Δοκιμές Διείσδυσης

CSP010_S_E

ΠΑΡΟΥΣΙΑΣΗ ΑΠΟ:
ΚΟΥΤΡΑΣ ΔΗΜΗΤΡΗΣ

CyberSecPro

CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Περιβάλλον προσομοίωσης και λειτουργίες

01. Στόχοι: Ποιος-Τι-Γιατί πρέπει να επιλέξει αυτή την εκπαίδευση

02. Επιμελητεία εκπαίδευσης: Πότε-Πού-Πώς

03. Μαθησιακά αποτελέσματα

04. Περίγραμμα εκπαίδευσης

05. Πρακτικές πληροφορίες και απαιτήσεις

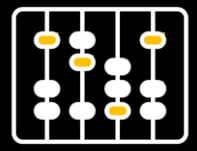
06. Πληροφορίες εγγραφής και επαφές

Στόχοι: Ποιος-Τι-Γιατί πρέπει να παρακολουθήσει αυτή την εκπαίδευση

ΠΟΙΟΣ

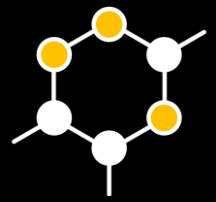
Όλοι όσοι έχουν βασικές γνώσεις και ενδιαφέρονται για τις ενεργειακές συσκευές - ασφάλεια λογισμικού

ΤΙ



Ναυτιλιακά περιβάλλοντα προσομοίωσης και επιχειρήσεις στον κυβερνοχώρο για διευθυντές, ηγέτες και επαγγελματίες

ΓΙΑΤΙ



Εξοπλίζει τους συμμετέχοντες με τις γνώσεις και τις δεξιότητες που απαιτούνται για δημιουργία στρατηγικής για την προστασία κρίσιμων συστημάτων και δεδομένων

Προτάσεις Αξίας

Οφέλη για τους συμμετέχοντες

- Επίπεδο Εκπαιδευτικής Ενότητας: Προχωρημένο
- Επαγγελματική κατάρτιση στον τομέα της κυβερνοασφάλειας
- Πρακτική ανάπτυξη δεξιοτήτων
- Πρωτοποριακές πληροφορίες από ειδικούς ακαδημαϊκούς και επαγγελματίες βιομηχανίας
- Βοηθά στην ανάπτυξη δεξιοτήτων και στην επαγγελματική ανέλιξη

ΠΟΙΟΣ

Προφίλ των συμμετεχόντων στην κατάρτιση

- Διευθυντές και ηγέτες
- Επαγγελματίες εργασιακού χώρου
- Υπάλληλοι ΜΜΕ και δημοσίου
- Επαγγελματίες και λάτρεις της κυβερνοασφάλειας

ΠΟΙΟΣ

Προφίλ του εκπαιδευτή

- Ο Δημήτρης Κούτρας είναι υποψήφιος διδάκτορας στην ασφάλεια δικτύων του τμήματος Πληροφορικής στο Πανεπιστήμιο Πειραιώς. Έλαβε πτυχίο τεχνολογίας πληροφοριών και μηχανικός υπολογιστών από το Τεχνολογικό Εκπαιδευτικό Ίδρυμα Ελλάδας (Λαμία-2016). Στη συνέχεια, απέκτησε μεταπτυχιακό τίτλο σπουδών (ΠΜΣ) στη μηχανική διαχείρισης ασφάλειας από το Πανεπιστήμιο Πειραιώς (Πειραιάς-2019). Αυτή τη στιγμή συμμετέχει σε ευρωπαϊκά ερευνητικά προγράμματα ως ερευνητής του Ερευνητικού Κέντρου του Πανεπιστημίου Πειραιώς. Συμμετέχει επίσης ως εκπαιδευτής σε διάφορα σεμινάρια κυβερνοασφάλειας, που αφορούν τη ναυτιλία, την υγειονομική περίθαλψη και την εφοδιαστική αλυσίδα. Είναι κάτοχος πιστοποίησης ISO 27001:2013 επικεφαλής ελεγκτής για την ασφάλεια των πληροφοριών. Το ερευνητικό του έργο αφορά την ανάλυση ασφάλειας δικτύων, την αξιολόγηση κινδύνων και την ασφάλεια λειτουργικών συστημάτων. Ο Δημήτρης έχει συνεργαστεί με το UPRC σε διάφορα σημαντικά έργα, συμπεριλαμβανομένων των CyberSec for Europe, CyberSecPro, MELITY και ARTEMIS, που χρηματοδοτούνται από την Ευρωπαϊκή Ένωση και την ελληνική κυβέρνηση

ΤΙ

Θέματα κατάρτισης

- Σώμα πληροφοριών για την ασφάλεια στον κυβερνοχώρο
- Απειλές και Ευπάθειες
- Σχεδιασμός και υλοποίηση αρχιτεκτονικής ασφάλειας
- Επιλογή και υλοποίηση ελέγχων ασφαλείας
- Δοκιμές διείσδυσης

ΓΙΑΤΙ

Μαθησιακά αποτελέσματα

- Κατανόηση των απειλών στον κυβερνοχώρο που αφορούν συγκεκριμένο λιμένα: Οι συμμετέχοντες θα αποκτήσουν ολοκληρωμένη κατανόηση των μοναδικών απειλών στον κυβερνοχώρο που αντιμετωπίζουν οι θαλάσσιοι λιμένες, συμπεριλαμβανομένων των ευπαθειών και των δυνητικών φορέων επίθεσης.
- Γνώση τεχνικών δυαδικής εκμετάλλευσης ευπάθειας: Οι εκπαιδευόμενοι θα αναπτύξουν δεξιότητες λογισμικού στη δυαδική εκμετάλλευση, μαθαίνοντας πώς να εντοπίζουν και να εκμεταλλεύονται ευπάθειες σε λογισμικό που χρησιμοποιείται σε συστήματα λιμένων.
- Αποτελεσματική αντιμετώπιση επιθέσεων στον κυβερνοχώρο: Οι συμμετέχοντες θα εκπαιδευτούν σε πρακτικές τεχνικές αντιμετώπισης επιθέσεων στον κυβερνοχώρο, επιτρέποντάς τους να διαχειρίζονται και να μετριάζουν περιστατικά σε πραγματικό χρόνο.
- Δεξιότητες αξιολόγησης και διαχείρισης κινδύνων: Ικανότητα διεξοδικής αξιολόγησης κινδύνων, εντοπισμού κρίσιμων περιουσιακών στοιχείων και υλοποίησης ισχυρών στρατηγικών διαχείρισης κινδύνων ειδικά για περιβάλλοντα λιμένα.
- Πρακτική εμπειρία με εργαλεία κυβερνοασφάλειας: Πρακτική εμπειρία με δημοφιλή εργαλεία και πλατφόρμες κυβερνοασφάλειας, συμπεριλαμβανομένων των εργαλείων δοκιμών διείσδυσης και εργαλεία κόκκινης ομάδας.

Περίγραμμα κατάρτισης

Ημέρα-1

Θέμα-1: Εισαγωγή στους κύριους τομείς της ενέργειας Κυβερνοασφάλεια

Θέμα-2: Περιβάλλον ασφαλείας: επικρατούσα κατάσταση

Θέμα-3: Δυαδικά αρχεία

Θέμα-4: Δοκιμές διείσδυσης

Γνωστικό υπόβαθρο και προαπαιτούμενα

Γνωστικό Υπόβαθρο

Βασική κατανόηση των υπολογιστών και της δικτύωσης

Εξοικείωση με τις συνήθεις απειλές και ευπάθειες ασφάλειας του διαδικτύου

Ενημέρωση για την ασφάλεια στον κυβερνοχώρο

Προαπαιτούμενα:

Κανένα

Τεχνικά εργαλεία και άλλες απαιτήσεις

Τεχνικά εργαλεία

Υπολογιστής με πρόσβαση στο διαδίκτυο

Τεχνικά εργαλεία: Kali Linux, Virtual Machine, NMap, Wireshak, μεταγλωττιστές, C.

Άλλες απαιτήσεις

Γνώση βασικών εννοιών υπολογιστών / Ενημέρωση για τις πρακτικές ασφάλειας στο διαδίκτυο / Προθυμία για μάθηση και πειραματισμό / Ενεργή συμμετοχή

Πρόοδος μαθημάτων

01 Πλοήγηση στις απειλές στον κυβερνοχώρο: Ο κίνδυνος των ευάλωτων δυαδικών συστημάτων στον τομέα της ενέργειας

02. Από το λογισμικό στα δυαδικά αρχεία

03. Μνήμη

04. Δοκιμές διείσδυσης Black Box

Εισαγωγή

Τι θα αντιμετωπίσουμε;

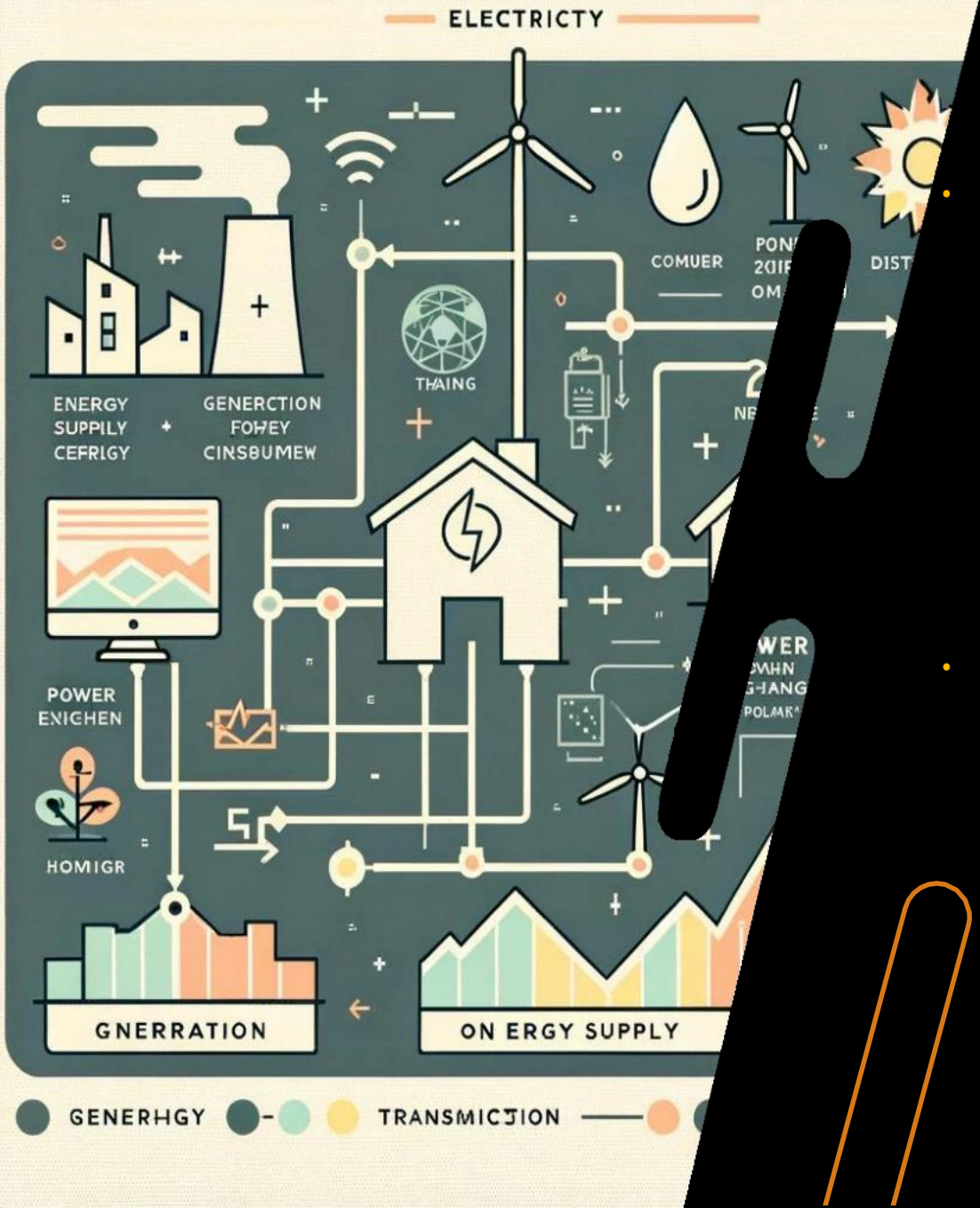
- Ανταλλαγή πληροφοριών στον ενεργειακό τομέα με την παρουσίαση των επιλεγμένων ενεργειακών υποτομέων
  - Ηλεκτρισμός,
  - Πετρέλαιο και φυσικό αέριο,
  - Πυρηνική ενέργεια,
  - και εναλλακτικά καύσιμα

όπως προσδιορίζεται από την οδηγία NIS (ασφάλεια δικτύων και πληροφοριών).

- Κατανόηση των κύριων ζητημάτων και προκλήσεων της ανταλλαγής πληροφοριών για την ασφάλεια στον κυβερνοχώρο

Ο υποτομέας της ηλεκτρικής ενέργειας

- **Ευαίσθητοι τύποι δεδομένων:**
  - **Δεδομένα κατάστασης δικτύου ηλεκτροδότησης:** Λειτουργικά επίπεδα των δικτύων ηλεκτροδότησης σε πραγματικό χρόνο, συμπεριλαμβανομένων των συνθηκών και των μετρήσεων απόδοσης.
  - **Οικονομικά στοιχεία:** Συναλλαγές, τιμολόγηση και συμμετοχή στην αγορά πληροφορίες σχετικά με την εμπορία και τις πωλήσεις ενέργειας.
  - **Δεδομένα κατανάλωσης και χρέωσης:** Λεπτομερή αρχεία των μοτίβων χρήσης ενέργειας των πελατών, λεπτομέρειες τιμολόγησης και προσωπικές πληροφορίες.
- **Στρατηγική σημασία:**
  - **Κρίσιμες υποδομές:** Τα δίκτυα ηλεκτροδότησης είναι θεμελιώδη για την εθνική ασφάλεια, την οικονομία και τη δημόσια ευημερία. Οι διακοπές μπορούν να οδηγήσουν σε εκτεταμένες κοινωνικές επιπτώσεις.
  - **Κορμός άλλων τομέων:** Η παροχή ηλεκτρικής ενέργειας είναι ζωτικής σημασίας για τη λειτουργία της υγειονομικής περίθαλψης, των οικονομικών, των μεταφορών και άλλων βασικών τομέων, καθιστώντας την αδιάλειπτη παροχή της ζωτικής σημασίας.



Ο υποτομέας της ηλεκτρικής ενέργειας

- **Κίνδυνοι εκμετάλλευσης στον κυβερνοχώρο:**
  - **Διάσπαση του εφοδιασμού:** Οι κυβερνοεπιθέσεις θα μπορούσαν να ανατρέψουν την παραγωγή, τη μεταφορά ή τη διανομή ηλεκτρικής ενέργειας, οδηγώντας σε διακοπές ρεύματος.
  - **Οικονομική χειραγώγηση:** Η πρόσβαση σε οικονομικά δεδομένα μπορεί να επιτρέψει χειραγώγηση της αγοράς, με αποτέλεσμα οικονομικές απώλειες ή αθέμιτα πλεονεκτήματα.
  - **Παραβιάσεις δεδομένων:** Η παραβίαση των πληροφοριών κατανάλωσης και χρέωσης εγκυμονεί κινδύνους κλοπής ταυτότητας και παραβίασης της ιδιωτικής ζωής των καταναλωτών.
  - **Χειραγώγηση δικτύου ηλεκτροδότησης:** Οι κυβερνοεισβολές θα μπορούσαν να ενεργοποιήσουν τον ανεξουσιοδότητο έλεγχο των λειτουργιών του δικτύου, προκαλώντας δυνητικά φυσική ζημία στις υποδομές.
- **Απαιτούμενα αμυντικά μέτρα:**
  - **Να είστε προσεκτικοί με τα πρωτόκολλα κυβερνοασφάλειας** για τα δίκτυα ελέγχου διεργασιών (PCN) και τα συστήματα για την αποτροπή ανεξουσιοδότητης πρόσβασης και τη διασφάλιση της ακεραιότητας των δεδομένων.
  - **Τακτικές αξιολογήσεις ασφαλείας** για την αντιμετώπιση των εξελισσόμενων απειλών στον κυβερνοχώρο.
  - **Ανταλλαγή πληροφοριών** μεταξύ των οντοτήτων του υποτομέα της ηλεκτροδότησης για τον γρήγορο εντοπισμό απειλών και για τη διάδοση βέλτιστων πρακτικών για εξομάλυνση.
  - **Συνεργασία με κυβερνητικούς** και ρυθμιστικούς φορείς για την καθιέρωση ολοκληρωμένων προτύπων ασφάλειας και την αποτελεσματική αντιμετώπιση περιστατικών.

Ο υποτομέας πετρελαίου και φυσικού αερίου

Ευαίσθητοι τύποι δεδομένων:

- **Δεδομένα έρευνας και παραγωγής:** Λεπτομερή γεωλογικά και λειτουργικά δεδομένα κρίσιμα για την ανακάλυψη και την εξόρυξη αποθεμάτων πετρελαίου και φυσικού αερίου.
- **Λειτουργικά δεδομένα υποδομής:** Πληροφορίες σχετικά με τη λειτουργική κατάσταση και τις επιδόσεις των κρίσιμων υποδομών, συμπεριλαμβανομένων των αγωγών δεδομένων, των διυλιστηρίων και των εγκαταστάσεων αποθήκευσης.
- **Δεδομένα αγοράς και οικονομικά στοιχεία:** Περιλαμβάνει πληροφορίες τιμολόγησης, συναλλαγών και λεπτομέρειες επενδύσεων που είναι κρίσιμες για τις λειτουργικές απαιτήσεις και την ανταγωνιστική τοποθέτηση.

- **Στρατηγική σημασία:**
  - **Ενεργειακή ασφάλεια:** Το πετρέλαιο και το φυσικό αέριο είναι ζωτικά για τον παγκόσμιο εφοδιασμό, επηρεάζοντας την εθνική ασφάλεια και τις γεωπολιτικές δυναμικές.
  - **Οικονομικός αντίκτυπος:** Ο τομέας συμβάλλει σημαντικά στην παγκόσμια οικονομία, με τις διακυμάνσεις των τιμών να επηρεάζουν ένα ευρύ φάσμα οικονομικών δραστηριοτήτων.
  - **Ρυθμιστική χειραγώγηση:** Η μη εξουσιοδοτημένη πρόσβαση σε ρυθμιστικά δεδομένα θα μπορούσε να οδηγήσει σε παραποιημένες αναφορές συμμόρφωσης, θέτοντας σε κίνδυνο τη δημόσια ασφάλεια.

Ο υποτομέας πετρελαίου και φυσικού αερίου

Κίνδυνοι εκμετάλλευσης στον κυβερνοχώρο:

- **Παρεμβολές στη λειτουργία:** Οι κυβερνοεπιθέσεις με στόχο τις λειτουργικές τεχνολογίες μπορούν να οδηγήσουν σε διακοπές λειτουργίας ή δυσλειτουργίες στις επιχειρήσεις εξόρυξης, αγωγών δεδομένων και διυλιστηρίων.
- **Περιβαλλοντικοί κίνδυνοι:** εισβολές στα συστήματα ελέγχου μπορούν να προκαλέσουν διαρροές ή σε άλλα συμβάντα με σοβαρές συνέπειες για το περιβάλλον και τη δημόσια υγεία.
- **Οικονομική χειραγώγηση:** Η ανεξουσιοδότητη πρόσβαση σε δεδομένα της αγοράς και οικονομικά δεδομένα θα μπορούσε να
οδηγούν σε εσωτερική πληροφόρηση, χειραγώγηση της αγοράς ή κατασκοπία στην οικονομία .
- **Σαμποτάζ υποδομών:** Οι προηγμένες επίμονες απειλές (APTs) θα μπορούσαν να στοχεύσουν σε φυσικές υποδομές, οδηγώντας σε μακροχρόνιες ζημιές και ανατρεπτικές αλυσίδες εφοδιασμού.

- **Απαιτούμενα αμυντικά μέτρα:**
  - **Στιβαρά** πλαίσια λογισμικού για **την ασφάλεια** τόσο για την τεχνολογία πληροφοριών (IT) όσο και για τα συστήματα επιχειρησιακής τεχνολογίας (OT) για άμυνα απέναντι σε επιθέσεις.
  - **Υλοποίηση συστημάτων παρακολούθησης σε πραγματικό χρόνο** και ανίχνευσης ανωμαλιών για τον άμεσο εντοπισμό δυνητικών απειλών στον κυβερνοχώρο.
  - **Ενίσχυση της συνεργατικής δράσης** εντός του τομέα και με κυβερνητικές υπηρεσίες για την ανταλλαγή πληροφοριών και κοινές πρωτοβουλίες για την ασφάλεια στον κυβερνοχώρο.
  - **Ανάπτυξη λογισμικού ταχείας αντίδρασης** και ανάκαμψης για την ελαχιστοποίηση των επιπτώσεων των περιστατικών στον κυβερνοχώρο και τη διασφάλιση της ανθεκτικότητας των λειτουργικών.

Ο υποτομέας πυρηνικής ενέργειας

Ευαίσθητοι τύποι δεδομένων:

- **Λειτουργικά δεδομένα:** Περιλαμβάνει λεπτομερείς πληροφορίες σχετικά με τις λειτουργική κατάσταση των πυρηνικών αντιδραστήρων, της χρήσης καυσίμων και την αποθήκευση αποβλήτων.
- **Δεδομένα συστήματος ασφαλείας:** Κρίσιμες πληροφορίες σχετικά με την κατάσταση και την ακεραιότητα των συστημάτων ασφαλείας που έχουν σχεδιαστεί για την πρόληψη ατυχημάτων.
- **Δεδομένα κανονιστικών ρυθμίσεων και συμμόρφωσης:** Έγγραφα και καταγραφές που αφορούν τη συμμόρφωση με τις κανονιστικές διατάξεις, τους ελέγχους ασφαλείας και τις επιθεωρήσεις.

Στρατηγική σημασία:

- **Εθνική ασφάλεια:** Οι πυρηνικές εγκαταστάσεις αποτελούν βασικές δομές με επιπτώσεις στην εθνική ασφάλεια λόγω του δυνητικού κινδύνου έκδοσης ραδιενέργειας.
- **Ενεργειακή σταθερότητα:** Η πυρηνική ενέργεια συμβάλλει σημαντικά στη σταθερότητα και την αξιοπιστία του δικτύου ηλεκτροδότησης σε πολλές χώρες.

Ο υποτομέας πυρηνικής ενέργειας

Κίνδυνοι εκμετάλλευσης στον κυβερνοχώρο:

- **Υποβιβασμός ασφάλειας:** Οι κυβερνοεπιθέσεις με στόχο τα συστήματα ελέγχου θα μπορούσαν δυνητικά να θέσουν σε κίνδυνο τους μηχανισμούς ασφαλείας, οδηγώντας σε επικίνδυνα περιστατικά.
- **Επιχειρησιακές παρεμβολές:** Εισβολές σε λειτουργικά δίκτυα θα μπορούσαν να οδηγήσουν σε διακοπή λειτουργίας ή δυσλειτουργία πυρηνικών αντιδραστήρων, επηρεάζοντας τον ενεργειακό εφοδιασμό.
- **Κλοπή πληροφοριών:** Η κατασκοπεία με στόχο την απόκτηση ευαίσθητων τεχνολογικών ή λειτουργικών πληροφοριών μπορεί να υπονομεύσει την εθνική ασφάλεια.
- **Ρυθμιστική χειραγώγηση:** Η μη εξουσιοδοτημένη πρόσβαση σε ρυθμιστικά δεδομένα θα μπορούσε να οδηγήσει σε παραποιημένες αναφορές συμμόρφωσης, θέτοντας σε κίνδυνο τη δημόσια ασφάλεια.

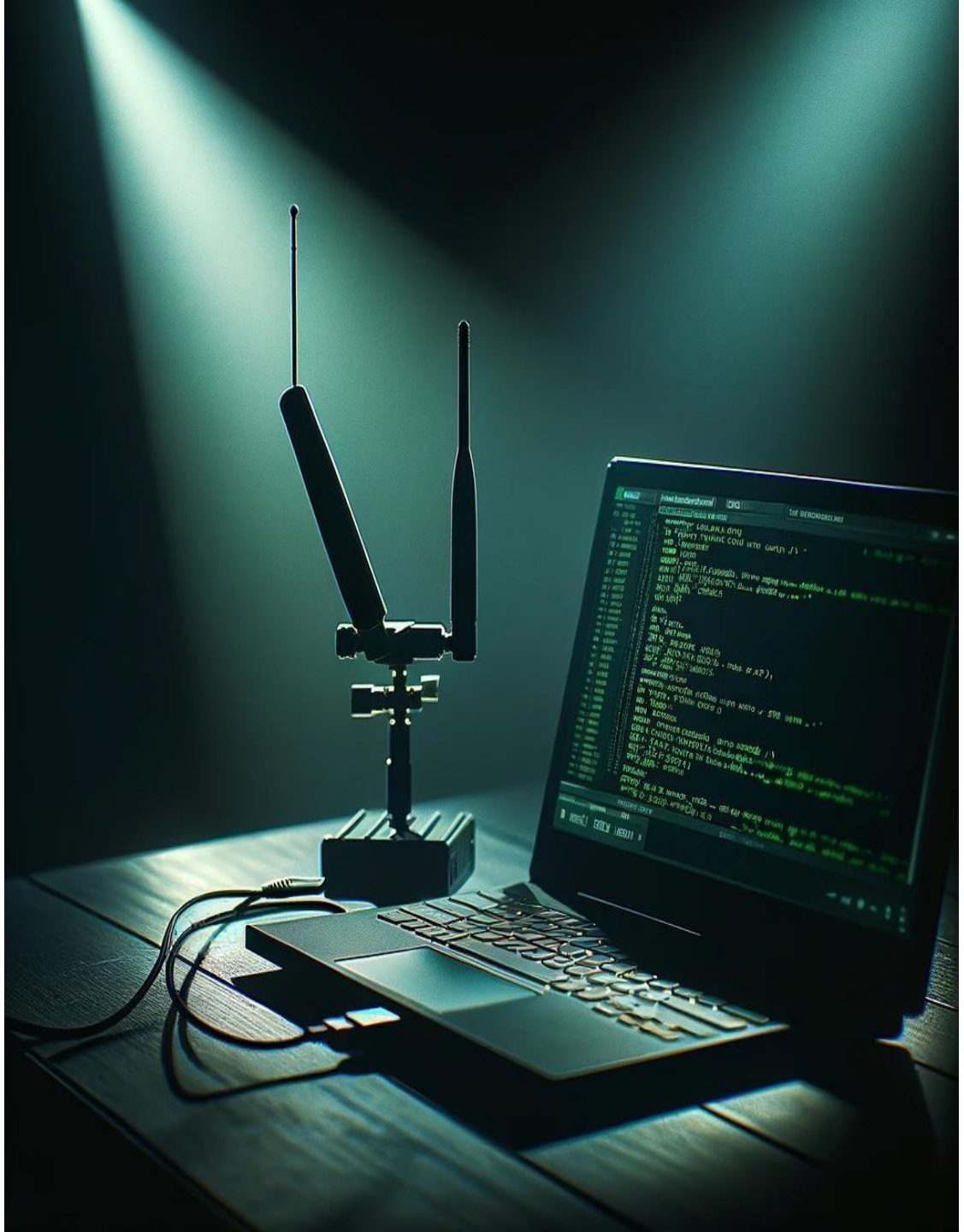
- **Απαιτούμενα αμυντικά μέτρα:**
  - **Προηγμένες άμυνες κυβερνοασφάλειας** για δίκτυα βιομηχανικών συστημάτων ελέγχου (ICS) και επιχειρησιακής τεχνολογίας (OT) για την προστασία από συγκεκριμένες απειλές για τις πυρηνικές εγκαταστάσεις.
  - Συστήματα **συνεχούς παρακολούθησης** και ανίχνευσης σε πραγματικό χρόνο για τον γρήγορο εντοπισμό και την αντιμετώπιση δυνητικών περιστατικών κυβερνοασφάλειας.
  - **Ολοκληρωμένες στρατηγικές αντιμετώπισης καταστάσεων έκτακτης ανάγκης,** συμπεριλαμβανομένων σχεδίων αντιμετώπισης περιστατικών κυβερνοασφάλειας, ώστε να διασφαλίζεται ο γρήγορος περιορισμός και μετριασμός.
  - **Διεθνής συνεργασία** σε πρότυπα και βέλτιστες πρακτικές πυρηνικής κυβερνοασφάλειας για την ενίσχυση της καθολικής στάσης ασφαλείας έναντι κοινών απειλών.

Υποτομέας εναλλακτικών καυσίμων

- **Ευαίσθητοι τύποι δεδομένων:**
  - **Δεδομένα παραγωγής:** πληροφορίες σχετικά με τις διαδικασίες παραγωγής, τα ποσοστά και τις τεχνολογικές καινοτομίες για εναλλακτικά καύσιμα όπως το βιοντίζελ, η αιθανόλη και το υδρογόνο.
  - **Δεδομένα εφοδιαστικής αλυσίδας:** Λεπτομέρειες σχετικά με την εφοδιαστική, τη διανομή
    δίκτυα και εγκαταστάσεις αποθήκευσης για εναλλακτικές πηγές καυσίμων.
  - **Δεδομένα έρευνας και ανάπτυξης λογισμικού:** Κρίσιμα δεδομένα σχετικά με νέες τεχνολογίες, διπλώματα ευρεσιτεχνίας και πειραματικές διαδικασίες με στόχο τη βελτίωση της αποδοτικότητας και τη μείωση του κόστους.
- **Στρατηγική σημασία:**
  - **Αειφορία και ενεργειακή μετάβαση:** Τα εναλλακτικά καύσιμα είναι το κλειδί για τη μείωση στην εξάρτηση από τα ορυκτά καύσιμα και την επίτευξη των στόχων βιωσιμότητας.
  - **Οικονομική ανάπτυξη:** Ο τομέας αποτελεί αναπτυσσόμενη αγορά με σημαντικές επενδύσεις σε R&D, συμβάλλοντας στην οικονομική διαφοροποίηση και την καινοτομία.

Υποτομέας εναλλακτικών καυσίμων

- **Κίνδυνοι εκμετάλλευσης στον κυβερνοχώρο:**
  - **Κλοπή πνευματικής ιδιοκτησίας:** Κατασκοπεία στον κυβερνοχώρο με στόχο την κλοπή ιδιοταγών τεχνολογιών και δεδομένων R&D για την απόκτηση ανταγωνιστικών πλεονεκτημάτων.
  - **Παρεμβολές αλυσίδας εφοδιασμού:** Οι επιθέσεις στα δεδομένα της αλυσίδας εφοδιασμού μπορεί να οδηγήσουν σε διαταραχές στη διανομή και τη διαθεσιμότητα εναλλακτικών καυσίμων.
  - **Σαμποτάζ παραγωγής:** Οι κυβερνοεπιθέσεις με στόχο τα συστήματα ελέγχου των εγκαταστάσεων παραγωγής θα μπορούσαν να οδηγήσουν σε διακοπή της παραγωγής, καταστροφή του εξοπλισμού ή υποβάθμιση της ασφάλειας.
  - **Χειραγώγηση της αγοράς:** Η πρόσβαση σε ευαίσθητα δεδομένα της αγοράς και οικονομικά δεδομένα θα μπορούσε να χρησιμοποιηθεί για εμπιστευτικές συναλλαγές ή για χειραγώγηση των τιμών της αγοράς.
- **Απαιτούμενα αμυντικά μέτρα:**
  - **Ισχυρά μέτρα κυβερνοασφάλειας** προσαρμοσμένα για την προστασία τόσο των περιβαλλόντων IT όσο και των περιβαλλόντων επιχειρησιακής τεχνολογίας (OT) που εμπλέκονται στην παραγωγή και την R&D.
  - **Υλοποίηση ασφαλών πρωτοκόλλων ανταλλαγής δεδομένων** για την προστασία των πληροφοριών της αλυσίδας εφοδιασμού και τη διασφάλιση της ακεραιότητας των κατανεμημένων ενεργειακών πόρων.
  - **Ενισχυμένα προγράμματα ευαισθητοποίησης στον κυβερνοχώρο** για τους υπαλλήλους για τον μετριασμό των κινδύνων από επιθέσεις «ψαρέματος» και εσωτερικές απειλές.
  - **Συνεργασία με ρυθμιστικούς φορείς** και ομάδες του κλάδου για την ανάπτυξη και τήρηση προτύπων κυβερνοασφάλειας ειδικά για τον τομέα των εναλλακτικών καυσίμων.



Το λογισμικό είναι απαραίτητο, αλλά...

Δεδομένα ...

- Κίνητρο - Μεγάλο -> Μεγάλα χρηματικά ποσά από **ανταγωνιστή** ή κάποιο με **διαφορετικά επιχειρηματικά ενδιαφέροντα**
- Μεγάλη δεξαμενή διαφορετικών λογισμικών = υψηλή πιθανότητα για τον επιτιθέμενο να βρει μια ευπάθεια
- Υλική ενσωμάτωση ασφάλειας
- Δεν μπορείτε να αφήσετε κάποιον κοντά με ένα φορητό υπολογιστή και μια κεραία

Κατανόηση των κινδύνων - μετριασμοί

- Κίνδυνος Αξιολόγηση
  - Δήλωση περιουσιακών στοιχείων και υπολογισμός αντίκτυπου
- Εντοπισμός Ευπαθών δυαδικών αρχείων
  - Μικρές δοκιμές διεισδύσεων σε κάθε διαφορετικό δυαδικό σύστημα
- Στρατηγικές μετριασμού
  - Προστασία δικτύου
  - Προστασία λογισμικού
- Ανθρώπινο λάθος
  - Εκπαίδευση ναυτικού προσωπικού

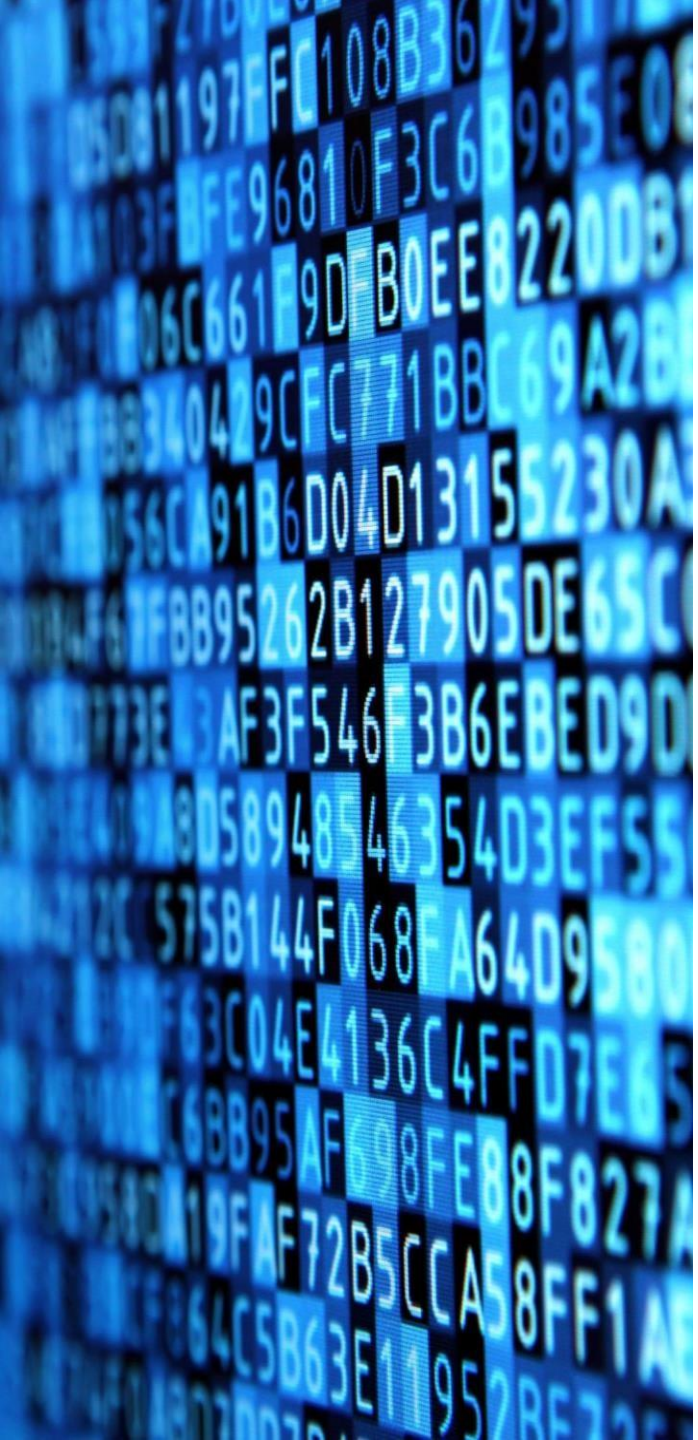
Πρόοδος μαθημάτων

01. Πλοήγηση στις απειλές στον κυβερνοχώρο: Ο κίνδυνος των ευάλωτων δυαδικών συστημάτων στα θαλάσσια συστήματα

02. Από το λογισμικό στα δυαδικά αρχεία

03. Μνήμη

04. Black Box δοκιμές διείσδυσης



Από το λειτουργικό λογισμικό στο ευάλωτο δυαδικό σύστημα

Τι είναι το δυαδικό σύστημα;

Τα δυαδικά αρχεία, είναι αρχεία υπολογιστή που περιέχουν μεταγλωττισμένο κώδικα προγραμματισμού από γλώσσες προγραμματισμού όπως η C ή η C++.

Δυαδική μορφή, σημαίνει ότι είναι εγγεγραμμένα στο δυαδικό αριθμητικό σύστημα που αποτελείται μόνο από 1 και 0.

Μηχανική γλώσσα που μπορεί η CPU ενός υπολογιστή να χρησιμοποιήσει άμεσα.

Δίνει εντολή στον υπολογιστή να αποδίδει συγκεκριμένες λειτουργίες

Ευπάθειες στα δυαδικά αρχεία

Πού μπορούμε να βρούμε ευπάθειες;

- **Φάση προγραμματισμού κώδικα**
  - Οι προγραμματιστές ενδέχεται να εγγραφούν κώδικας προγραμματισμού που δεν είναι ασφαλής, όπως για παράδειγμα να μην χειρίζονται σωστά την είσοδο εξωτερικών δεδομένων.
- **Φάση μεταγλωττισμού**
  - Οι βελτιστοποιήσεις του μεταγλωττιστή ή οι παρανοήσεις της πρόθεσης του κώδικα προγραμματισμού μπορούν να εισάγουν ευπάθειες.
- **Προαπαιτούμενα**
  - Εάν ο κώδικας προγραμματισμού βασίζεται σε εξωτερικές βιβλιοθήκες ή εξαρτήματα που είναι τα ίδια μη ασφαλή
- **Περιβάλλοντα**
  - Το περιβάλλον στο οποίο μεταγλωττίζεται ο κώδικας προγραμματισμού (όπως το λειτουργικό σύστημα) μπορεί να εισάγει ευπάθειες, ιδίως αν είναι διαφορετικό από το περιβάλλον στο οποίο γράφτηκε ο κώδικας.

Πρόοδος μαθημάτων

01. Πλοήγηση στις απειλές στον κυβερνοχώρο: Ο κίνδυνος των ευάλωτων δυαδικών συστημάτων στα θαλάσσια συστήματα

02. Από το λογισμικό στα δυαδικά αρχεία

03. Μνήμη

04. Black Box δοκιμές διείσδυσης

Σφάλματα φθοράς μνήμης

Παρόν σε λογισμικό που προγραμματίζεται από προγραμματιστές που

- επιτρέπουν κατευθύνσεις μνήμης Assembly, C, C++, ...)
  - *p = value; - pointers
- να μην αποδίδει ελέγχους εκτός ορίων σε λειτουργικές πράξεις τύπου array
  - a[++i] = 4;

Σφάλματα φθοράς μνήμης

Επίσης, επηρεάζουν το λογισμικό που βασίζεται σε εξαρτήματα που είναι ευάλωτα σε σφάλματα φθοράς μνήμης. Για παράδειγμα:

- Η Java δεν επιτρέπει κατευθύνσεις μνήμης και εγείρει εξαίρεση κατά το χρόνο εκτέλεσης σε σφάλματα δείκτη συστοιχίας
  - Ωστόσο, η JVM είναι ευάλωτη σε σφάλματα φθοράς της μνήμης
  - Οι εγγενείς βιβλιοθήκες του JDK είναι ευάλωτες σε σφάλματα διαφθοράς μνήμης
  - Η εκτέλεση αναξιόπιστου κώδικα bytecode σε JVM θα μπορούσε να προκαλέσει τέτοια σφάλματα π.χ. applets φυλλομετρητών).

Τα σφάλματα φθοράς μνήμης είναι παντού

- Λειτουργικό σύστημα Kernels
- Βιβλιοθήκες συστήματος
- Εργαλεία συστήματος
- Λογισμικό για ενσωματωμένα συστήματα (δρομολογητές, τηλεοράσεις, κινητές συσκευές, ...)
- Υπηρεσίες διαδικτύου
- Μητρικές βιβλιοθήκες
- Φυλλομετρητές Web
- Λογισμικό υποστήριξης συστημάτων SCADA
- ...

Επιπτώσεις των σφαλμάτων φθοράς μνήμης

- Το πρόγραμμα συνεχίζει να εργάζεται με τροποποιημένα δεδομένα στη μνήμη
- Αλλαγή χρόνου εκτέλεσης στην επιχειρησιακή λογική
- Άρνηση παροχής υπηρεσιών (διακοπή λειτουργίας προγράμματος)
- Εκτέλεση κώδικα προγραμματισμού
- Παράκαμψη ελέγχου ασφαλείας
- Αποκάλυψη ευαίσθητων πληροφοριών

Κοινά σφάλματα φθοράς μνήμης

- Υπερχείλιση ρυθμιστικού διαστήματος
- Σφάλματα off-by-one
- Μη αξιόπιστα σφάλματα ανάκλησης δείκτη
  - γράψε **κάτι** *κάπου* τύπου λάθη
- Σφάλματα συμβολοσειράς μορφοποίησης

Υπερχείλιση ρυθμιστικού διαστήματος

- Τα δεδομένα εγγράφονται μετά το τέλος buffer, αλλοιώνοντας τα περιεχόμενα των παρακείμενων θέσεων μνήμης.
- Παράδειγμα:

```
/* attacker controls all img.hdr data */
memcpy(dest, &(img.hdr), img.hdr.size);
```

- Τι γίνεται αν ένας επιτιθέμενος κάνει το img.hdr.size μεγαλύτερο από το μέγεθος του dest buffer;
- Συνήθεις τύποι
  - Υπερχείλιση ρυθμιστικού διαφράγματος στοίβας (τοπικές μεταβλητές κ.λπ)
  - Υπερχείλιση buffer σωρού (δυναμικά εκχωρημένες μεταβλητές/αντικείμενα)
- Άλλοι τύποι
  - Υπερχείλιση ρυθμιστικού διαφράγματος BSS (καθολικές μεταβλητές με δυνατότητα εγγραφής)
- Πρόταση: αποδίδει λειτουργίες ελέγχου ορίων / περιόρισε τη λειτουργία αντιγραφής στο μέγεθος του ρυθμιστικού διαύλου προορισμού.

Υπερχείλιση ρυθμιστικού διαστήματος

Συνήθως οφείλεται στη χρήση *μη ασφαλών* συναρτήσεων της libc: gets(3),scanf(3), sprintf(3), strcpy(3), strcat(3), ...

Αυτές οι συναρτήσεις σταματούν την αντιγραφή δεδομένων όταν βρουν NULL οκτάδα-byte στον πηγαίο buffer (ή EOF για την gets(3)), ανεξάρτητα από το μέγεθος του buffer προορισμού.

```
char argument[100]; strcpy(argument, argv[2]);
```

Υπάρχουν *ασφαλείς* εναλλακτικές λύσεις: fgets(3), snprintf(3), strncpy(3), strncat(3), ...

επιτρέπουν στους προγραμματιστές να καθορίσουν τον μέγιστο αριθμό των οκτάδων-byte που θα εγγραφούν στο buffer προορισμού

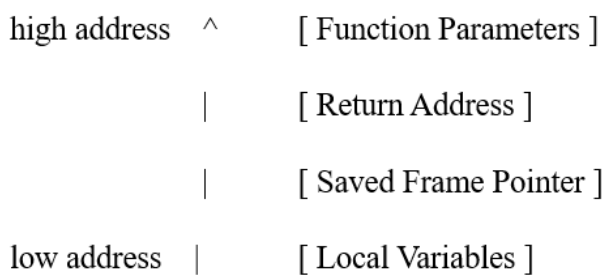
Υπερχείλιση ρυθμιστικού διαστήματος

Οι επιτιθέμενοι μπορούν να προκαλέσουν υπερχείλιση buffer όταν ελέγχουν τουλάχιστον μία από τις παρακάτω παραμέτρους

- το μέγεθος των δεδομένων που αντιγράφονται
- η θέση του buffer εισόδου δεδομένων
- τα δεδομένα που αντιγράφονται (και το λογισμικό αναμένει συγκεκριμένο σύμβολο τερματισμού στα δεδομένα)
- το μέγεθος του buffer εξόδου
- η θέση του buffer εξόδου

Εκμετάλλευση ευπάθειας στη στοίβα

- Στοίβα κλήσης συναρτήσεων



  - Μια υπερχείλιση σε τοπική μεταβλητή μπορεί να αντικαταστήσει τη διεύθυνση επιστροφής της συνάρτησης
  - Η διεύθυνση επιστροφής καθορίζει την δοσμένη εντολή που θα εκτελεστεί μόλις η συνάρτηση εξέρχεται
  - Ένας επιτιθέμενος μπορεί να εκμεταλλευτεί την υπερχείλιση για να ανακατευθύνει τη ροή προγραμματισμού σε:
    - κώδικα προγραμματισμού που παρέχεται ως μέρος της υπερχείλισης
    - άλλο κώδικας προγραμματισμού εντός του χώρου μνήμης της διεργασίας

Σφάλματα off-by-one

- Παράδειγμα:

```
void func(....)
{
        char buf [255] ;
        char data [255] ;

        ...
        for (i = 0; i <= sizeof(buf); i++)
        buf[i] = data[i];
        ...
}
```

- Πολύ δημοφιλή σφάλματα που οφείλονται στη σημασιολογία C ή στη σημασιολογία του API (π.χ. το strncpy) δεν τερματίζει εξόδου με NULL, αντιγράφει έως και *n* οκτάδες-byte
- Πρόταση: να μην αντιγράφετε περισσότερες οκτάδες-bytes από το μέγεθος του buffer προορισμού.

Εκμετάλλευση ευπάθειας off-by-one

Αντικατάσταση μιας οκτάδας-byte του αποθηκευμένου δείκτη πλαισίου

Μια υπερχείλιση off-by-one στη μεταβλητή ακριβώς δίπλα στον δείκτη του αποθηκευμένου πλαισίου θα αλλάξει μια οκτάδα-byte
στη διεύθυνση του δείκτη του αποθηκευμένου πλαισίου

Αυτή η διεύθυνση μπορεί να δείχνει σε ψεύτικο πλαίσιο στοίβας μέσα στα δεδομένα που παρέχει ο επιτιθέμενος.

Στον επίλογο της Ευπάθειας: ESP=EBP,EBP= modified frame pointer

Στον επίλογο του καλούντος: ESP= διαμορφωμένος δείκτης πλαισίου, αλλά η οδηγία ret (επιστροφή) θα χρησιμοποιήσει διεύθυνση που βρίσκεται στην «ψεύτικη» στοίβα πλαισίου

Μη εκτελέσιμες σελίδες

Η W^X φιλοσοφία των εγγράψιμων σελίδων δεν πρέπει να είναι εκτελέσιμες

Οι πρόσφατες CPU επιτρέπουν στις σελίδες να χαρακτηρίζονται ως μη εκτελέσιμες

AMD NXbit Intel XD bit

Ένα εκτελέσιμο αρχείο ή βιβλιοθήκη μπορεί να περιγράψει ποια τμήματα πρέπει να φορτωθούν σε μη εκτελέσιμες σελίδες

Το W^X μπορεί να προσομοιωθεί στο λογισμικό

- χρήση του καταχωρητή CS για τον περιορισμό του εκτελέσιμου μέρους τμήματος του έργου ExecShield

Προληπτικό χαρακτηριστικό ασφαλείας: μπορεί να σταματήσει τους επιτιθέμενους από το να εκτελέσουν κώδικα στη στοίβα κ.λπ.

Προστασία στοίβας

Κάνοντας την στοίβα μη εκτελέσιμη

Αναδιάταξη μεταβλητών για την προστασία των δεικτών συναρτήσεων

Οι δείκτες συναρτήσεων τοποθετούνται σε χαμηλότερες διευθύνσεις μνήμης για να προστατεύονται από υπερχειλίσεις πινάκων ή άλλων μεταβλητών

Canaries

Μια τυχαία τιμή (canary) τοποθετείται αμέσως μετά από τοπικές παραμέτρους συνάρτησης

Εάν η συνάρτηση εξέλθει και το canary έχει αλλάξει, αυτό είναι ένδειξη υπερχείλισης και η εφαρμογή αμέσως βγάζει gcc-fstack- protector-all

Επιλογή μεταγλωττιστή Visual Studio /GS

Προγραμματισμός προσανατολισμένος στην επιστροφή

- Εάν η διεύθυνση κάποιου μέρους του κώδικα προγραμματισμού (εκτελέσιμο / βιβλιοθήκη / άλλος κώδικας προγραμματισμού) μπορεί να βρεθεί τυχαία, τότε ένας επιτιθέμενος μπορεί να δανειστεί τον κώδικα
  για να εκτελεί εντολές (ή να παρακάμπτει τις προστασίες μνήμης)
- Για παράδειγμα, αν η διεύθυνση της system () μπορεί να βρεθεί τυχαία, τότε ο επιτιθέμενος μπορεί να αποδώσει επίθεση «return to libc» κλήση συστήματος με τις σωστές παραμέτρους
- Προγραμματισμός προσανατολισμένος στην επιστροφή (ROP): η επόμενη διεύθυνση προς εκτέλεση αφαιρείται τη στοίβα λόγω μιας εντολής ret

Προγραμματισμός προσανατολισμένος στην επιστροφή

- Εναλλακτικά, με τη χρήση αποσπασμάτων δανεισμένου κώδικα προγραμματισμού («gadgets»), ένας επιτιθέμενος μπορεί να εκτελέσει αλυσιδωτά μια εκμετάλλευση ευπάθειας που:
  - κατανέμει νέα σελίδα μνήμης εκτελέσιμης εφαρμογής
  - εγγράφει Shellcode σε αυτή τη σελίδα
  - εκτελεί το Shellcode
- Τεχνικές αλυσιδωτής σύνδεσης:
  - παροχή στον κώδικα προγραμματισμού διευθύνσεων μικροεφαρμογών π.χ. μέσω του buffer στη στοίβα)
    - κάθε gadget εκτελείται και επιστρέφει έτσι ώστε η επόμενη διεύθυνση επιστροφής να να χρησιμοποιηθεί)
  - αντί για δηλώσεις επιστροφής, επίσης μπορούν να χρησιμοποιηθούν τεχνικές (μεταβάσεις κ.λπ.)

Σφάλματα συμβολοσειράς μορφοποίησης

- Ορισμένες φορές οι προγραμματιστές επιτρέπουν την είσοδο δεδομένων μορφής από τους χρήστες

```
strcpy(fmt_buf, "user id: %i user: ");
strcat(fmt_buf, username);
sprintf(formatted_str, fmt_buf, id);
```

- Ή επιτρέψτε στους χρήστες τον πλήρη έλεγχο των συμβολοσειρών μορφοποίησης

```
printf(username);
```

- Εάν ένας επιτιθέμενος τοποθετήσει προσδιορισμό %s, η επόμενη διεύθυνση στη θα θεωρηθεί ότι δείχνει σε μια συμβολοσειρά και όλα τα περιεχόμενα (που οδηγούν σε ένα NULL) θα απορριφθούν ως μέρος της κλήσης.
- Καθοριστής %n: *Ο αριθμός των χαρακτήρων που έχουν εγγραφεί μέχρι στιγμής αποθηκεύεται στον ακέραιο που υποδεικνύεται από το όρισμα δείκτη int * (ή παραλλαγή). Κανένα όρισμα δεν μετατρέπεται.*
  - Κάθε προσδιορισμός μορφής %n που παρέχεται από έναν επιτιθέμενο θα εγγραφεί σε ένα διεύθυνση που βρέθηκε στη στοίβα η οποία μπορεί να ελεγχθεί από τον επιτιθέμενο!

Σφάλματα συμβολοσειράς μορφοποίησης

```
#include <stdio.h>
#include <stdlib.h>

int main(int argc, char *
argv[]){
  int x = 0xdeadbeef;
  printf("%%d:(%d)\n",x);
  printf("%%u:(%u)\n",x);
  printf("%%x:(%x)\n",x);
  printf("%%#x:(%#x)\n",x);
  printf("%%#50x:(%#50x)\n",x);
  printf("%%#050x:(%#050x)\n",x);
  printf("%%1$#050x %%1$d:(%1$#050x
%1$d)\n",x);
  printf("%%#050x:(%#050x)\n",x);
  printf("%%1$#050x %%1$d:(%1$#050x
%1$d)\n",x);
}
```

Σφάλματα συμβολοσειράς μορφοποίησης

```
user@si485H-base:demo$ ./unusual_formats
%d:(-559038737)
%u:(3735928559)
%x:(deadbeef)
%#x:(0xdeadbeef)
%#50x:(                                  0xdeadbeef)
%#050x:(0x00000000000000000000000000000000deadbeef)
%1$#050x %1$d:(0x00000000000000000000000000000000deadbeef -559038737)
%1$#050hx %1$hd:(0x0000000000000000000000000000000000000beef -16657)
%1$#050hhx %1$hd:(0x000000000000000000000000000000000000000ef -17)
```

Παραπομπές δείκτη NULL

- Παράδειγμα:

```
x = userinput () ;

p = malloc (x * sizeof (struct FILE_OPS) ) ;

fop = & (p [FILE_TYPE] ) ;

fop->remove (file) ;
```

- Τι γίνεται αν η κλήση στη malloc αποτύχει;
- Αυτό είναι επικίνδυνο σφάλμα για τον κώδικα κλήσης συστήματος (σε συστήματα που έχουν ενοποιημένο διευθύνσεων μεταξύ πυρήνα και userland), καθώς μια διεργασία μπορεί να αντιστοιχίσει τις σελίδες εκτελέσιμο κώδικα προγραμματισμού.
- Πρόταση: Πάντα να ελέγχετε την τιμή επιστροφής των συναρτήσεων κατανομής μνήμης.
- Προληπτικό μέτρο για σφάλματα Kernel: απαγορεύστε την πρόσβαση στις πρώτες σελίδες μνήμης.

Παραπομπές δείκτη NULL

```
int a, b, c; // some integers
int *pi; // a pointer to an integer

a = 5;
pi = &a; // pi points to a
 b = *pi; // b is now 5
pi = NULL;
 c = *pi; // this is a NULL pointer dereference
```

Πρόοδος μαθημάτων

01. Πλοήγηση στις απειλές στον κυβερνοχώρο: Ο κίνδυνος των ευάλωτων δυαδικών συστημάτων στα θαλάσσια συστήματα

02. Από το λογισμικό σε δυαδικά αρχεία

03. Μνήμη

04. Black Box δοκιμές διείσδυσης

Εξερευνώντας το δυαδικό σύστημα

Μορφή αρχείου

- Η χρησιμότητα του 'file'

```
$ file foo
foo: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.24, BuildID[sha1]=0x628d57caa90b9cb4d373105a9b17da72aa4bb0d7, not stripped
$
```

Εξερευνώντας την λειτουργικότητα της εφαρμογής

Εκτέλεση της εφαρμογής για τον εντοπισμό των βασικών λειτουργιών

Καταστάσεις εφαρμογής

Σημεία εισαγωγής του χρήστη / έξοδοι

στοιχεία που θα ήταν ευάλωτα εάν ευπάθεια στην εφαρμογή εκμεταλλευόταν σε υψηλό επίπεδο ελέγχων ασφαλείας

άδειες αρχείου

αναγκαία/αποκτηθέντα προνόμια

Προαπαιτούμενα σε δυναμικές βιβλιοθήκες

- Χρησιμοποιήστε το 'ldd' για να εντοπίσετε προαπαιτούμενα σε δυναμικές βιβλιοθήκες

```
$ ldd foo

        linux-gate.so.1 => (0x00602000)
        libc.so.6 => /lib/i386-linux-gnu/libc.so.6 (0x00110000)
        /lib/ld-linux.so.2 (0x005c8000)

$
```

Ενσωματωμένες στατικές βιβλιοθήκες

- Αναζητήστε ενδιαφέροντα σύμβολα με 'nm' ή 'objdump'

```
$ objdump-d foo
...
804c315: e8 b6 00 00 00 call 804c3d0 <SSL_library_init>
...
$
```

Παρακολούθηση εκτέλεσης

Χρησιμοποιήστε το 'strace' για να εντοπίσει τις κλήσεις συστήματος

```
$ strace-fF ./foo
...
[pid 16155] execve("/bin/mount", ... ) = 0
...
$
Use ’ltrace’ to trace library calls
$ ltrace ./foo
...
strcpy(0xbfc0343d, 0xbfc0451a) = 0xbfc0343d
...
$
```

Αναζήτηση Ευπαθειών

Μορφή αρχείου

- Η χρησιμότητα του 'file'

```
$ file foo
foo: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared
libs), for GNU/Linux 2.6.24, BuildID[sha1]=0x628d57caa90b9cb4d373105a9b17da72aa4bb0d7,
not stripped
$
```

Εξερευνώντας τη λειτουργικότητα της εφαρμογής

Εκτέλεση της εφαρμογής για τον εντοπισμό των βασικών λειτουργιών

Καταστάσεις εφαρμογής

Σημεία εισαγωγής του χρήστη / έξοδοι

στοιχεία που θα ήταν ευάλωτα εάν ευπάθεια στην εφαρμογή εκμεταλλευόταν σε υψηλό επίπεδο ελέγχων ασφαλείας

άδειες αρχείου

αναγκαία/αποκτηθέντα προνόμια

Προαπαιτούμενα σε δυναμικές βιβλιοθήκες

- Χρησιμοποιήστε το 'ldd' για να εντοπίσετε προαπαιτούμενα σε δυναμικές βιβλιοθήκες

```
$ ldd foo
        linux-gate.so.1 => (0x00602000)
        libc.so.6 => /lib/i386-linux-gnu/libc.so.6 (0x00110000)
        /lib/ld-linux.so.2 (0x005c8000)
$
```

Ενσωματωμένες στατικές βιβλιοθήκες

- Αναζητήστε ενδιαφέροντα σύμβολα με 'nm' ή 'objdump'

$ objdump -d foo

...

804c315: e8 b6 00 00 00 call 804c3d0 <SSL_library_init>...

$

Παρακολούθηση εκτέλεσης

Χρησιμοποιήστε το 'strace' για να εντοπίσει τις κλήσεις συστήματος

$ strace-fF ./foo

...

[pid 16155] execve("/bin/mount", ...) = 0

...

$

Use ’ltrace’ to trace library calls

$ ltrace ./foo

...

strcpy(0xbfc0343d, 0xbfc0451a) = 0xbfc0343d

...

$

Δοκιμές Fuzz

- Δοκιμές άγριων τιμών εισόδου δεδομένων σε παραμέτρους που ελέγχονται από τον χρήστη
- Χρήση αυτοματοποιημένων fuzzers
  - Πρωτόκολλο δοκιμής fuzz με 'peach'
  - Δοκιμή fuzz με το 'honggfuzz'

Έλεγχος αν ένα «crash» λόγω φθοράς της μνήμης είναι ενδιαφέρον/εκμεταλλεύσιμο

Χρησιμοποιήστε πρόγραμμα εντοπισμού σφαλμάτων (όπως το 'gdb') για να ελέγξετε αν:

Η EIP ορίστηκε σε τιμή ελεγχόμενη από τον χρήστη

Η είσοδος δεδομένων αντικατέστησε δεδομένα ελέγχου στη στοίβα π.χ. αποθηκευμένο στοίβας / EIP

Η είσοδος αντικατέστησε ελεγχόμενα δεδομένα στο σωρό (π.χ. ελεύθερη λίστα δεικτών)

Η είσοδος δεδομένων αντικατέστησε ευαίσθητα δεδομένα στη στοίστο σωρό (π.χ. συναρτήσεων)

Εντοπισμός και εκμετάλλευση λειτουργιών με γνωστές ευπάθειες

- μια υπερχείλιση buffer *strcpy*
- μια υπερχείλιση του buffer *memcpy*
- μια *printf* με σφάλμα συμβολοσειράς μορφοποίησης
- ...

Αποσυναρμολόγηση

- Χρησιμοποιήστε αποσυναρμολογητή (όπως το 'objdump') για να δείτε πόσο ενδιαφέρων είναι ο κώδικας προγραμματισμού
- Χρησιμοποιήστε πρόγραμμα εντοπισμού σφαλμάτων (όπως το 'gdb') για να ακολουθήσετε ενδιαφέρουσες διαδρομές κώδικα προγραμματισμού

Διερευνήστε τον τύπο της ευπάθειας

- Ανατρέξτε στο /proc/{PID}/maps για να διαπιστώσετε αν ένας υπερχειλισμένος buffer ανήκει στο σωρό ή στη στοίβα

...

09133000-09431000 rw-p 00000000 00:00 0 [heap]

...

bfc44000-bfc65000 rw-p 00000000 00:00 0 [stack]

...

Καταγραφή ευπάθειας

- Καταγράψτε τον ευάλωτο κώδικα
- Καταγράψτε τον τύπο ευπάθειας
- Καταγράψτε το έναυσμα
- Λάβετε υπόψη ότι πολλαπλές αδυναμίες μπορεί να φανούν χρήσιμες κατά τη φάση της εκμετάλλευσης ευπάθειας (π.χ. διαρροή διευθύνσεων και αλλοίωση μνήμης σε σελίδες κοντά στη διεύθυνση που διέρρευσε).

Σας ευχαριστούμε

Παρακαλούμε στείλτε όλες τις ερωτήσεις στη διεύθυνση:
dkoutras@unipi.gr