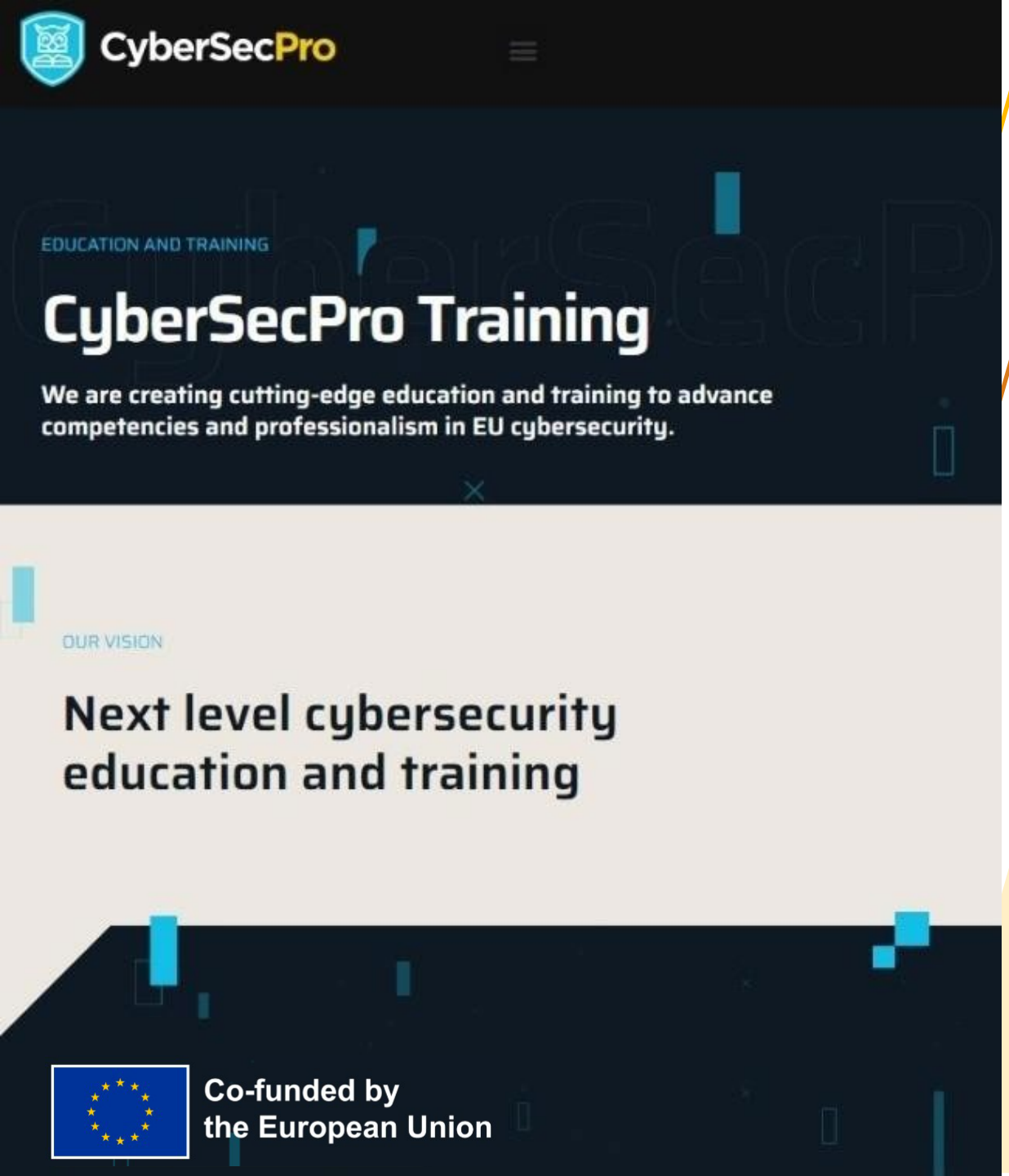
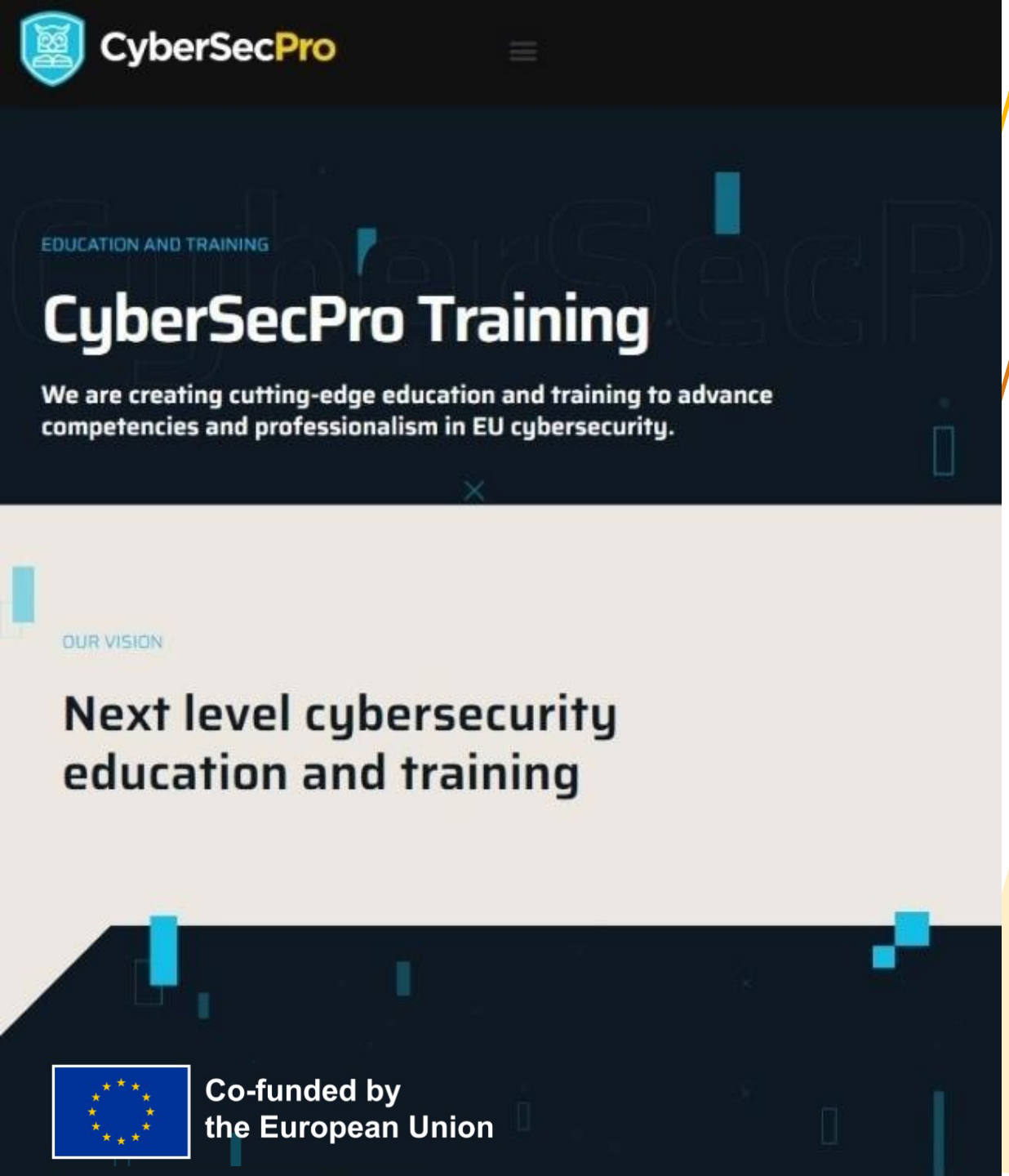


Προστασία Σταθμών Φόρτισης από Συγκεκριμένες Απειλές - Protecting Charging Stations Against Specific Threats

CSP008_S_E

ΠΑΡΟΥΣΙΑΣΗ ΑΠΟ:
DR. ELIAS ATHANASOPOULOS
UNIVERSITY OF CYPRUS
DR. ABDELKADER SHAABAN
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY



Αναγνώριση

Συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση. Οι απόψεις και οι γνώμες που εκφράζονται είναι, ωστόσο, μόνο του/των συγγραφέα/ων και δεν αντικατοπτρίζουν απαραίτητα εκείνες της Ευρωπαϊκής Ένωσης ή του HADEA. Ούτε η Ευρωπαϊκή Ένωση ούτε η χορηγούσα αρχή μπορούν να θεωρηθούν υπεύθυνες γι' αυτές.

Project Agreement no. 101083594

the

Προστασία σταθμών φόρτισης από συγκεκριμένες απειλές

Επισκόπηση

- Θέμα-1: Εισαγωγή στις Υποδομές Χρέωσης Ενέργειας
- Θέμα-2: Προκλήσεις ασφάλειας στους σταθμούς φόρτισης ενέργειας
- Θέμα-3: Αλυσιδωτές επιπτώσεις και το αντίκτυπο σε άλλες κρίσιμες υποδομές
- **Θέμα-4: Μέτρα ασφαλείας και βέλτιστες πρακτικές για σταθμούς φόρτισης**

Ατζέντα

1. Ορθές Πρακτικές
2. Αντίμετρα

Ορθές Πρακτικές

Σταθμοί Φόρτισης

Είναι ουσιαστικά κυβερνοφυσικά συστήματα με πολλά στοιχεία

Τα στοιχεία έχουν διαφορετικές αρχιτεκτονικές που αλληλεπιδρούν μεταξύ τους

- Το αυτοκίνητο μπορεί να λειτουργεί με διάφορους μικροεπεξεργαστές
- Ο σταθμός φόρτισης ενδέχεται να λειτουργεί με διαφορετικό λογισμικό/υλικό

Τα στοιχεία πρέπει να δημιουργήσουν επικοινωνία

Πολυεπίπεδα μέτρα ασφαλείας

Μπορούμε να χωρίσουμε έναν σταθμό φόρτισης σε διαφορετικά επίπεδα

- Π.χ., το τμήμα συστήματος του αυτοκινήτου βρίσκεται σε διαφορετικό επίπεδο με τη διεπαφή που συνδέεται με τον σταθμό

Στη συνέχεια, μπορούμε να υποθέσουμε διαφορετικά μοντέλα απειλών ανά επίπεδο

- Κάθε μοντέλο απειλής στοχεύει σε διαφορετικά μέρη του κυβερνοφυσικού συστήματος.

Τελικά, εξάγουμε άμυνες ασφαλείας για κάθε μοντέλο απειλής

- Οι άμυνες ασφαλείας δεν είναι κάτι καινούργιο, αλλά προσαρμοσμένες σε αυτό το περιβάλλον

Επίπεδα Σταθμού Φόρτισης

Σύστημα

Υλοποιείται με κώδικα χαμηλού επιπέδου (C/C++) και εκτελείται

Εφαρμογή

Υλοποιείται σε κώδικα υψηλού επιπέδου (π.χ., εφαρμογή/υπηρεσία ιστού)

Επικοινωνία

Καλύπτει την επικοινωνία μεταξύ υποσυστημάτων

Επίπεδο Συστήματος

Ο κώδικας συστήματος χρησιμοποιείται για την εκτέλεση των χαμηλών λειτουργιών ενός στοιχείου

- Π.χ., το αυτοκίνητο διαθέτει πολλαπλούς μικροεπεξεργαστές και επιπλέον υπάρχουν λειτουργικά συστήματα

Ο κώδικας συστήματος συνήθως υλοποιείται σε μη ασφαλείς γλώσσες προγραμματισμού (C/C++)

Η μνήμη διαχειρίζεται ο προγραμματιστής

Το βασικό πρόβλημα στον κώδικα συστήματος είναι η αλλοίωση της μνήμης

Διαστρέβλωση Μνήμης

Ένα θέμα ευπάθειας στην καταστροφή μνήμης προκύπτει όταν ένας προγραμματιστής χειρίζεται τη μνήμη απρόσεκτα

- Για παράδειγμα, ένα αντίγραφο μνήμης τοποθετεί περισσότερα δεδομένα στην ενδιάμεση μνήμη προορισμού από όσα χωράει, και η υπερβολική ποσότητα δεδομένων **καταστρέφει τη μνήμη**.
- Η διαφθορά σημαίνει ότι η μνήμη θα γραφτεί με νέα δεδομένα που συνήθως ελέγχονται από τον εισβολέα.

Ο κώδικας συστήματος, ανεξάρτητα από την εφαρμογή, μπορεί να υποφέρει από ευπάθειες καταστροφής μνήμης

Διαστρέβλωση μνήμης στον σταθμό φόρτισης

Η διαστρέβλωση μνήμης μπορεί να αξιοποιηθεί με κακόβουλες εισόδους

Στον σταθμό φόρτισης, υπάρχουν πολλοί επιτηθέμενοι που μπορούν να δημιουργήσουν κακόβουλα μηνύματα

- Εάν το αυτοκίνητο είναι ευάλωτο, τότε ο σταθμός μπορεί να επιτεθεί στο αυτοκίνητο
- Εάν ο σταθμός είναι ευάλωτος, τότε το αυτοκίνητο μπορεί να επιτεθεί στον σταθμό

Σε όλες τις περιπτώσεις, οι υπάρχουσες άμυνες είναι παρόμοιες

Προστασία από Διαστρέβλωση Μνήμης

Προστασία από Διαστρέβλωση Μνήμης είναι ένα ανοιχτό πρόβλημα

Ωστόσο, υπάρχουν υπάρχουσες τεχνικές ανεθκτικότητας που μπορούν να δυσχεράνουν την εκμετάλλευση

Η ενίσχυση είναι βασισμένη βασίζεται σε μηχανισμούς διαστρέβλωσης της μνήμης και προσπαθεί να διαταράξει μέρη της

Η ενίσχυση προϋποθέτει την ύπαρξη μιας ευπάθειας και ο στόχος είναι η αποτροπή της εκμετάλλευσής της.

Υπάρχουσες Προστασίας

Οι περισσότερες πλατφόρμες, λειτουργικά συστήματα και αρχιτεκτονικές υποστηρίζουν ορισμένες τυπικές άμυνες.

- Μη εκτελέσιμες Σελίδες
- Στοίβες canaries
- Τυχαιοποίηση

Επιπλέον, υπάρχουν ορισμένες ερευνητικές προτάσεις για Προηγμένη Ενίσχυση

- Μερικά από αυτά (SafeStack, CFI) μπορούν να βρεθούν ως επιλογές σε σύγχρονους μεταγλωττιστές (π.χ., στο clang)

Ορισμένες αρχιτεκτονικές CPU έχουν προγραμματισμένες άμυνες στο επίπεδο h/w

- Η Intel ενσωματώνει shadow stacks σε ορισμένες από τις πρόσφατες CPU της

Μη εκτελέσιμες σελίδες

Η Διαστρέβλωση Μνήμης μπορεί να χρησιμοποιηθεί για να εγχύσει κώδικα σε μια διεργασία

- Ένας εισβολέας μπορεί να εισάγει κώδικα σε μια κακόβουλη είσοδο και, εάν τα δεδομένα ελέγχου είναι κατεστραμμένα, τότε ο κώδικας του εισβολέα μπορεί να εκτελεστεί.

Η εισαγωγή κώδικα βασίζεται κυρίως στην εκτέλεση δεδομένων (ενσωματωμένων σε κακόβουλες εισόδους)

- Για την αντιμετώπιση της εισαγωγής κώδικα, οι σελίδες μνήμης μπορούν να είναι εκτελέσιμες αλλά όχι εγγράψιμες (σελίδες κώδικα) ή εγγράψιμες αλλά όχι εκτελέσιμες (σελίδες στοίβας, heap και άλλες σελίδες δεδομένων).
- Δυστυχώς, οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν τον Προγραμματισμό με Προσανατολισμό στην Επιστροφή (ROP) και την επαναχρησιμοποίηση κώδικα.

Stack canaries (Σημάδια ασφαλείας)

Η διαστρέβλωση μνήμης μπορεί εύκολα να χρησιμοποιηθεί όταν υπερχειλίζουν τα buffer στη στοίβα μιας διεργασίας.

- Ο συνήθης τρόπος είναι να υπερχειλίσετε ένα buffer και να αλλάξετε την τιμή της διεύθυνσης επιστροφής

Τα Stack Canaries είναι τυχαίες τιμές που τοποθετούνται στη στοίβα, μεταξύ των buffer και της διεύθυνσης επιστροφής.

- Η αλλαγή της διεύθυνσης επιστροφής μέσω γραμμικής υπερχείλισης θα αλλάξει την τιμή του canary.
- Η αρχική τιμή του καναρινιού αποθηκεύεται σε ένα καταχωρητή h/w

Τα stack canaries μπορούν να παρακαμφθούν χρησιμοποιώντας διαρροές πληροφοριών και ευπάθειες στο heap.

Τυχαιοποίηση

Οι εγχύσεις κώδικα μπορούν να αποτραπούν χρησιμοποιώντας μη εκτελέσιμες σελίδες. Ωστόσο, η εκμετάλλευση εξακολουθεί να είναι δυνατή χρησιμοποιώντας ROP.

- Το ROP χρησιμοποιεί τον υπάρχοντα κώδικα της εικόνας διεργασίας που συναρμολογείται ως μια σειρά από ROP gadgets
- Το ROP βασίζεται στην ακριβή γνώση της διάταξης του κώδικα
- Με την τυχαιοποίηση του χώρου διευθύνσεων, οι επιτιθέμενοι δεν γνωρίζουν πού βρίσκονται οι συσκευές ROP.
  - Οι διαρροές πληροφοριών μπορούν να καταστήσουν την τυχαιοποίηση αναποτελεσματική

Προηγμένη Ενίσχυση

Έχουν προταθεί αρκετές τεχνικές (π.χ., CFI) για να καταστεί δυσκολότερη η εκμετάλλευση της διαστρέβλωσης μνήμης.

- Η Ακεραιότητα Ροής Ελέγχου υπολογίζει στατικά το γράφημα ροής ελέγχου ενός προγράμματος και στη συνέχεια προσπαθεί να το επιβάλει κατά τον χρόνο εκτέλεσης.
- Το CFG περιέχει όλες τις νόμιμες μεταφορές ελέγχου του προγράμματος

Το CFI μπορεί να βρεθεί σε όλους τους πρόσφατους μεταγλωττιστές ως επιλογή

Διαστρέβλωση Μνήμης – Δοκιμασίες για τους Σταθμούς Φόρτισης

Οι σταθμοί φόρτισης περιλαμβάνουν πολλά ενσωματωμένα συστήματα

- Είναι ένα κυβερνοφυσικό σύστημα που περιέχει πολλούς «μικρούς υπολογιστές» (εξαρτήματα)
- Συνήθως, τα ενσωματωμένα συστήματα εκτελούν κώδικα συστήματος που έχει υλοποιηθεί σε C/C++ και είναι ευάλωτα σε αλλοίωση μνήμης.

Οι άμυνες είναι συνηθισμένες σε πιο ώριμα συστήματα

- Πλήρη λειτουργικά συστήματα
- Μεταγλωττιστές τελευταίας τεχνολογίας
- Πλούσιες σε λειτουργικότητα CPU (π.χ., Intel)

CSP TRAINING MODULE NAME: PRESENTATION TEMPLATE CREATED BY PR

Επίπεδο Εφαρμογής

Ο κώδικας συστήματος εκτελεί κώδικα εφαρμογής, ο οποίος συνήθως αναπτύσσεται σε γλώσσες υψηλότερου επιπέδου

Στο δικό μας περιβάλλον, ο Κώδικας Εφαρμογής μπορεί να είναι μια υπηρεσία Ιστού

Charging Stations may offer their functionality as a Web Service

Οι σταθμοί φόρτισης μπορούν να προσφέρουν τη λειτουργικότητά τους ως διαδικτυακή υπηρεσία

Επίθεση στον κώδικα ιστού

Code Injections – Εγχύσεις Κώδικα (XSS)

- Οι διαδικτυακές εφαρμογές ενδέχεται να υποφέρουν από εγχύσεις κώδικα όταν ο κώδικας αναμειγνύεται με δεδομένα
- Για μια διαδικτυακή εφαρμογή, ο κώδικας εκφράζεται σε JavaScript που μπορεί να ενσωματωθεί σε ένα αίτημα HTTP και να αντικατοπτριστεί πίσω στο πρόγραμμα περιήγησης ενός άλλου θύματος.

Cross-site Request Forgery - **Εξαναγκασμένη Ενέργεια μέσω Διαδικτύου** (CSRF)

- Οι κακόβουλοι ιστότοποι μπορούν να εξαναγκάσουν ένα πρόγραμμα περιήγησης να εκτελέσει αιτήματα σε άλλους ιστότοπους όπου ο χρήστης διατηρεί έναν λογαριασμό

Προστασία από Cross-Site Scripting (XSS)

Οι εγχύσεις κώδικα μπορούν να μετριαστούν φιλτράροντας τον κώδικα από τα δεδομένα

- Αυτό είναι ένα δύσκολο πρόβλημα

Μια άλλη λύση είναι να περιορίσετε τους ιστότοπους που χρησιμοποιούνται για τη φόρτωση κώδικα JavaScript.

- CSP προτεινόμενο από Mozilla

Προστασία Cross-site Request Forgery

Οι επιθέσεις CSRF μπορούν να μετριαστούν με την χρήση CSRF τυχαία tokens

- Οι ευαίσθητες φόρμες μπορούν να περιλαμβάνουν ένα τυχαίο διακριτικό που θα πρέπει να υποβληθεί μαζί με την ενέργεια της φόρμας.
- Ο ιστότοπος που χρειάζεται να προστατεύσει τους χρήστες του, χρειάζεται να δημιουργήσει περισσότερες καταστάσεις για τη δημιουργία κώδικα από την πλευρά του διακομιστή (δηλαδή, να αντιστοιχίσει τυχαία διακριτικά με υποβολές φορμών)

Έχουν προταθεί και άλλες κεφαλίδες (Επικεφαλίδα προέλευσης)

Επιθέσεις Ιστού – Προκλήσεις για τους Σταθμούς Φόρτισης

Σε σύγκριση με τους παραδοσιακούς ιστότοπους, οι σταθμοί φόρτισης είναι κλειστά περιβάλλοντα

- Μπορεί να ενσωματώνουν εφαρμογές ιστού, αλλά αυτές μπορούν να αντιμετωπιστούν μεμονωμένα, σε σύγκριση με το υπόλοιπο οικοσύστημα ιστού.
- Εξετάστε τις εφαρμογές ιστού για έναν μόνο ιστότοπο

Η αντιμετώπιση των XSS, CSRF θα μπορούσε να θεωρηθεί ευκολότερη σε αυτήν τη ρύθμιση.

- Ωστόσο, θα πρέπει να υπάρχει προσοχή (π.χ., κακόβουλοι σταθμοί φόρτισης)

Επίπεδο Επικοινωνίας

Σε έναν σταθμό φόρτισης υπάρχει επικοινωνία

Η προστασία των επικοινωνιών από επιτιθέμενους man-in-the-middle μπορεί να επιτευχθεί χρησιμοποιώντας κρυπτογράφηση

- Το πρωτόκολλο is TLS
- Πέρα από την τυπική κρυπτογράφηση, το TLS χρειάζεται PKI

Ασφάλεια επιπέδου μεταφοράς (TLS)

Το TLS είναι το de facto πρωτόκολλο για την ασφάλεια των επικοινωνιών χρησιμοποιώντας κρυπτογραφία

- Προσφέρει προστασία για παθητικούς και ενεργούς επιτιθέμενους MitM

Βασισμένο σε συμμετρική κρυπτογραφία, ασύμμετρη κρυπτογραφία και κρυπτογραφικές συναρτήσεις κατακερματισμού/MACDeployed by many applications (web, e-mail, etc.)

Υπάρχουν αρκετές επιθέσεις για το TLS, αλλά είναι η καλύτερη που έχουμε μέχρι στιγμής

Δομή Δημόσιου Κλειδιού - Public Key Infrastructure (PKI)

Το TLS, για την κρυπτογράφηση επικοινωνιών, χρειάζεται μια υποδομή PKI

◦ Αυτό είναι ένα οικοσύστημα για την οικοδόμηση εμπιστοσύνης μεταξύ απομακρυσμένων μερών

Κατά τη διάρκεια του TLS, τα δύο επικοινωνούντα μέρη πρέπει να καταλήξουν σε ένα συμμετρικό κλειδί.

◦ Αυτή η δημιουργία κλειδιού πραγματοποιείται χρησιμοποιώντας κρυπτογραφία δημόσιου κλειδιού

◦ Η αξιοπιστία ενός απομακρυσμένου δημόσιου κλειδιού γίνεται μέσω πιστοποιητικών

Είναι ένα πολύπλοκο οικοσύστημα, με πολλά προβλήματα, ειδικά για τη συντήρηση

Επικοινωνίες – Προκλήσεις για του Σταθμούς Φόρτισης

MitM η επικοινωνία με έναν σταθμό φόρτισης είναι δυνατή
- Ωστόσο, και πάλι το σύστημα μπορεί να θεωρηθεί κλειστό σε σύγκριση με ολόκληρο το Διαδίκτυο.

Από την άλλη πλευρά, η διατήρηση πιστοποιητικών για τέτοια κλειστά συστήματα μπορεί να θεωρηθεί πολύ πιο δύσκολη.n

Σύνοψη

Επίπεδο Συστήματος

Μη εκτελέσιμα δεδομένα
Τυχαιοποίηση
Προχωρημένη Ενίσχυση

Επίπεδο Εφαρμογής

CSP
CSRF Tokens

Επίπεδο Επικοινωνίας

TLS

Αντίμετρα

Πιθανές Απειλές OCPP-v2.0.1

Επισκόπηση των προτεινόμενων μετριασμών στο πλαίσιο του αναλυμένου CSMS.

Απειλές	Μέτρα Μετριασμού
DoS σε Σταθμούς Φόρτισης (CS)	- Χρήση TLSv1.3 με προφίλ ασφαλείας OPCC 3 ή IPSec για αποφυγή ενεργειών MitM - Χρήση συναρτήσεων κατακερματισμού για επαλήθευση της ακεραιότητας των στοιχείων λογισμικού στους CS - Ψηφιακή υπογραφή για κάθε συναλλαγή OCPP ή χρήση λειτουργιών MAC - Περιοδική ενημέρωση της λίστας χρηστών με εξουσιοδότηση αλλαγής ενέργειας στους CS - Χρήση εφεδρικών μηχανισμών (όπως proxies, συνδέσεις επικοινωνίας) για πρόληψη επιθέσεων ενδιάμεσης διαδρομής ή αυθεντικοποίηση σε offline λειτουργία - Συνεχής συντήρηση και πιστοποίηση στοιχείων υλικού και λογισμικού - Χρήση μηχανισμών φήμης για εκτίμηση ανώμαλης συμπεριφοράς χρηστών και συσκευών - Ιχνηλασιμότητα δεδομένων για εντοπισμό περιστασιακών ή συχνών αποκλίσεων σε μία ή περισσότερες συναλλαγές - Επιτήρηση και ανθεκτικές σε παραβιάσεις κατασκευές - Διαγνωστικά, ανίχνευση και διαχείριση δυναμικών συμβάντων
Χειραγώγηση των CVs του OCPP	- Χρήση TLSv1.3 με προφίλ ασφαλείας OPCC 3 ή IPSec για αποφυγή ενεργειών MitM - Κρυπτογράφηση ευαίσθητων δεδομένων (όπως CVs του OCPP, IDs) - Χρήση συναρτήσεων κατακερματισμού για επαλήθευση της ακεραιότητας των δεδομένων στους CS - Ψηφιακή υπογραφή για κάθε συναλλαγή OCPP ή χρήση λειτουργιών MAC - Ιχνηλασιμότητα δεδομένων για εντοπισμό αποκλίσεων σε μία ή περισσότερες συναλλαγές - Επιτήρηση και ανθεκτικές σε παραβιάσεις κατασκευές

Πιθανές Απειλές OCPP-v2.0.1

Απειλές	Μέτρα Μετριασμού
CS Spoofing	- Διαγνωστικά, ανίχνευση και διαχείριση δυναμικών συμβάντων - Χρήση TLSv1.3 με προφίλ ασφαλείας OPCC 3 για αποφυγή χρήσης στοιχείων ταυτοποίησης (CVs) και επιθέσεων MitM ή IPSec - Διαχείριση μοναδικών IDs για κάθε χρήστη, συσκευή και συναλλαγή - Ψηφιακή υπογραφή για κάθε συναλλαγή OCPP ή χρήση λειτουργιών MAC - Επιτήρηση και ανθεκτικές σε παραβιάσεις κατασκευές - Διαγνωστικά, ανίχνευση και διαχείριση δυναμικών συμβάντων
Χειραγώγηση των DERs και συστημάτων αποθήκευσης	- Περιοδική επαλήθευση ηλεκτρικών συνιστωσών για συμμόρφωση με κανονιστικά πλαίσια - Συνεχής συντήρηση και πιστοποίηση ενεργειακών συνιστωσών - Ιχνηλασιμότητα δεδομένων για εντοπισμό αποκλίσεων - Επιτήρηση και ανθεκτικές σε παραβιάσεις κατασκευές - Διαγνωστικά, ανίχνευση και διαχείριση δυναμικών συμβάντων

Πιθανές Απειλές OCPP-v2.0.1

Επισκόπηση των προτεινόμενων μετριασμών στο πλαίσιο του αναλυμένου CSMS.

Απειλές	Μέτρα Μετριασμού
User, CSMS και EMS spoofing	- Χρήση TLSv1.3 με προφίλ ασφαλείας OPCC 3 για αυθεντικοποίηση κάθε μέρους (CSMS, EMS, CS) ή IPSec - Διαχείριση μοναδικών IDs για κάθε χρήστη, συσκευή και συναλλαγή - Ευαισθητοποίηση των τελικών χρηστών για τη σημασία προστασίας διαπιστευτηρίων και IDs - Ευαισθητοποίηση των ανθρώπινων χειριστών για τη σημασία προστασίας του οικοσυστήματος - Έλεγχος πρόσβασης στο CS σύμφωνα με την αρχή της ελάχιστης αναγκαίας πρόσβασης - Ψηφιακή υπογραφή για κάθε συναλλαγή OCPP ή χρήση λειτουργιών MAC - Διαγνωστικά, ανίχνευση και διαχείριση δυναμικών συμβάντων
Διαρροή πληροφοριών (Information disclosure)	- Χρήση TLSv1.3 με προφίλ ασφαλείας OPCC 3 για αυθεντικοποίηση κάθε μέρους (CSMS, CS) ή IPSec - Κρυπτογράφηση ευαίσθητων δεδομένων (π.χ. OCPP CVs, IDs) - Αρχές ελάχιστης αναγκαίας πρόσβασης και διαχωρισμός λειτουργιών για αποφυγή κλιμάκωσης δικαιωμάτων - Τεχνολογίες και προσεγγίσεις ενίσχυσης της ιδιωτικότητας για το CSMS και το EMS

Πιθανές Απειλές OCPP-v2.0.1

Επισκόπηση των προτεινόμενων μετριασμών στο πλαίσιο του αναλυμένου CSMS.

Απειλές	Μέτρα Μετριασμού
Εξουσιοδότηση Χρηστών και Διαχειριστών στο CSMS	- Χρήση TLSv1.3 με προφίλ ασφαλείας OPCC 3 για αυθεντικοποίηση κάθε μέρους (CSMS, CS) ή χρήση IPSec - Χρήση έγκυρων τοπικών λιστών εξουσιοδότησης με μοναδικά IDs που σχετίζονται με έγκυρες οντότητες και λαμβάνονται από έγκυρο CSMS - Αποφυγή όσο το δυνατόν περισσότερο της αυθεντικοποίησης σε λειτουργία offline και χρήση proxies για διαχείριση ελέγχου πρόσβασης μέσω CSMS - Εφαρμογή αρχών ελάχιστης αναγκαίας πρόσβασης και διαχωρισμού λειτουργιών για αποφυγή κλιμάκωσης δικαιωμάτων - Ψηφιακή υπογραφή για κάθε συναλλαγή OCPP ή χρήση λειτουργιών MAC - Διαγνωστικά, ανίχνευση και διαχείριση δυναμικών συμβάντων

Αντίμετρα μετριασμού

CWE-ID	Ευπάθειες	Μέτρα Μετριασμού
79	XSS	Καθαρισμός των δεδομένων εισόδου που ελέγχονται από τον χρήστη
89	SQLi	Χρήση παραμετροποιημένων ερωτημάτων
200	Αποκάλυψη Πληροφοριών	Επιβολή αυθεντικοποίησης σε όλα τα σημεία πρόσβασης
306	Έλλειψη Αυθεντικοποίησης	Επιβολή αυθεντικοποίησης σε όλες τις λειτουργίες
321	Ενσωματωμένα Μυστικά	Απαίτηση κρυπτογραφικών κλειδιών κατά την εκτέλεση
352	CSRF	Χρήση τυχαίων tokens με όλα τα αιτήματα
425	Forced Browsing	Ενίσχυση των μηχανισμών ελέγχου πρόσβασης
798	Hard-Coded Credentials	Επιβολή πολιτικής ενημέρωσης διαπιστευτηρίων
799	Έλλειψη Περιορισμού Ρυθμού	Πρόληψη υπερβολικών και ταχύτατων αιτημάτων
918	SSRF	Καθαρισμός διευθύνσεων IP/URL στις παραμέτρους
942	Λάθος Ρυθμίσεις CORS	Επιβολή αυστηρότερης πολιτικής cross-domain
942	Λάθος Ρυθμίσεις FCDP	Επιβολή αυστηρότερης πολιτικής cross-domain
1236	CSVi	Ασφαλής ανάλυση αρχείων CSV

Συνδεθείτε με CyberSecPro:
Πως να εγγραφείτε & άλλες πρακτικές πληροφορίες

1. Ιστοσελίδα: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Co-funded by the European Union

Co-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

Σας ευχαριστώ

Για απορίες στείλτε εδώ:
Dr. Elias Athanasopoulos
athanasopoulos.elias@ucy.ac.cY

Dr. Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at