

“Aplikazio industrialetako zibersegurtasuna: gaur egungo egoera eta joerak”

Gipuzkoako Zientzia eta Teknologia Parkea, Orona Fundazioa
Hernaniko Campusa - Galarreta (Gipuzkoa)
2017/10/17, asteartea

1. JARDUNALDIAREN DESKRIBAPENA

Azken urteotan, gora egin du eta asko zabaldu da, oro har, Interneten erabilera; horren ondorioz alor guztietan zabaldu diren aukerek industriaren esparrura hurbilarazi dituzte orain arte ia salerosketen eta zerbitzuen esparruan edo kontsumo-produktuei lotutakoetan soilik erabili izan diren tresnak eta estrategiak. Oso urrats garrantzitsua da hori halako enpresa guztientzat, zeinak, oro har, Internet ez baitute erabiltzen marketinerako eta komunikazioetarako baizik.

Oso denbora gutxian, halabeharrezko errealitate bihurtu dira hainbat gauza: telefonia- eta datu-sare nonahikoak daude, informazio-kantitate handiak era fidagarrian eta denbora errealean transmititzeko ahalmena dutenak; elektronikan, bai miniaturizazioan, bai zehaztasunean eta prezioan izandako aurrerapen handiei esker, ezin konta ahala sentso-re eta monitorizazio- eta komunikazio-sistema agertu dira; merkatuak globalizatu dira, eta, ondorioz, bezeroak fisikoki urrutiago daude eta lehiakide berriak agertzen dira; balio erantsi handiko produktu berriak jarri beharra dago merkatuan, lehia handiago horri aurre egiteko eta bezeroak leialtzeko (adibidez, pertsonalizazio-maila handia eskainiz). Eta, hori guztia, oso azkar ari da hazten, eta, bide horretatik, lerro, behar eta aukera berriak ari dira zabaltzen.

Normala denez, ordea, aukera berri horiek arrisku berriak dakartzate. Arrisku nagusietako bat, oso larria, komunikazioen eta trukatzeko dugun informazioaren segurtasuna da. Izan dira kasu entzutetsuak, eta ez dago gogorarazi beharrik, non lehen mailako erakundeek sistemak eraso zibernetikoak jasan baitituzte; datuak galdu dituzte, edo argitaratu nahiz bahitu egin dizkiete, eta, ondorioz, kalte ekonomikoak izan dituzte, eta ospea galdu.

Gure industria-enpresak hasi dira Internetera konektatutako ekipoak masiboki erabiltzen, eta gauzen Interneten eztanda horrek zibersegurtasun-ahalmen aurreratuak izatera behartzen du, gorago aipatutako arriskuak minimizatzeke.

Egoera hori izanik, IK4 Research Alliancek jardunaldi bat antolatu du, enpresei, unibertsitateei, ikerketa-zentroei eta alor horretako azken errealitateak, joerak eta etorkizuneko erronkak alderdi teknikoak zein diren jakin nahi duten eragile orori zuzendua.

Eusko Jaurlaritzaren eta Gipuzkoako Aldundia gurekin izango dira, alor horretan dituzten ekimen gailenak azaltzeko. Daimler Trucks etxeko aditu batek ekingo die hitzaldi teknikoak. Tresna horiek industria- eta zerbitzu-estrategian pixkanaka sartzeari lotuta, bere esperientzia, etorkizuneko lan-lerroak, eta prozesu horrek dakartzan inplikazio, aukera eta erronken ikuspegi orokorra azalduko ditu.

Ondoren, teknologia horren zenbait alderdi landuko dituzte gainerako hizlariak, etorkizun hurbilean izango dugun panorama zehazteko asmoz, betiere arreta jarrita berrikuntza edo maila zientifiko eta teknologiko handiena duten alderdietan eta haien aplikazio jakinetan.

EGITARAUA

- 09:30 – 09:35 Agurra eta jardunaldiaren aurkezpena: IK4 Research Alliance
- 09h35 – 09h50 Gipuzkoako Foru Aldundia. Gipuzkoako administrazioak industriako zibersegurtasunean zer estrategia darabilen.
Ainhoa Aizpuru, Ekonomia Sustapena, Landa Ingurunea eta Lurralde Oreko foru-diputata
- 09:50 – 10:05 Eusko Jaurlaritza. EAEko administrazioak industriako zibersegurtasunean zer estrategia eta zer interes dituen.
Estibaliz Hernáez, Teknologia, Berrikuntza eta Lehiakortasuneko sailburuordea
- 10:05 – 10:25 IK4 Research Alliance. Industriako zibersegurtasunaren gaur egungo ikuspegi orokorra.
- 10:25 – 11:05 DAIMLER TRUCKS. Zibererasoak! – Ibilgailuen kontrolari eragiten dion eta sortzen ari den arriskua
- 11:05 – 11:35 atsedena eta kafea
- 11:35 – 11:55 CEIT-IK4. Gauzen Interneten inguruneetako zibersegurtasuna eta azpiegitura erabakigarrietan duen inpaktuaren ebaluazioa.
- 11:55 – 12:15 IK4-IKERLAN. Sistema txertatuen segurtasuna: negozioa babesteko faktore gakoa
- 12:15 – 12:35 VICOMTECH-IK4. Big Dataren erabilera zibersegurtasunean.
- 12:35 – 13:15 hizlarien mahai-ingurua, galderak eta amaiera
- 13:15 – 15:00 pintxoak eta harremanak

OHARRAK:

- Doako jardunaldia; sarrera doan, alde zuzenetik izena emanez gero.
- Daimler Trucks-en hitzaldia ingelesez izango da eta ez da aldibereko itzulpenik egingo.
- Moderatzailea eta jardunaldiaren gidaria: Javier Laucirica, IK4 erakundeko zuzendari zientifiko eta teknologikoa.
- AHOLKULARITZA-ZERBITZUA: jardunaldia amaitutakoan, CDTIko langileak prest izango dira erakunde horrek I+G+Bko proiektuak martxan jartzeko dituen tresnei eta laguntzei buruzko informazioa emateko, interesa duen orori. Hala bada, jakinarazi jardunaldira sartzean, akreditazioak egiteko unean.

LAGUNTZAILEAK:



2. HITZALDIAK

DAIMLER TRUCKS



Izenburua:

Zibererasoak! – Ibilgailuen kontrolari eragiten dion eta sortzen ari den arriskua

Laburpena:

Ibilgailuen gidatzea gero eta automatizatuagoa dago, elektronikan eta softwarean egiten ari diren aurrerapenei esker. Horren ondorioz, kontrol-sistemei informatikoki eraso egiteko atea zabaltzen da, eta arrisku larrian jar daitezke eraso jasan duen ibilgailuko bidaiariak, harekin batera dauden gainerako ibilgailuak, oinezkoak eta azpiegiturak.

Hizlaria: Roland Trauter

Software-integrazioko zuzendaria, Daimler Trucks Advanced Engineering (Stuttgart). Daimlerreko ikerketa-dibisioan, software-analisan eta objektuei zuzendutako softwarearen berringeniaritzan aritu da lanean, zenbait lanpostutan.

Daimlerreko ecoDriver proiektuaren burua izan da, non arreta berezia jarri baita aplikazio-prototipoen garapenean, errepideko probetan, onarpen-azterketetan eta jarraipen-datuen analisan.

Orain, nabigazio aurreratuan jarraitzen du lanean, bereziki segurtasuna (*safety* eta *security*) kontuan hartuta.

Horren aurretik, Autosar garapenean eta gidatzeko laguntza-sistema aurreratuen softwarearen kalitatea bermatzen egin du lan.

CEIT-IK4



Izenburua:

Gauzen Interneten inguruneetako zibersegurtasuna eta azpiegitura erabakigarrietan duen inpaktuaren ebaluazioa.

Laburpena:

Kontuan hartuta kate-maila ahulenaren segurtasunak ezartzen duela sistema osoaren segurtasuna, oso garrantzitsua da komunikazio-kate osoa izatea gogoan, hasi amaierako gailuetatik (gauzen Internet) eta hodeiraino. Komunikazioen zifratutik harago dauden eta kontuan hartu behar diren alderdi garrantzitsuak nabarmenduko dira, eta zenbait gako azalduko dira gauzen Interneten arkitektura ziberseguruak lortzeko. Landuko da, orobat, bidegabe sartzen direnek edo erasoek duten inpaktuaren ebaluazioari dagokion problematika, hurbilketen eta adibide errealen bidez; izan ere, funtsezkoa da, azpiegitura esangarrietan bereziki. Azkenik, gai horren inguruan gaur egun dauden ikerketa-lerroak aipatuko dira.

Hizlaria: Javier Añorga

Ingeniaritza Aplikatuko doktorea (Nafarroako Unibertsitateko Ingeniaritzako Goi Eskola - Tecnun) eta Telekomunikazio ingeniaria (Nafarroako Unibertsitateko Ingeniaritzako Goi Eskola - Tecnun). EC-Council-en CEH (Certified Ethical Hacker) ziurtagiria.

IKTen dibisioko Datuen Analisia eta Informazioaren Kudeaketa taldeko ikertzailea (Ceit-IK4). Ceit-IK4n ikerlanetan eta Tecnunen irakasle aritzen da, eta Segurtasun Klubeko eta Hacking Etikoko burua da. Gaur egun, bere lanak datuen komunikazio-sareetan eta zibersegurtasunean du ardatza. I+Gko zenbait proiektutan aritu da lankidetzan, eta 13 argitalpen zientifikotan hartu du parte (egile edo egilekide gisa); argitalpen horien artean, badaude aldizkari indexatuak eta nazioarteko kongresuak.

IK4-IKERLAN

IK4  IKERLAN
Research Alliance

Izenburua:

Sistema txertatuen segurtasuna: negozioa babesteko faktore gakoa

Laburpena:

Sistema txertatuen papera funtsezkoa da industrian (prozesuen kontrolean) eta beste sektore askotan (automobilgintza, trengintza, sarbide-kontrola, etab.). Sistema horien garapenean, lehentasuna eman zaie, historikoki, segurtasun funtzionaleko alderdiei (safety) eta denbora errealarari, eta oso segurtasun eskasa (security) eman zaie, eman bazaie. Gauzen Interneten paradigma bat-batean eta indarrez sartu da; horrek eta konektagarritasunak etengabe gora egiteak eraginda, gailu horiek urrutiko erasoan arriskuan geratu dira, eta, askotan, sistemen kate-maila ahul bihurtu dira. Hauek dira egoera horretara eraman gaituzten faktoreetako batzuk: hornitzailearen eta azken bezeroaren kontzientziazio-maila txikia eta erreferentziako araudirik ez izatea.

Azken urteotan, egoera aldatzen ari da, eta fabrikatzaileak ikusten ari dira beren produktuak segurtasun-neurri egokiekin fabrikatzeko beharra dagoela. Hala ere, erabilgarri dauden segurtasun-teknologia asko informazioaren teknologien esparrukoak dira, eta ez dira erraz aplikatzen sistema txertatuetan, baliabide gutxiago izaten direlako, protokolo espezializatuak dituztelako, denbora errealeko beharrak daudelako, segurtasun funtzionaleko neurriak bateratu behar direlako edo teknologia barreiatuak dituztelako. Hitzaldi honetan, sistema txertatuen segurtasunean sakonduko da, eta faktore gakotzat hartuko dira, negozioa babesteko, zerbitzua fidagarritasunez ematen dela bermatzeko, eta zerbitzu berriak zabaltzeko aukera izateko. Segurtasuna diseinutik kontuan hartzeak dituen arriskuak eta abantailak azalduko dira, baita soluzio teknologiko posibleak, aplikazio-kasuak eta araudi-betetzea eta ziurtagiriak ere.

Hizlaria: David González

Seinaleen eta komunikazioen prozesamenduko masterra (Edinburgoko Unibertsitatea), Automatikako eta Elektronikako ingeniaria (Mondragon Unibertsitatea).

IK4-IKERLANeko Industrial Security ikertalderen arduraduna.

Gaur egun, IK4-IKERLANeko sistema txertatu fidagarrien alorrean egiten du lan, Industrial Security ikertaldearen arduradun gisa. Sistema txertatuen alorrean aerosorgailuen sektoreko enprekin egiten den lankidetzaren arduraduna da, besteak beste, eta turbina eolikoaren ikuskapen- eta kontrol-sistemen garapena eta mantentze-lanak lantzen dituzte. Urteetan, osasunaren eta energiaren sektoreetako plataforma txertatuen diseinuan eta garapenean egin du lan, eta Espainiako eta Europako zenbait proiektutan parte hartu du. Horren aurretik, hardware-plataforma, birtualizazio eta kritikotasun mistoko sistemetako ikerketen arduradun izan da.



Izenburua:

Big Dataren erabilera zibersegurtasunean.

Laburpena:

Gai hauek izango dira hitzaldiaren ardatza: datu-bolumen handien kudeaketa; bideo, irudi, audio, sentzore, prozesu-egunkari eta abarretatik datozen datu heterogeneoak eta haien denbora errealeko prozesamendua, anomaliak eta jokaera arraroak hautemateko. Prozesamendu hori guztia denbora errealean egin beharra dago, eta, patrioiak erraz, bizkor eta eraginkortasunez hautematen laguntzeko, analisi bisualeko tresnekin osatuta.

Hizlariak: Igor García Olaizola

Informatikan doktorea (Euskal Herriko Unibertsitatea) eta Elektronika eta Automatika Industrialeko ingeniaria (Nafarroako Unibertsitatea - Tecnun).

VICOMTECH-IK4ko Data Intelligence departamenduko burua; analisi estatistikoa eta Big Data tekniken aplikazioa lantzen dituzte. Tecnuneko irakasle elkartua ere bada.

Master-tesia Zirkuitu Integratuen Fraunhofer Institutuan (Erlagen, Alemania) egin zuen, non urtebetez aritu baitzen ikerketa-laguntzaile gisa MPEG (MP3 eta AAC) estandarren araberako audioaren deskodetarekin erlazionatutako zenbait proiektutan.

2002an, VICOMTECH-IK4ko ikertzaile bihurtu zen. 2006an, urte eta erdiz, teknologia-aholkulari gisa aritu zen Vilau enpresan (zentroaren spin-off bat), non TDT interaktiboko goiburuak diseinatzeko eta zabaltzeko zenbait proiekturen buru izan baitzen. 2007an VICOMTECH-IK4ko Digital Media departamenduaren zuzendaria izatera pasatu zen. Irudien deskriptore globalen bidezko irudi-karakterizazioan eta adimen artifizialeko tekniketara oinarritzen da haren tesia.

3. JARDUNALDIA NON EGINGO DEN

"Aplikazio industrialetako zibersegurtasuna: gaur egungo egoera eta joerak"

Gipuzkoako Zientzia eta Teknologia Parkea, Orona Fundazioa
Hernaniko Campusa - Galarreta (Gipuzkoa)

Jauregi Bailara kalea, z.g.
20120 Hernani (Gipuzkoa)
tel.: (+34) 943 335588

<https://goo.gl/maps/dLUMdACToKT2>

Latitudea: 43°16'34.3"N | Longitudea: 1°59'08.2"W

