Κρυπτογράφηση σε υποδομή καταλόγου και περιβάλλον GDPR

Το περιβάλλον του νέου κανονισμού προστασίας προσωπικών δεδομένων GDPR επιβάλλει μεγάλη προσοχή στη διαχείριση και αποθήκευση προσωπικών δεδομένων. Ως εκ τούτου είναι σημαντικό να υπάρχουν οι τεχνικές προϋποθέσεις για την ασφαλή αποθήκευση και χειρισμό δεδομένων. Η υποδομή καταλόγου (Directory Service) στο διαδίκτυο γίνεται με χρήση του προτύπου LDAP – Light Directory Access Protocol και των επικουρικών τεχνικών συστάσεων [1]. Ένας *κατάλογος* στο διαδίκτυο είναι ένα αρχείο το οποίο ακολουθεί ένα συντακτικό (schema) για να αποτυπωθεί ένα δομημένο (structured) αρχείο από *attribute:value*. Ένας τυπικός κατάλογος μπορεί να περιγράφει φυσικά πρόσωπα με στοιχεία επικοινωνίας (π.χ. email, τηλ) και στοιχεία κωδικού/συνθηματικού (username/password) χρήστη. Το αρχείο αποθήκευσης μια υποδομής καταλόγου είναι ένα δομημένο αρχείο με τα παραπάνω στοιχεία. Το περιεχόμενα του αρχείου ανακτώνται μέσω αναζητήσεων με βάση το κλειδί-attribute (π.χ. e-mail). Η προστασία των δεδομένων στα πλαίσια λειτουργίας του καταλόγου γίνεται με χρήση ταυτοποίησης(Authentication) και λιστών πρόσβασης (Access lists). Κάθε ταυτοποιημένος χρήστης έχει πρόσβαση στα πεδία και τιμές των πεδίων που προστατεύονται από το συνθηματικό του και σε όλα τα γενικά πεδία όλων των άλλων χρηστών. Οι περιορισμοί πρόσβασης με ACL προστατεύει την πρόσβαση των δεδομένων μέσω του πρωτοκόλλου LDAP. Εν τούτοις το αρχείο αποθήκευσης των δεδομένων είναι πάντα ακρυπτογράφητο. Μια υποτιθέμενη παραβίαση ασφάλειας του συστήματος που εξυπηρετεί την υπηρεσία καταλόγου μπορεί να θέσει σε κίνδυνο τα προσωπικά δεδομένα όλων των χρηστών.

Υποψήφιοι μηχανισμοί προστασίας είναι η κρυπτογράφηση ή/και το hashing. Η κρυπτογράφηση των τιμών (key) μπορεί να γίνει είτε σε επίπεδο File System (Συστήματος Αρχείων) του λειτουργικού συστήματος (operating System) είτε στα πλαίσια της εφαρμογής. Η κρυπτογράφηση σε επίπεδο συστήματος αρχείων διασφαλίζει την απόκρυψη των περιεχομένων του αρχείου ακόμη και σε περίπτωση που κλαπεί ο δίσκος του συστήματος.

Στα πλαίσια αυτής της διπλωματικής αυτής θα χρειαστεί να εγκατασταθεί, παραμετροποιηθεί και δοκιμαστεί μια υποδομή καταλόγου (Directory Service) που λειτουργεί με το πρωτόκολλο LDAP και κρυπτογράφηση πεδίων (attribute encryption) τα οποία χρειάζονται προστασία. Θα χρειαστεί να γίνουν συγκριτικές δοκιμές λειτουργίας οι οποίες θα αποτυπώνουν το σχετικό φορτίο λόγω της κρυπτογράφησης κατά την εγγραφή και ανάγνωση/αναζήτηση σε περιβάλλον υψηλής διαθεσιμότητας multimaster. Θα χρειαστεί να αποτυπωθεί ο τρόπος με τον οποίο γίνεται η διαχείριση και ο κύκλος ζωής των κλειδιών (π.χ. ανά πεδίο, χρήστη ή/και εφαρμογή), και πώς επηρεάζονται οι λίστες πρόσβασης (ACL) του υποσυστήματος καταλόγου.

Σχετικοί σύνδεσμοι:
[1] Σχετικά RFC με το LDAP https://ldap.com/ldap-related-rfcs/
[2] Υποψήφιο λογισμικό ανοικτού κώδικα DS389 https://directory.fedoraproject.org/ και τεκμηρίωση στο https://directory.fedoraproject.org/docs/389ds/documentation.html#database

Επικοινωνία: Ε. Δ. Συκάς (sykas@cn.ntua.gr), Δ. Καλογεράς (dkalo@noc.ntua.gr)