R+D+I EN CIBERSEGURETAT A LA UPC

2023

Generalitat de Catalunya

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Cofinançat per la Unió Europea

CONTINGUT

01

LA UPC

Coneix la Universitat Politècnica de Catalunya (UPC) i descobreix algunes de les seves xifres.

02

CIBERSEGURETAT

Què s'entén per ciberseguretat? I per què és clau en el desenvolupament?

03

RECERCA I INNOVACIÓ

Descripció de l'activitat, els grups de recerca, els centres i instituts que generen coneixement en l'àmbit de la ciberseguretat.

04

R+D+I D'EXCEL·LÈNCIA UPC

Selecció dels projectes, articles i tesis doctorals de més impacte en relació amb la ciberseguretat de la UPC.

05

FORMACIÓ

Graus, màsters i doctorats que s'ofereixen a la UPC en l'àmbit de la ciberseguretat.

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

01 LA UPC

La Universitat Politècnica de Catalunya (UPC) és una universitat pública de recerca i educació superior en els àmbits de l'enginyeria, l'arquitectura, les ciències i la tecnologia, amb forta implantació i presència activa en els nuclis industrials del territori. La UPC participa en el sistema d'innovació de Catalunya amb projectes i contractes de recerca, desenvolupament, valorització del coneixement i comercialització de tecnologia, per tal de resoldre els grans reptes de la societat.

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

ACTIVITAT DE RECERCA, DESENVOLUPAMENT I INNOVACIÓ A LA UPC 2022

227
Projectes nacionals

162
Projectes internacionals

1.011
Projectes d'R+D+I actius en total

78,1 M€
En ingressos de projectes

121,9 M€
En ingressos per contractes

2526
Articles en revistes

331
Tesis doctorals llegides

14
Patents registrades

13
Empreses de Base Tecnològica

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

02 Ciberseguretat

Abasta la seguretat dels sistemes d'informació, els dispositius digitals i les xarxes de dades. El terme ciberseguretat inclou mesures físiques, lògiques i de gestió destinades tant a la protecció digital d'actius com d'entitats i persones. En l'actualitat, és essencial poder-se comunicar garantint la seguretat, la privacitat, la protecció del coneixement, l'autenticitat i l'auditabilitat.

ÀMBITS DE LA CIBERSEGURETAT

SEGURETAT A LA XARXA

En un món cada cop més connectat, protegir la **dimensió virtual de la infraestructura** on es desenvolupa tota l'activitat en línia és una de les principals prioritats.

L'àmbit de la seguretat en xarxa se centra a protegir les xarxes de comunicació i els dispositius connectats a elles contra amenaces i atacs cibernètics.

Això inclou la implementació de ***firewalls***, detecció d'intrusions, **xifrat de dades**, i altres mesures de seguretat per prevenir l'accés no autoritzat.

SEGURETAT DE LA INFORMACIÓ

En l'àmbit de les xarxes, la informació fa referència a les dades digitals que es transmeten i es comparteixen entre dispositius interconnectats. Aquesta informació pot abastar des de missatges de text i correus electrònics fins a arxius multimèdia, com ara imatges i vídeos. **La gestió eficaç d'aquesta informació és essencial per garantir la comunicació efectiva.**

La protecció de la informació emmagatzemada i transmesa a través de sistemes informàtics és fonamental. Això implica el **xifrat de dades**, la gestió d'accés, la implementació de polítiques de seguretat i altres mesures per garantir la **confidencialitat, integritat i disponibilitat de la informació.**

SEGURETAT DE LA INTEL·LIGÈNCIA ARTIFICIAL

Aquesta tecnologia ja és present a gairebé tots els aspectes de la nostra vida. Des dels assistents virtuals que ens ajuden a planificar el nostre dia fins als **cotxes autònoms** que prometen un futur més segur al trànsit, la IA ens fa la vida més fàcil. Millora la nostra atenció mèdica, personalitza les nostres experiències d'aprenentatge i **ens ajuda a prendre decisions** informades en les nostres finances.

A mesura que la IA i l'aprenentatge automàtic juguen un paper cada vegada més important en la tecnologia, es requereix seguretat per protegir els models, les dades i les **decisions basades en IA contra atacs**.

ÀMBITS DE LA CIBERSEGURETAT

SEGURETAT EN LA CADENA DE SUBMINISTRAMENT

La digitalització, **l'automatització** i l'adopció de sistemes de gestió de la cadena de subministrament basats a la núvol permeten una major eficiència i visibilitat en tot el procés. A més, **la connectivitat global facilita la col·laboració en temps real amb proveïdors**, transportistes i clients arreu del món, agilitzant la entrega de productes i serveis. La tecnologia i la connectivitat són pilars fonamentals per a una cadena de subministrament àgil, eficient i **capaç d'adaptar-se** a les demandes canviant del mercat global.

A mesura que les organitzacions depenen d'una cadena de subministrament global, és important garantir que els components i productes adquirits **no estiguin compromesos per amenaces cibernètiques.**

SEGURETAT DEl NÚVOL

La ciberseguretat al núvol és essencial en un món cada vegada més digitalitzat. A mesura que les organitzacions migren les seves dades i aplicacions a entorns de núvol públic, privat o híbrid, s'enfronten a nous reptes de seguretat. **La protecció de dades confidencials, la prevenció d'amenaces cibernètiques i la garantia de la continuïtat del negoci són prioritats crítiques.** Això implica la implementació de mesures de seguretat robustes, com **l'encriptació de dades**, l'autenticació de múltiples factors i la supervisió constant. La col·laboració entre proveïdors de serveis al núvol i empreses és clau per garantir un entorn segur al núvol i **protegir la confidencialitat i la integritat dels actius digitals.**

A mesura que més empreses adopten serveis al núvol, la seguretat del núvol s'ha tornat crítica. Això inclou **protegir les dades** i les aplicacions emmagatzemades en entorns de núvol públic, privat o híbrid.

L’ R+D+I impulsa la creació de noves tecnologies i eines de ciberseguretat, com ara sistemes de detecció d'amenaces avançats, solucions d'autenticació biomètrica, algoritmes de xifrat més forts i tècniques d'intel·ligència artificial per a la identificació d'amenaces.

Els investigadors i les investigadores en ciberseguretat realitzen anàlisis exhaustius per identificar vulnerabilitats en sistemes i programari existents. Aquesta investigació permet a les organitzacions aplicar correccions i protegir els seus sistemes contra amenaces conegudes. A més, també es realitzen simulacions i exercicis de ciberseguretat per avaluar la preparació d'organitzacions i governs davant possibles ciberatacs.

Conceptes bàsics (Termcat)

Firewall

“El tallafoc (en anglès, firewall) és programari o maquinari que gestiona i controla les comunicacions d'una xarxa local amb altres xarxes externes per tal de garantir-ne la seguretat."

Malware

"Programari concebut específicament per a prendre el control d'un sistema informàtic, interferir en el seu funcionament normal, desestabilitzar-lo o danyar-lo.”

Autenticació de doble factor

“Comprovació de la identitat d’un usuari basada en un sistema de doble clau, és a dir, que utilitza dos elements de seguretat diferents per a acreditar la identitat i iniciar la sessió.”

Big Data

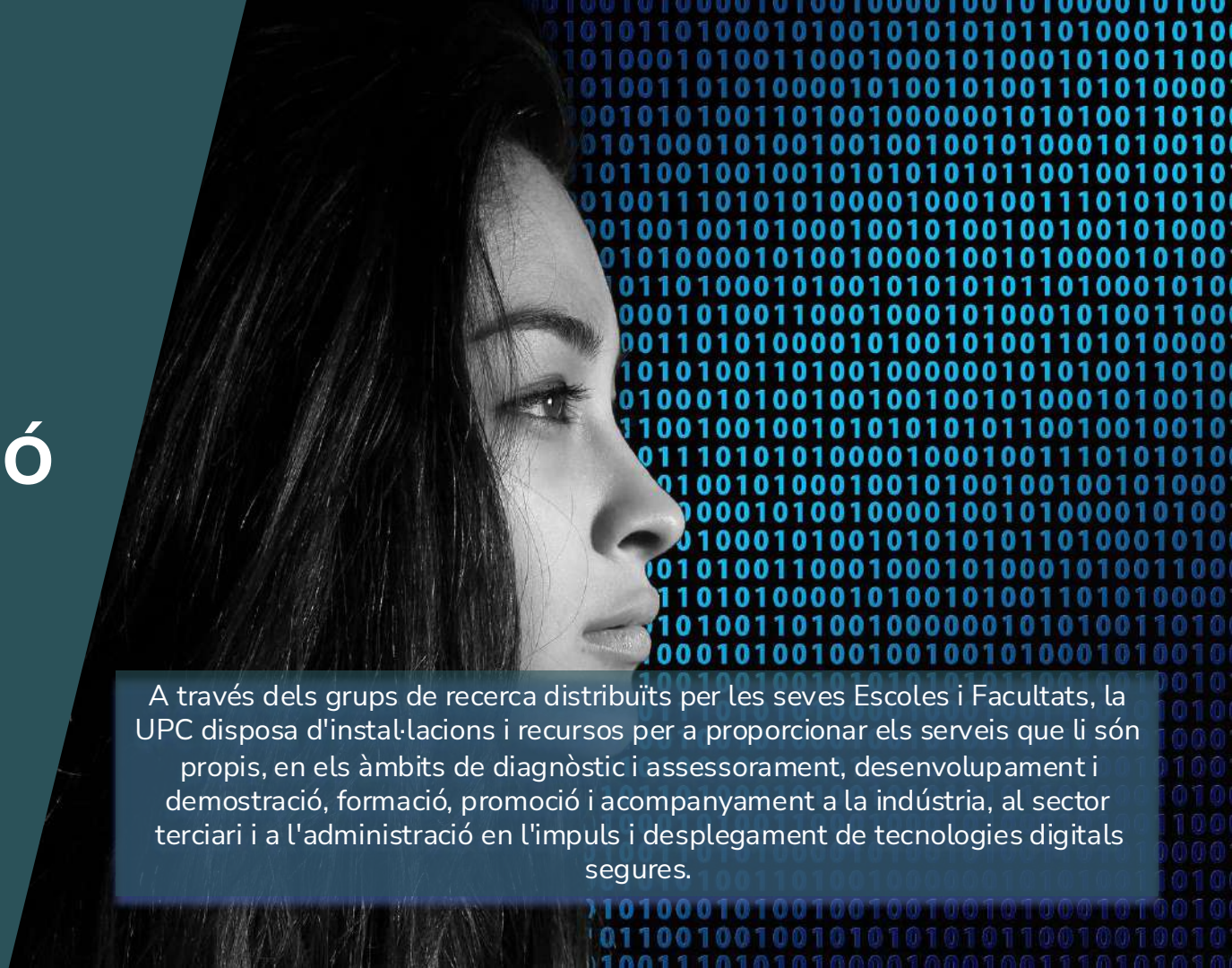
“Conjunt de dades que pel seu volum, la seva naturalesa i la velocitat a què han de ser processades ultrapassen la capacitat dels sistemes informàtics habituals.”

Phishing

“Pràctica fraudulenta consistent a simular una identitat falsa, sovint per suplantació de la identitat d'una persona o un organisme determinats, sigui per correu electrònic, en una trucada o per altres mitjans, amb l'objectiu d'incitar les possibles víctimes a fer una acció que permeti robar-los dades personals.”

03

RECERCA I INNOVACIÓ



A través dels grups de recerca distribuïts per les seves Escoles i Facultats, la UPC disposa d'instal·lacions i recursos per a proporcionar els serveis que li són propis, en els àmbits de diagnòstic i assessorament, desenvolupament i demostració, formació, promoció i acompanyament a la indústria, al sector terciari i a l'administració en l'impuls i desplegament de tecnologies digitals segures.

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Exemples d'activitat I

Softwarització de serveis i aplicacions de xarxa d'Internet per a 5G.

Disseny de xarxes de nova generació, incloent routing, SDN, gestió de xarxes, seguretat, etc.

Gestió de la informació, fent èmfasi en aspectes relatius a la qualitat de la informació, l'exploració de la informació provinent de fonts de dades diverses i els grans volums de dades.

Desenvolupament científic i tecnològic d'equips i sistemes d'adquisició remota de dades.

Desenvolupament de tècniques de protecció de la informació, especialment en l'anonimat de les bases de dades per protegir la privacitat dels usuaris quan aquestes dades són analitzades per tercers.

Auditoria i anàlisi de riscos de sistemes informàtics i industrials.

Resposta a incidents i anàlisi forense de sistemes informàtics compromesos.

Exemples d’activitat II

Augment de la capacitat dels sistemes de ràdio perquè puguin processar grans quantitats de trànsit i d'alta velocitat, per a maximitzar la capacitat del sistema i oferir qualitat de servei.

Estudi dels protocols que permeten l'autoconfiguració d'una xarxa, incloent l'estudi dels protocols d'encaminament ad hoc, el descobriment de recursos i l'autoconfiguració.

Garantia de la resiliència cibernètica en la cadena de subministrament de sistemes de TIC en entorns complexos.

Mineria, validació, correcció i fusió de dades heterogènies per al suport d'informació cognitiva.

Tractament digital de senyals, el disseny electrònic de sistemes d’adquisició de dades i l’automatització de sistemes complexos de mesurament basats en la utilització de dispositius intel·ligents de supervisió i control.

Optimització en la gestió de recursos hardware i software, tant per part del sistema operatiu com per part dels elements virtualitzats.

Disseny de sistemes de diagnosi i control tolerants a fallades, resilients i segurs.

GRUPS DE RECERCA I LABORATORIS UPC EN CIBERSEGURETAT

- BAMPLA - Disseny i Avaluació De Xarxes i Serveis de Banda Ampla
- CBA - Broadband Communications Systems and Architectures Research Group
- CRAAX - Advanced Network Architectures Lab
- DAMA – Data Management Group
- IMP – Information Modeling and Processing
- ISG - Information Security Group
- InLAB FIB – Laboratori de Projectes Informàtics
- MAK - Matemàtica Aplicada a la Criptografia
- MCIA - Motion Control and Industrial Applications Research Group
- SAC – Sistemes Avançats De Control
- SISCOM – Smart Services for Information Systems and Communication Network
- WNG - Wireless Networks Group

CENTRES ESPECÍFICS DE RECERCA UPC

CCABA – Centre De Comunicacions Avançades de Banda Ampla

El CCABA té com a objectius generar estructures de recerca envers l'aparició de les noves tecnologies (5G, 6G, IoT, Virtualització de Xarxes i Serveis, Intel¿ligència Artificial i Realitat Augmentada, Maching Learning, Smart Cities, etc.).

CS2AC – Supervision, Safety and Automatic Control

És un grup multidisciplinari de professors de la UPC i investigadors/es del CSIC dedicats a l'ampli camp del control automàtic i sistemes de monitoratge. L'objectiu principal de CER CS2AC-UPC és contribuir a la competitivitat de les nostres empreses i al coneixement científic i tècnic mitjançant el desenvolupament de sistemes de control avançats i el disseny de sistemes òptims, així com el control tolerant a fallades de sistemes complexos.

SARTI - Centre de Desenvolupament Tecnològic de Sistemes d'Adquisició Remota i Tractament de la Informació

L'objectiu del grup és el desenvolupament científic i tecnològic de sistemes i equips d'adquisició remota, amb un èmfasi particular en la instrumentació virtual i la oceanografia, incloent simulacions i mètodes d'anàlisi estadística, mitjançant l'ús de tècniques avançades de disseny electrònic.

IDEAI-Intelligent Data Science & Artificial Intelligence Research Center

IDEAI-UPC és un centre de recerca amb certificat de grup de recerca consolidat d'excel·lència reconeguda per AGAUR (SGR-1532), integrat per set nuclis especialitzats de recerca de les diferents branques de la IA, amb més de 80 investigadors i investigadores a temps complert, 72 investigadors i investigadores sènior permanents i 150 doctorands i estudiants de màster.

LABORATORIS I INSTITUTS

Laboratoris

- **RDLAB – Research and Development Lab**

  El laboratori d'Investigació i Desenvolupament (/rdlab) se centra en millorar els processos d'investigació i transferència de tecnologia mitjançant un suport i serveis de TI.

Instituts

IRI – Institut de Robòtica i Informàtica Industrial

L'Institut té tres objectius principals: promoure la recerca fonamental en Robòtica i Informàtica Aplicada, col·laborar amb la comunitat en projectes tecnològics industrials i oferir educació científica mitjançant cursos de postgrau.

04

PROJECTES D'EXCEL·LÈNCIA UPC

En aquest document es consideren projectes d'excel·lència aquells en què:

- El procés científic és rigorós i compleix amb estàndards de qualitat elevats.
- Són estratègics i tractors.
- Adquireixen un compromís amb els reptes socials i tenen un gran impacte científic i socioeconòmic.
- Tenen repercussió al territori.
- Compten amb diferents entitats participants de la quàdruple hèlix, fet que fa que els projectes siguin multidisciplinaris.

Els projectes d'excel·lència UPC estan finançats per diversos programes, com per exemple, del Plan Estatal o l'Horizon Europe.

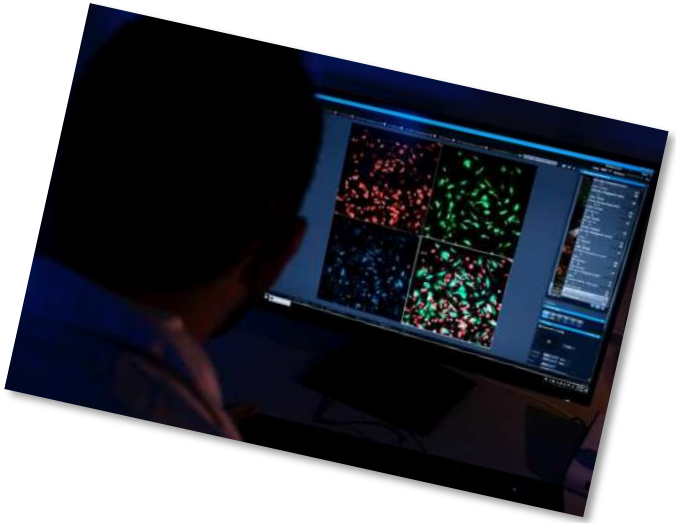
UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

PROJECTES D'EXCEL·LÈNCIA UPC

MEDSURANCE - Advanced Security-for-safety Assurance for Medical Device IoT

Els avenços en els sistemes de tecnologia sanitària han donat lloc a arquitectures socio-tècniques complexes que ofereixen serveis centrats en el pacient. Tanmateix, juntament amb els beneficis clínics, també han sorgit riscos de seguretat que cal gestionar.

El projecte MEDSECURANCE busca desenvolupar noves metodologies i tecnologies per assegurar la gestió efectiva i contínua de sistemes segurs a l'Internet de les Coses Mèdiques (IoMT). El seu enfocament inclou comprendre les amenaces de l'IoMT, considerant la interdependència de sistemes, l'intercanvi d'informació i les implicacions regulatories. Proporcionarà solucions escalables de gestió de sistemes segurs que millorin la **presa de decisions en defensa cibernètica i automatitzaran la garantia de ciberseguretat**, treballant en col·laboració amb socis de la indústria mèdica i parts interessades de l'atenció mèdica.



Imatge cedida per Toni Santiso

Grup de recerca UPC implicat: IMP - Information Modeling and Processing

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

PROJECTES D'EXCEL·LÈNCIA UPC

FISHY - A coordinated framework for cyber resilient supply chain systems over complex ICT infrastructures

El projecte FISHY té com a objectiu desenvolupar una plataforma que garanteixi la resiliència cibernètica en la cadena de subministrament de sistemes de TIC en entorns complexos. Aquesta plataforma permetrà l'orquestació segura de sistemes de TIC complexos des de l'IoT fins a la infraestructura de núvol i xarxes, **gestionant riscos, vulnerabilitats i mètriques de seguretat**. Fer servir interfícies basades en la intenció i tecnologies com l'anàlisi de dades, els registres distribuïts i la intel·ligència artificial serà fonamental. **A més, la plataforma estarà dissenyada per adaptar-se en temps real i respondre als ciberatacs, especialment en l'àmbit de l'IoT.** Aquest projecte inclou casos d'ús en sectors com l'agricultura, la manufactura i el transport, amb l'objectiu de demostrar una prova de concepte de la plataforma FISHY i establir estratègies d'adopció i difusió a gran escala.

Grup de recerca UPC implicat: CRAAX

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

PROJECTES D'EXCEL·LÈNCIA UPC

i3-MARKET - Intelligent, Interoperable, Integrative and deployable open source MARKETplace with trusted and secure software tools for incentivising the industry data economy

El projecte i3-MARKET aborda la creixent demanda d'un Mercat Únic de Dades Europeu innovant en les plataformes de mercat, demostrant amb implementacions industrials que el creixement de l'economia de dades és possible. La proposta d'i3-MARKET proporciona tecnologies per a una col·laboració i federació de plataformes de mercat existents i futures, centrant una atenció especial en les dades industrials i en els actius comercials sensibles de les pimes i les grans corporacions industrials.

És conegut que, malgrat diversos intents d'investigació i innovació en la gestió de Big Data, **la integració i seguretat de dades personals i industrials, no existeix un mercat de dades àmpliament acceptat**, fiable i segur. **i3-MARKET abordarà això desenvolupant tecnologies i solucions que falten per a una infraestructura fiable**, interoperable i descentralitzada, anomenada Marc de Programari i3-MARKET o també conegut com a i3-MARKET Backplane, que permet la federació mitjançant la interoperabilitat dels espais i mercats de dades existents i emergents.

Grup de recerca UPC implicat: ISG - Information Security Group

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

PROJECTES D'EXCEL·LÈNCIA UPC

COMPROMISE - Enhancing Communication Protocols with Machine Learning while Protecting Sensitive Data. Data privacy for communication networks and dynamic databases

El projecte COMPROMISE aborda el repte de **protegir la privadesa en un món digital altament connectat.** Se centra a millorar la privadesa en els protocols de xarxa i prevenir atacs a la privadesa. El projecte busca equilibrar la utilitat de la tecnologia amb la protecció de les dades personals, utilitzant coneixements en seguretat, privadesa, protocols de comunicació i aprenentatge automàtic. A més, s'aplica en xarxes sense fils i protocols d'enrutament. Un cas pràctic és MobilitApp, una aplicació que utilitza dades de sensors per millorar els serveis de transport públic.

Grup de recerca UPC implicat: SISCOM

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

PROJECTES D'EXCEL·LÈNCIA UPC

RISEBLOCK - Privacy and security in public blockchains and their application to data marketplaces

Els actuals mercats de dades estan tancats i controlats per uns pocs, la qual cosa limita la competència. Les *Blockchains* públiques ofereixen transparència i confiança basada en contractes intel·ligents, però plantegen reptes de privadesa. Les Proves de Coneixement Zero (ZKPs) poden abordar aquests problemes. Aquest projecte se centra a crear mercats de dades basats en *Blockchains* públiques i en investigar la seguretat de les *Blockchains* públiques en general. També s'aborda la gestió de dades en aquestes *Blockchains* i com controlar-ne la redistribució. L'objectiu és promoure una economia de dades competitiva i segura on tots els interessats puguin participar lliurement sota regles justes.

Grup de recerca UPC implicat: ISG - Information Security Group

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

PROJECTES D'EXCEL·LÈNCIA UPC

IRIS - Artificial Intelligence threat Reporting and Incident response System

Els avanços en la intel·ligència artificial (IA) i l'Internet de les coses (IoT) han augmentat de manera exponencial en els darrers anys, i amb això també han crescut les preocupacions sobre la **ciberseguretat**. El projecte IRIS, finançat per la Unió Europea, abordarà els reptes dels sistemes TIC impulsats per IoT i AI mitjançant un enfocament col·laboratiu centrat en equips de resposta a incidents de seguretat informàtica (CERTs/CSIRTs).

Específicament, el projecte proporcionarà als CERTs/CSIRTs un conjunt d'eines de resposta a incidents d'última generació per **avaluar, detectar, respondre i compartir informació sobre amenaces i vulnerabilitats de sistemes** TIC impulsats per IoT i AI. El projecte establirà la primera formació en línia dedicada i exercicis cibernètics per preparar els CERTs/CSIRTs per p**rotegir de manera col·laborativa infraestructures crítiques i sistemes contra amenaces transfronterisses d'AI i IoT**. Es realitzaran demostracions pilot a Helsinki, Tallinn i Barcelona.

Grup de recerca UPC implicat: IMP – Information Modeling and Processing

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

PROJECTES D'EXCEL·LÈNCIA UPC

Investigació i recerca d'eines i malware en ciberatacs a infraestructures d'empreses

El projecte de doctorat se centrarà en la creació d'eines, la definició de procediments durant la resposta d'incidents de ciberseguretat i l'anàlisis de ***software* de tipus *malware* utilitzat pels atacants**. Aquesta resposta implicarà la investigació i l'anàlisi de les tècniques i tàctiques utilitzades pels ciberdelinqüents, permetent definir mesures de prevenció i d'actuació enfront aquestes amenaces.

Les eines per l'anàlisi, la resolució de la resposta i la implementació de mesures de protecció podran implicar l'ús de tecnologies diverses, que podran incloure des de projectes de software lliure, programes de pagament dedicats, *hardware* de tipus divers, implementació d'eines amb intel·ligència artificial, etc. **L'anàlisi previ a la implementació de les mesures de protecció implicarà l'estudi del *software* maliciós**, tant de manera estàtica (*reversing*) com de manera dinàmica.

Grup de recerca UPC implicat: ISG - Information Security Group

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

ALGUNES PUBLICACIONS I

Ganguly, A.; S. Abadal; Thakkar, I.; Enright, N.; Riedel, M.; Babaie, M.; Balasubramonian, R.; Sebastian, A.; Pasricha, S.; Taskin, B. (2022) .Interconnects for DNA, Quantum, In-Memory, and Optical Computing: Insights from a panel discussion. IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/9714013
L'article aborda l'aparició de nous paradigmes informàtics, com la computació d'ADN, quàntica, òptica i en memòria, impulsats per avenços tecnològics. També es discuteix el paper de les interconnexions i la integració de tecnologies mitjançant arquitectures basades en xiplets.

Leyva-Pupo, I., Cervello-Pastor, C., Anagnostopoulos, C., & Pezaros, D. P. (2022). Dynamic UPF placement and chaining reconfiguration in 5G networks. Computer Networks, 215, 109200. https://doi.org/10.1016/j.comnet.2022.109200
L'article destaca la importància de la virtualització de funcions de xarxa (NFV) i la computació a la vora d'accés múltiple (MEC) en el desenvolupament de xarxes 5G. Proposa solucions per optimitzar la ubicació i seqüenciació de funcions de xarxa virtuals, garantint eficiència i qualitat de servei en entorns MEC.

Pujol-Perich, D., Suárez-Varela, J., Cabellos-Aparicio, A., & Barlet-Ros, P. (2022). Unveiling the potential of graph neural networks for robust intrusion detection. Performance evaluation review, 49(4), 111-117. https://doi.org/10.1145/3543146.3543171
Els darrers anys han experimentat un augment d'atacs amb greus danys econòmics i de privadesa, destacant la necessitat de sistemes precisos de Detecció d'Intrusos en Xarxa (NIDS). L'article proposa un model de Xarxes Neuronals en Grafo (GNN) que, en considerar les relacions entre les connexions de xarxa, assoleix una robustesa excepcional davant d'atacs adversos en comparació amb tècniques de ML convencionals.

ALGUNES PUBLICACIONS II

Rodríguez, E., Otero, B., & Canal, R. (2023). A survey of machine and deep learning methods for privacy protection in the internet of Things. Sensors, 23(3), 1252. https://doi.org/10.3390/s23031252
L'article examina solucions basades en *Machine Learning* i *Deep Learning* per preservar la privacitat a l'Internet de les Coses (IoT), considerant amenaces i atacs actuals en entorns com ciutats intel·ligents i vehicles autònoms.

Rodríguez, E., Valls, P., Otero, B., Costa, J. J., Verdú, J., Pajuelo, M. A., & Canal, R. (2022). Transfer-Learning-Based Intrusion Detection Framework in IoT networks. Sensors, 22(15), 5621. https://doi.org/10.3390/s22155621
L'article aborda l'increment dels ciberatacs a l'Internet de les Coses (IoT) i proposa una solució basada en transferència de coneixement (TL) per detectar eficaçment atacs zero-day en xarxes IoT 5G amb manca de dades etiquetades. Aquest enfocament supera altres sistemes en la detecció d'atacs, demostrant l'eficàcia del TL en entorns IoT.

Sedar, R.; Kalalas, C.; Vazquez, F.; Alonso, L.; Alonso, J. (2023). A comprehensive survey of V2X cybersecurity mechanisms and future research paths. IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/10026338
L'article tracta els avenços recents en la comunicació de vehicle a tot (V2X), posant èmfasi en les millores en la connectivitat i autonomia de conducció en el transport.

05 FORMACIÓ

UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

GRAUS - UPC

- Grau en Enginyeria de Sistemes de Telecomunicació (EETAC)
- Grau en Enginyeria de Sistemes TIC (EPSEM)
- Grau en Enginyeria de Tecnologies i Serveis de Telecomunicació (ETSETB)
- Grau en Enginyeria Electrònica de Telecomunicació (ETSETB)
- Grau en Enginyeria en Geoinformació i Geomàtica (EPSEB)

MÀSTERS - UPC

- Master's degree in Cybersecurity (ETSETB)
- Master's degree in Advanced Telecommunication Technologies (ETSETB) i (EETAC)

PROGRAMES DE DOCTORAT

- Doctorat en Computació
- Doctorat en Intel·ligència Artificial

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Més màsters: https://www.upc.edu/ca/masters
Més programes de doctorat: https://doctorat.upc.edu/ca/programes/

UPC-SCHOOL

- Màster en Cybersecurity Management
- Posgrau en Detecció i Resposta de Ciberatacs
- Posgrau en Planificació i Gestió de la Ciberseguretat
- Posgrau microcredencial en Ciberseguretat a les nostres ciutats

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Més graus: https://www.upc.edu/ca/graus/

SERVEI DE SUPORT A LA RECERCA I LA INNOVACIÓ

https://rdi.upc.edu
@RDI_UPC

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH