ΠΛΗΡΟΦΟΡΙΚΟΣ

Περιοδική έκδοση της Ένωσης Πληροφορικών Ελλάδας

Τεύχος 18ο	Οκτώβριος 2022	Διανέμεται ελεύθερα

✔ Πρόσκληση συμμετοχής στην επικείμενη Γενική Συνέλευση το *Σάββατο 22 Οκτωβρίου 2022, ώρα 17:00 (ηλεκτρονικά)* και τις Αρχαιρεσίες της Ένωσης Πληροφορικών Ελλάδας

Αγαπητά μέλη της Ένωσης Πληροφορικών Ελλάδας,

Φέτος συμπληρώνονται 22 χρόνια από την ίδρυση της Ένωσης. Όσες και όσοι την ιδρύσαμε το κάναμε γιατί διαπιστώσαμε την ανάγκη να εκπροσωπηθεί αυθεντικά ο κλάδος μας χωρίς εκπτώσεις σε σχέση με την επιστημονική και επαγγελματική μας ταυτότητα, πέρα από μηχανισμούς που ταλαιπωρούν για δεκαετίας τον λεγόμενο συνδικαλισμό στη χώρα μας.

Σε αυτά τα 22 χρόνια η Ένωση, παρά τις τεράστιες δυσκολίες που οφείλονται στον περιορισμένο αριθμό ενεργών μελών και την εχθρότητα, τολμώ να πω, του πολιτικού προσωπικού απέναντι σε φορείς που κινούνται εκτός του "συστήματος", έχει καταφέρει σημαντικές επιτυχίες. Δεν θα τις απαριθμήσω καθώς νομίζω ότι σας είναι γνωστές...

Η Ένωση βρίσκεται σε ένα σημείο καμπής. Οι ραγδαίες κοινωνικές και τεχνολογικές εξελίξεις στη χώρα μας και παγκοσμίως καθιστούν αναγκαία την ενδυνάμωση της Ένωσης και την ανάδειξη μιας κεντρικής διοίκησης που θα μπορέσει με επάρκεια να ασχοληθεί με τα φλέγοντα προβλήματα του κλάδου μας αλλά και με τα ευρύτερα πολιτικά-κοινωνικά-επιστημονικά ζητήματα που άπτονται της ανάπτυξης και αξιοποίησης των ψηφιακών τεχνολογιών. Χρειαζόμαστε φρέσκες ιδέες και καινούργια πρόσωπα ικανά να συνεγείρουν τα μέλη και δυνάμει μέλη μας διαμορφώνοντας ένα momentum που θα επιταχύνει τις διαδικασίες πραγμάτωσης των προτάσεών μας. Που θα πάρουν

πρωτοβουλίες για να διευρυνθεί ο κύκλος των συνομιλητών της Ένωσης σε διεθνές επίπεδο αξιοποιώντας τους συναδέλφους που σταδιοδρομούν στο εξωτερικό ακαδημαϊκά και επαγγελματικά.

Η Ένωση Πληροφορικών Ελλάδος υπάρχει για να δημιουργεί τις προϋποθέσεις για την προαγωγή της Πληροφορικής, αξιοποιώντας τις δυνάμεις των Πληροφορικών και ικανοποιώντας τις εργασιακές και επιστημονικές τους ανάγκες όπου και αν εργάζονται ή διαμένουν.

Είναι η κατάληξη της αναζήτησης όλων των Πληροφορικών για ένα ισχυρό φορέα του κλάδου που να αναδεικνύει αξιόπιστα τον κοινωνικό τους ρόλο και να τους εκπροσωπεί αυθεντικά σε όλα τα πεδία των ενδιαφερόντων τους.

Είναι η αφετηρία μιας μεγαλόπνοης προσπάθειας που επιδιώκει να κινητοποιήσει όλες τις ζωντανές δυνάμεις της κοινωνίας και να πορευτεί, μαζί μ΄ αυτές, προς έναν καλύτερο κόσμο για όλους.

Αυτά αναφέρει το Όραμά μας και είναι, νομίζω, αξιοσημείωτο ότι ένα κείμενο γραμμένα πριν από 22 χρόνια καθίσταται σήμερα περισσότερο επίκαιρο από ποτέ δεδομένης της διεθνούς συγκυρίας και των απειλών που αντιμετωπίζει σήμερα η ανθρωπότητα. Αλλά και η χώρα μας...

Έχω την πεποίθηση, την είχα από τότε που ιδρύαμε την Ένωση, ότι δημιουργούμε κάτι πολύ σημαντικό που μπορεί να επηρεάσει θετικά το γίγνεσθαι της πατρίδας μας και όχι μόνο. Αρκεί να βρεθούν οι κατάλληλοι Άνθρωποι επικεφαλής. Εμείς οι "παλιοί" επιθυμούμε και είναι βέβαιο ότι θα στηρίξουμε κάθε προσπάθεια της διοίκησης που θα αναδειχθεί στις επικείμενες αρχαιρεσίες. Θα ήταν, όμως, ανακόλουθο προς τις αρχές και τα ιδανικά της Ένωσης οι ίδιοι άνθρωποι να ανακυκλώνονται στο ΔΣ. Γι' αυτό σας καλώ όλες και όλους, ειδικά τα νέα μέλη, να συμμετέχετε μαζικά και ουσιαστικά στην επικείμενη εκλογοαπολογιστική γενική συνέλευση στις 22 Οκτωβρίου 2022. Σας καλώ επίσης να σκεφτείτε σοβαρά το ενδεχόμενο να υποβάλετε υποψηφιότητα για κάποιο από τα 3 κεντρικά όργανα (Διοικητικό Συμβούλιο, Επιτροπή Δεοντολογίας και Ελεγκτική Επιτροπή) ανάλογα και με το χρόνο που μπορείτε να διαθέσετε για την Ένωση.

Νεκτάριος Μουμουτζής

Περιοδική έκδοση της
Ένωσης Πληροφορικών Ελλάδας
www.epe.org.gr

Τεύχος 18ο – Οκτώβριος 2022

Διανέμεται ελεύθερα

Επικοινωνία:
newsletter@epe.org.gr

Συντακτική ομάδα:

- Φώτης Αλεξάκος
- Νίκος Αναστόπουλος
- Χάρης Γεωργίου
- Νεκτάριος Μουμουτζής
- Γιάννης Φαρσάρης

Οι απόψεις των συντακτών είναι προσωπικές και δεν εκφράζουν απαραίτητα την Ένωση Πληροφορικών Ελλάδας

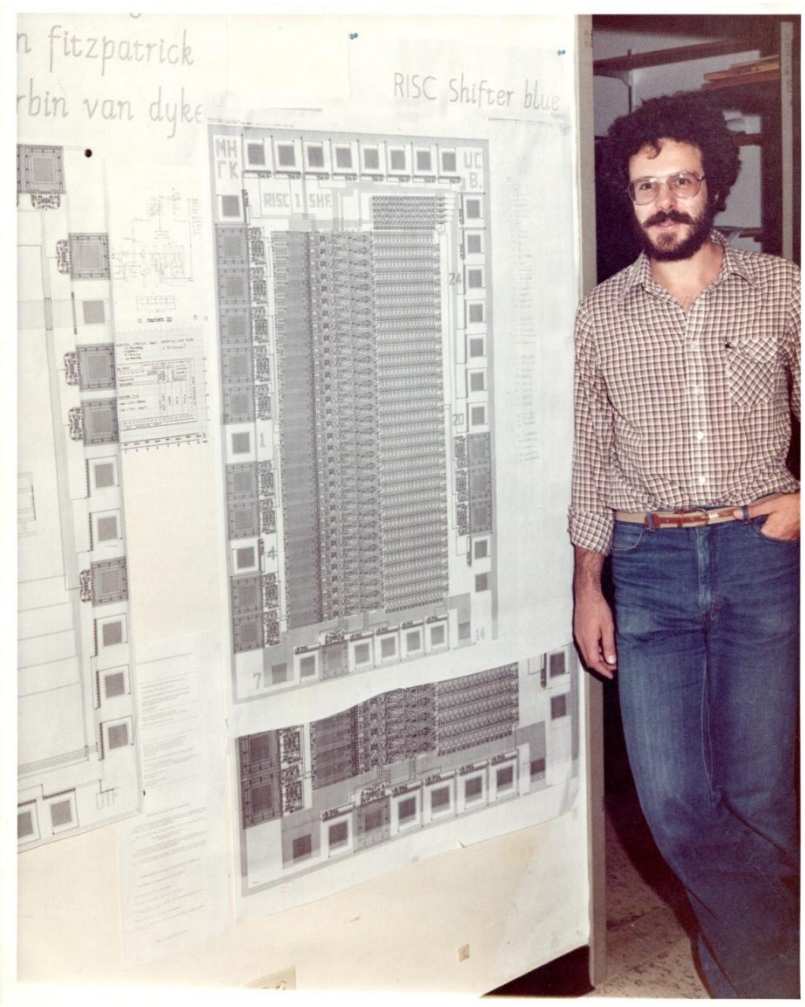
ΠΕΡΙΕΧΟΜΕΝΑ

✔ Συνέντευξη με τον κ. Μανόλη Κατεβαίνη

Καθηγητή στο Τμήμα Επιστήμης Υπολογιστών του Πανεπιστημίου Κρήτης,
Επικεφαλής του Εργαστηρίου Αρχιτεκτονικής Υπολογιστών και
Συστημάτων VLSI του Ινστιτούτου Πληροφορικής,
Ίδρυμα Τεχνολογίας και Έρευνας (ΙΤΕ)

Μανόλης Γ.Η. Κατεβαίνης

Στις αρχές της δεκαετίας του '80 ήσασταν ο πρωτεργάτης της υλοποίησης του μικροεπεξεργαστή RISC-II στο Πανεπιστήμιο της Καλιφόρνιας στο Berkeley, γεγονός που σας απέφερε δύο πολύ σημαντικά βραβεία. Ποιο ήταν το κίνητρο που σας έκανε να επιστρέψετε το 1985 στην Ελλάδα και να προσφέρετε τις υπηρεσίες σας στο νεοϊδρυθέν τότε τμήμα Επιστήμης Υπολογιστών του Πανεπιστημίου Κρήτης στο Ηράκλειο και στο Ίδρυμα Τεχνολογίας και Έρευνας;



1981: ο Μανόλης Κατεβαίνης στη διάρκεια των διδακτορικών του σπουδών στο Berkeley, μπροστά σε ένα checkplot του ολισθητή που μόλις είχε σχεδιάσει για τον επεξεργαστή RISC-I

Το βασικό μου κίνητρο ήταν και είναι η αγάπη για την Ελλάδα, μαζί και μ' ένα αίσθημα καθήκοντος να προσφέρω στην πατρίδα μου. Αυτά τα είχα μέσα μου από παιδί, αλλά δυνάμωσαν ιδιαίτερα στη διάρκεια των προπτυχιακών μου σπουδών στο Πολυτεχνείο της Αθήνας, τα χρόνια εκείνα που μας και με σημάδεψαν –1973 έως 1978– κι έτσι από την πρώτη κιόλας στιγμή που έφυγα για μεταπτυχιακά ήθελα να ξαναγυρίσω. Επιπροσθέτως, ο Αμερικανικός τρόπος ζωής και η νοοτροπία των ανθρώπων εκεί διαφέρουν σημαντικά απ' ό,τι στην Ευρώπη, κι ακόμα περισσότερο από την Ελλάδα, κι έτσι δεν αισθάνθηκα ποτέ ότι μου ταίριαζε η Βόρεια Αμερική. Κι ακόμη, ένιωθα ότι η συνεισφορά μου στην τεχνολογία και στην πρόοδο της κοινωνίας θα αποτελούσε σταγόνα εν τω ωκεανώ σ' εκείνη την απέραντη χώρα, ενώ εδώ στην πατρίδα μου θα μπορούσε ίσως αυτή να είναι ορατή –να «πιάσει τόπο», λίγο.

Υποδέχεστε τους πρωτοετείς φοιτητές σας στο μάθημα «Ψηφιακή Σχεδίαση» με ένα υπέροχο εμπνευσμένο κείμενο και πιο πρόσφατα με διαφάνειες. Πιστεύετε πως οι νέοι επιστήμονες της Πληροφορικής θα μπορούσαν να αποτελέσουν πυρήνα σημαντικών διεργασιών και αλλαγών στη χώρα μας;

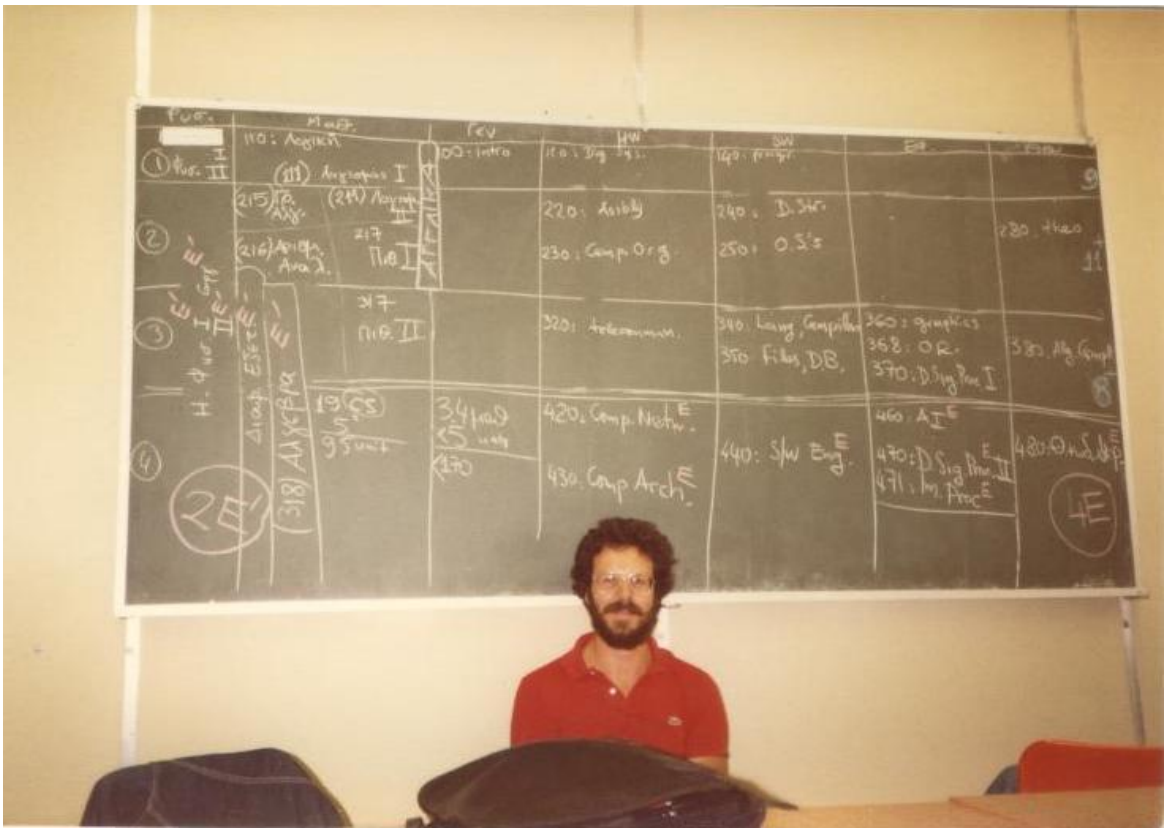
Όχι απλώς «θα μπορούσαν», αλλά είναι *απαραίτητοι* και αποτελούν *προϋπόθεση* για να προοδεύσει η χώρα μας –όπως συμβαίνει και παντού ανά τον κόσμο εξ άλλου– και επίσης ήδη το κάνουν, όχι μόνο οι νέοι αλλά και όλοι οι επιστήμονες Πληροφορικής. Αφ' ενός το gov.gr καθώς και ο νέος, ψηφιοποιημένος τρόπος λειτουργίας της οικονομικής και κοινωνικής ζωής το δείχνουν ανάγλυφα, αφ' ετέρου η ύπαρξη σημαντικού αριθμού καλά εκπαιδευμένων τέτοιων επιστημόνων αποτελεί ίσως τον σημαντικότερο παράγοντα έλξης διεθνών επενδύσεων και εταιρειών υψηλής τεχνολογίας στη χώρα μας, καθώς και φυτώριο ανάπτυξης εγχώριων καινοτόμων τεχνολογικών εταιρειών. Επίσης, πρέπει να τονίσουμε ότι όχι μόνο δεν υπάρχει κίνδυνος ανεργίας των Πληροφορικών εάν υπάρξουν πολλοί περισσότεροι τέτοιοι απόφοιτοι, αλλά αντίθετα το να υπάρξουν πολλοί περισσότεροι –και καλοί!– τέτοιοι απόφοιτοι είναι αυτό που θα επιταχύνει την πρόοδο της χώρας.

Ιούλιος 1984: Συνέλευση Τμήματος Επιστήμης Υπολογιστών Π.Κ., Πτέρυγα Γ κτιρίου Κνωσού, κάτω επίπεδο. Από αριστερά: Στέλιος Ορφανουδάκης, Χρίστος Χαμζάς, Διονύσης Τσιχριτζής, Γιάννης Βασιλείου, Γιάννης Μυλόπουλος, άλλος συνεργάτης, Μανόλης Κατεβαίνης, Βαγγέλης Γερανιώτης, Καίτη Χούστη, Θανάσης Καμπουρέλης, και πίσω από το φακό ο φωτογράφος που δεν φαίνεται: Πάνος Κωνσταντόπουλος

Η δημιουργική σας συνεισφορά αφορά πρωτίστως την Ευρώπη, όμως έχετε σπουδάσει και εργαστεί για χρόνια στην Αμερική. Τι είναι αυτό που πιστεύετε πως κάνει τους δύο αυτούς κόσμους διαφορετικούς;

Από τη μια, οι Αμερικάνοι έχουν το πλεονέκτημα της αμεσότητας, της πρακτικότητας, και της ενεργητικότητας στη λύση των προβλημάτων: όταν υπάρχει ένα πρόβλημα, «βουτάνε μεσ' τα όλα» και επιδιώκουν να το λύσουν στην πράξη ("just do it"). Έτσι βρίσκουν πρόσφορο έδαφος και οι τεχνοβλαστοί και αναπτύσσονται. Οι Ευρωπαίοι πρέπει να διδαχτούμε από αυτό: να μην αφήνουμε να μας καθυστερούν η αίσθηση ότι έχουμε όλο το χρόνο στη διάθεσή μας, ή οι ατέρμονες θεωρητικολογίες, ή οι υπερβολικές προσπάθειες επίτευξης συναίνεσης, ή οι γραφειοκρατίες.

Από την άλλη, η Ευρώπη έχει καλύτερη ποιότητα ζωής, και νομίζω και ανθρώπους που νοιάζονται περισσότερο ο ένας για τον άλλον, και αυτό πρέπει να το διατηρήσουμε.



Μετά τη Συνέλευση Τμήματος του Ιουλίου 1984, το πρώτο Πρόγραμμα Σπουδών του Τμήματος Επιστήμης Υπολογιστών Π.Κ. όπως αυτή το καθόρισε και όπως το κατέγραψε στον πίνακα ο Μανόλης Κατεβαίνης

Εργάζεστε σήμερα, μεταξύ άλλων, πάνω στη δημιουργία του Ευρωπαϊκού Επεξεργαστή RISC-V. Μιλήστε μας για τις καινοτομίες που ετοιμάζετε.

Η δουλειά μας στον Ευρωπαϊκό Επεξεργαστή είναι όλων των μελών του Εργαστηρίου Αρχιτεκτονικής Υπολογιστών και Συστημάτων VLSI (Εργαστήριο CARV) του Ινστιτούτου Πληροφορικής του ΙΤΕ, και όχι εμένα προσωπικά. Η Ευρώπη συνειδητοποίησε πριν περίπου δέκα χρόνια ότι οι επεξεργαστές αποτελούν βασική υποδομή για τη σύγχρονη κοινωνία, και άρα έχει μεγάλη σημασία η αυτοτέλεια (όπως το συνειδητοποιούμε τώρα ακόμα, δυστυχώς, και σε άλλους κρίσιμους τομείς όπως η ενέργεια), και ότι έχει μείνει πίσω σε σχέση με την Άπω Ανατολή και με τις ΗΠΑ σε αυτόν τον τομέα – κι έτσι ξεκίνησε το εμβληματικό αυτό έργο για να ανακτήσει το χαμένο έδαφος. Η καλλιέργεια αυτού του Ευρωπαϊκού Οικοσυστήματος της σχεδίασης επεξεργαστών στηρίζεται σε δύο ρεπερτόρια εντολών (instruction sets) μεγάλης σημασίας: το ρεπερτόριο ARM που προσφέρει άμεση πρόσβαση στην αγορά, και το ρεπερτόριο RISC-V που ναι μεν θα αποδώσει καρπούς πιο μακροπρόθεσμα, αλλά από την άλλη προσφέρει πραγματική αυτοτέλεια χάρις στο εντελώς ανοικτό (open) της προδιαγραφής του. Θεωρείται σήμερα πιθανό το ανοικτό ρεπερτόριο RISC-V να φέρει στο hardware την επανάσταση που έφερε στα λειτουργικά συστήματα το επίσης ανοικτό LINUX. Εντός του Ευρωπαϊκού Επεξεργαστή, εμείς εργαζόμαστε περισσότερο στο κομμάτι RISC-V. Η Ελλάδα, και ιδιαίτερα το Εργαστήριο CARV, συνεισφέρουμε σε κάμποσα θέματα, με έμφαση στο λογισμικό συστήματος και στον FPGA emulator όπου αναπτύσσεται αυτό, και σε καινοτόμες μεθόδους διαχείρισης της συνοχής των κρυφών μνημών (cache coherence), στην IOMMU (συσκευές εισόδου/εξόδου που λειτουργούν με εικονικές διευθύνσεις και πώς αυτές μεταφράζονται σε φυσικές), και σε διεπαφές δικτύου (network interfaces) που συνδέονται στενά με τον επεξεργαστή και επικοινωνούν μαζί του εντός ολίγων κύκλων ρολογιού μόνο, και χωρίς κάλεσμα λειτουργικού συστήματος. Για περισσότερες πληροφορίες σχετικά με την Ελλάδα σε σχέση με τον Ευρωπαϊκό Επεξεργαστή και την έρευνα σε Υπερυπολογιστές (HPC) – 5η ανάμεσα στις χώρες της Ευρώπης η Ελλάδα σε αυτούς τους τομείς– προτείνω το άρθρο μου στις σελίδες 7-8 του 5ου τεύχους (καλοκαίρι 2022) του περιοδικού «Τρίτων» του Πανεπιστημίου Κρήτης.

Πρώτο δοκιμαστικό chip του Ευρωπαϊκού Επεξεργαστή RISC-V που έδωσε τα πρώτα σημάδια ζωής του στην Κρήτη το Σεπτέμβριο 2021

Ποιον άνθρωπο της Επιστήμης των Υπολογιστών αληθινά θαυμάζετε; (Είτε ιστορικό πρόσωπο, είτε σύγχρονο)

Πολλούς θαυμάζουμε όλοι μας, κι εγώ μαζί. Εμένα προσωπικά, επειδή και τον γνώρισα καλά, ο πρώτος που μου έρχεται στο μυαλό είναι ο co-advisor του διδακτορικού μου, David Patterson –που όρισε την αρχιτεκτονική των επεξεργαστών RISC-I και RISC-II, και εισήγαγε και το όνομα "RISC" (Reduced Instruction Set Computer), εμπνευστής και του RISC-V, και αποδέκτης και του Βραβείου Turing 2018 της ACM (κάτι σαν το Νόμπελ της Πληροφορικής) μαζί με τον John Hennessy (και συγγραφείς των βιβλίων που αναφέρω παρακάτω). Θαυμάζω επίσης και τους εμπνευστές των καινοτόμων εταιρειών υψηλής τεχνολογίας του χώρου μας, με πρώτην εκείνην που είδα να ξεπηδά από τους χώρους που βρέθηκα κι εγώ νέος, την SUN Microsystems.

Μάρτιος 2021 (επί κορωνοϊού): ο Μανόλης Κατεβαίνης με τη βοήθεια του γιού του Γιώργου φυτεύουν το δεύτερο δέντρο που δώρισε έξω από την είσοδο του Τμ. Επ. Υπολογιστών Π.Κ., έναν Φίκο

Θα θέλατε να μας προτείνετε 3 βιβλία που αξίζει να διαβάσουμε;

Δεν ξέρω για εσάς τι αξίζει να διαβάσετε. Θα σας πω τρία πολύ ετερογενή βιβλία που για εμένα έχουν μεγάλη αξία. Πρώτον, στην επιστημονική μου περιοχή, το ζευγάρι βιβλίων *Οργάνωσης - Αρχιτεκτονικής Υπολογιστών* των Patterson & Hennessy που ανέφερα προηγουμένως –αυτά που διδάσκουμε κι εμείς στο Πανεπιστήμιο Κρήτης (την Οργάνωση, την έκδοση RISC-V), όπως τα διδάσκουν και σε πάμπολλα άλλα μέρη. Δεύτερον, στην Πληροφορική γενικά, αλλά απευθυνόμενο στο ευρύ κοινό –καλό και για τις σχολικές ηλικίες για να εισάγει και προσελκύσει μαθητές στην Πληροφορική: *«Εννέα Αλγόριθμοι που άλλαξαν το Μέλλον – Οι εκπληκτικές ιδέες που κινούν τους σημερινούς υπολογιστές»*, από τον John McCormick, σε Ελληνική μετάφραση από τις Πανεπιστημιακές Εκδόσεις Κρήτης. Το τρίτο βιβλίο είναι πολύ διαφορετικό – με είχε επηρεάσει σημαντικά όταν ήμουν στην Αμερική και θα γύριζα στην Ελλάδα, και είχα βρει μέσα του πολλά και δικά μου στοιχεία: η *«Αναφορά στον Γκρέκο»* του Νίκου Καζαντζάκη.

Το κτίριο Επιστήμης Υπολογιστών Π.Κ. στα Βασιλικά Βουτών, όπου μετακόμισε το Τμήμα την Άνοιξη του 2013.
Μπροστά στην είσοδο, ο Πλάτανος που φύτεψε στις 9/5/2013 και έκτοτε ποτίζει ο Μανόλης Κατεβαίνης (φωτογραφία: Οκτ. 2016)

Ποια συμβουλή θα δίνατε σήμερα σ' έναν φοιτητή ή νέο απόφοιτο της Πληροφορικής;

Να αγαπάει με πάθος αυτό που κάνει! Μόνο αν το αγαπάει μπορεί να το κάνει καλά. Αν δεν αγαπάει την Πληροφορική, θα πρέπει να βρει κάτι άλλο που αγαπάει, και εκείνο να κάνει. Τα υπόλοιπα έρχονται σχεδόν από μόνα τους: χρειάζεται σοβαρότητα, ποιότητα, εργατικότητα, υπευθυνότητα, συνέπεια, επαγγελματισμός –αλλά όταν αγαπάμε, αυτά έρχονται σαν συνέπειες. Και να αφήσει τη δημιουργικότητά του ελεύθερη. Και να στέργει να κατανοεί όλα τα πράγματα σε βάθος –από την βαθιά κατανόηση πηγάζει η καλή η λύση.

✔ Μια βαθιά επισκόπηση σε ένα μηδενικού κλικ exploit του iMessage από την NSO: Απομακρυσμένη εκτέλεση κώδικα

Δημοσιεύτηκε από τους ***Ian Beer & Samuel Groß*** *του* ***Google Project Zero***

// Μετάφραση: ***Νικόλας Αναστόπουλος***

Νωρίτερα φέτος, το Citizen Lab κατάφερε να καταγράψει ένα exploit μηδενικού κλικ της NSO που βασίζεται στο iMessage το οποίο χρησιμοποιήθηκε για να στοχεύσει έναν Σαουδάραβα ακτιβιστή. Σε αυτήν τη σειρά αναρτήσεων, θα περιγράψουμε για πρώτη φορά πώς λειτουργεί ένα μηδενικό κλικ στο iMessage.

Με βάση την έρευνα και τα ευρήματά μας, εκτιμούμε ότι αυτό είναι ένα από τα πιο εξελιγμένα τεχνικά κατορθώματα που έχουμε δει ποτέ, αποδεικνύοντας περαιτέρω ότι οι δυνατότητες που παρέχει η NSO ξεπερνάει εκείνες που προηγουμένως θεωρούνταν προσβάσιμες μόνο σε λίγα κράτη.

Η ευπάθεια που συζητήθηκε σε αυτήν την ανάρτηση διορθώθηκε στις 13 Σεπτεμβρίου 2021 στο iOS 14.8 ως CVE-2021-30860.

NSO

Ο Όμιλος NSO είναι ένας από τους διασημότερους παρόχους «πρόσβασης ως υπηρεσίας» ("access-as-a-service"), ο οποίος εμπορεύεται έτοιμες λύσεις hacking που επιτρέπουν σε φορείς επιπέδου κρατών, χωρίς εγχώρια επιθετική ικανότητα στον κυβερνοχώρο, να «πληρώσουν για να παίξουν» ("pay-to-play"), επεκτείνοντας σε μεγάλο βαθμό τον αριθμό των εθνών με τέτοιες δυνατότητες στον κυβερνοχώρο.

Για χρόνια, ομάδες όπως το Citizen Lab και η Διεθνής Αμνηστία παρακολουθούν τη χρήση του πακέτου λογισμικού κατασκοπείας για κινητά της NSO "Pegasus". Παρά τους ισχυρισμούς της NSO ότι «[αξιολογούν] τις πιθανές αρνητικές επιπτώσεις στα ανθρώπινα δικαιώματα που προκύπτουν από την κακή χρήση προϊόντων της NSO», το Pegasus έχει συνδεθεί με το χακάρισμα του δημοσιογράφου των New York Times Μπεν Χάμπαρντ από το καθεστώς της Σαουδικής Αραβίας, το χακάρισμα υπερασπιστών ανθρωπίνων δικαιωμάτων στο Μαρόκο και Μπαχρέιν, την στοχοποίηση προσωπικού της Διεθνούς Αμνηστίας και δεκάδες άλλες υποθέσεις.

Τον περασμένο μήνα, οι Ηνωμένες Πολιτείες πρόσθεσαν την NSO στη «λίστα οντοτήτων» ("Entity List"), περιορίζοντας σοβαρά τη δυνατότητα των αμερικανικών εταιρειών να συναλλάσσονται με την NSO και αναφέροντας σε ένα δελτίο τύπου ότι «[τα εργαλεία της NSO] επέτρεψαν στις ξένες κυβερνήσεις να διεξάγουν διεθνική καταστολή, όπως είναι η πρακτική αυταρχικών κυβερνήσεων που στοχεύουν αντιφρονούντες, δημοσιογράφους και ακτιβιστές εκτός των κυρίαρχων συνόρων τους για να φιμώσουν τους διαφωνούντες».

Το Citizen Lab μπόρεσε να ανακτήσει αυτά τα Pegasus exploits από ένα iPhone και επομένως αυτή η ανάλυση καλύπτει τις δυνατότητες της NSO έναντι του iPhone. Γνωρίζουμε ότι η NSO εμπορεύεται παρόμοιες δυνατότητες μηδενικού κλικ που στοχεύουν συσκευές Android· το Project Zero δεν έχει δείγματα αυτών των exploits, αλλά αν έχετε, παρακαλώ επικοινωνήστε.

Από το ένα στο μηδέν

Σε προηγούμενες περιπτώσεις, όπως το Million Dollar Dissident από το 2016, στους στόχους στάλθηκαν μηνύματα SMS με σύνδεσμους:

Στιγμιότυπα οθόνης από μηνύματα ηλεκτρονικού «ψαρέματος» που αναφέρθηκαν στο Citizen Lab το 2016

πηγή:
https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

Ο στόχος παραβιάστηκε μόνο όταν έκαναν κλικ στον σύνδεσμο, μια τεχνική γνωστή ως exploit μοναδικού κλικ ("one-click"). Πρόσφατα, ωστόσο, έχει τεκμηριωθεί ότι η NSO προσφέρει στους πελάτες της τεχνολογία exploits μηδενικού κλικ ("zero-click"), όπου ακόμη και τεχνικά πολύ έμπειροι στόχοι που ενδέχεται να μην έκαναν κλικ σε έναν σύνδεσμο ηλεκτρονικού «ψαρέματος» ("phishing"), δεν γνωρίζουν καν ότι στοχεύονται. Στο σενάριο μηδενικού κλικ δεν απαιτείται αλληλεπίδραση χρήστη. Αυτό σημαίνει ότι ο εισβολέας δεν χρειάζεται να στέλνει μηνύματα ηλεκτρονικού «ψαρέματος»· το exploit λειτουργεί απλώς αθόρυβα στο παρασκήνιο . Εκτός από τη μη χρήση κάποιας συσκευής, δεν υπάρχει τρόπος να αποτραπεί ένα exploit μηδενικού κλικ· είναι ένα όπλο ενάντια στο οποίο δεν υπάρχει άμυνα.

Ένα περίεργο κόλπο

Το αρχικό σημείο εισόδου για το Pegasus στο iPhone είναι το iMessage. Αυτό σημαίνει ότι ένα θύμα μπορεί να στοχευτεί χρησιμοποιώντας τον αριθμό τηλεφώνου του ή το όνομα χρήστη του Apple ID του.

Το iMessage έχει εγγενή υποστήριξη για εικόνες GIF, τις τυπικά μικρές και χαμηλής ποιότητας κινούμενες εικόνες που είναι δημοφιλείς στην κουλτούρα των μιμιδίων. Μπορείτε να στέλνετε και να λαμβάνετε GIF σε συνομιλίες iMessage και αυτά εμφανίζονται στο παράθυρο συνομιλίας. Η Apple ήθελε να κάνει αυτά τα GIF να επαναλαμβάνονται ατελείωτα αντί να παίζουν μόνο μία φορά, οπότε πολύ νωρίς στη αλυσίδα ανάλυσης και επεξεργασίας του iMessage (μετά τη λήψη ενός μηνύματος αλλά πολύ πριν από την εμφάνιση του μηνύματος), το iMessage καλεί την ακόλουθη μέθοδο στη διεργασία IMTranscoderAgent (εκτός του "BlastDoor" sandbox), περνώντας σε αυτή οποιοδήποτε αρχείο εικόνας που λαμβάνεται με την επέκταση .gif:

[IMGIFUtils copyGifFromPath:toDestinationPath:error]

Κοιτάζοντας το όνομα της μεθόδου, η πρόθεση εδώ ήταν πιθανώς να

αντιγραφτεί απλώς το αρχείο GIF πριν γίνει επεξεργασία του πεδίου μέτρησης βρόχου ("counter"), αλλά η σημασιολογία αυτής της μεθόδου είναι διαφορετική. Κάτω από το καπό χρησιμοποιεί το CoreGraphics API για να *αποδώσει ("render")* την πηγαία εικόνα σε ένα νέο αρχείο GIF στη διαδρομή προορισμού. Και επειδή το όνομα του αρχείου προέλευσης πρέπει να τελειώνει σε .gif , αυτό δεν σημαίνει ότι είναι πραγματικά ένα αρχείο GIF.

Η βιβλιοθήκη ImageIO, όπως περιγράφεται λεπτομερώς σε προηγούμενη ανάρτηση του Project Zero, χρησιμοποιείται για να μαντέψει τη σωστή μορφή του πηγαίου αρχείου και να το αναλύσει ("parse"), αγνοώντας εντελώς την επέκταση του αρχείου. Χρησιμοποιώντας αυτό το τέχνασμα «ψεύτικου gif», πάνω από 20 κωδικοποιητές εικόνων ξαφνικά αποτελούν μέρος της επιφάνειας επίθεσης μηδενικού κλικ του iMessage, συμπεριλαμβανομένων ορισμένων πολύ σκοτεινών και πολύπλοκων φορμά, εκθέτοντας εξ αποστάσεως πιθανώς εκατοντάδες χιλιάδες γραμμές κώδικα.

Σημείωση: Η Apple μας ενημερώνει ότι έχει περιορίσει τα διαθέσιμα φορμά του ImageIO προσβάσιμα από το IMTranscoderAgent ξεκινώντας από το iOS 14.8.1 (26 Οκτωβρίου 2021) και έχει αφαιρέσει εντελώς τη διαδρομή κώδικα GIF από το IMTranscoderAgent ξεκινώντας από το iOS 15.0 (20 Σεπτεμβρίου 2021), με την αποκωδικοποίηση GIF να πραγματοποιείται εξ ολοκλήρου εντός του BlastDoor.

Ένα PDF στο GIF σας

Η NSO χρησιμοποιεί το τέχνασμα «ψεύτικου gif» για να στοχεύσει μια ευπάθεια στον αναλυτή ("parser") PDF του CoreGraphics.

Το PDF ήταν ένας δημοφιλής στόχος για εκμετάλλευση πριν από περίπου μια δεκαετία, λόγω της πανταχού παρουσίας και της πολυπλοκότητάς του. Επιπλέον, η διαθεσιμότητα JavaScript μέσα σε αρχεία PDF έκανε την ανάπτυξη αξιόπιστων exploits πολύ πιο εύκολη. Ο αναλυτής ("parser") PDF του CoreGraphics δεν *φαίνεται* να ερμηνεύει τη JavaScript, αλλά η NSO κατάφερε να βρει κάτι εξίσου ισχυρό μέσα στον αναλυτή ("parser") PDF του CoreGraphics...

Ακραία συμπίεση

Στα τέλη της δεκαετίας του 1990, το εύρος ζώνης και ο αποθηκευτικός χώρος ήταν πολύ πιο σπάνια από ό,τι είναι τώρα. Σε αυτό το περιβάλλον εμφανίστηκε το πρότυπο JBIG2. Το JBIG2 είναι ένας εξειδικευμένος κωδικοποιητής εικόνων που έχει σχεδιαστεί για τη συμπίεση εικόνων που τα εικονοστοιχεία μπορεί να είναι μόνο μαύρα ή λευκά.

Αναπτύχθηκε για την επίτευξη εξαιρετικά υψηλών αναλογιών συμπίεσης για σαρώσεις εγγράφων κειμένου και υλοποιήθηκε και χρησιμοποιήθηκε σε συσκευές σαρωτών/εκτυπωτών γραφείου προηγμένης τεχνολογίας, όπως η συσκευή XEROX WorkCentre που φαίνεται παρακάτω. Εάν χρησιμοποιήσατε τη λειτουργία *σάρωσης σε PDF* σε μια συσκευή όπως αυτή πριν από μια δεκαετία, το PDF σας πιθανότατα είχε μέσα μια ροή JBIG2.

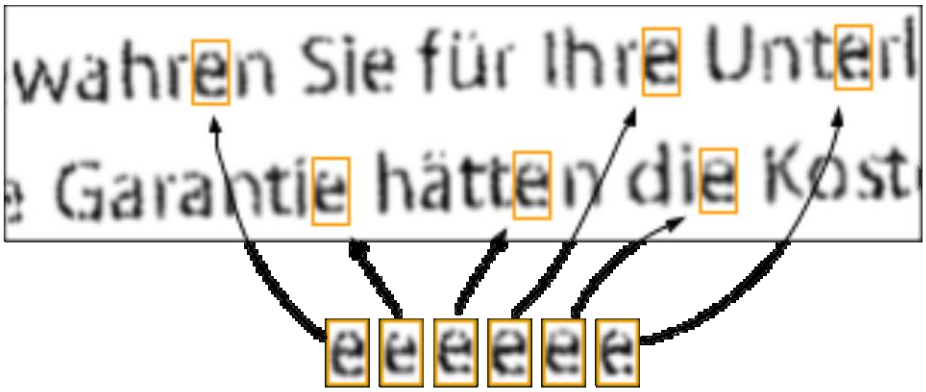
Ένας πολυλειτουργικός εκτυπωτής Xerox WorkCentre 7500 series, ο οποίος χρησιμοποιούσε JBIG2 για τη λειτουργία σάρωσης σε PDF

(Πηγή: https://www.office.xerox.com/en-us/multifunction-printers/workcentre-7545-7556/specifications)

Τα αρχεία PDF που παράγονται από αυτούς τους σαρωτές ήταν εξαιρετικά μικρά, ίσως μόνο μερικά kilobytes. Υπάρχουν δύο καινοτόμες τεχνικές που χρησιμοποιεί το JBIG2 για να επιτύχει αυτούς τους ακραίους λόγους συμπίεσης οι οποίες σχετίζονται με αυτό το exploit:

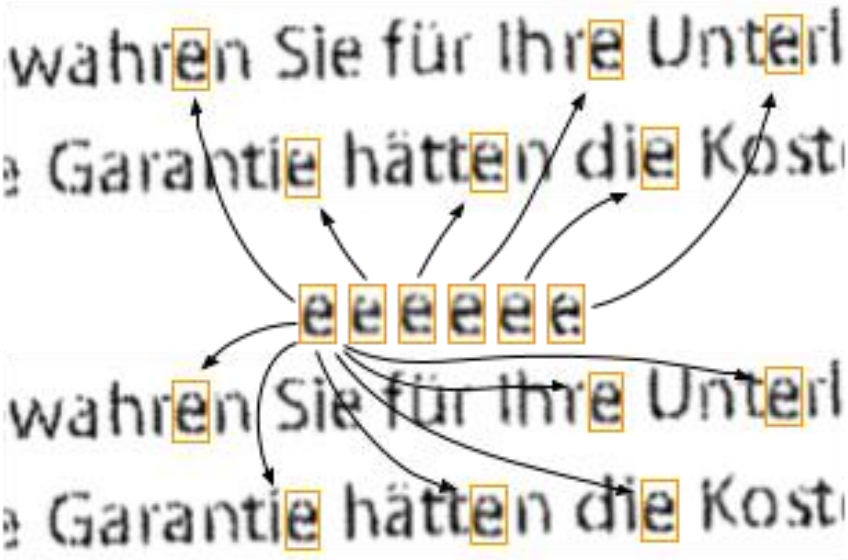
Τεχνική 1: Τμηματοποίηση και αντικατάσταση

Ουσιαστικά, κάθε έγγραφο κειμένου, ειδικά αυτά που είναι γραμμένα σε γλώσσες με μικρά αλφάβητα όπως τα αγγλικά ή τα γερμανικά, αποτελείται από πολλά επαναλαμβανόμενα γράμματα (επίσης γνωστά ως γλυφές / glyphs) σε κάθε σελίδα. Το JBIG2 προσπαθεί να τμηματοποιήσει κάθε σελίδα σε γλυφές και στη συνέχεια χρησιμοποιεί απλή αντιστοίχιση μοτίβων για να ταιριάξει τους γλυφούς που μοιάζουν:



Η απλή αντιστοίχιση μοτίβων μπορεί να βρει όλα τα σχήματα που μοιάζουν σε μια σελίδα, εν προκειμένω όλα τα 'e'

Το JBIG2 στην πραγματικότητα δεν γνωρίζει τίποτα για τους γλυφούς και δεν κάνει OCR (οπτική αναγνώριση χαρακτήρων.) Ένας κωδικοποιητής JBIG απλώς αναζητά συνδεδεμένες περιοχές εικονοστοιχείων και ομαδοποιεί περιοχές παρόμοιας εμφάνισης μαζί. Ο αλγόριθμος συμπίεσης είναι απλώς να αντικαταστήσει όλες τις επαρκώς παρόμοιες περιοχές με ένα αντίγραφο μόνο μιας εξ αυτών:



Η αντικατάσταση όλων των εμφανίσεων παρόμοιων γλυφών με το αντίγραφο μόνο ενός, συχνά οδηγεί σε ένα έγγραφο που εξακολουθεί να είναι αρκετά ευανάγνωστο και επιτρέπει πολύ υψηλούς λόγους συμπίεσης

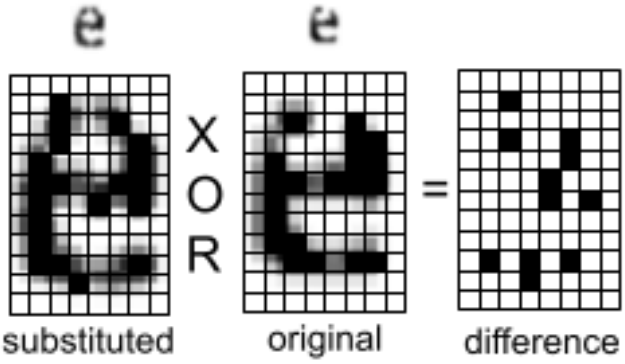
Σε αυτή την περίπτωση η έξοδος είναι αναγνώσιμη τέλεια, αλλά ο όγκος των πληροφοριών που πρέπει να αποθηκευτεί μειώνεται σημαντικά. Αντί να χρειάζεται να αποθηκεύσετε όλες τις αρχικές πληροφορίες εικονοστοιχείων για ολόκληρη τη σελίδα, χρειάζεστε μόνο μια συμπιεσμένη έκδοση του «γλύφου αναφοράς» για κάθε χαρακτήρα και τις σχετικές συντεταγμένες όλων των σημείων όπου πρέπει να παραχθούν τα αντίγραφα. Στη συνέχεια, ο αλγόριθμος αποσυμπίεσης αντιμετωπίζει τη σελίδα εξόδου σαν καμβά και «σχεδιάζει» τον ίδιο ακριβώς γλύφο σε όλες τις αποθηκευμένες τοποθεσίες.

Υπάρχει ένα σημαντικό ζήτημα σε ένα τέτοιο σχέδιο: είναι πολύ εύκολο για έναν φτωχά υλοποιημένο κωδικοποιητή να ανταλλάξει κατά λάθος παρόμοιους χαρακτήρες και αυτό μπορεί να συμβεί με ενδιαφέρουσες συνέπειες. Το ιστολόγιο του D. Kriesel έχει μερικά ενθαρρυντικά παραδείγματα που τα PDF σαρωμένων τιμολογίων έχουν διαφορετικά ψηφία ή τα PDF σαρωμένων κατασκευαστικών σχεδίων καταλήγουν με λανθασμένες μετρήσεις. Αυτά δεν είναι τα ζητήματα που εξετάζουμε, αλλά είναι ένας σημαντικός λόγος για τον οποίο το JBIG2 δεν είναι πλέον μια κοινή μορφή συμπίεσης.

Τεχνική 2: Κωδικοποίηση βελτίωσης

Όπως αναφέρθηκε παραπάνω, η έξοδος συμπίεσης με βάση την αντικατάσταση έχει απώλεια. Μετά από έναν γύρο συμπίεσης και αποσυμπίεσης, η απόδοση ("render") της εξόδου δεν μοιάζει ακριβώς με την είσοδο. Αλλά το JBIG2 υποστηρίζει επίσης συμπίεση χωρίς απώλεια καθώς και μια ενδιάμεση λειτουργία συμπίεσης με «λιγότερη απώλεια».

Αυτό το κάνει αποθηκεύοντας (και συμπιέζοντας) τη *διαφορά* μεταξύ του αντικατεστημένου γλυφού και κάθε αρχικού γλυφού. Ακολουθεί ένα παράδειγμα που δείχνει μια μάσκα διαφοράς μεταξύ ενός αντικατεστημένου χαρακτήρα στα αριστερά και του αρχικού χαρακτήρα χωρίς απώλεια στη μέση:



Χρήση του τελεστή XOR σε bitmaps για τον υπολογισμό μιας διαφοράς εικόνας

Σε αυτό το απλό παράδειγμα, ο κωδικοποιητής μπορεί να αποθηκεύσει τη μάσκα διαφοράς που εμφανίζεται στα δεξιά, και στη συνέχεια κατά τη διάρκεια της αποσυμπίεσης η μάσκα διαφοράς μπορεί να εφαρμόσει τον τελεστή XOR με τον αντικατεστημένο χαρακτήρα για να ανακτήσει τα ακριβή εικονοστοιχεία που αποτελούν τον αρχικό χαρακτήρα. Υπάρχουν μερικά ακόμη κόλπα εκτός του πεδίου αυτής της ανάρτησης για περαιτέρω συμπίεση αυτής της μάσκας διαφοράς χρησιμοποιώντας τις ενδιάμεσες μορφές του υποκατεστημένου χαρακτήρα ως «πλαίσιο» για τη συμπίεση.

Αντί να κωδικοποιήθει πλήρως ολόκληρη η διαφορά ένα πέρασμα, μπορεί να γίνει σε βήματα, με κάθε επανάληψη να χρησιμοποιεί έναν λογικό τελεστή (ένα από τα AND, OR, XOR ή XNOR) ώστε να ορίσει, να διαγράψει ή να αναστρέψει bits. Κάθε διαδοχικό βήμα βελτίωσης φέρνει την απόδοση της εξόδου πιο κοντά στην αρχική εικόνα και αυτό επιτρέπει ένα επίπεδο ελέγχου της «απώλειας» της συμπίεσης. Η υλοποίηση αυτών των βημάτων βελτίωσης της κωδικοποίησης είναι πολύ ευέλικτη και μπορούν επίσης να «διαβάσουν» τιμές που υπάρχουν ήδη στον καμβά εξόδου.

Μια ροή JBIG2

Το μεγαλύτερο μέρος του αποκωδικοποιητή PDF του Core Graphics φαίνεται να είναι κλειστός κώδικας της Apple, αλλά η υλοποίηση JBIG2 προέρχεται από το Xpdf, ο πηγαίος κώδικας του οποίου διατίθεται δωρεάν.

Το φορμά JBIG2 είναι μια σειρά τμημάτων, τα οποία μπορούν να θεωρηθούν ως μια σειρά από εντολές σχεδίασης που εκτελούνται διαδοχικά σε ένα μόνο πέρασμα. Ο αναλυτής (“parser”) JBIG2 του CoreGraphics υποστηρίζει 19 διαφορετικούς τύπους τμημάτων που περιλαμβάνουν λειτουργίες όπως ο ορισμός μιας νέας σελίδας, η αποκωδικοποίηση ενός πίνακα Huffman ή η απόδοση (“rendering”) ενός bitmap σε δεδομένες συντεταγμένες στη σελίδα.

Τα τμήματα αντιπροσωπεύονται από την κλάση JBIG2Segment και τις υποκλάσεις της JBIG2Bitmap και JBIG2SymbolDict.

Ένα JBIG2Bitmap αντιπροσωπεύει μια ορθογώνια διάταξη εικονοστοιχείων. Το πεδίο data δείχνει σε ένα backing-buffer που περιέχει τον καμβά απόδοσης (“rendering canvas”).

Ένα JBIG2SymbolDict ομαδοποιεί τα JBIG2Bitmaps. Η σελίδα προορισμού αναπαρίσταται ως JBIG2Bitmap, όπως και οι μεμονωμένοι γλυφοί.

Τα JBIG2Segments μπορούν να αναφέρονται με έναν αριθμό τμήματος και ο διανυσματικός τύπος GList αποθηκεύει δείκτες προς όλα τα JBIG2Segments. Για να αναζητήσετε ένα τμήμα βάσει αριθμού τμήματος, η GList σαρώνεται σειριακά.

Η ευπάθεια

Η ευπάθεια είναι μια κλασική υπερχείλιση ακέραιου αριθμού κατά τη ταξινόμηση των αναφερόμενων τμημάτων:

```
 Guint numSyms; // (1)
 numSyms = 0;
 for (i = 0; i < nRefSegs; ++i) {
  if ((seg = findSegment(refSegs[i]))) {
    if (seg->getType() == jbig2SegSymbolDict) {
      numSyms += ((JBIG2SymbolDict *)seg)->getSize();  // (2)
    } else if (seg->getType() == jbig2SegCodeTable) {
      codeTables->append(seg);
    }
  } else {
    error(errSyntaxError, getPos(),
          "Invalid segment reference in JBIG2 text region");
    delete codeTables;
    return;
  }
 }
...
 // get the symbol bitmaps
 syms = (JBIG2Bitmap **)gmallocn(numSyms, sizeof(JBIG2Bitmap *)); // (3)
 kk = 0;
```

```
for (i = 0; i < nRefSegs; ++i) {
  if ((seg = findSegment(refSegs[i]))) {
    if (seg->getType() == jbig2SegSymbolDict) {
      symbolDict = (JBIG2SymbolDict *)seg;
      for (k = 0; k < symbolDict->getSize(); ++k) {
        syms[kk++] = symbolDict->getBitmap(k); // (4)
      }
    }
  }
}
```

Το numSyms είναι ένας ακέραιος αριθμός 32 bit που δηλώνεται στο (1) . Παρέχοντας προσεκτικά κατασκευασμένα τμήματα αναφοράς είναι δυνατό η επαναλαμβανόμενη προσθήκη στο (2) να προκαλέσει υπερχείλιση του numSyms σε μια ελεγχόμενη, μικρή τιμή.

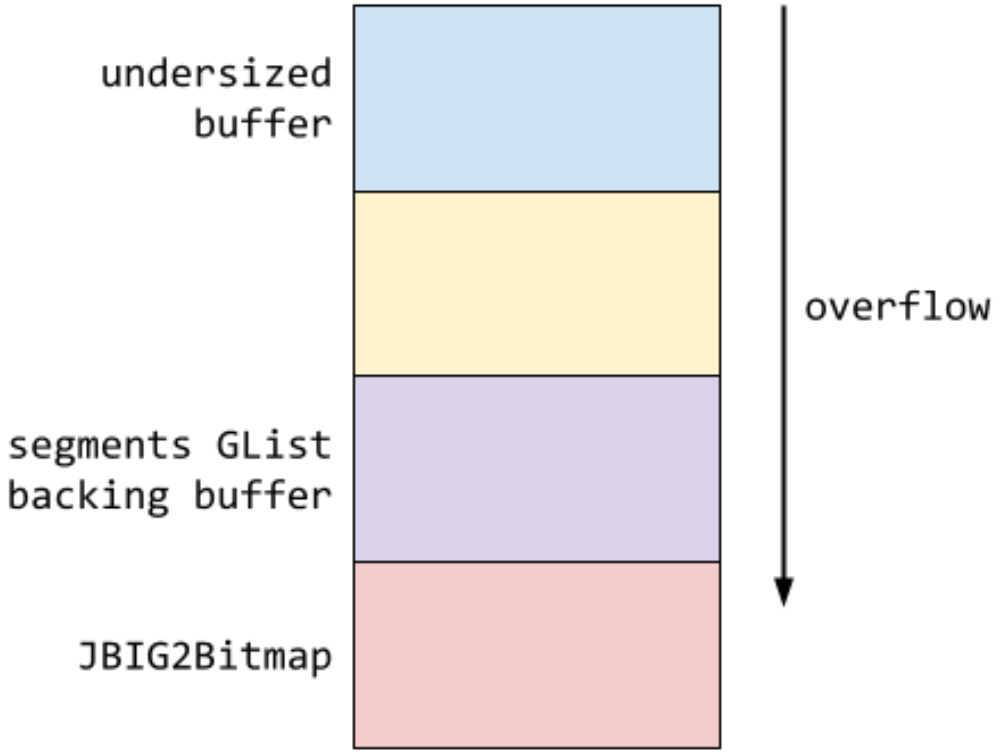
Αυτή η μικρότερη τιμή χρησιμοποιείται για το μέγεθος εκχώρησης σωρού ("heap allocation size") στο (3) που σημαίνει ότι το syms δείχνει σε ένα buffer μικρότερου μεγέθους ("undersized").

Στο εσωτερικό του πιο εσωτερικού βρόχου στο (4) οι τιμές του δείκτη της JBIG2Bitmap εγγράφονται στο undersized buffer syms.

Χωρίς άλλο τέχνασμα, αυτός ο βρόχος θα έγραφε πάνω από 32 GB δεδομένων στο undersized buffer syms, προκαλώντας σίγουρα ένα σφάλμα. Για να αποφευχθεί αυτό το σφάλμα, ο σωρός ("heap") είναι καλλωπισμένος έτσι ώστε οι πρώτες λίγες διαγραφές από το τέλος του buffer syms να καταστρέφουν το backing buffer της GList. Αυτή η GList αποθηκεύει όλα τα γνωστά τμήματα και χρησιμοποιείται από τη ρουτίνα findSegments για την αντιστοίχιση των αριθμών τμημάτων που μεταβιβάζονται στην refSegs σε δείκτες της JBIG2Segment. Η υπερχείλιση προκαλεί την αντικατάσταση των δεικτών της JBIG2Segment στη GList με δείκτες της JBIG2Bitmap στο (4).

Βολικά καθώς η JBIG2Bitmap κληρονομεί από την JBIG2Segment την εικονική κλήση seg->getType() επιτυγχάνεται ακόμη και σε συσκευές όπου είναι ενεργοποιημένος ο έλεγχος ταυτότητας δείκτη ("Pointer Authentication" - ο οποίος χρησιμοποιείται για την εκτέλεση

ελέγχου σε εικονικές κλήσεις αδύναμων τύπων), αλλά ο τύπος που επιστρέφεται **δεν** θα είναι πλέον ίσος με το jbig2SegSymbolDict προκαλώντας έτσι τη μη επίτευξη περαιτέρω εγγραφής στο (4) και οριοθετώντας την έκταση της καταστροφής της μνήμης.

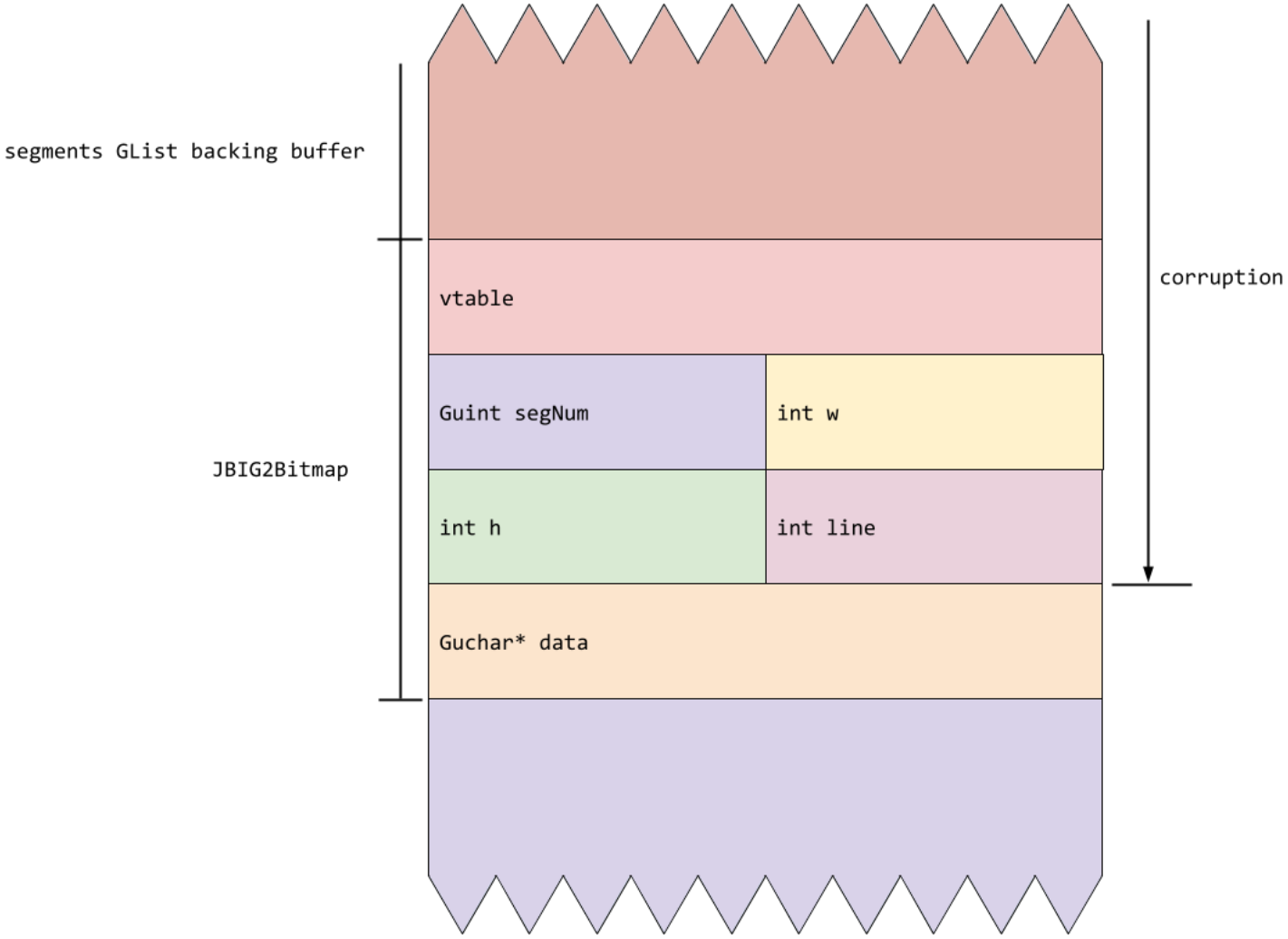


Μια απλοποιημένη προβολή της διάταξης της μνήμης όταν εμφανίζεται η υπερχείλιση σωρού που δείχνει το undersized-buffer κάτω από το backing buffer της GList και το JBIG2Bitmap

Περιθώρια χωρίς όρια

Αμέσως μετά τα κατεστραμμένα τμήματα της GList, ο εισβολέας διασκευάζει το αντικείμενο JBIG2Bitmap που αντιπροσωπεύει την τρέχουσα σελίδα (το μέρος όπου αποδίδονται οι τρέχουσες εντολές σχεδίασης).

Τα JBIG2Bitmaps είναι απλά wrappers γύρω από ένα backing buffer, που αποθηκεύει το πλάτος και το ύψος του buffer (σε bit) καθώς και μια τιμή γραμμής που καθορίζει πόσα byte αποθηκεύονται σε κάθε γραμμή.



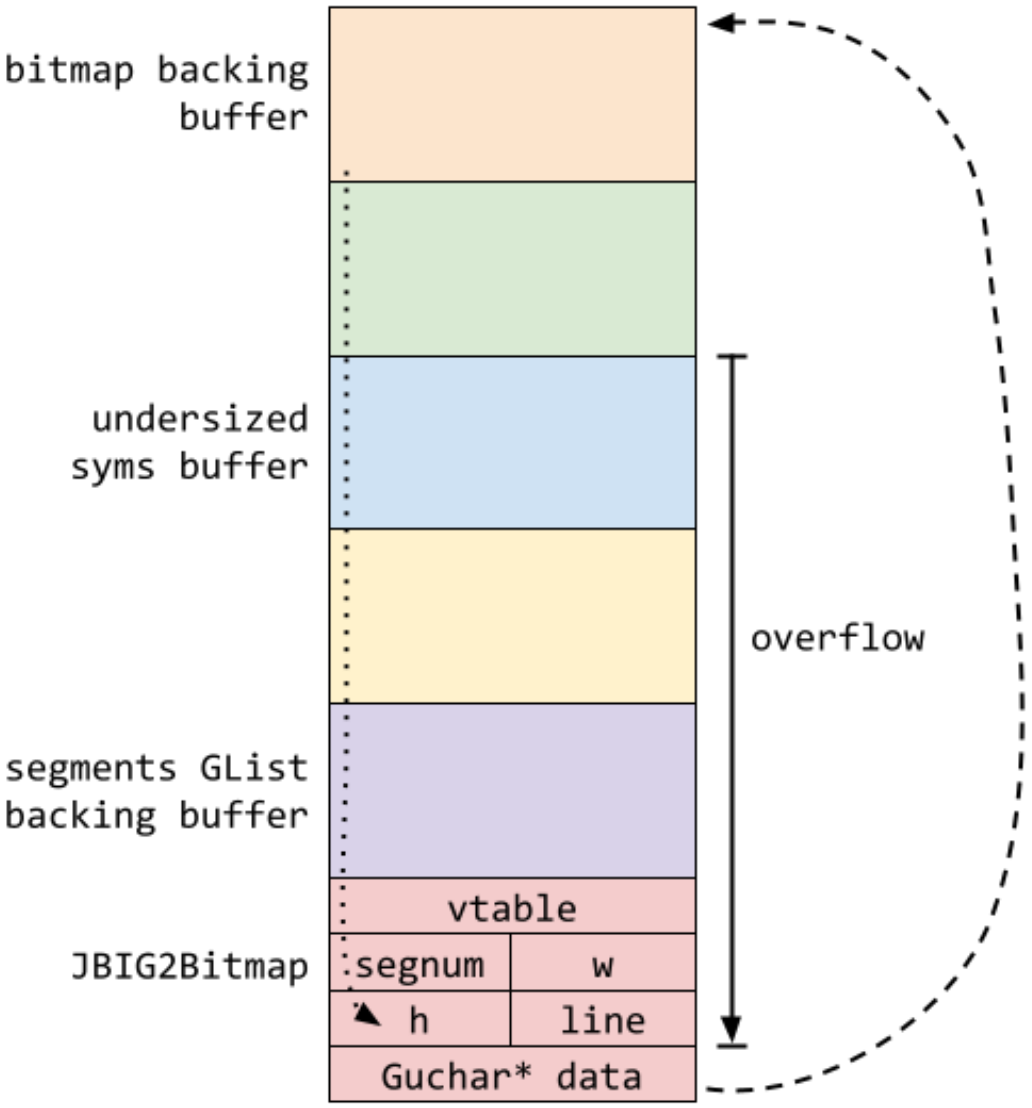
Η διάταξη μνήμης του αντικειμένου JBIG2Bitmap που δείχνει τα πεδία segnum, w, h και line που είναι κατεστραμμένα κατά τη διάρκεια της υπερχείλισης

Δομίζοντας προσεκτικά τα refSegs μπορούν να σταματήσουν την υπερχείλιση αφού γράψουν ακριβώς τρεις ακόμη δείκτες JBIG2Bitmap μετά το τέλος της προσωρινής μνήμης segments της GList. Αυτό αντικαθιστά τον δείκτη vtable και τα τέσσερα πρώτα πεδία του JBIG2Bitmap που αντιπροσωπεύουν την τρέχουσα σελίδα. Λόγω της φύσης της διάταξης του χώρου διευθύνσεων του iOS, αυτοί οι δείκτες είναι πολύ πιθανό να βρίσκονται στο δεύτερο μέρος 4 GB εικονικής μνήμης, με διευθύνσεις μεταξύ 0x100000000 και 0x1fffffff. Δεδομένου ότι όλες οι συσκευές με iOS είναι little endian (που σημαίνει ότι τα πεδία w και line είναι πιθανό να αντικατασταθούν με 0x1 —το most-significant μισό ενός δείκτη JBIG2Bitmap) και τα πεδία

segNum και h είναι πιθανό να αντικατασταθούν με το least-significant μισό ενός τέτοιου δείκτη, μια αρκετά τυχαία τιμή ανάλογα με τη διάταξη του σωρού ("heap") και το ASLR κάπου μεταξύ 0x100000 και 0xffffffff.

Αυτό δίνει στην τρέχουσα σελίδα προορισμού της JBIG2Bitmap μια άγνωστη, αλλά πολύ μεγάλη τιμή για το h. Δεδομένου ότι αυτή η τιμή h χρησιμοποιείται για τον έλεγχο ορίων και υποτίθεται ότι αντικατοπτρίζει το εκχωρημένο μέγεθος του backing buffer της σελίδας, αυτό έχει ως αποτέλεσμα την «αποδέσμευση» του καμβά σχεδίασης. Αυτό σημαίνει ότι οι επόμενες εντολές του JBIG2 τμήματος μπορούν να διαβάζουν και να γράφουν μνήμη εκτός των αρχικών ορίων του backing buffer της σελίδας.

Ο heap groom τοποθετεί επίσης το backing buffer της τρέχουσας σελίδας ακριβώς κάτω από το undersized buffer syms, έτσι ώστε όταν η σελίδα JBIG2Bitmap είναι απεριόριστη ("unbounded"), να μπορεί να διαβάζει και να γράφει τα δικά της πεδία:



Η διάταξη μνήμης που δείχνει πώς το απεριόριστο ("unbounded") bitmap backing buffer μπορεί να αναφέρει το αντικείμενο JBIG2Bitmap και να τροποποιεί πεδία σε αυτό καθώς βρίσκεται μετά την backing buffer στη μνήμη

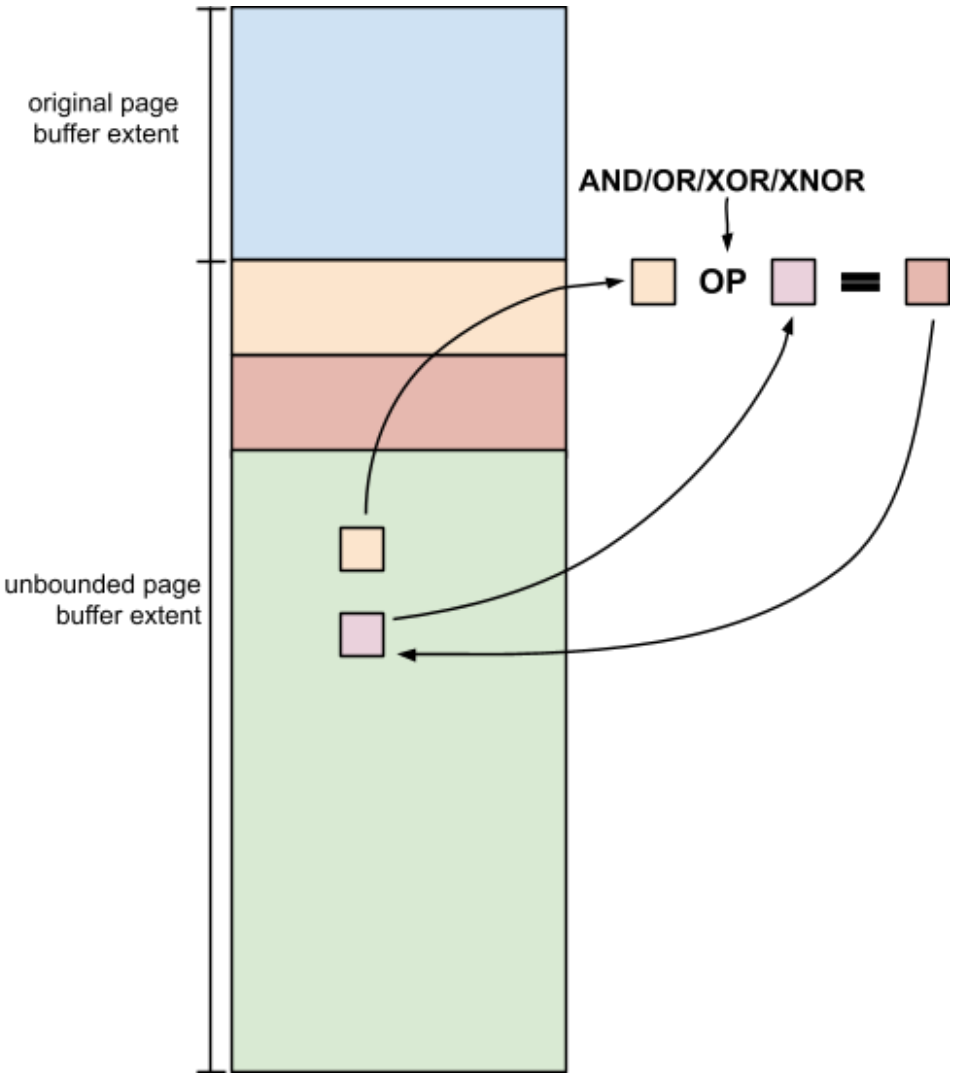
Αποδίδοντας ("rendering") τετράμπιτα ("4-byte") bitmaps στις σωστές συντεταγμένες του καμβά μπορούν να εγγραφούν όλα τα πεδία της σελίδας JBIG2Bitmap και επιλέγοντας προσεκτικά νέες τιμές για w , h και line, μπορούν να εγγραφούν αυθαίρετες μετατοπίσεις ("offsets") από το backing buffer της σελίδας.

Σε αυτό το σημείο θα ήταν επίσης δυνατό να γράψετε σε αυθαίρετες διευθύνσεις απόλυτης μνήμης, εάν γνωρίζατε τις μετατοπίσεις ("offsets") τους το backing buffer της σελίδας. Αλλά πώς να υπολογίσετε αυτές τις μετατοπίσεις; Μέχρι στιγμής, αυτό το exploit έχει προχωρήσει με τρόπο πολύ παρόμοιο με ένα «κανονικό» exploit μιας scripting γλώσσας, το οποίο στην JavaScript μπορεί να καταλήξει με ένα απεριόριστο ("unbounded") αντικείμενο ArrayBuffer με πρόσβαση στη μνήμη. Αλλά σε αυτές τις περιπτώσεις ο εισβολέας έχει τη δυνατότητα να εκτελεί αυθαίρετη JavaScript, η οποία προφανώς μπορεί να χρησιμοποιηθεί για τον υπολογισμό των μετατοπίσεων και την εκτέλεση αυθαίρετων υπολογισμών. Πώς το κάνετε αυτό σε έναν αναλυτή εικόνας ενός περάσματος;

Το άλλο φορμά συμπίεσης μου είναι Turing-complete!

Όπως αναφέρθηκε προηγουμένως, η σειρά των βημάτων που εφαρμόζουν το ραφινάρισμα ("refinement") του JBIG2 είναι πολύ ευέλικτη. Τα βήματα ραφιναρίσματος μπορούν να αναφέρονται τόσο στο bitmap εξόδου όσο και σε τυχόν τμήματα που δημιουργήθηκαν προηγουμένως, καθώς και να αποδώσουν ("render") την έξοδο είτε στην τρέχουσα σελίδα είτε σε ένα τμήμα. Δημιουργώντας προσεκτικά το εξαρτώμενο από το context τμήμα της ραφιναρισμένης αποσυμπίεσης, είναι δυνατό να δημιουργηθούν ακολουθίες τμημάτων όπου μόνο οι συνδυαστικοί τελεστές ραφιναρίσματος έχουν οποιοδήποτε αποτέλεσμα.

Στην πράξη, αυτό σημαίνει ότι είναι δυνατή η εφαρμογή των λογικών τελεστών AND, OR, XOR και XNOR μεταξύ των περιοχών μνήμης σε αυθαίρετες μετατοπίσεις ("offsets") από το JBIG2Bitmap backing buffer της τρέχουσας σελίδας. Και δεδομένου ότι αυτό είναι απεριόριστο… είναι δυνατό να εκτελεστούν αυτές οι λογικές πράξεις στη μνήμη σε αυθαίρετες μετατοπίσεις εκτός ορίων ("out-of-bounds"):



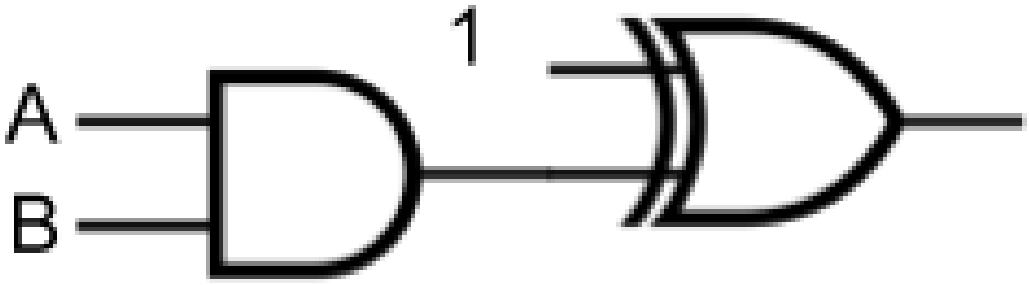
Η διάταξη μνήμης που δείχνει πώς μπορούν να εφαρμοστούν λογικοί τελεστές εκτός ορίων ("out-of-bounds")

Όταν το πας αυτό στην πιο ακραία του μορφή, τα πράγματα αρχίζουν να γίνονται πραγματικά ενδιαφέροντα. Τι θα γινόταν αν αντί να λειτουργήσετε σε υπο-ορθογώνια μεγέθους γλυφών ("glyph-sized sub-rectangles"), λειτουργούσατε με μεμονωμένα bits;

Μπορείτε τώρα να παρέχετε ως είσοδο μια ακολουθία εντολών στο τμήμα JBIG2 που υλοποιούν μια ακολουθία λογικών πράξεων προς εφαρμογή στη σελίδα. Και δεδομένου ότι το buffer της σελίδας είναι απεριόριστο ("unbounded"), αυτές οι λογικές

πράξεις μπορούν να εφαρμοστούν αυθαίρετα στην μνήμη.

Με ένα πρόχειρο σκαρίφημα μπορείτε να πείσετε τον εαυτό σας ότι ακόμα και μόνο με τους διαθέσιμους λογικούς τελεστές AND, OR, XOR και XNOR μπορείτε στην πραγματικότητα να υπολογίσετε *οποιαδήποτε* υπολογίσιμη συνάρτηση - η πιο απλή απόδειξη είναι ότι μπορείτε να δημιουργήσετε ένα λογικό τελεστή NOT κάνοντας XOR με 1 και μετά βάζοντας μια πύλη AND μπροστά από αυτό για να σχηματιστεί μια πύλη NAND:



Μια πύλη AND συνδεδεμένη σε μια είσοδο μιας πύλης XOR. Η άλλη είσοδος της πύλης XOR συνδέεται με τη σταθερή τιμή 1 δημιουργώντας ένα NAND.

Μια πύλη NAND είναι ένα παράδειγμα μιας καθολικής λογικής πύλης· μία από την οποία μπορούν να κατασκευαστούν όλες οι άλλες πύλες και από την οποία μπορεί να κατασκευαστεί ένα κύκλωμα για τον υπολογισμό οποιασδήποτε υπολογίσιμης συνάρτησης.

Πρακτικά κυκλώματα

Το JBIG2 δεν έχει δυνατότητες scripting, αλλά όταν συνδυάζεται με μια ευπάθεια, έχει τη δυνατότητα να μιμείται κυκλώματα αυθαίρετων λογικών πυλών που λειτουργούν σε αυθαίρετες περιοχές μνήμης. Γιατί λοιπόν να μην το χρησιμοποιήσετε αυτό για να δημιουργήσετε *τη δική σας* αρχιτεκτονική υπολογιστών και να την προγραμματίσετε!; Αυτό ακριβώς κάνει αυτό το exploit. Χρησιμοποιώντας περισσότερες από 70.000 εντολές τμήματος που ορίζουν λογικές πράξεις, ορίζουν μια μικρή αρχιτεκτονική υπολογιστών με χαρακτηριστικά όπως καταχωρητές και έναν πλήρη αθροιστή 64-bit που χρησιμοποιούν για

αναζήτηση στη μνήμη και εκτέλεση αριθμητικών πράξεων. Δεν είναι τόσο γρήγορο όσο η JavaScript, αλλά είναι θεμελιωδώς υπολογιστικά ισοδύναμο.

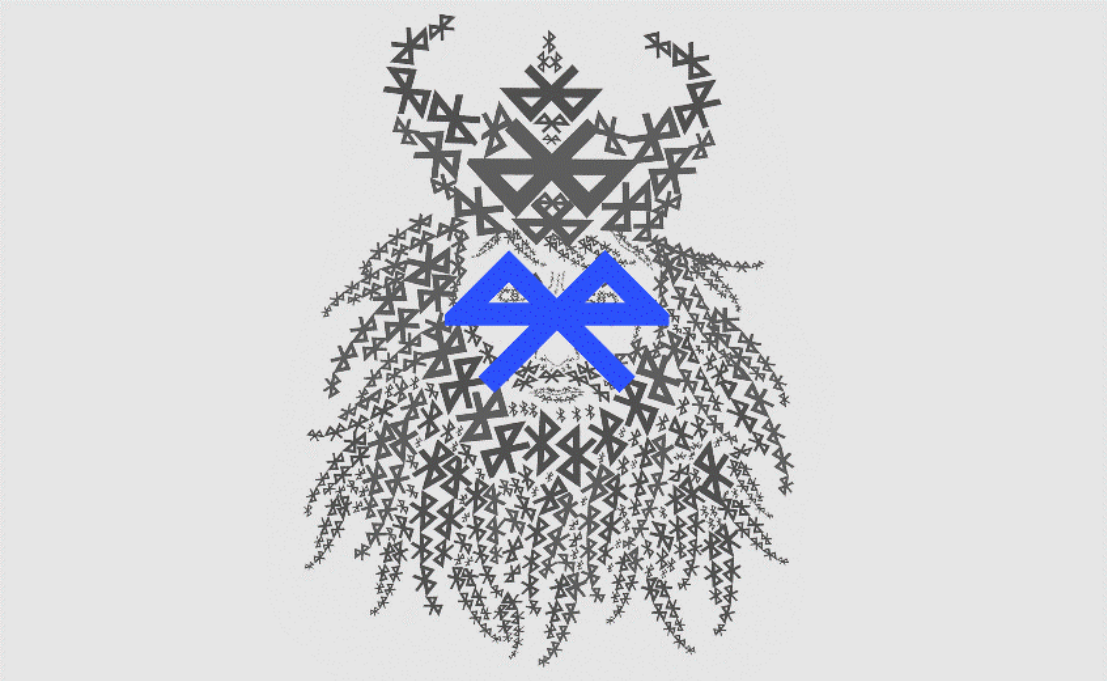
Οι λειτουργίες bootstrapping για το exploit διαφυγής από το sandbox είναι γραμμένες για να εκτελούνται σε αυτό το λογικό κύκλωμα και όλο το πράγμα εκτελείται σε αυτό το παράξενο, εξομοιούμενο περιβάλλον που δημιουργήθηκε μέσα από την αποσυμπίεση μονού περάσματος μιας ροής JBIG2. Είναι αρκετά απίστευτο, και ταυτόχρονα, αρκετά τρομακτικό.

Σε μια μελλοντική ανάρτηση (αυτή τη στιγμή ολοκληρώνεται), θα ρίξουμε μια ματιά στο πώς ακριβώς ξεφεύγουν από το sandbox της IMTranscoderAgent.

✔ **Bluetooth**: Η απίθανη ιστορία του βασιλιά με το χαλασμένο δόντι που έδωσε το όνομά του στην ασύρματη τεχνολογία

Ένας Δανός Βίκινγκ βασιλιάς, ο Χάραλντ Γκόρμσον, είχε το παρατσούκλι Γαλαζοδόντης ή Κυανόδους (Bluetooth).

Το όνομά του, Bluetooth, δόθηκε στην ευρέως χρησιμοποιούμενη ασύρματη τηλεπικοινωνιακή τεχνολογία μικρών αποστάσεων που εφευρέθηκε από τη σουηδική εταιρεία Ericsson και στη συνέχεια έγινε παγκόσμιο πρότυπο, βρίσκεται στο επίκεντρο μιας νέας διένεξης που έχει να κάνει με τον τόπο της ταφής του.

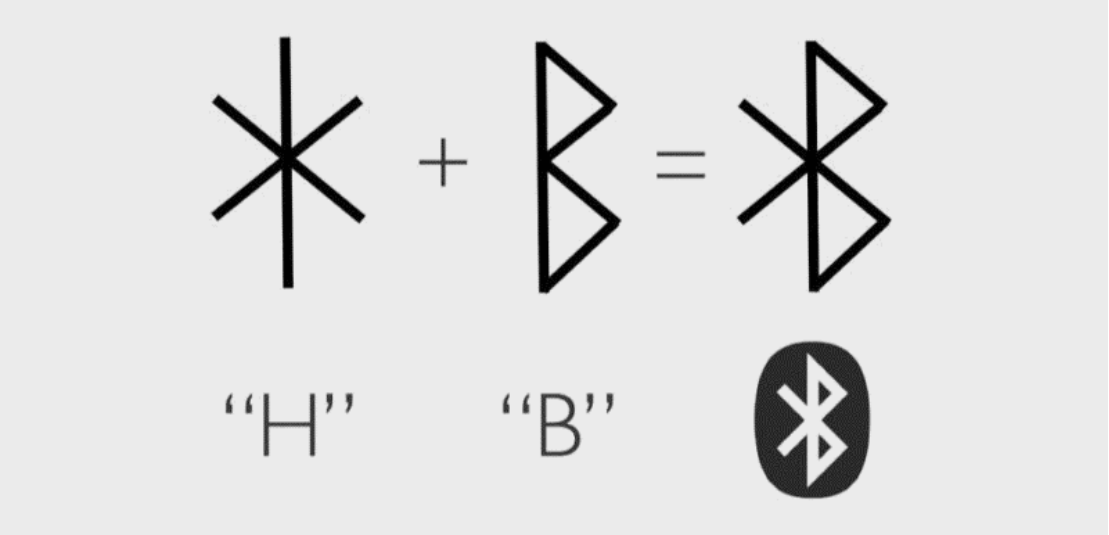


Η ιστορία του βασιλιά Bluetooth

Ο βασιλιάς πέθανε το 985 μ.Χ. και το επίμαχο ζήτημα είναι αν έχει ταφεί στη Δανία ή στην Πολωνία (και πού ακριβώς στην τελευταία).

Μεσαιωνικά χρονικά αναφέρουν ότι ο Χάραλντ είχε ένα δόντι γαλαζωπό (πιθανώς επειδή ήταν χαλασμένο), εξ ου και πήρε το ανάλογο προσωνύμιο. Ένα χρονικό τοποθετεί την ταφή του στο Ροσκίλντε της Δανίας, αλλά δύο νέες ανεξάρτητες δημοσιεύσεις ενός Σουηδού και ενός Πολωνού ερευνητή, σύμφωνα με το Associated Press, υποστηρίζουν ότι έχει ταφεί πιθανότατα στο χωριό Βιέκοβο της σημερινής βορειοδυτικής Πολωνίας, που είχε στενούς δεσμούς με τους Βίκινγκ εκείνη την εποχή.

Η εταιρεία Ericsson επέλεξε το παρατσούκλι Bluetooth για τη νέα τεχνολογία της στα τέλη της δεκαετίας του 1990, θέλοντας να σηματοδοτήσει την ικανότητά της να συνδέει ασύρματα διάφορες συσκευές, με το σκεπτικό ότι ο συγκεκριμένος «Γαλαζοδόντης» βασιλιάς είχε ενώσει μεγάλο μέρος της Σκανδιναβίας. Μάλιστα το λογότυπο του Bluetooth σχεδιάστηκε με βάση τα σκανδιναβικά ρουνικά γράμματα για τα αρχικά HB του βασιλιά.



Η απίθανη ιστορία του ονόματος Bluetooth

Ο Μάρεκ Κρίντα, συγγραφέας του φετινού βιβλίου «Πολωνία των Βίκινγκ», υποστηρίζει ότι τα λείψανα του βασιλιά βρίσκονται κάτω από μια ρωμαιοκαθολική εκκλησία του 19ου αιώνα στο πολωνικό χωριό Βιέκοβο. Βασίζει την πεποίθησή του στο ότι δορυφορικές εικόνες αποκαλύπτουν έναν αφανή στρογγυλό ταφικό τύμβο που παραπέμπει σε ταφικά έθιμα των Βίκινγκ.

Όμως ο Σουηδός αρχαιολόγος Σβεν Ρόσμπορν σε δικό του βιβλίο, που εκδόθηκε το 2021 («Ο χρυσός θησαυρός του Βίκινγκ βασιλιά Χάραλντ»), θεωρεί ότι ο Χάραλντ, ο οποίος είχε μεταστραφεί από τον παγανισμό στον Χριστιανισμό και ίδρυσε στη συνέχεια εκκλησίες στην Πολωνία, έχει ταφεί σε κανονικό χριστιανικό τάφο κάπου αλλού στην περιοχή, πιθανότατα στο προαύλιο κάποιας εκκλησίας αφιερωμένης στην Παναγία.

Από την πλευρά τους, οι ιστορικοί του Δανικού Εθνικού Μουσείου στην Κοπεγχάγη μάλλον προτιμούν την εκδοχή ότι ο βασιλιάς αναπαύθηκε οριστικά στο δικό τους έδαφος.

Ο Χάραλντ ήταν ένας από τους τελευταίους Βίκινγκ βασιλιάδες που κυβέρνησε τη σημερινή Δανία, τη βόρεια Γερμανία και τμήματα της Σουηδίας και της Νορβηγίας, παίζοντας σημαντικό ρόλο στην εξάπλωση του Χριστιανισμού στην επικράτειά του.

Ασφαλώς δεν θα μπορούσε να διανοηθεί ότι επρόκειτο να δώσει το όνομά του σε μια καινοτόμα ασύρματη τεχνολογία Bluetooth!

[Πηγή]

✔ Ηλεκτρονική διακυβέρνηση και "εξανθρωπισμένη" τεχνολογία: Το παράδειγμα της Βαρκελώνης

Πώς μπορούν οι πόλεις να μετρήσουν πόσο καλά εμπλέκουν τους πολίτες στην ηλεκτρονική τους διακυβέρνηση; Οι πόλεις βάζουν πραγματικά τους ανθρώπους στο επίκεντρο των ψηφιακών τους υπηρεσιών; Η Βαρκελώνη δεν έχει απαντήσει σε όλες τις ερωτήσεις ακόμα. Αυτοί είναι μερικοί από τους γρίφους που ελπίζουν να λύσουν με τους συνεργάτες του έργου **UserCentriCities** .

Ο **Joan Batlle Montserrat**, Υπεύθυνος για την Τεχνολογία και τα Ψηφιακά Δικαιώματα στην Επιτροπή Ψηφιακής Καινοτομίας στην πόλη της Βαρκελώνης , απάντησε σε μερικές ερωτήσεις σχετικά με τις συνεχιζόμενες εργασίες και τις προσδοκίες του έργου.

Πώς έχει εργαστεί η Βαρκελώνη για τη συμμετοχή των πολιτών μέχρι τώρα;

Τα τελευταία 25-30 χρόνια, συνεργαστήκαμε με συλλόγους που διανέμονται στην επικράτεια και συνδέονται με συγκεκριμένους τομείς. Μέσω εκλεγμένου αντιπροσώπου, οι οργανώσεις αυτές συμμετείχαν στις συζητήσεις του δημοτικού συμβουλίου.

Το 2018, το Δημοτικό Συμβούλιο της Βαρκελώνης παρουσίασε επίσης την ψηφιακή πλατφόρμα **Decidim.Barcelona** . Αυτό άνοιξε την πόρτα για πιο άμεση συμμετοχή των πολιτών που συμπλήρωνε αυτό που ήδη υπήρχε. Η πλατφόρμα φιλοξενεί πολλές διαφορετικές διαδικασίες. μερικά είναι στην κλίμακα ολόκληρης της πόλης, άλλα είναι προσαρμοσμένα στο επίπεδο της γειτονιάς.

Δημιουργήσαμε επίσης ένα Meta-Decidim που περιλαμβάνει ερευνητές, ακτιβιστές και ενώσεις για να συζητήσουμε πώς θα πρέπει να εξελιχθεί η πλατφόρμα. Αυτό που μάθαμε είναι ότι η πλατφόρμα λειτουργεί καλύτερα όταν συνδυάζεται με εκδηλώσεις στις γειτονιές, συνελεύσεις και συζητήσεις πρόσωπο με πρόσωπο με ανθρώπους. Η συμμετοχή των πολιτών αφορά τη συζήτηση θεμάτων που επηρεάζουν άμεσα τους ανθρώπους.

Στην τρέχουσα εντολή, δημιουργήσαμε επίσης το εργαστήριο δημοκρατικής συμμετοχής – ένα ζωντανό εργαστήριο που συνεργάζεται με τους πολίτες για τον τρόπο με τον οποίο πρέπει να ασκείται και να εξελίσσεται η τοπική και συμμετοχική δημοκρατία.

Πώς ελπίζετε ότι το έργο UserCentriCities θα βοηθήσει τη Βαρκελώνη να επιτύχει τους στόχους της όσον αφορά τη συμμετοχή των πολιτών;

Υπό την ηγεσία της Αντιδημάρχου Laia Bonet, εργαζόμαστε πάνω σε μια νέα ιδέα για την κατανόηση της ψηφιοποίησης στις πόλεις: την «εξανθρωπισμό της τεχνολογίας». Αυτό σημαίνει ηθική χρήση της τεχνολογίας. Η τεχνολογία πρέπει να χρησιμοποιείται για να λύνονται τα ζητήματα των ανθρώπων και γι' αυτό πρέπει να ακούμε τους ανθρώπους και να κατανοούμε τις ανησυχίες τους.

Το επόμενο βήμα μας είναι να αναπτύξουμε έναν τρόπο για να μετρήσουμε την πρόοδό μας προς τον εξανθρωπισμό της τεχνολογίας, προς

την κατεύθυνση της τοποθέτησης των ανθρώπων στο επίκεντρο. Έτσι, αρχίσαμε να εξετάζουμε τι έκαναν άλλοι για να αναπτύξουν δείκτες που θα μπορούσαν να το μετρήσουν.

Έτσι βρήκαμε UserCentriCities. Για εμάς, είναι ενδιαφέρον να συνεργαζόμαστε και να μαθαίνουμε από αυτό το έργο για τον εντοπισμό δεικτών με επίκεντρο τον χρήστη, επειδή η εύρεση δεικτών που μπορούν να σας δώσουν μια ακριβή εικόνα της προόδου σας είναι πρόκληση.

Γιατί είναι σημαντικό να αναπτυχθούν τέτοιοι δείκτες;

Οι δείκτες έχουν διαφορετικές χρήσεις. Πρέπει να χρησιμοποιήσετε δείκτες για να μετρήσετε την εργασία σας, αλλά μπορείτε να μετρήσετε άλλα πράγματα με αυτούς. Η αξία των δεικτών είναι να μετρήσετε αυτό που κάνετε σε σύγκριση με τον τελικό σας στόχο.

Οι δείκτες είναι επίσης απαραίτητοι για τη συγκριτική αξιολόγηση, που μπορούν να χρησιμοποιηθούν για να κατανοήσουμε τι έχουν κάνει οι άλλοι για να επιτύχουν τον ίδιο στόχο και να χρησιμοποιήσουμε αυτή τη γνώση για να βελτιώσουμε τη στρατηγική ή το σχέδιο δράσης σας.

Οι δείκτες και η συγκριτική αξιολόγηση σάς δίνουν πληροφορίες που μπορείτε να χρησιμοποιήσετε για να σχεδιάσετε καλύτερα τις μελλοντικές σας ενέργειες. Έτσι μαθαίνουμε: παρατηρείς, αναλύεις, κάνεις ερωτήσεις για τη

διαδικασία και τα αποτελέσματα και μπορείς να εμπνέεσαι από άλλους.

Ποια είναι τα επόμενα βήματα για τη Βαρκελώνη και το έργο;

Έχουμε ήδη αναλύσει διάφορα ερωτήματα που σχετίζονται με την εστίαση στον χρήστη μέσω του έργου – για παράδειγμα, προσβασιμότητα, κατανόηση, δυνατότητα εύρεσης, ποιότητα – και τώρα πρέπει να καταλάβουμε πώς μπορούμε να αναπτύξουμε έναν μικρό αριθμό αποτελεσματικών δεικτών για τη μέτρησή τους.

Μας ενδιαφέρει να δούμε τι κάνουν οι άλλες πόλεις του έργου. Και ανυπομονούμε να χρησιμοποιήσουμε τη συγκριτική αξιολόγηση ως εργαλείο που βοηθά να προσδιορίσουμε τι λειτουργεί, να το αναλύσουμε και να το προσαρμόσουμε στο περιβάλλον μας.

Στο μέλλον, ελπίζουμε να επιτύχουμε ευρύτερη χρήση της μεθοδολογίας. Όσο περισσότερες πόλεις θα εμπλέξουμε μόλις αναπτυχθεί η μεθοδολογία, τόσο περισσότερες βέλτιστες πρακτικές θα εντοπίσουμε και θα μάθουμε από αυτές.

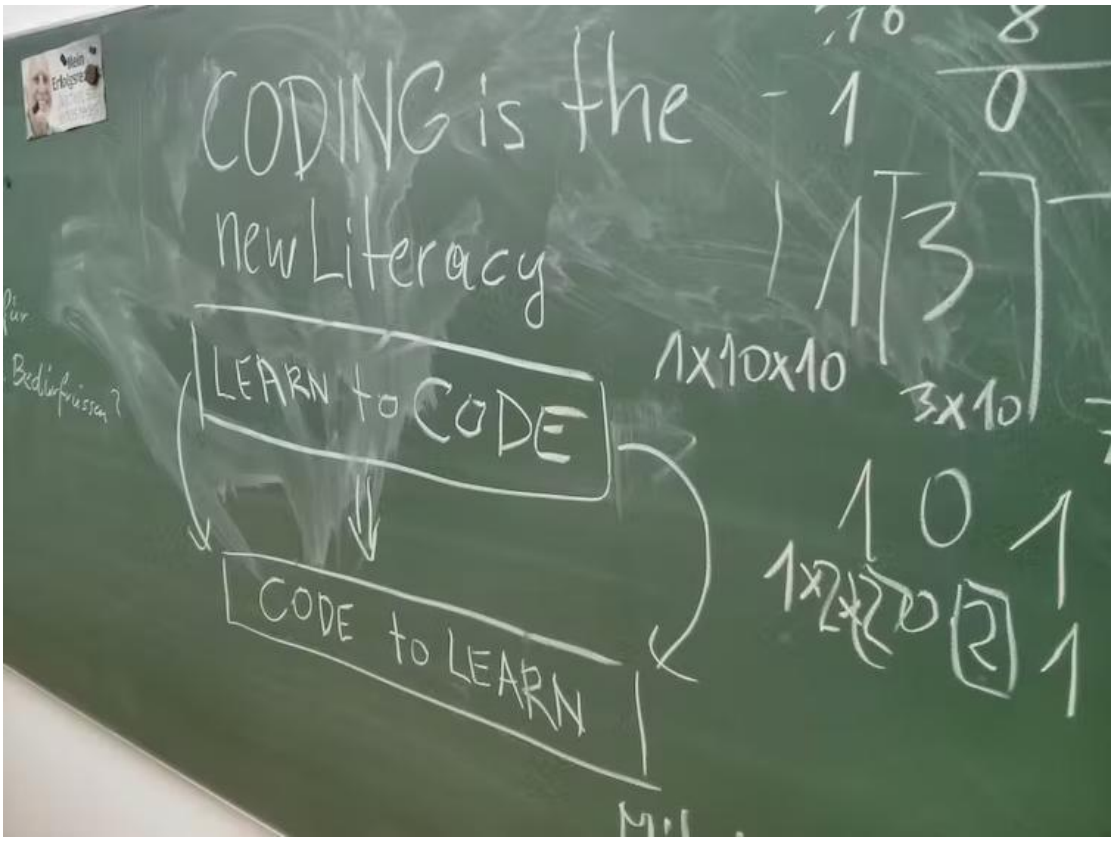
Παρακολουθήστε την πρόοδο του έργου UserCentriCities και λάβετε μέρος σε μελλοντικές εκδηλώσεις **εδώ** .

[Πηγή άρθρου: https://smartcities.ellak.gr/ | https://www.citybranding.gr/]

✔ Το μέλλον των Πληροφορικών και της Πληροφορικής...

Γράφει ο Νεκτάριος Μουμουτζής

Μοιράζομαι μαζί σας κάποιες σκέψεις για το μέλλον του "σιναφιού" μας. Οι σκέψεις αυτές εκκινούν από ένα πανθομολογούμενο γεγονός: Ολοένα και περισσότερο προωθείται ο προγραμματισμός υπολογιστών ως μια "δεξιότητα για όλους" (https://bre.is/wmRPeRXyJ), ανάλογη με τη δεξιότητα γραμματισμού (γραφή κι ανάγνωση)... Αν, λοιπόν, όλοι γνωρίζουν να προγραμματίζουν υπολογιστές, ποιος ο δικός μας ρόλος, ποια η επαγγελματική μας αποστολή, πώς θα "βιοποριζόμαστε"; Ή, μήπως, όπως διατείνονται κάποιοι, θα αναγκαστούμε να (αυτο)καταργηθούμε καθώς "όλοι θα ξέρουν να προγραμματίζουν υπολογιστές";



Ας δούμε καταρχήν μια ιστορική αναλογία: Οι δεξιότητες γραμματισμού, όταν πρωτοεμφανίστηκαν, αποτελούσαν προνόμιο και επτασφράγιστο μυστικό ενός ιερατείου. Προφανώς αυτό το ιερατείο δεν θα αντιμετώπισε θετικά την προοπτική του να μάθουν να γράφουν και διαβάζουν όλοι... Πραγματικά, ο εκδημοκρατισμός της γραφής και της ανάγνωσης (που ολοκληρώθηκε με την επινόηση της τυπογραφίας η οποία έκανε, σταδιακά, προσιτά τα βιβλία σε όλους) ανέτρεψε τους συσχετισμούς. Ωστόσο, δεν έπαψαν να υπάρχουν οι λογοτέχνες και οι φιλόλογοι! Έτσι, σήμερα μπορεί όλοι να ξέρουμε να γράφουμε και διαβάζουμε αλλά αυτό δεν καταργεί την ανάγκη για λογοτέχνες που θα συγγράψουν το κείμενα εκείνα που θα απολαύσουμε ως αναγνώστες. Ούτε καταργεί την ανάγκη των φιλολόγων που θα αναλύσουν τα λογοτεχνικά έργα και θα μας μάθουν να γράφουμε και να διαβάζουμε! Εν τέλει, ζούμε σε έναν κόσμο πολύ καλύτερο και πιο ορθολογικό από εκείνο της εποχής των ιερατείων...

Κατ' αναλογία οι βασικές δεξιότητες ψηφιακής γραφής και ανάγνωσης (προγραμματισμού) όχι μόνο δεν καταργούν την ανάγκη για Πληροφορικούς αλλά δημιουργούν και έναν καλύτερο κόσμο για όλους! Ωστόσο, θα πρέπει κι εμείς να ξεφύγουμε από λογικές "ιερατείου" και να κινηθούμε προς τη λογική "λογοτεχνών" και "φιλολόγων". Σκεφτείτε το λίγο:

- Ο **λογοτέχνης** διαφέρει από τον απλό γνώστη του γραπτού λόγο κατά το ότι γνωρίζει την τέχνη της μυθοπλασίας, της χρήσης της γλώσσας με δημιουργικό τρόπο, φτιάχνοντας "κόσμους" στους οποίους καλεί του αναγνώστες του να μεταφερθούν, να τους βιώσουν, και να πάρουν μαθήματα ζωής. Αντίστοιχα, ο **Πληροφορικός-Λογοτέχνης** της Νέας Εποχής είναι εκείνος ο οποίος γνωρίζει τις μεθοδολογίες και τα εργαλεία που του επιτρέπουν να δημιουργεί νέους ψηφιακούς κόσμους τους οποίους μπορούν να "εποικίσουν" οι "χρήστες". Κόσμους όπου η χρήση γλωσσών προγραμματισμού (κυρίως ειδικού σκοπού) τους επιτρέπει να εξελίσσουν και να αξιοποιούν αποτελεσματικά!

- Ο **φιλόλογος** πάλι διαφέρει κι εκείνος από τον απλό γνώστη του γραπτού λόγου κατά το ότι γνωρίζει σε βάθος τους "νόμους" της γλώσσας, μπορεί να αναλύσει τα έργα των λογοτεχνών, να τα διδάξει και να μάθει τους άλλους να αξιοποιούν αποτελεσματικά τη γλώσσα. Αντίστοιχα, ο **Πληροφορικός-Φιλόλογος** της Νέας Εποχής είναι εκείνος ο οποίος έχοντας βαθιά γνώση της Πληροφορικής αλλά και του κοινωνικών/παιδαγωγικών όρων για την ευρεία διάδοσή της ως "γλώσσας" μπορεί να μεταλαμπαδεύσει τις

απαιτούμενες γνώσεις σε ευρύτερα τμήματα της κοινωνίας και να τα υποστηρίξει στην πορεία αξιοποίησης της Πληροφορικής. Είναι ο Πληροφορικός της Εκπαίδευσης, του Εμπορίου των Πληροφορικών Αγαθών, ο Σύμβουλος Πληροφορικής... Είναι εκείνος που δεν αναπτύσσει, κατά κύριο λόγο, ψηφιακά συστήματα αλλά διαμορφώνει τις κοινωνικές συνθήκες που επιτρέπουν την ορθολογική και τεχνικά άρτια αξιοποίηση και εξέλιξή τους!

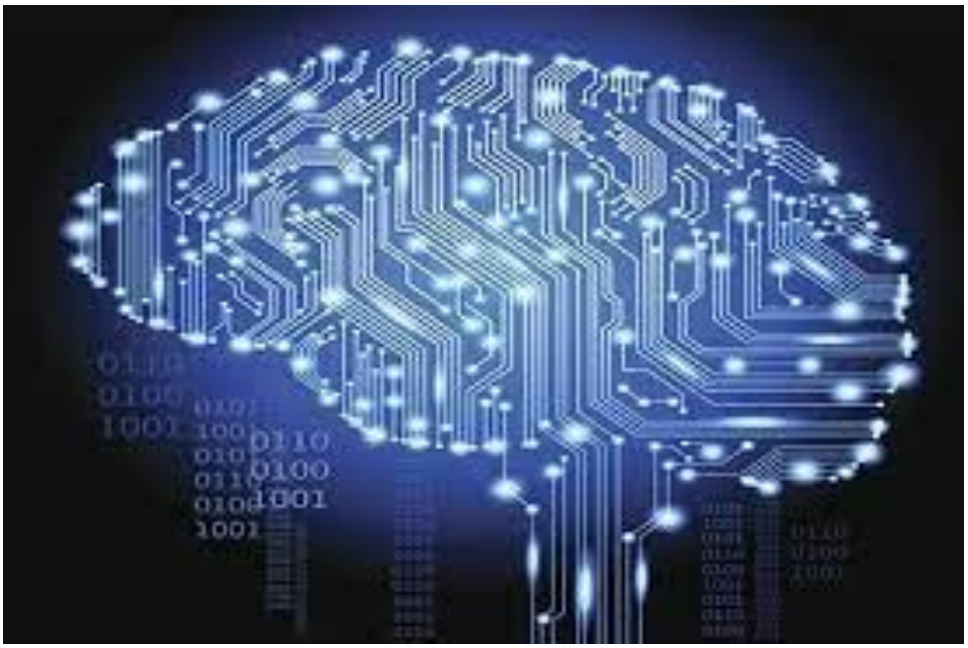
Αυτές είναι οι σκέψεις που μοιράζομαι μαζί σας ευελπιστώντας σε έναν εποικοδομητικό διάλογο που θα καταλήξει, είμαι βέβαιος, σε μια αποκρυστάλλωση της επαγγελματικής μας ταυτότητας και την οριοθέτηση/διάκριση του Πληροφορικού έναντι όλων των υπολοίπων που "ξέρουν να προγραμματίζουν"...

Αν κάποια ή κάποιος επιθυμεί μια λεπτομερέστερη ανάλυση με πλήθος από άκρως ενδιαφέρουσες αναφορές: https://theconversation.com/the-promise-of-the-learn-to-code-movement-107836

✔ Brain – train

Γρίφοι & προβλήματα από την Επιστήμη των Υπολογιστών για μαθητές

Επιμέλεια: **Φώτης Αλεξάκος**



✔ Εξάσκηση 1

Ζόρικα ξεκίνησαν το εντελώς 1ο τους εξάμηνο οι φοιτητές του Τμήματος Πληροφορικής. Ο -γνωστός- κος Κατεβαίνης έβαλε την παρακάτω άσκηση στο μάθημα "Εισαγωγή στην Επιστήμη των Η/Υ":

Να γραφεί πρόγραμμα σε γλώσσα ***C*** *που αντιμεταθέτει τις τιμές δυο ακεραίων μεταβλητών* ***x*** *και* ***y χωρίς*** *να χρησιμοποιηθεί καμία απολύτως άλλη μεταβλητή.*

✔ Εξάσκηση 2

Ο απογραφέας επισκέπτεται την οικία Παραξενίδη και ξεκινά τη δουλειά του ρωτώντας πόσοι κατοικούν στο σπίτι και τι ηλικίες έχουν. Ο κος Παραξενίδης του απαντά εν είδει γρίφου: Εδώ ζούνε τρεις (3) άνθρωποι των οποίων οι ηλικίες έχουν γινόμενο **1296** και άθροισμα όσο ο αριθμός του σπιτιού που τον έχεις ήδη σημειώσει. Ο υπάλληλος της στατιστικής υπηρεσίας όμως του εξηγεί ευγενικά πως τα δεδομένα αυτά δεν αρκούν για να συμπεράνει τα στοιχεία που ζητά. Έτσι, ο αρχηγός της οικογενείας του δίνει επιπλέον την πληροφορία ότι ένας από τους ενοίκους έχει ηλικία όση το πλήθος των αυτοκινήτων που φαίνονται παρκαρισμένα στην απέναντι μεριά του δρόμου. Τότε ο απογραφέας ικανοποιημένος αποχωρεί έχοντας μάθει ό,τι ζητούσε. Μπορείτε να βρείτε τον αριθμό του σπιτιού; (Εννοείται πως ηλικίες κλπ. είναι ακέραιοι αριθμοί).

(Περιοδικό "Pixel", τ. 36, Σεπ. 1987)

✔ Εξάσκηση 3

Για δοθέντα φυσικό αριθμό Ν, βρείτε όλους τους φυσικούς Χ των οποίων το παραγοντικό (Χ! = 1*2*3*4*...*Χ) έχει ακριβώς Ν ψηφία. Θεωρήστε ότι: Ν≤150.000

(Βαλκανιάδα Πληροφορικής 1997)

✔ *Στείλτε αν θέλετε τις δικές σας λύσεις στο* newsletter@epe.org.gr

☆ *Οι απαντήσεις των γρίφων θα δημοσιευθούν στο επόμενο τεύχος*

Επισκεφθείτε μας στο web
www.epe.org.gr

Γίνετε μέλος της ΕΠΕ

Για την ανάδειξη της
Πληροφορικής στη χώρα

Η Ένωση Πληροφορικών Ελλάδος υπάρχει για να δημιουργεί τις προϋποθέσεις για την προαγωγή της Πληροφορικής, αξιοποιώντας τις δυνάμεις των Πληροφορικών και ικανοποιώντας τις εργασιακές και επιστημονικές τους ανάγκες όπου και αν εργάζονται ή διαμένουν.
Είναι η κατάληξη της αναζήτησης όλων των Πληροφορικών για ένα ισχυρό φορέα του κλάδου που να αναδεικνύει αξιόπιστα τον κοινωνικό τους ρόλο και να τους εκπροσωπεί αυθεντικά σε όλα τα πεδία των ενδιαφερόντων τους.
Είναι η αφετηρία μιας μεγαλόπνοης προσπάθειας που επιδιώκει να κινητοποιήσει όλες τις ζωντανές δυνάμεις της κοινωνίας και να πορευτεί, μαζί μ ' αυτές, προς έναν καλύτερο κόσμο για όλους.
Σταθμός σε αυτή την πορεία και στρατηγικός στόχος της ΕΠΕ είναι η δημιουργία του Επιμελητηρίου Πληροφορικής.
Η δράση και οι παρεμβάσεις της είναι ο καταλύτης για την ωρίμανση των αναγκαίων κοινωνικών και πολιτικών συνθηκών.
Οι αξίες που καλλιεργεί θα αποτελέσουν την κληρονομιά και το όραμα του θεσμικού αυτού φορέα. Για να μπορέσουν όλοι οι πληροφορικοί να βρουν τη θέση που τους αξίζει στον κόσμο που όλοι μας οραματιζόμαστε.

LIKE US ON facebook
https://www.facebook.com/EnosiPliroforikonElladas

LinkedIn
https://www.linkedin.com/groups?gid=66328

twitter
https://twitter.com/epe_gr

YouTube
https://www.youtube.com/user/hiuaccount

RSS
http://www.epe.org.gr/index.php?id=7&type=100