



S² Hack4Energy HACKATHON

Συνδιοργάνωση από τα έργα SPEAR & SIT4Energy

Πρόσκληση Συμμετοχής

Εισαγωγή

Η ταχεία εξέλιξη των Τεχνολογιών Πληροφορικής και Επικοινωνιών μεταμορφώνει το ηλεκτρικό δίκτυο σε ένα νέο πρότυπο που ονομάζεται Έξυπνο Ηλεκτρικό Δίκτυο (Smart Grid - SG). Αυτή η νέα πραγματικότητα προσφέρει πολύτιμα οφέλη όπως η διανεμημένη παραγωγή, η αυτο-παρακολούθηση, η αυτό-θεραπεία, ο πιο λεπτομερής έλεγχος, η αμφίδρομη επικοινωνία μεταξύ επιχειρήσεων κοινής ωφέλειας και καταναλωτών/παραγωγών ενέργειας, καθώς και η καλύτερη αξιοποίηση των υφιστάμενων πόρων. Το SG διευκολύνει την ανάπτυξη έξυπνων εφαρμογών που σχετίζονται με την ενέργεια, λαμβάνοντας υπόψη τόσο τα δυναμικά απόδοσης στην τοπική παραγωγή ενέργειας όσο και την κατανάλωση ενέργειας. Ωστόσο, ταυτόχρονα, αυτή η επανάσταση δημιουργεί σοβαρά προβλήματα στον τομέα της ασφάλειας στον κυβερνοχώρο, δεδομένου ότι το SG χαρακτηρίζεται από πολλαπλές ετερογενείς και διασυνδεδεμένες τεχνολογίες. Σε αυτό το πλαίσιο, τα προγράμματα SPEAR (<https://www.spear2020.eu>) και SIT4Energy (<https://sit4energy.eu>) ενώνουν τις δυνάμεις τους για τη συνδιοργάνωση ενός hackathon που θα επικεντρωθεί σε καινοτόμες προσεγγίσεις στον τομέα της ενέργειας σε θέματα κυβερνο-ασφάλειας και εμπλοκής των τελικών χρηστών, αντίστοιχα.

Ημερομηνία

Το hackathon απαρτίζεται από 4 προκλήσεις (2 ανα έργο) και θα κρατήσει δύο μέρες στις **23-24 Οκτωβρίου 2019**.

Τοποθεσία

Το Hackathon θα πραγματοποιηθεί διαδικτυακά μέσα από την πλατφόρμα [F6S](#). Για κάθε ενδιαφερόμενο που θα ήθελε να συμμετάσχει από κοντά, η οργάνωση θα φιλοξενηθεί στις εγκαταστάσεις του ΕΚΕΤΑ στο 6^ο χλμ Χαριλάου – Θέρμης, στη Θεσσαλονίκη. Πάρτε τους φορητούς σας υπολογιστές, και ετοιμαστείτε να συμμετάσχετε σε αυτή τη μοναδική εμπειρία.

Πρόγραμμα

Τετάρτη 23 Οκτ. 2019		Πέμπτη 24 Οκτ. 2019	
09:00	Υποδοχή	16:00	Ολοκλήρωση S ² Hack4Energy
09:15	Χαιρετισμός από την Ελληνική Ομάδα Κυβερνοασφάλειας <i>Ομιλήτης: Δρ. Χρήστος Ξενάκης</i>	16:00	Χαιρετισμός Χορηγού Ubitech
09:25	Το έργο SPEAR <i>Ομιλητής: Δρ. Παναγιώτης Σαριγιαννίδης</i>	16:20	Χαιρετισμός Χορηγού WATT+VOLT
09:35	Το έργο SIT4Energy <i>Ομιλητής: Δρ. Δημήτριος Τζοθάρας</i>	16:40	Χαιρετισμός Χορηγού MLS
09:45	Οδηγίες S ² Hack4Energy <i>Ομιλητές: Υπεύθυνοι Προκλήσεων</i>	17:00	Αποτελέσματα & Βραβεύσεις
11:00	Έναρξη S ² Hack4Energy		

Πώς να συμμετάσχετε

Το μόνο που πρέπει να κάνετε είναι να πάρετε ένα εισιτήριο από την πλατφόρμα της εκδήλωσης S² Hack4Energy (www.f6s.com/s2hack4energy).

Εγγραφείτε! (Αλλά πρώτα, βεβαιωθείτε ότι έχετε διαβάσει και συμφωνείτε με τους Όρους και Προϋποθέσεις Συμμετοχής)

Βραβεία

Για να γίνει ακόμα πιο μοναδική η εμπειρία οι νικητές του διαγωνισμού θα κερδίσουν μοναδικά βραβεία:

- **1^ο Βραβείο:** Dell Latitude 5501, I7-9850H/15.6 FHD/16GB/512GB SSD/Webcam/Win10 Pro, Black
- **2^ο Βραβείο:** 300,00 € Amazon Gift Card
- **3^ο Βραβείο:** MLS Trophy Tablet

Οι νικητές θα ανακοινωθούν στις 24 Οκτωβρίου 2019, αφού ολοκληρωθεί ο διαγωνισμός σύμφωνα με το πρόγραμμα της εκδήλωσης.

S² Hack4Energy Προκλήσεις

SPEAR Πρόκληση #1: Οι τεχνικές Οπτικής Αναλυτικής αποτελούν ένα σημαντικό εργαλείο για το διαχειριστή ασφαλείας, παρέχοντας την ικανότητα αναγνώρισης πιθανών ανωμαλιών όταν οι τυπικοί μηχανισμοί ασφαλείας δεν μπορούν να τα αντιμετωπίσουν. Μπορεί να θεωρηθεί ως η επιστήμη της αναλυτικής συλλογιστικής που ασχολείται με τα προβλήματα ανάλυσης δεδομένων, χρησιμοποιώντας οπτικές διεπαφές. Ειδικότερα, όταν τα αυτοματοποιημένα αντίμετρα ασφαλείας δεν είναι σε θέση να αναγνωρίσουν κακόβουλα μοτίβα, οι τεχνικές οπτικοποίησης και αλληλεπίδρασης μπορούν να διευκολύνουν τη διαδικασία λήψης αποφάσεων συμβάλλοντας σημαντικά στην ανθρώπινη αντίληψη και διαίσθηση. Η συγκεκριμένη **πρόκληση** αποσκοπεί στην ανάπτυξη κατάλληλων μηχανισμών απεικόνισης, οι οποίοι θα απεικονίζουν τα λειτουργικά δεδομένα που σχετίζονται με τις μετρήσεις ηλεκτρικής ενέργειας, ώστε ο διαχειριστής ασφαλείας να είναι σε θέση να κατανοήσει τις κανονικές τους κλίμακες χωρίς να διερευνά διεξοδικά κάθε μετρική.

Υπεύθυνος: κ. Νικόλαος Βακάκης, ΕΚΕΤΑ, Θεσσαλονίκη, nikovaka@iti.gr

SPEAR Πρόκληση #2: Τα σύγχρονα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems - IDS) χρησιμοποιούν τεχνικές ταξινόμησης με μηχανική μάθηση (ML), προκειμένου να εντοπίσουν έγκαιρα τις πιθανές κυβερνοεπιθέσεις. Ένα σημαντικό πλεονέκτημα αυτών των συστημάτων IDS σε σύγκριση με τα συμβατικά IDS που βασίζονται σε υπογραφές (όπως το Snort και το Suricata) είναι ότι είναι σε θέση να εντοπίσουν πιθανές zero-day κυβερνοεπιθέσεις και άγνωστες ανωμαλίες. Οι ροές δικτύου TCP/IP περιλαμβάνουν σημαντικά χαρακτηριστικά, όπως τη διάρκεια της ροής, τα συνολικά πακέτα ανά δευτερόλεπτο, τον συνολικό αριθμό των bytes που αποστέλλονται στο αρχικό παράθυρο, κλπ., Τα οποία μπορούν να χρησιμοποιηθούν από IDS που στηρίζονται σε ανίχνευση ανωμαλιών. Ο στόχος αυτής της **πρόκλησης** είναι να αναπτυχθεί ένα μοντέλο ταξινόμησης με υψηλές επιδόσεις ανίχνευσης, το οποίο θα χρησιμοποιεί τεχνικές ML για τον εντοπισμό διαφόρων κυβερνοεπιθέσεων, περιλαμβανομένων: α) επιθέσεις brute force, β) Denial of Service (DoS), γ) επιθέσεις ανίχνευσης

θυρών, δ) botnets, και ε) διεισδύσεις. Όσον αφορά τη διαδικασία εκπαίδευσης, θα παρασχεθεί ένα σύνολο δεδομένων εκπαίδευσης με ετικέτες ροής δικτύου. Αυτό το σύνολο δεδομένων μπορεί να χρησιμοποιηθεί από τους συμμετέχοντες τόσο για εκπαίδευση όσο και για τις δοκιμές. Η διαδικασία αξιολόγησης θα ελέγξει την απόδοση των παρεχόμενων μοντέλων, χρησιμοποιώντας ένα διαφορετικό σύνολο δεδομένων.

Υπεύθυνος: κ. Οδυσσεάς Νικολής, ΕΚΕΤΑ, Θεσσαλονίκη, odynik@iti.gr

SIT4Energy Πρόκληση #1: Στην προσπάθειά μας να εμπλέξουμε τους τελικούς χρήστες και να αλλάξουμε τη συμπεριφορά κατανάλωσης ενέργειας, οι απεικόνιση των δεδομένων αποτελεί αναπόσπαστο εργαλείο. Προσφέρει μια επισκόπηση των δεδομένων που σχετίζονται με την ενέργεια και προσθέτουν διαδραστικότητα στην υλοποίηση. Αν δεν ήταν εύκολα προσβάσιμα, θα ήταν άχρηστα, γι' αυτό και επιλέξαμε να τα ενσωματώσουμε σε μια εφαρμογή για έξυπνες φορητές συσκευές (smart phones, tablets, etc), καθώς οι κινητές συσκευές είναι πανταχού παρούσες. Κατά συνέπεια, ο χρήστης είναι σε θέση να βλέπει το ιστορικό ενεργειακής συμπεριφοράς του σε ένα συνοπτικό και αλληλεπιδραστικό περιβάλλον, το οποίο με τη σειρά του μπορεί να έχει επιρροή στην παρακίνηση του χρήστη για φιλικές προς την ενεργειακή εξοικονόμηση συμπεριφορές. Η συγκεκριμένη **πρόκληση** αποσκοπεί στην ανάπτυξη μιας εφαρμογής Android, η οποία θα απεικονίζει τα δεδομένα που σχετίζονται με την ηλεκτρική ενέργεια, τις μικρο-στιγμές και την ανθρώπινη παρουσία, με ελκυστικό και ενημερωτικό τρόπο. Τα παρεχόμενα δεδομένα είναι μετρήσεις κατανάλωσης ενέργειας, μικρο-στιγμές, και ανθρώπινης παρουσίας στις εγκαταστάσεις του ΕΚΕΤΑ.

Υπεύθυνος: Δρ. Στέλιος Κρηνίδης, ΕΚΕΤΑ, Θεσσαλονίκη, krinidis@iti.gr

SIT4Energy Πρόκληση #2: Η παροχή προτάσεων σχετικά με την ενέργεια είναι ένα κατάλληλο συμπληρωματικό εργαλείο πέρα από τις ενημερωτικές οπτικές αναλύσεις. Παρόλο που η ενημέρωση του χρήστη είναι ζωτικής σημασίας για την αλλαγή συμπεριφοράς, ο συγχρονισμός είναι εξίσου σημαντικός, διότι όσο ενδιαφέρουσα είναι μια σύσταση, ο χρήστης θα την απορρίψει εάν είναι απασχολημένος. Η ανίχνευση μικρο-στιγμών αντιμετωπίζει αυτό το ζήτημα επισημαίνοντας τις στιγμές που ο χρήστης είναι αδρανής. Ο χρήστης δεν μπορεί να είναι αδρανής εάν εκτελεί μια δυναμική φυσική δραστηριότητα, επομένως είναι απαραίτητη η αναγνώριση σωματικής δραστηριότητας. Αυτή η **πρόκληση** αποσκοπεί στην ανάπτυξη ενός μοντέλου μηχανικής μάθησης, το οποίο θα είναι σε θέση να προσδιορίσει τις φυσικές δραστηριότητες χρησιμοποιώντας αποτελεσματικά το σύνολο δεδομένων WISDM (Data Sensor Data Mining). Το σύνολο δεδομένων WISDM περιλαμβάνει δεδομένα τριών αξόνων επιταχυνσιόμετρο, τα οποία αντιστοιχούν σε συγκεκριμένες ετικέτες φυσικής δραστηριότητας. Πιο συγκεκριμένα, οι πιθανές σωματικές δραστηριότητες περιλαμβάνουν: α) κατάβαση, β) τζόκινγκ, γ) καθιστική στάση, δ) όρθια στάση, ε) ανάβαση και στ) το περπάτημα. Οι συμμετέχοντες μπορούν να χρησιμοποιήσουν το παρεχόμενο σύνολο δεδομένων τόσο για εκπαίδευση όσο και για δοκιμές. Όσον αφορά τη διαδικασία αξιολόγησης, θα χρησιμοποιηθεί διαφορετικό σύνολο δεδομένων δοκιμών.

Υπεύθυνος: κ. Κωνσταντίνος Πέππας, ΕΚΕΤΑ, Θεσσαλονίκη, kpeppas@iti.gr

Όροι & Προϋποθέσεις Συμμετοχής

Με την εγγραφή σας και την απόκτηση εισιτηρίου, όλοι οι συμμετέχοντες αποδέχονται τους όρους και προϋποθέσεις του S² Hack4Energy hackathon. Οι Όροι και οι Προϋποθέσεις είναι διαθέσιμοι [εδώ](#).

Χορηγοί

Ένα τεράστιο ευχαριστώ στους χορηγούς. Η υποστήριξή τους είναι πολύτιμη για να γίνει η εκδήλωση πραγματικά μοναδική!



Η εκδήλωση συν-διοργανώνεται από τα έργα SPEAR & SIT4Energy. Το πρώτο χρηματοδοτείται από το πρόγραμμα Horizon 2020 της Ευρωπαϊκής Ένωσης κάτω από τη συμφωνία χρηματοδότησης 787011 και το δεύτερο από το Γερμανικό Υπουργείο Παιδείας και Έρευνας (ΓΥΠΕ) και από τη Γενική Γραμματεία Έρευνας και Τεχνολογίας (ΓΓΕΤ) στο πλαίσιο της Ελληνογερμανικής πρόσκλησης υποβολής προτάσεων για τη διμερή συνεργασία στην Έρευνα και Καινοτομία, 2016. Κάθε σχετικό περιεχόμενο της εκδήλωσης αντικατοπτρίζει μόνο την άποψη των διοργανωτών και όχι τις απόψεις των οργανισμών χρηματοδότησης. Η Ευρωπαϊκή Επιτροπή, το ΓΥΠΕ και η GSRT δεν είναι υπεύθυνα για οποιαδήποτε χρήση των πληροφοριών που είναι διαθέσιμες σε αυτή την εκδήλωση.



Με την υποστήριξη των:

ΕΚΕΤΑ:

Δρ. Δημήτριος Τζοβάρας, Διευθυντής

Δρ. Δημοσθένης Ιωαννίδης

Δρ. Κωνσταντίνος Βότης



Πανεπιστήμιο Δυτικής Μακεδονίας:

Δρ. Παναγιώτης Σαριγιαννίδης

κ. Δημήτριος Πλιάσιος

κ. Παναγιώτης Ράδογλου Γραμματικής



SPEAR: Secure and PrivatE smArt gRid

Κατά την τελευταία δεκαετία, οι κυβερνοεπιθέσεις έχουν γίνει ιδιαίτερα σύνθετες, μη εντοπίσιμες, στοχευμένες και πολύπλευρες οι οποίες μπορεί να εκμεταλλεύονται ευπάθειες τύπου zero day και ιδιαίτερες δημιουργικές διεπιστημονικές μεθόδους επιθέσεων. Καθώς η κοινωνία μας γίνεται ολοένα και περισσότερο εξαρτώμενη από υποδομές ζωτικής σημασίας, χρειάζονται καινούριες τεχνολογίες για να αυξηθούν οι ικανότητες εντοπισμού και απόκρισης σε τέτοιου είδους επιθέσεις, κάτι το οποίο έχει αποδειχτεί ιδιαίτερος δύσκολο όταν ο επιτιθέμενος είναι άτομο με ισχυρό κίνητρο, με ικανότητες και καλή χρηματοδότηση. Μια από τις πιο ευάλωτες ζωτικές υποδομές αλλά και με μεγάλη επιρροή είναι το έξυπνο δίκτυο διανομής ενέργειας, το οποίο θεωρείται ως το σύστημα διανομής ενέργειας της επόμενης γενιάς και υπόσχεται αυτοαποκατάσταση, ανθεκτικότητα, βιωσιμότητα και αποτελεσματικότητα στις υποδομές διανομής ενέργειας ζωτικής σημασίας. Ωστόσο η προστασία των έξυπνων δικτύων ηλεκτρικής ενέργειας απέναντι σε επιθέσεις είναι ζωτικής σημασίας για την εθνική ασφάλεια και τη δημόσια ασφάλεια, επειδή η κατάρρευση μιας μονάδας παραγωγής ενέργειας μπορεί να κοστίσει ανθρώπινες ζωές, εκατομμύρια ευρώ, αποκλεισμό από ένα τόσο σημαντικό αγαθό όπως η ενέργεια και μέρες ίσως και μήνες αποκατάστασης. Με βάση αυτά το SPEAR στοχεύει: α) στον εντοπισμό και στην απόκριση σε κυβερνοεπιθέσεις χρησιμοποιώντας καινούριες τεχνολογίες και δυνατότητες, β) στον έγκαιρο εντοπισμό απειλών και ανωμαλιών, γ) στην ανάπτυξη all-in-one λύσεων ασφάλειας, δ) στην εκμετάλλευση εξελιγμένων μεθόδων εγκληματολογίας οι οποίες στοχεύουν στην διατήρηση της ιδιωτικότητας ε) στην αντιμετώπιση προηγμένων επίμονων απειλών και στοχευμένων επιθέσεων σε έξυπνα δίκτυα, στ) στην αύξηση της ανθεκτικότητας της καινοτομίας στα έξυπνα δίκτυα διανομής ενέργειας, ζ) στην ανακούφιση του προβλήματος της έλλειψης εμπιστοσύνης ανάμεσα στους χειριστές έξυπνων δικτύων και η) στην ενδυνάμωση της ευρωπαϊκής προτυποποίησης και ευρείας χρήσης κοινής τεχνολογίας. Στο πλαίσιο του SPEAR τέσσερα proof-of-concept σενάρια χρήσης σχεδιάζονται με σκοπό την επικύρωση και την αξιολόγηση των υλοποιημένων εργαλείων ασφάλειας και ιδιωτικότητας.



Κοινοπραξία



SIT4Energy: Smart IT for Energy Efficiency and Integrated Demand Management

Η βιώσιμη ενέργεια περνάει μια από τις μεγαλύτερες προκλήσεις της εποχής μας. Καθώς η ΕΕ εστιάζει στην επίτευξη των στόχων της για το 2020, ο ρόλος των ιδιωτικών καταναλωτών ενέργειας καθίσταται κυρίαρχος. Η ΕΕ και τα κράτη μέλη αρχίζουν να κατανοούν την ανάγκη ενίσχυσης μέτρων που σχετίζονται με την προσφορά (π.χ. έξυπνα / αποδοτικά κτίρια, έξυπνες συσκευές και έξυπνους μετρητές) με πρωτοβουλίες που επηρεάζουν την κατανάλωση (π.χ. ενδυνάμωση των καταναλωτών, πληροφόρηση και εκπαίδευση, ενεργειακοί φόροι και κίνητρα). Ωστόσο, τόσο οι ερευνητές όσο και οι επαγγελματίες του χώρου έχουν συνειδητοποιήσει ότι το να πειστούν οι καταναλωτές (μεταξύ των οποίων και εκείνοι που παράγουν επίσης μέρος της δικής τους ενέργειας, π.χ. μέσω φωτοβολταϊκών εγκαταστάσεων) για να αλλάξουν τη συμπεριφορά τους, αποτελεί μία δύσκολα υλοποιήσιμη πραγματικότητα. Ταυτόχρονα, οι δυσκολίες στις υποδομές σε συνδυασμό με την εγγενή τεχνική φύση των λογαριασμών ενέργειας και το σύστημα τιμολόγησης γενικά παρεμποδίζουν περαιτέρω την ικανότητά μας να προσφέρουμε την πολύ αναγκαία ενδυνάμωση των καταναλωτών.



Ο στόχος του έργου SIT4Energy είναι να καταδείξει πώς μπορεί να επιτευχθεί ολοκληρωμένη διαχείριση της ενέργειας για τα σενάρια καταναλωτών που παράγουν μέρος της ενέργειάς τους, μέσω μιας έξυπνης λύσης πληροφορικής που λαμβάνει υπόψη τόσο τις δυνατότητες αποδοτικότητας στην τοπική παραγωγή ενέργειας όσο και την κατανάλωση ενέργειας. Για το σκοπό αυτό, το έργο υλοποιεί μια έξυπνη υπηρεσία παροχής συμβουλών για κινητά τηλέφωνα/tablets με σκοπό την ευαισθητοποίηση του χρήστη μέσω γνώσης και μία διεπαφή Έξυπνης Ενεργειακής Διαχείρισης που εκμεταλλεύεται έξυπνες τεχνικές για την ανάλυση δεδομένων κατανάλωσης, μοντέλων συμπεριφοράς και εξωτερικών πληροφοριών περιβάλλοντος (π.χ. τιμολόγηση, καιρός) για την παροχή συστάσεων για τη βελτιστοποίηση των τρόπων παραγωγής/κατανάλωσης ενέργειας. Αυτό περιλαμβάνει μία φιλική προς τον χρήστη παρουσίαση των αποτελεσμάτων με κέντρο των καταναλωτή, βασισμένη σε τεκμηριωμένα στοιχεία σχετικά με το κόστος και τα οφέλη των τεχνικών ενεργειακής απόδοσης που βασίζονται στις τεχνολογίες πληροφορικής και επικοινωνιών, σε συνδυασμό με σαφή και έγκαιρη καθοδήγηση και υποστήριξη για τον τρόπο επίτευξης της διαθέσιμης εξοικονόμησης ενέργειας, ώστε να αυξηθεί η υιοθέτηση τέτοιων τεχνικών από τους χρήστες και η αποτελεσματικότητά τους.

Κοινοπραξία



CERTH
CENTRE FOR
RESEARCH & TECHNOLOGY
HELLAS

