# An implementation of Zero Trust Architecture to secure sensitive data.

Αναγνωστόπουλος Άγγελος Νικόλαος up1066593

Επιβλέπων: Φείδας Χρήστος

Πανεπιστήμιο Πατρών
Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών

Οκτώβριος 2022

# Το πρόβλημα

Προβλήματα ασφάλειας με το network access management μοντέλο του legacy VPN (Castle and moat).

Roaming users και outsoursing υπηρεσιών σε cloud service providers κάνουν δύσκολο τον ορισμό ενός network perimiter πάνω στο οποίο θα εφαρμοστούν security policies.

# Λύση: Zero trust architecture

1. Collect data for every request and action on network
2. **Remove** implicit **trust from actors** from within the network.
3. **Assume breach.**
4. **Use dynamic policy for accessing requests.**
5. **Authorise and authenticate resources before access is allowed.**
6. Secure communications regardless of location
7. Grant access on per-session basis.

# Μέχρι τώρα

Proprietary implementations (Cloudfare, Google, CISCO κ.α.)

Αρκετές ερευνητικές εργασίες στην αρχιτεκτονική (Και από πανεπιστήμια και grey literature).

Κάθε βέντορας ασχολείται ιδιωτικά με την ευχρηστότητα του προϊόντος, παρόλα αυτά δεν υπάρχει πολλή βιβλιογραφία στο θέμα αλληλεπίδρασης με το χρήστη.

Όλοι παρέχουν λύσεις όμως αυτές είναι κλειστού κώδικα.

# Προτάσεις προς υλοποίηση

Υλοποίηση λογισμικού policy enforcement point για identity based access management.

Υλοποίηση λογισμικού "client – side" για σύνδεση στο δίκτυο.

Γλώσσα συγγραφής πιθανότατα Golang (εναλλακτικά Python).

Ανοιχτά τα πάντα προς το κοινό στο github σαν open source software.

Auditing για κάθε request/event.

# Θέματα που δεν θα εστιάσουμε

Εκτεταμένη υλοποίηση zero trust solutions.

Κάλυψη πολλαπλών πλατφορμών/δικτύων.

# Εφαρμογή - Παρουσίαση

Χρήση των papers της BeyondCorp και της αναφοράς του NIST για το zero trust architecture ώστε να φτιάξουμε ένα user friendly λογισμικό.

Αιτήματα πρόσβασης σε κάποιο resource από διάφορους χρήστες/υπολογιστές (απλό χρήστη, admin, unregistered user, unregistered device).

Συλλογή/Ανάγνωση logs σε κάθε περίπτωση για να δούμε success/failure στα αιτήματα μας.