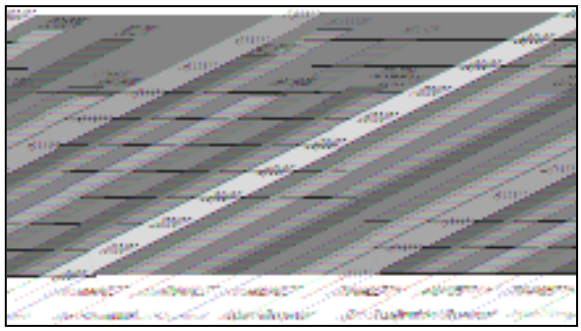
Εικόνα 33: Ευκολία στην εκμάθηση του τρόπου λειτουργίας κάθε μεθόδου, σε σχέση με την ηλικία των χρηστών.

Ας εξετάσουμε επίσης πόσο εύκολο είναι για κάποιον να χρησιμοποιήσει τις τρεις μεθόδους πιστοποίησης, δηλαδή με άλλα λόγια τη φιλικότητά τους προς τον χρήστη (Εικόνα 34). Τα text passwords, όπως είναι φυσικό αφού είναι τα μοναδικά που χρησιμοποιούνται σήμερα, θεωρούνται η πιο εύχρηστη μέθοδος σε ποσοστό 92%. Αμέσως μετά ακολουθούν τα visual passwords σε ποσοστό 76% και τέλος έχουμε τα graphical passwords με ένα ελάχιστα μικρότερο ποσοστό – 71%.



Εικόνα 34: Φιλικότητα προς τον χρήστη των τριών μεθόδων

Στο σημείο αυτό παρατηρούμε ότι οι χρήστες αποδέχονται πολύ πιο εύκολα τα visual απ' ότι τα graphical passwords, παρά το γεγονός ότι (όπως θα δούμε αργότερα) δημιουργούν γραφικά passwords ευκολότερα στην απομνημόνευσή και δυσκολότερα στο να σπάσουν, σε σχέση με τα visual, χωρίς καθόλου προσπάθεια.

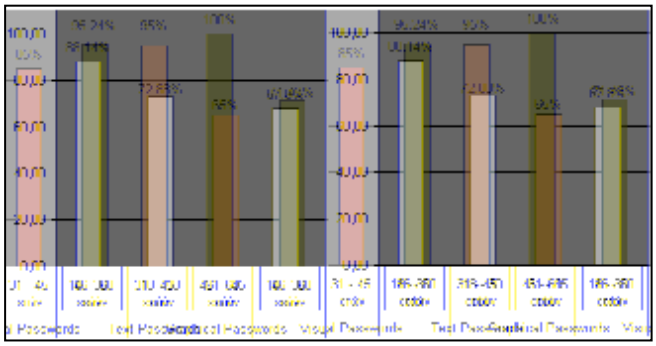


Εικόνα 35: Φιλικότητα των μεθόδων προς τον χρήστη ανάλογα με το φύλλο.

Ανάμεσα στα δύο φύλα (Εικόνα 35), αυτό που θα πρέπει να αναφέρουμε είναι η αρκετά μεγάλη διαφορά των ανδρών (69.39%) και των γυναικών (84.31%), για την περίπτωση των visual passwords. Γενικότερα τα ποσοστά των γυναικών για τις δύο νέες μεθόδους είναι μεγαλύτερα από αυτά των ανδρών, ίσως γιατί εντυπωσιάζονται περισσότερο από εικόνες και σχέδια. Αντίθετα στην περίπτωση των text passwords, όπως παρατηρούμε, οι ρόλοι αντιστρέφονται και το ποσοστό των ανδρών είναι μεγαλύτερο.

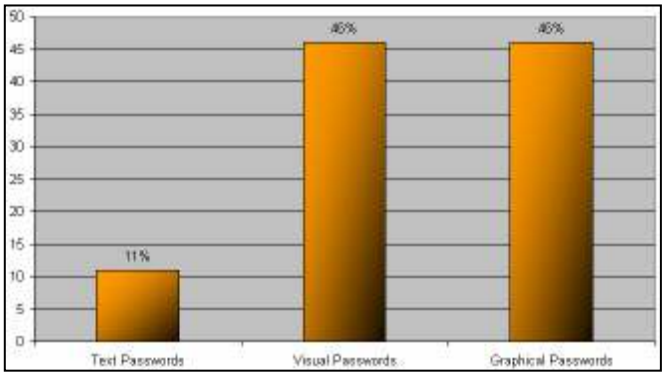
Εξετάζοντας τώρα τη φιλικότητα των τριών μεθόδων με βάση την ηλικία (Εικόνα 36), βλέπουμε ότι οι νεότερες ηλικίες είναι αυτές που σε μεγαλύτερο ποσοστό θεωρούν φιλικά τα γραφικά passwords. Στην περίπτωση τώρα των text και visual passwords, οι χρήστες ηλικίας έως 30 ετών είναι εκείνοι που σε μικρότερο ποσοστό (88.14% και 67.8% αντίστοιχα) τα θεωρούν φιλικά, ενώ οι μεγαλύτεροι χρήστες έχουν και τα

μεγαλύτερα ποσοστά, είτε γιατί έχουν ακόμη εμπιστοσύνη στον παραδοσιακό τρόπο, είτε γιατί εντυπωσιάστηκαν ευκολότερα από την πληθώρα εικόνων και χρωμάτων.



Εικόνα 36: Φιλικότητα των μεθόδων προς τον χρήστη ανάλογα με την ηλικία τους.

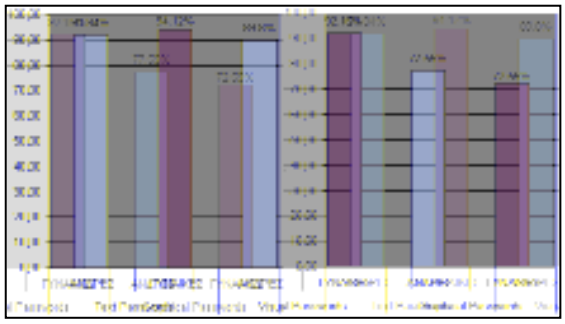
Όσον αφορά τώρα τον χρόνο που καταναλώνουν οι χρήστες για την είσοδό του σε ένα σύστημα, οι περισσότεροι (89%) πιστεύουν ότι τα text passwords δεν είναι καθόλου χρονοβόρα (Εικόνα 37). Αντίθετα το 46% των χρηστών αυτών πιστεύουν, για διαφορετικούς λόγους κάθε φορά, ότι και στην περίπτωση των visual, αλλά και των graphical passwords, η όλη διαδικασία απαιτεί πολύ χρόνο. Πιο συγκεκριμένα, οι συμμετέχοντες πιστεύουν ότι χρησιμοποιώντας τα visual passwords, υπάρχει περίπτωση ο χρήστης να μπερδευτεί με τόσες πολλές εικόνες και να χάσει χρόνο στον εντοπισμό τους, ακόμη και αν θυμάται το password πολύ καλά. Επιπλέον, ο λόγος που πιστεύουν ότι τα graphical passwords είναι χρονοβόρα, στην επιβεβαίωση του κωδικού του θα πρέπει να θυμάται ακριβώς τα κελιά από τα οποία έχει περάσει κατά τη δημιουργία του προσωπικού του σχεδίου.



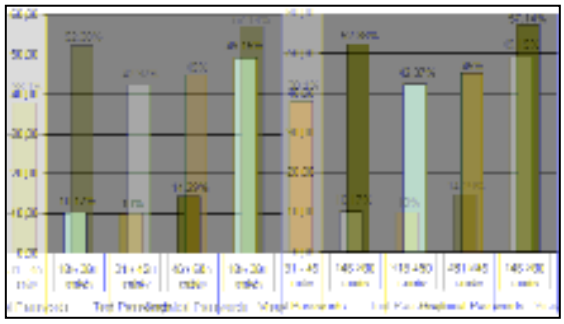
Εικόνα 37: Πόσο χρονοβόρες είναι οι τρεις μέθοδοι πιστοποίησης

Όσον αφορά τα δύο φύλα, παρατηρούμε ότι οι γυναίκες είναι αυτές που σε μεγαλύτερο ποσοστό θεωρούν χρονοβόρα τα text και visual passwords (Εικόνα 38). Τα ποσοστά αντιστρέφονται στα γραφικά, αφού περισσότεροι άνδρες (77.55%) και λιγότερες

γυναίκες (72.55%) θεωρούν ότι η διαδικασία χρειάζεται δαπάνη πολύ χρόνου. Εάν εξετάσουμε τώρα τη διαφορά μεταξύ των διαφόρων ηλικιών (Εικόνα 39), αυτό που πρέπει να αναφέρουμε είναι ότι για οι δύο καινούργιες μέθοδοι θεωρούνται πιο χρονοβόρες από τα άτομα μεγαλύτερων ηλικιών, αν και ακόμη και αυτοί όπως έχουμε δει, τις υποστηρίζουν και είναι θετικοί απέναντί τους.

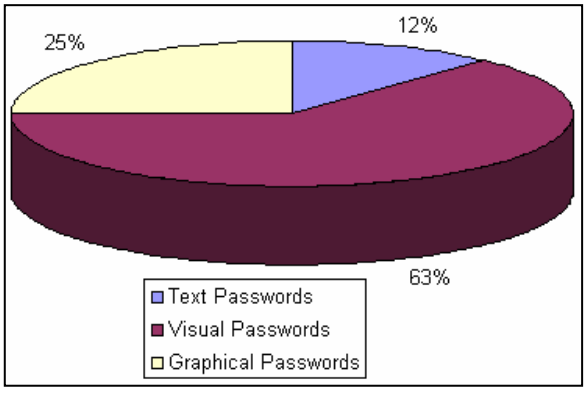


Εικόνα 38: Πόσο χρονοβόρες θεωρούνται οι τρεις μέθοδοι στα δύο φύλα.



Εικόνα 39: Πόσο χρονοβόρες θεωρούνται οι τρεις μέθοδοι στις διάφορες ηλικίες.

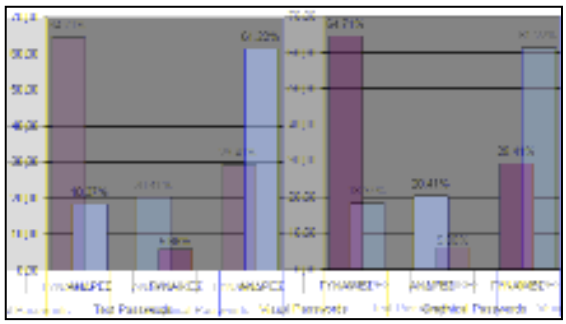
Τελειώνοντας θα εξετάσουμε τη γνώμη των χρηστών για την αισθητική της κάθε μεθόδου. Με βάση την Εικόνα 40, οι περισσότεροι προτιμούν αισθητικά τα visual passwords (63%). Ακολουθούν τα graphical passwords με ένα πολύ μικρότερο ποσοστό (25%), ενώ τα text passwords συγκεντρώνουν μόνο το 12% των χρηστών. Το αποτέλεσμα αυτό ήταν κάτι αναμενόμενο, ένα σύνολο εικόνων, με διαφορετικά θέματα και χρώματα, είναι πολύ πιο ελκυστικό από ένα απλό σχέδιο ή μια αλληλουχία χαρακτήρων.



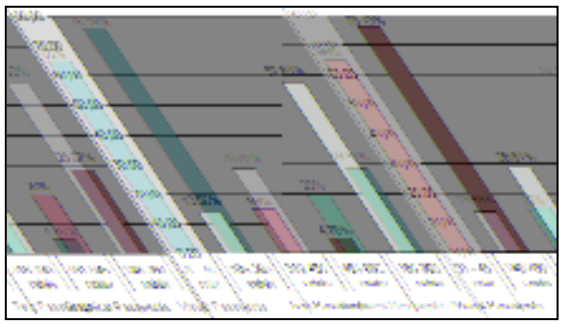
Εικόνα 40: Καλύτερη μέθοδος αισθητικά.

Στο σημείο αυτό, εξετάζοντας την Εικόνα 41, παρατηρούμε ότι οι γυναίκες είναι αυτές που εντυπωσιάστηκαν περισσότερο από τα visual και graphical passwords, κάτι που

εξηγεί το γεγονός εκείνες είναι που σε σχέση με τους άνδρες θεωρούν τις μεθόδους πολύ πιο φιλικές απέναντί τους. Επίσης εάν κάνουμε ανάμεσα στις διάφορες ηλικίες (Εικόνα 42), παρατηρούμε ότι τα visual passwords άγγιξαν αισθητικά περισσότερο άτομα μεγαλύτερης ηλικίας, ενώ αντίθετα τα text που χρησιμοποιούνται σήμερα δεν τους εντυπωσιάζουν καθόλου. Τα γραφικά από την άλλη έχουν μια παρόμοια αντιμετώπιση από νεότερους και μεγαλύτερους, ενώ λίγο μικρότερο είναι το αντίστοιχο ποσοστό στα άτομα ηλικίας 31-45 ετών. Τέλος, το σημείο αυτό θα πρέπει να αναφέρουμε ότι από τους χρήστες που προτιμούν αισθητικά τα text passwords, το μεγαλύτερο ποσοστό (67%) είναι νεαρής ηλικίας, μέχρι 30 χρονών.



Εικόνα 41: Καλύτερη μέθοδος αισθητικά για τα δύο φύλα.



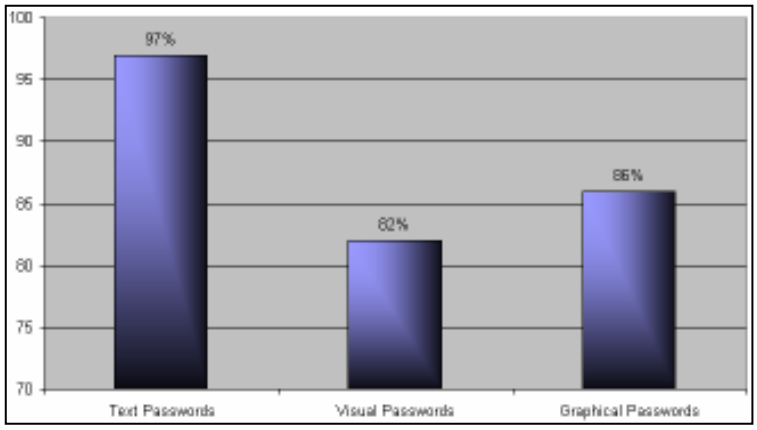
Εικόνα 42: Καλύτερη μέθοδος αισθητικά για τις διάφορες ηλικίες.

5.5. ΕΠΙΒΕΒΑΙΩΝΟΝΤΑΣ ΤΑ TEXT, VISUAL και GRAPHICAL PASSWORDS

Στην ενότητα αυτή θα αναλύσουμε κατά πόσο οι χρήστες που συμμετείχαν στην έρευνά μας επιβεβαίωσαν σωστά τους τρεις διαφορετικούς προσωπικούς κωδικούς που δημιούργησαν (Εικόνα 43).

Σχεδόν όλοι οι χρήστες (97%) επιβεβαίωσαν σωστά τα text passwords που είχαν δημιουργήσει, κάτι που δείχνει ότι σήμερα πλέον έχουμε εξοικειωθεί πολύ με τον τρόπο αυτό εισόδου μας σε ένα σύστημα. Ένα μικρότερο ποσοστό συμμετεχόντων (86%) επιβεβαίωσαν σωστά τα graphical passwords. Το αποτέλεσμα αυτό βέβαια θεωρείται πολύ καλό, καθώς αναφερόμαστε σε μια πολύ καινούργια μέθοδο, που με βάση τα προηγούμενα αποτελέσματα θεωρείται αρκετά δύσκολη. Τέλος, ακόμη λιγότεροι συμμετέχοντες (82%) επιβεβαίωσαν σωστά τα visual passwords. Το αποτέλεσμα αυτό

μπορεί να θεωρηθεί λίγο παράξενο, εάν σκεφτούμε ότι το 57% των χρηστών πιστεύουν ότι τα visual passwords είναι ευκολότερα στην απομνημόνευσή τους από τα γραφικά (Εικόνα 28). Από αυτούς τους χρήστες, το 17.54% δεν επιβεβαίωσαν σωστά τα visual passwords που δημιούργησαν, ακόμη και αν πίστευαν ότι η μέθοδος ήταν ευκολότερη από τα graphical. Το ποσοστό αυτό φαίνεται ακόμη χειρότερο εάν λάβουμε υπόψιν ότι τα περισσότερα visual passwords αποτελούνται από 4 ή 5 εικόνες, έναν αριθμό που δημιουργεί ένα password καθόλου ασφαλή και πολύ ευαίσθητο στις κακόβουλες επιθέσεις.



Εικόνα 43: Επιτυχημένη επιβεβαίωση των τριών passwords που δημιούργησαν οι χρήστες.

5.6. ΟΜΑΔΟΠΟΙΩΝΤΑΣ ΤΑ TEXT, VISUAL και GRAPHICAL PASSWORDS ΜΕ ΒΑΣΗ ΤΟ ΒΑΘΜΟ ΔΥΣΚΟΛΙΑΣ ΤΟΥΣ

Στην ενότητα αυτή ομαδοποιούμε κάθε έναν από τους τρεις τύπους passwords σε τρεις κατηγορίες, με σκοπό να ανακαλύψουμε πόσο δύσκολα passwords δημιουργούν οι χρήστες. Οι τρεις αυτές κατηγορίες είναι:

- Εύκολα passwords
- Μεσαία passwords
- Δύσκολα passwords

Για το λόγο αυτό, για κάθε έναν από τους τύπους password θα υπολογίσουμε το ***"full password space"***. Όταν μιλάμε για full password space εννοούμε όλους τους συνδυασμούς που μπορούν να γίνουν, χρησιμοποιώντας όλα τα διαθέσιμα σε κάθε περίπτωση στοιχεία, εάν θεωρήσουμε ότι η επιλογή των στοιχείων γίνεται τυχαία

(randomly). Με άλλα λόγια, η όλη διαδικασία που περιγράψαμε καλείται *"brute force attack"*, σε αντίθεση με το *"dictionary attack"*, όπου τα στοιχεία για την επίθεση δεν επιλέγονται τυχαία, αλλά με βάση αυτοματοποιημένα λεξικά.

- **Text passwords**

Για να δημιουργήσουμε ένα text password έχουμε στη διάθεσή μας 95 χαρακτήρες (52 γράμματα – κεφαλαία και μικρά, 10 αριθμούς και 33 σύμβολα). Με βάση αυτά το ***"full password space"*** για τα text passwords είναι $95^{n,}$ όπου $n \geq 4$ είναι ο αριθμός των χαρακτήρων στο password που δημιουργήσαμε. Στη συνέχεια, θα υπολογίσουμε τον αριθμό των διαφορετικών συνδυασμών των χαρακτήρων για διάφορες τιμές του n.

$n=8 \rightarrow 95^8$ συνδυασμοί $\rightarrow \approx \left(2^{6,57}\right)^8 \approx 2^{53}$
$n=7 \rightarrow 95^7$ συνδυασμοί $\rightarrow \approx \left(2^{6,57}\right)^7 \approx 2^{46}$
$n=6 \rightarrow 95^6$ συνδυασμοί $\rightarrow \approx \left(2^{6,57}\right)^6 \approx 2^{39}$
$n=5 \rightarrow 95^5$ συνδυασμοί $\rightarrow \approx \left(2^{6,57}\right)^5 \approx 2^{33}$
$n=4 \rightarrow 95^4$ συνδυασμοί $\rightarrow \approx \left(2^{6,57}\right)^4 \approx 2^{36}$

$\Rightarrow$

$n \geq 8$ Δύσκολο password
$n=7, n=6$ Μεσαίο password
$n=5, n=4$ Εύκολο password

Αυτό που κάναμε παραπάνω είναι να στρογγυλοποιήσουμε τον αριθμό τον χαρακτήρων (95) και τον κάνουμε δύναμη του 2, με σκοπό να κάνουμε πολύ πιο εύκολες τις συγκρίσεις με τα άλλα είδη passwords. Βασιζόμενοι στον αριθμό των διαφορετικών συνδυασμών, στην προσωπική μας γνώση για τα μυστικά passwords και τις διάφορες γνώμες των χρηστών και των διαφόρων ερευνητών, ταξινομήσαμε τα text passwords σε τρεις διαφορετικές κατηγορίες i) δύσκολα να σπάσουν για $n \geq 8$, ii) μέτριας δυσκολίας για να σπάσουν για n=6 ή 7, iii) εύκολα να σπάσουν για $n \leq 5$.

- **Visual passwords**

Για να δημιουργήσουμε ένα visual password στην έρευνά μας, μπορούμε να χρησιμοποιήσουμε $8 \times 9 = 72$ εικόνες. Έτσι, το ***"full password space"*** εδώ είναι 72^n, όπου $n \geq 4$ είναι ο αριθμός των εικόνων που επιλέγονται για τη δημιουργία του password. Όπως ακριβώς κάναμε και προηγουμένως, θα υπολογίσουμε και τώρα τον αριθμό των διαφορετικών συνδυασμών των εικόνων για διάφορες τιμές του n.

$n=9 \rightarrow 72^9$ συνδυασμοί $\rightarrow \approx \left(2^{6,17}\right)^9 \approx 2^{55}$

$n=8 \rightarrow 72^8$ συνδυασμοί $\rightarrow \approx \left(2^{6,17}\right)^8 \approx 2^{49}$

$n=7 \rightarrow 72^7$ συνδυασμοί $\rightarrow \approx \left(2^{6,17}\right)^7 \approx 2^{43}$

$n=6 \rightarrow 72^6$ συνδυασμοί $\rightarrow \approx \left(2^{6,17}\right)^6 \approx 2^{37}$

$n=5 \rightarrow 72^5$ συνδυασμοί $\rightarrow \approx \left(2^{6,17}\right)^5 \approx 2^{31}$

$\Rightarrow$

$n \geq 8$ Δύσκολο password

$n=7, n=6$ Μεσαίο password

$n \leq 5$ Εύκολο password

Βασιζόμενοι στην κατηγοριοποίηση που κάναμε παραπάνω για τα text passwords, χωρίσαμε κι εδώ τα visual passwords σε τρεις κατηγορίες: i) δύσκολα να σπάσουν για $n \geq 8$, ii) μέτριας δυσκολίας για να σπάσουν για n=6 or 7, iii) εύκολα να σπάσουν για $n \leq 5$.

- **Graphical passwords**

Τέλος για να δημιουργήσουμε ένα γραφικό password έχουμε στη διάθεσή μας $5 \times 5 = 25$ κελιά και ένα pen up event όταν σηκώνουμε το μολύβι, δηλαδή συνολικά 26 διαφορετικές επιλογές. Έτσι στην περίπτωση αυτή το ***"full password space"*** είναι 26^n, όπου $n \geq 4$ ο αριθμός των κελιών και pen up events για κάθε password. Για άλλη μία φορά λοιπόν θα υπολογίσουμε αριθμό των διαφορετικών συνδυασμών των κελιών και pen ups για διάφορες τιμές του n.

$n=12 \rightarrow 26^{12}$ συνδυασμοί $\rightarrow \approx \left(2^{4,7}\right)^{12} \approx 2^{56}$

$n=11 \rightarrow 26^{11}$ συνδυασμοί $\rightarrow \approx \left(2^{4,7}\right)^{11} \approx 2^{52}$

$n=10 \rightarrow 26^{10}$ συνδυασμοί $\rightarrow \approx \left(2^{4,7}\right)^{10} \approx 2^{47}$

$n=9 \rightarrow 26^9$ συνδυασμοί $\rightarrow \approx \left(2^{4,7}\right)^9 \approx 2^{42}$

$n=8 \rightarrow 26^8$ συνδυασμοί $\rightarrow \approx \left(2^{4,7}\right)^8 \approx 2^{38}$

$n=7 \rightarrow 26^7$ συνδυασμοί $\rightarrow \approx \left(2^{4,7}\right)^7 \approx 2^{33}$

$\Rightarrow$

$n \geq 11$ Δύσκολο password

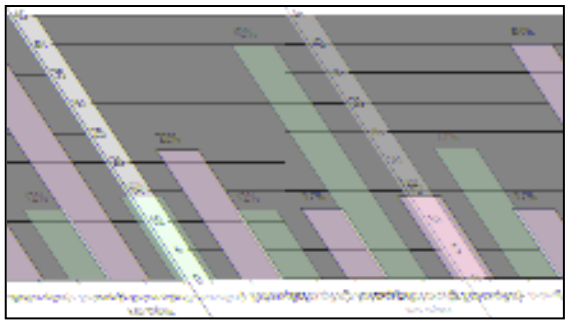
$8 \leq n \leq 10$ Μεσαίο password

$n \leq 7$ Εύκολο password

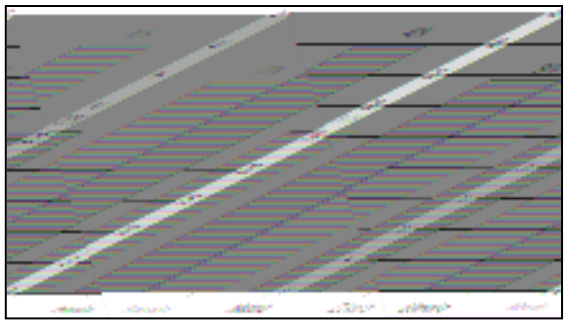
Αντίστοιχα με παραπάνω, ομαδοποιούμε τα γραφικά passwords σε τρεις διαφορετικές κατηγορίες: i) δύσκολα να σπάσουν για $n \geq 11$, ii) μέτριας δυσκολίας για να σπάσουν για n=8, 9, or 10, iii) εύκολα να σπάσουν για $n \leq 7$.

Έχοντας αναλύσει πλέον το full password space για κάθε μια από τις τρεις μεθόδους που εξετάζουμε, θα καθορίσουμε τη δυσκολία που παρουσιάζουν στο να σπάσουν, τα passwords που δημιούργησαν οι χρήστες μας.

Όσον αφορά τα text passwords, πολλοί από τους συμμετέχοντες (40%) χρησιμοποιούν 8 χαρακτήρες και πάνω στο password που δημιουργούν, φτιάχνοντας έτσι, με βάση τους παραπάνω υπολογισμούς, ένα password δύσκολο να σπάσει.(Εικόνα 44). Επιπλέον το 34% δημιουργεί password με 4 ή 5 χαρακτήρες, δηλαδή πολύ εύκολα και καθόλου ασφαλή. Η Εικόνα 45 παρουσιάζει την ομαδοποίηση των text passwords στις τρεις κατηγορίες (δύσκολα, μέτρια, εύκολα) και τα αντίστοιχα ποσοστά κάθε κατηγορίας.

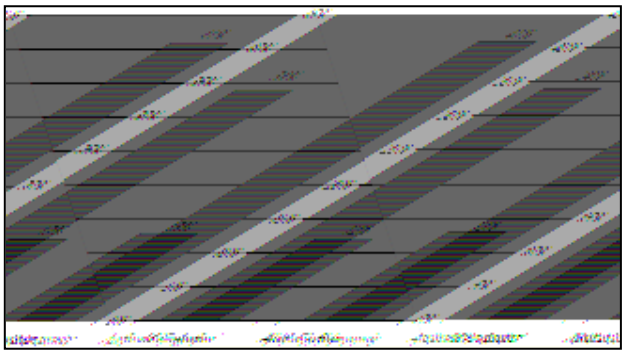


Εικόνα 44: Αριθμός χαρακτήρων στα text passwords.



Εικόνα 45: Ομαδοποίηση των text passwords με βάση τη δυσκολία τους.

Με μια πρώτη ματιά θα μπορούσαμε να χαρακτηρίσουμε τα αποτελέσματα αυτά αρκετά ικανοποιητικά. Παρόλα αυτά, εξετάζοντας με μεγαλύτερη προσοχή τα text passwords που δημιούργησαν οι χρήστες, συμπεραίνουμε ότι τι 54% των συμμετεχόντων δημιούργησαν passwords που αποτελούνται μόνο από ονόματα, αριθμούς ή γνωστές σε αυτούς ημερομηνίες (Εικόνα 46). Τα χαρακτηριστικά όμως αυτά έχουν ως αποτέλεσμα τα passwords που δημιουργούνται τελικά να είναι προβλέψιμα και άρα πολύ εύκολα να σπάσουν. Επίσης διαπιστώσαμε ότι το 34% των χρηστών χρησιμοποιούν στους



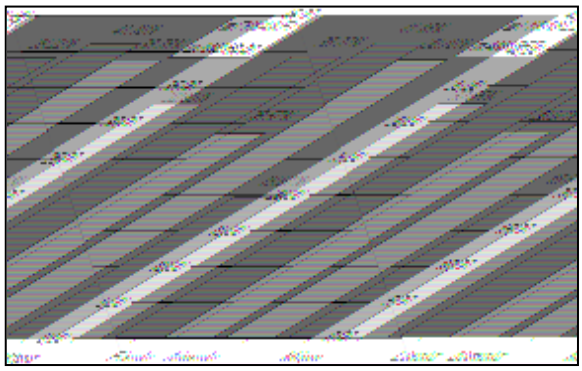
Εικόνα 46: Προβλέψιμα text passwords.

κωδικούς που δημιουργούν αριθμούς μαζί με γράμματα και μόνο το 13% χρησιμοποιεί ταυτόχρονα και σύμβολα

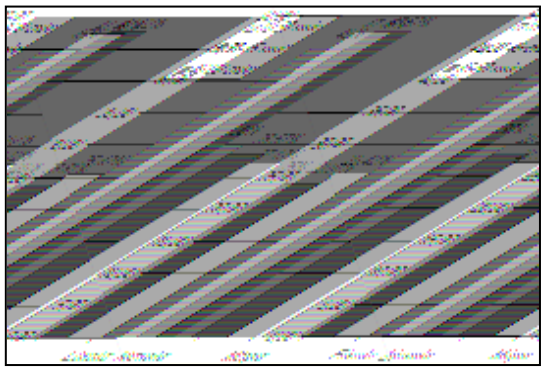
Εξετάζοντας τώρα μόνο τα δύσκολα text passwords, διαπιστώνουμε ότι το 42.5% αυτών είναι προβλέψιμα. Άρα ακόμη και αν το 97% των χρηστών επιβεβαίωσαν με επιτυχία τον κωδικό που είχαν δημιουργήσει, ουσιαστικά δεν έχει μεγάλη σημασία αφού τα περισσότερα passwords είναι προβλέψιμα και άρα ευαίσθητα στις επιθέσεις.

Εξετάζοντας τώρα τα text passwords που δημιουργούνται σε σχέση με το φύλο των χρηστών (Εικόνα 47), παρατηρούμε ότι περισσότερες γυναίκες (39.22%) απ' ότι άνδρες (28.57%), δημιούργησαν εύκολα passwords. Παρόμοια, μπορούμε να πούμε ότι περισσότερες γυναίκες (41.18%) απ' ότι άνδρες (39.78%), δημιούργησαν δύσκολα passwords. Σε αντίθεση με αυτά παρατηρούμε επίσης ότι περισσότεροι άνδρες (32.65%) απ' ότι γυναίκες (19.61%) δημιούργησαν passwords μέτριας δυσκολίας.

Αναλύοντας τέλος τα text passwords των χρηστών σε σχέση με την ηλικία τους (Εικόνα 48), διαπιστώσαμε ότι τα περισσότερα άτομα ηλικίας μέχρι 30 ετών (47.46%) δημιουργούν δύσκολα passwords, ενώ άνω των 30 ετών δημιουργούν εύκολα passwords (πάνω από 45%).



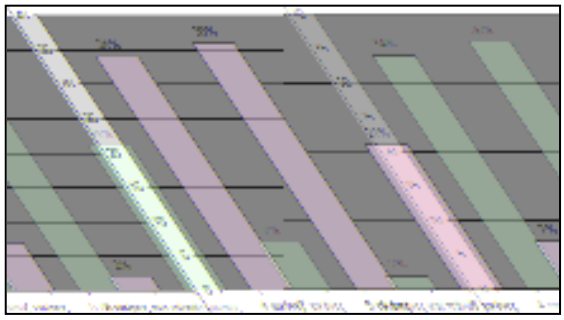
Εικόνα 47: Η δυσκολία των text passwords που δημιουργούν τα δύο φύλλα



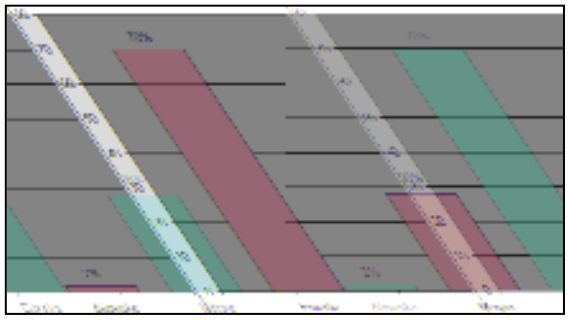
Εικόνα 48: Η δυσκολία των text passwords που δημιουργούν οι χρήστες με βάση την ηλικία των χρηστών.

Στη συνέχεια θα εξετάσουμε με τον ίδιο τρόπο τα visual passwords, με σκοπό να ανακαλύψουμε μέσα από τις προσωπικές επιλογές των χρηστών, εάν αναφερόμαστε πραγματικά σε μια μέθοδο καλύτερη από τα text passwords.

Η Εικόνα 49 δείχνει τον αριθμό των εικόνων που επέλεξαν οι χρήστες για τη δημιουργία των visual passwords. Με βάση αυτά δημιουργήσαμε την Εικόνα 50 η οποία μας δείχνει πόσο δύσκολα visual passwords δημιουργούν τελικά οι χρήστες. Οι περισσότεροι συμμετέχοντες (70%), επέλεξαν 4 ή 5 εικόνες για τον κωδικό τους (ο μέσος αριθμός εικόνων που γενικά επιλέγουν οι χρήστες είναι 5.07), πράγμα που σημαίνει ότι τα passwords που δημιούργησαν θεωρούνται πολύ εύκολα. Το ποσοστό αυτό φαίνεται ακόμη χειρότερο, εάν σκεφτούμε τις επιτυχημένες και μη επιτυχημένες επιβεβαιώσεις των visual passwords. Μπορούμε λοιπόν πλέον να καταλάβουμε ότι το 18% που αντιστοιχεί στο ποσοστό των ατόμων που δεν επιβεβαίωσαν σωστά τον visual κωδικό τους είναι ένα πολύ μεγάλο ποσοστό, καθώς την ίδια στιγμή ένας πολύ μεγάλος αριθμός των visual passwords αποτελούνται από 5 εικόνες ή και λιγότερες.



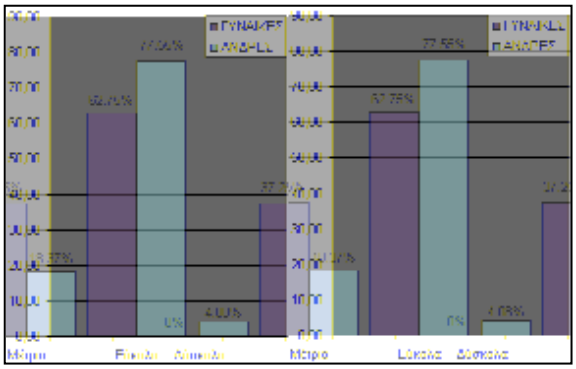
Εικόνα 49: Αριθμός των εικόνων στα visual passwords.



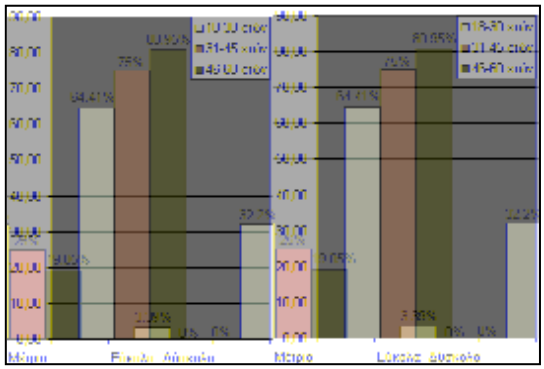
Εικόνα 50: Ομαδοποίηση των visual passwords με βάση την δυσκολία τους.

Συγκρίνοντας τις επιλογές των ανδρών και των γυναικών (Εικόνα 51), διαπιστώσαμε ότι περισσότεροι άνδρες (77.55%) απ' ότι γυναίκες (62.75%) δημιούργησαν εύκολα visual passwords. Αντίθετα πολύ περισσότερες γυναίκες (37.25%) απ' ότι άνδρες (18.37%) δημιούργησαν passwords μέτριας δυσκολίας. Τέλος, αυτοί που τελικά δημιούργησαν δύσκολα visual passwords ήταν αποκλειστικά άνδρες, σε ένα πολύ μικρό ποσοστό (4%).

Εξετάζοντας τώρα τις ηλικίες των συμμετεχόντων (Εικόνα 52), ανακαλύψαμε ότι οι περισσότεροι χρήστες δημιουργούν εύκολα visual passwords ανεξάρτητα με την ηλικία τους. Οι περισσότεροι χρήστες (80.95%) ηλικίας 46 έως 60 ετών δημιούργησαν εύκολα passwords, ενώ από αυτούς που δημιούργησαν passwords μέτριας δυσκολίας το μεγαλύτερο ποσοστό (32.20%) ανήκει σε νεαρά άτομα μέχρι 30 ετών. Όσον αφορά τώρα τη δημιουργία δύσκολων visual κωδικών, το αντίστοιχο ποσοστό είναι πολύ μικρό (3.39%) και ανήκει αποκλειστικά σε άτομα μικρής ηλικίας.

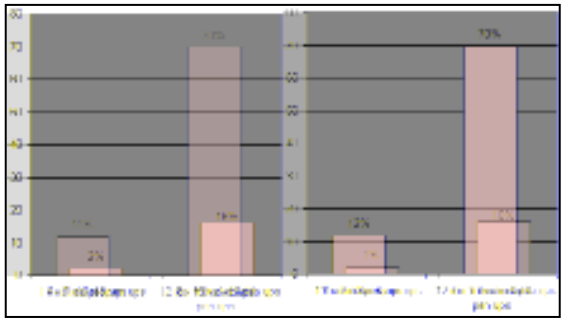


Εικόνα 51: Η δυσκολία των visual passwords που δημιουργούν τα δύο φύλλα.

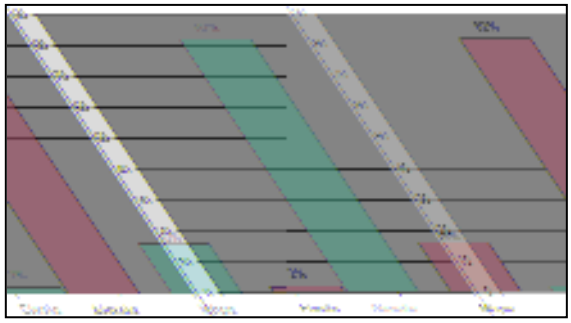


Εικόνα 52: Η δυσκολία των text passwords που δημιουργούν οι χρήστες με βάση την ηλικία των χρηστών.

Τελειώνοντας, θα εξετάσουμε τις ίδιες παραμέτρους και για τα graphical passwords. Αφού δημιούργησε ο κάθε χρήστης το δικό του γραφικό password, υπολογίσαμε για κάθε ένα από αυτά, τον ακριβή αριθμό κελιών και pen up events που έχουν (Εικόνα 53). Με βάση τώρα την κατηγοριοποίηση που κάναμε στην αρχή της ενότητάς μας, δημιουργήσαμε την Εικόνα 54 η οποία μας δείχνει ότι οι περισσότεροι συμμετέχοντες (82%) δημιούργησαν πολύ δύσκολα graphical passwords, που διαθέτουν περισσότερα από 11 κελιά και pen up events. Είναι επίσης πολύ σημαντικό να αναφέρουμε ότι ο μέσος αριθμός κελιών και pen ups είναι 16.15. Αυτό σημαίνει ότι ακόμη και αν οι χρήστες δεν μπόρεσαν να το κατανοήσουν (καθώς επέλεξαν τα visual passwords ως την ευκολότερη στην απομνημόνευση μέθοδο), είχαν τη δυνατότητα να δημιουργήσουν χωρίς δυσκολίες, γραφικά passwords που είναι πολύ δύσκολο να σπάσουν, έχοντας ταυτόχρονα ένα πολύ μικρό ποσοστό μη επιτυχημένων επιβεβαιώσεών τους (14% - Εικόνα 43).

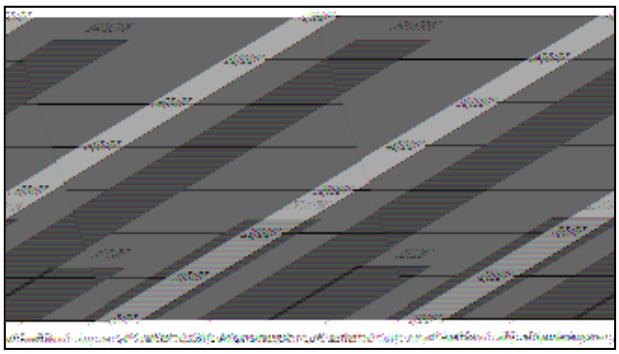


Εικόνα 53: Αριθμός κελιών και pen up events στα graphical passwords.



Εικόνα 54: Ομαδοποίηση των graphical passwords με βάση την δυσκολία τους.

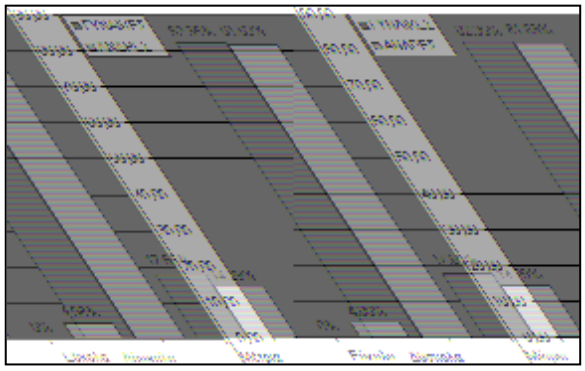
Η Εικόνα 55 στη συνέχεια, δείχνει πως κατανέμεται ο αριθμός των κελιών και των pen ups στα δύσκολα graphical passwords. Η πλειοψηφία λοιπόν των δύσκολων γραφικών passwords (64.63%) αποτελούνται από 11 έως 18 κελιά και pen ups. Εκτός από αυτό, αρκετά μεγάλα ποσοστά των γραφικών passwords αποτελούνται από 19 έως 25 κελιά και pen ups (23.17%) και 26 έως 34 κελιά και pen ups (12.2%).



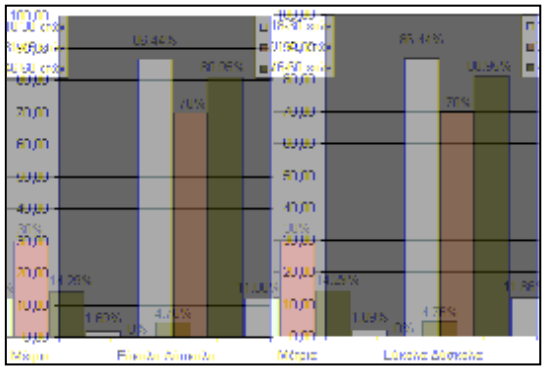
Εικόνα 55:.Κατανομή του αριθμού των κελιών και pen up events, στα δύσκολα graphical passwords.

Στο τέλος θα αναλύσουμε και για τα graphical passwords τα αποτελέσματα με βάση το φύλο των χρηστών (Εικόνα 56) και την ηλικία τους (Εικόνα 57). Έτσι έχουμε τα εξής συμπεράσματα:

- Και οι άνδρες αλλά και οι γυναίκες (σε σχεδόν ίσα ποσοστά), δημιουργούν πραγματικά δύσκολα γραφικά passwords. Επίσης, όσον αφορά τα passwords μέτριας δυσκολίας, δημιουργούνται από περισσότερες γυναίκες παρά άντρες.
- Η δημιουργία δύσκολων γραφικών passwords δεν είναι χαρακτηριστικό μόνο των μικρών σε ηλικία χρηστών, οι οποίοι βέβαια κατέχουν και το μεγαλύτερο ποσοστό (86.44%). Αντίθετα ακόμη και άτομα ηλικίας πάνω από 46 ετών (80.95), είναι ικανά να δημιουργήσουν δύσκολα graphical passwords.

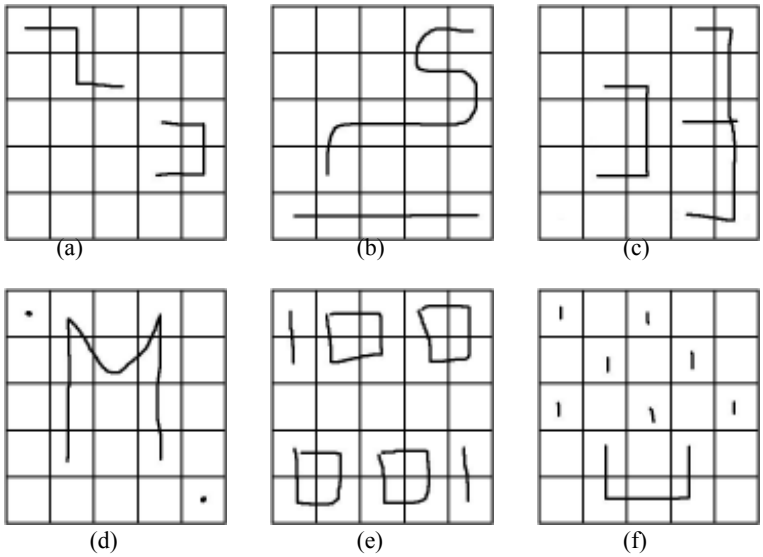


Εικόνα 56: Η δυσκολία των graphical passwords που δημιουργούν τα δύο φύλλα.



Εικόνα 57: Η δυσκολία των graphical passwords που δημιουργούν οι χρήστες με βάση την ηλικία των χρηστών.

Για να γίνουν τα πράγματα λίγο πιο ξεκάθαρα, παρουσιάζουμε στην Εικόνα 58 μερικά τυχαία παραδείγματα γραφικών passwords που δημιούργησαν οι χρήστες που συμμετείχαν στην έρευνά μας. όπως μπορούμε να παρατηρήσουμε το πρώτο (Εικόνα 58a), είναι ένα πολύ εύκολο password, αφού περνάει από 8 κελιά και έχει μόνο ένα pen up event. Το δεύτερο (Εικόνα 58b) είναι λίγο πιο δύσκολο, ενώ το τρίτο και το τέταρτο (Εικόνες 58c και 58d) είναι ακόμη πιο δύσκολα, αφού έχουν 2 pen ups. Το πέμπτο γραφικό password (Εικόνα 58e), είναι ένα πραγματικά δύσκολο password καθώς καλύπτει 24 κελιά και έχει 5 pen up events. Το μόνο μειονέκτημα εδώ είναι η συμμετρικότητά του, ένα χαρακτηριστικό που υπό κάποιες προϋποθέσεις μπορεί να το κάνει ευαίσθητο σε επιθέσει με αυτοματοποιημένα λεξικά. Το έκτο password τελικά (Εικόνα 58f), είναι το πιο δύσκολο από όλα καθώς έχει 7 pen up events και κανένα χαρακτηριστικό που μπορεί να το κάνει μην ασφαλή και εύκολο στο να σπάσει (δεν είναι συμμετρικό ή κεντραρισμένο).



Εικόνα 58: Τυχαία παραδείγματα graphical passwords.

5.7. ΠΑΡΑΤΗΡΗΣΕΙΣ ΤΩΝ ΣΥΜΜΕΤΕΧΟΝΤΩΝ

Όπως έχουμε ήδη αναφέρει, το ερωτηματολόγιο εκτός από τις 23 ερωτήσεις κλειστού τύπου που έχει, περιλαμβάνει στο τέλος και μια ανοιχτού τύπου ερώτηση, όπου ο κάθε χρήστης έχει τη δυνατότητα να αναφέρει την προσωπική του γνώμη, τους προβληματισμούς του ή οτιδήποτε άλλα θέλει πάνω στην όλη διαδικασία που υποβλήθηκε.

Αναλύοντας λοιπόν την ερώτηση αυτή, θα πρέπει αρχικά να πούμε ότι όλοι σχεδόν οι χρήστες κατανόησαν και τόνισαν ότι η ανάπτυξη καινούργιων μεθόδων πιστοποίησης, που να είναι πιο ασφαλείς από τα text passwords, ήταν ένα θέμα μείζονος σημασίας, που θα έπρεπε όσο γίνεται πιο γρήγορα να βρει τη λύση του. Οι χρήστες τώρα που προτιμούν τα visual passwords, ανέφεραν ότι τα θεωρούν πιο εύκολα στην απομνημόνευσή τους καθώς μπορούν να δημιουργήσουν τις δικές τους προσωπικές ιστορίες και με βάση αυτές να θυμούνται εύκολα τη σωστή σειρά των εικόνων. Από την άλλη πλευρά, πολλοί από τους συμμετέχοντες χρήστες που προτιμούν τα graphical passwords, ανέφεραν ένα σημαντικό μειονέκτημα των visual: ακόμη και αν είναι πιο ελκυστικά αισθητικά, μπορούν πολύ εύκολα να μπερδέψουν πολύ τον χρήστη εάν η εφαρμογή έχει πολλές εικόνες, με αποτέλεσμα η όλη διαδικασία να είναι πολύ

χρονοβόρα. Επιπλέον τονίσανε ότι κατά τη γνώμη τους είναι πολύ δύσκολο να θυμάται κάποιος πάνω από 5 εικόνες, ενώ στα γραφικά passwords είναι πολύ ευκολότερο να περνάς από πολλά κελιά και να δημιουργείς τελικά έναν δύσκολο κωδικό.

Οι χρήστες επίσης αναφέρανε ότι και οι δύο μέθοδοι είναι πολύ καλές και κινούν πολύ εύκολα την περιέργεια κάθε ανθρώπου. Ακόμη και αναλφάβητα άτομα μπορούν να εντυπωσιαστούν από τα οπτικά και γραφικά passwords, καθώς δεν θα πρέπει να γράψουν και να θυμούνται χαρακτήρες, αριθμούς ή σύμβολα, αλλά απλά να διαλέγουν μια σειρά από εικόνες ή να ζωγραφίζουν ένα προσωπικό σχέδιο. Μια πολύ καλή ιδέα που προτάθηκε από κάποιον χρήστη όσον αφορά τα γραφικά passwords, είναι να τοποθετηθεί ένα διαφορετικό χρώμα σε κάθε κελί, με σκοπό να απομνημονεύει ο χρήστης ευκολότερα τη σειρά των κελιών από τα οποία περνάει.

Τελειώνοντας, ένα θέμα που απασχόλησε κάποιους από τους χρήστες είναι το hardware το οποίο θα πρέπει να προστεθεί για την υλοποίηση των δύο νέων μεθόδων πιστοποίησης, δηλαδή μια γραφίδα για τα γραφικά passwords και μια οθόνη αφής για τα οπτικά. Εδώ θα πρέπει να τονίσουμε ότι κάτι τέτοιο δεν θα έπρεπε να τους απασχολεί, καθώς με την τόση μεγάλη ανάπτυξη της τεχνολογίας, μέσα σε λίγα χρόνια σχεδόν κάθε σύστημα και ηλεκτρονικός υπολογιστής, θα είναι εξοπλισμένος με ένα τέτοιο hardware. Έτσι, θα είναι πλέον πολύ εύκολο σε οποιονδήποτε που θα διαθέτει ένα υπολογιστή και εξασκηθεί και να υλοποιήσει τις δύο καινούργιες μεθόδους πιστοποίησης.

5.8. ΔΗΜΙΟΥΡΓΩΝΤΑΣ ΑΣΦΑΛΕΣΤΕΡΑ ΓΡΑΦΙΚΑ PASSWORDS

Αφού τελειώσαμε την επεξεργασία των δεδομένων και την ανάλυση των αποτελεσμάτων, είμαστε σε θέση να πούμε ότι τα γραφικά passwords είναι η ασφαλέστερη και πιο εύκολή στην απομνημόνευσή της μέθοδος, όπου οι χρήστες μπορούν να δημιουργήσουν passwords που είναι πραγματικά πολύ δύσκολο να σπάσουν.

Σκεπτόμενοι λοιπόν όλα αυτά, έχουμε τη δυνατότητα να δημιουργήσουμε ένα σύνολο συμβουλών και κανόνων που θα πρέπει να ακολουθούν οι χρήστες ώστε τα γραφικά passwords που θα δημιουργούν να μην είναι ευαίσθητα σε κακόβουλες επιθέσεις. Οι κανόνες αυτοί είναι:

- Να μην δημιουργούν συμμετρικά σχήματα
- Να μην δημιουργούν κεντραρισμένα σχήματα
- Να προσπαθούν να σχεδιάζουν πάνω από μία γραμμές
- Να περιλαμβάνουν στο σχέδιό τους όσα περισσότερα pen up events μπορούνε (το ίδιο σχέδιο, με περισσότερα pen up events είναι πολύ ασφαλέστερο)
- Να αποφεύγουν να ξεκινάνε το σχέδιό τους από τα 4 γωνιακά κελιά (οι θέσεις αυτές είναι πολύ ευαίσθητες σε αυτοματοποιημένες επιθέσεις)
- Εάν το σχέδιό τους είναι πολύ απλό, να προσπαθούν να κάνουν και ένα δεύτερο ή ακόμα και τρίτο, όμοιο με το αρχικό, αλλά που θα καλύπτει διαφορετικά κελιά
- Να αποφεύγουν να ζωγραφίζουν διαγώνιες γραμμές και άρα και γραμμές κοντά στην τομή των γραμμών που σχηματίζουν τα κελιά, επειδή είναι πολύ εύκολο να μπερδευτούν και να κάνουν λάθη μετατόπισης (shift errors).

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η διεξαγωγή της έρευνας αυτής έγινε με σκοπό να συγκρίνουμε τις proof by knowledge τεχνικές πιστοποίησης των χρηστών, δηλαδή τα text passwords, τα visual passwords και τα graphical passwords. Στην έρευνά μας συμμετείχαν 100 χρήστες, άνδρες και γυναίκες, ηλικίας από 18 έως 60 ετών. Αρχικά έγινε ενημέρωση των χρηστών πάνω στα προβλήματα που δημιουργούν τα text passwords αλλά και πάνω στις καινούργιες μεθόδους των visual και graphical passwords. Στη συνέχεια οι χρήστες, βασιζόμενοι στις πληροφορίες που πήραν, δημιούργησαν τα προσωπικά τους text, visual και graphical passwords, προσπάθησαν να τα επιβεβαιώσουν σωστά και τέλος απάντησαν και σε ένα ερωτηματολόγιο που τους δόθηκε, το οποίο περιείχε ερωτήσεις που αφορούσαν τους αλφαριθμητικούς κωδικούς που χρησιμοποιούν οι χρήστες σήμερα, αλλά και τη γνώμη τους πάνω στις νέες μεθόδους πιστοποίησης.

Στηριζόμενοι λοιπόν στα passwords που δημιούργησαν οι χρήστες και στις απαντήσεις τους στο ερωτηματολόγιο, καταλήξαμε σε ορισμένα συμπεράσματα που φάνηκαν πολύ χρήσιμα στην έρευνά μας. Αρχικά θα πρέπει να πούμε ότι στη σημερινή εποχή πλέον, όλοι οι άνθρωποι χρησιμοποιούν σχεδόν καθημερινά πολλά passwords για διάφορες εφαρμογές. Το γεγονός αυτό έχει ως αποτέλεσμα, αφού υπάρχει τόσο μεγάλη συσσώρευση πληροφοριών, οι χρήστες να αντιμετωπίζουν προβλήματα στην απομνημόνευση των προσωπικών τους κωδικών και προσπαθώντας να αντιμετωπίσουν την κατάσταση αυτή να δημιουργούν text passwords που είναι προβλέψιμα και άρα πολύ ευαίσθητα σε κακόβουλες επιθέσεις. Επιπλέον, για να μην υπάρχει ο φόβος να ξεχάσουν τους κωδικούς τους, χρησιμοποιούν διάφορες άλλες μεθόδους, όπως να τους μοιράζονται με άλλους ανθρώπους, να τους καταγράφουν κάπου ή να περιλαμβάνουν στο password κάτι ήδη γνωστό που δεν υπάρχει καμία περίπτωση να ξεχάσουν. Κατανοώντας λοιπόν οι χρήστες το μεγάλο πρόβλημα που υπάρχει και που αφορά την ασφάλεια τον προσωπικών τους κωδικών, έδειξαν πολύ θετική στάση απέναντι στις καινούργιες μεθόδους πιστοποίησης, τα visual και graphical passwords.

Με βάση λοιπόν τις προσωπικές απαντήσεις των χρηστών, μπορούμε να πούμε ότι μπορούσαν να θυμούνται τα visual passwords ευκολότερα, καθώς είναι πολύ πιο εύκολο να θυμούνται μια σειρά εικόνων απ’ ότι μια σειρά από χαρακτήρες. Ιδιαίτερα οι

χρήστες μεγαλύτερης ηλικίας βρήκαν πολύ εύχρηστη τη μέθοδο αυτή, ενώ το ίδιο πιστεύουν και περισσότερες γυναίκες σε σχέση με τους άνδρες, αν και γι' αυτές ήταν λίγο δυσκολότερη η εκμάθηση του τρόπου λειτουργίας της. Το πρόβλημα βέβαια που παρουσιάζεται εδώ είναι ότι ακόμη και αν τα visual passwords εντυπωσίασαν σε μεγάλο βαθμό τους χρήστες και των δύο φύλων και ιδιαίτερα ηλικίας άνω των 45 ετών, το password space των κωδικών αυτών παραμένει ίδιο με την περίπτωση των text passwords. Επιπλέον, οι περισσότεροι χρήστες επιλέγουν για τους κωδικούς τους ένα πολύ μικρό αριθμό εικόνων, με αποτέλεσμα να δημιουργούν πολύ εύκολα και άρα καθόλου ασφαλή visual passwords.

Η δεύτερη καινούργια μέθοδος πιστοποίησης, τα graphical passwords, αποδείχτηκε και η καλύτερη. Οι γυναίκες ήταν αυτές που σε μεγαλύτερο ποσοστό δε δυσκολεύτηκαν καθόλου στην εκμάθηση της λειτουργίας τους, παρά τους αρκετούς κανόνες που έχουν, ενώ τους φάνηκαν ιδιαίτερα εύχρηστα σε σχέση με τους άνδρες. Κάποια δυσκολία στην κατανόησή τους αντιμετώπισαν τα μεγαλύτερα σε ηλικία άτομα, η οποία ξεπεράστηκε αφού τελικά θεωρούν τα γραφικά passwords αρκετά εύχρηστα. Ακόμη λοιπόν και αν οι περισσότεροι χρήστες ανάφεραν ότι προτιμούσαν από κάθε άποψη τα visual passwords, όταν τους ζητήθηκε να δημιουργήσουν τα δικά τους graphical passwords, δημιούργησαν passwords ευκολότερα στην απομνημόνευση και πολύ ασφαλέστερα από αυτά που δημιούργησαν με τις άλλες δύο μεθόδους.

Γενικότερα και οι δύο νέες μέθοδοι μπορούν να χαρακτηριστούν αρκετά φιλικές για τους χρήστες, αλλά λίγο δύσκολες στην αρχή, μέχρι να μάθουν ακριβώς πως χρησιμοποιούνται. Αυτό τονίστηκε ιδιαίτερα από τους μεγαλύτερους σε ηλικία χρήστες, και περισσότερο όταν αναφέρθηκαν στα graphical passwords. Οι χρήστες αυτοί, κατέληξαν επίσης στο συμπέρασμα ότι και οι δύο νέες μέθοδοι είναι πιο χρονοβόρες από τα text passwords, χωρίς όμως τελικά να αλλάξουν την απόφασή τους στο να μάθουν περισσότερα για αυτές, καθώς είναι ασφαλέστερες από τις παραδοσιακές τεχνικές και πραγματικά εύκολες στη χρήση τους μετά από ένα διάστημα πρακτικής εξάσκησης.

Βασιζόμενοι λοιπόν σε όλα αυτά τα αποτελέσματα και στις προσωπικές μας γνώσεις πάνω στα passwords και την ασφάλειά τους, στο τέλος της έρευνάς μας προτείναμε μια λίστα κανόνων και συμβουλών που μπορούν να ακολουθούν οι χρήστες και έτσι να αποφεύγουν τη δημιουργία σχετικά εύκολων γραφικών passwords, που δεν θα είναι τόσο ασφαλή.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. A. De Angeli, L. Coventry, G. Johnson and K. Renaud, “Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems”, in *International Journal of Human-Computer Studies*, vol. 63, pp 128-152, July 2005.
2. A. Alexiadis, K. Chalkias and G. Stephanides**,** “Implementing a Graphical Password Scheme that uses Nested Grids*”*, in *International Conference for Internet Technology and Secured Transactions (ICITST 2006)*, London, United Kingdom, 2006.
3. A. Bauer, Gallery of random art, http://andrej.com/art, 1998, last accessed December 2006.
4. J.-C. Birget, D. Hong, and N. Memon, “Robust discretization with an application to graphical passwords’”, in *Cryptology ePrint Archive, Report 2003/168*, http://eprint.iacr.org, 2006, last accessed December 2006.
5. G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent, Ed. United States, 1996.
6. H. Bolande, “Forget passwords, what about pictures?”, 2000, http://zdnet.com.com/2102-11-525841.html.
7. K. Chalkias, A. Alexiadis, and G. Stephanides, “A Multi-Grid Graphical Password Scheme”, in *6th International Conference on Artificial Intelligence and Digital Communications*, Thessaloniki, Greece, 2006.
8. H. Davies. “Physiognomic Access Control”, in *Information Security Monitor,* vol. 10, no.3, pp 5-8, 2005.
9. D. Davis, F. Monrose, M.Reiter, “On User Choice in Graphical Password Schemes”, in *13th USENIX Security Symposium*, 2004.
10. R. Dhamija, A. Perrig, “Déjà Vu: A User Study Using Images for Authentication”, in *9th USENIX Security Symposium*, 2000.
11. K. Gilhooly, "Biometrics: Getting Back to Business," in *Computerworld, May 09*, 2005.
12. J. Goldberg, J. Hagman, and V. Sazawal, “Doodling Our Way to Better Authentication”, CHI '02 extended abstracts on Human Factors in Computer Systems, Minneapolis (ACM Press), 2002.
13. I. Irakleous, S.M. Furnell, P.S.Dowland and M.Papadaki, “An experimental comparison of secret-based user authentication technologies”, in *Information Management & Computer Security*, vol.10, pp. 100-108, 2002.
14. W. Jansen, “Authenticating Users on Handheld Devices”, in the *Canadian Information Technology Security Symposium*, 2003.
15. W. A. Jansen, “Authenticating Mobile Device Users Through Image Selection”, in *Data Security 2004*. May 2004.
16. W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R.Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR7030, http://csrc.nist.gov/publications/nistir/nistir-7030.pdf, 2003.
17. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in *Proceedings of the 8th USENIX Security Symposium*, 1999.

18. Y. Kim and T. Kwon, “An Authentication Scheme Based Upon Face Recognition for the Mobile Environment”, in *International symposium on computational and information science N°1*, Shanghai, China, 2004.
19. D. Klein. (1990), “Foiling the Cracker: a survey of, and improvements to, password security”, in *2n USENIX Security Workshop.* 5-14, 1990.
20. D. Nali and J. Thorpe, “Analysing user choice in graphical passwords”, *Tech. Report TR-04-01, School of Computer Science*, Carleton University, Canada, 2004.
21. P.C. van Oorschot, J. Thorpe. (2005), “On the Security of Graphical Password Schemes”, *Technical Report TR-05-11. Integration and extension of USENIX Security 2004 and ACSAC 2004 papers*.
22. Passlogix, "www.passlogix.com," last accessed in November 2006.
23. A. Perrig and D. Song. “Hash visualization: A new technique to improve real-world security.” in *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce (CryTEC ’99),*1999.
24. Real User Corporation, “About passfaces”, http://www.realuser.com/cgi-bin/ru.exe/_/homepages/ technology/passfaces.htm, last accessed in November 2006
25. Real User Corporation, *“The Science Behind Passfaces”*, Revision 2, September 2001, http://www.realuser.com/published/ScienceBehindPassfaces.pdf.
26. K. Renaud and A. De Angeli, “My password is here! An investigation into visuo-spatial authentication mechanisms”, in *Interacting with Computers*, vol. 16, pp 1017-1041, 2004.
27. L. Sobrado, J.C. Birget, Graphical passwords, The Rutgers Scholar, vol.4. http://RutgersScholar.rutgers.edu/volume04/contents.htm (2002).
28. X. Suo, Y. Zhu and G. S. Owen, “Graphical Passwords: A Survey”, in *Annual Computer Security Applications Conference*, Marriott University Park, Tucson, Arizona, 2005.
29. F. Tari, A. A. Ozok and S.H. Holden, “A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords”, in *ACM International Conference Proceeding Series*, vol. 149, pp. 56-66, 2006.
30. J. Thrope and P. van Oorschot, “Graphical dictionaries and the memorable space of graphical passwords”, in *Proceedings of the 13th UNIX Security Symposium,* August 2004
31. B. Tribelhorn, “End user security”, 2002, http://www.cs.hmc.edu/~mike/public_html/courses/security/s06/projects/index.html, last accessed in November 2006.
32. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in *Human-Computer Interaction International (HCII 2005)*. Las Vegas, NV, 2005.
33. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in *Symposium on Usable Privacy and Security (SOUPS)*. Carnegie-Mellon University, Pittsburgh, 2005.
34. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human Computer Studies (Special Issue on HCI Research in Privacy and Security)* 63, 102-127,2005.

35. J. Yan, Alan, Ross and Alasdair “Password Memorability and Security: Empirical Results”, in *IEEE Computer Society – IEEE Security & Privacy*, vol.2, pp. 25-31, September 2004.