PHD THESIS

EXPRESSIVE POLICY BASED AUTHORIZATION MODEL FOR RESOURCE-CONSTRAINED DEVICE SENSORS

MIKEL URIARTE ITZAZELAIA

Supervised by Jasone Astorga Burgo and Eduardo Jacob Taquet

University of the Basque Country UPV/EHU

Faculty of Engineering of Bilbao

Department of Communications Engineering

October 2018

Having somewhere to go is home.
Having someone to love is family.
Having both is a blessing.

Dedicated to my wife, my family and many friends.

ABSTRACT

Upcoming smart scenarios enabled by the Internet of Things (IoT) envision smart objects that expose services that can adapt to user behavior or be managed with the goal of achieving higher productivity, often in multi-stakeholder applications. In such environments, smart things are cheap sensors (and actuators) and, therefore, constrained devices. However, they are also critical components because of the importance of the provided information. Given that, strong security in general and access control in particular is a must.

However, tightness, feasibility and usability of existing access control models do not cope well with the principle of least privilege; they lack both expressiveness and the ability to update the policy to be enforced in the sensors. In fact, (1) traditional access control solutions are not feasible in all constrained devices due their big impact on the performance although they provide the highest effectiveness by means of tightness and flexibility. (2) Recent access control solutions designed for constrained devices can be implemented only in not so constrained ones and lack policy expressiveness in the local authorization enforcement. (3) Access control solutions currently feasible in the most severely constrained devices have been based on authentication and very coarse grained and static policies, scale badly, and lack a feasible policy based access control solution aware of local context of sensors.

Therefore, there is a need for a suitable End-to-End (E2E) access control model to provide fine grained authorization services in service oriented open scenarios, where operation and management access is by nature dynamic and that integrate massively deployed constrained but manageable sensors.

Precisely, the main contribution of this thesis is the specification of such a highly expressive E2E access control model suitable for all sensors including the most severely constrained ones.

Concretely, the proposed E2E access control model consists of three main foundations. (1) A hybrid architecture, which combines advantages of both centralized and distributed architectures to enable multi-step authorization.

Fine granularity of the enforcement is enabled by (2) an efficient policy language and codification, which are specifically defined to gain expressiveness in the authorization policies and to ensure viability in very-constrained devices. The policy language definition enables both to make granting de-

cisions based on local context conditions, and to react accordingly to the requests by the execution of additional tasks defined as obligations.

The policy evaluation and enforcement is performed not only during the security association establishment but also afterward, while such security association is in use. Moreover, this novel model provides also control over access behavior, since iterative re-evaluation of the policy is enabled during each individual resource access.

Finally, (3) the establishment of an E2E security association between two mutually authenticated peers through a security protocol named Hidra. Such Hidra protocol, based on symmetric key cryptography, relies on the hybrid three-party architecture to enable multi-step authorization as well as the instant provisioning of a dynamic security policy in the sensors. Hidra also enables delegated accounting and audit trail.

Proposed access control features cope with tightness, feasibility and both dimensions of usability such as scalability and manageability, which are the key unsolved challenges in the foreseen open and dynamic scenarios enabled by IoT.

Related to efficiency, the high compression factor of the proposed policy codification and the optimized Hidra security protocol relying on a symmetric cryptographic schema enable the feasibility as it is demonstrated by the validation assessment.

Specifically, the security evaluation and both the analytical and experimental performance evaluation demonstrate the feasibility and adequacy of the proposed protocol and access control model.

Concretely, the security validation consists of the assessment that the Hidra security protocol meets the security goals of mutual strong authentication, fine-grained authorization, confidentiality and integrity of secret data and accounting.

The security analysis of Hidra conveys on the one hand, how the design aspects of the message exchange contribute to the resilience against potential attacks. On the other hand, a formal security validation supported by a software tool named AVISPA ensures the absence of flaws and the correctness of the design of Hidra.

The performance validation is based on an analytical performance evaluation and a test-bed implementation of the proposed access control model for the most severely constrained devices.

The key performance factor is the length of the policy instance, since it impacts proportionally on the three critical parameters such as the delay, energy consumption, memory footprint and therefore, on the feasibility.

Attending to the obtained performance measures, it can be concluded that the proposed policy language keeps such balance since it enables expressive policy instances but always under limited length values. Additionally, the proposed policy codification improves notably the performance of the pro-

tocol since it results in the best policy length compression factor compared with currently existing and adopted standards.

Therefore, the assessed access control model is the first approach to bring to severely constrained devices a similar expressiveness level for enforcement and accounting as in current Internet. The positive performance evaluation concludes the feasibility and suitability of this access control model, which notably rises the security features on severely constrained devices for the incoming smart scenarios.

Additionally, there is no comparable impact assessment of policy expressiveness of any other access control model. That is, the presented analysis models as well as results might be a reference for further analysis and bench marking.

LABURPENA

Gaur egun darabilzkigun hainbeste gailutan mikroprozesadoreak daude txertatuta, eragiten duten prozesuan neurketak egin eta logika baten ondorioz ekiteko. Horretarako, bai sentsoreak eta baita aktuadoreak erabiltzen dira (hemendik aurrera, komunitatean onartuta dagoenez, sentsoreak esango diegu nahiz eta erabilpen biak izan). Orain arteko erabilpen zabalenetako konekzio motak, banaka edota sare lokaletan konekatuta izan dira. Era honetan, sentsoreak elkarlanean elkarreri eraginez edota zerbitzari nagusi baten agindupean, erakunde baten prozesuak ahalbideratu eta hobetzeko erabili izan dira.

Internet of Things (IoT) deritzonak, sentsoreak dituzten gailuak Internet sarearen bidez konektatu eta prozesu zabalagoak eta eraginkorragoak ahalbidetzen ditu. Smartcity, Smartgrid, Smartfactory eta bestelako *smart* adimendun ekosistemak, gaur egun dauden eta datozen komunikaziorako teknologien aukerak baliatuz, erabilpen berriak ahalbideratu eta eragina areagotzea dute helburu.

Era honetan, ekosistema hauek zabalak dira, eremu ezberdinetako erakundeek hartzen dute parte, eta berariazko sentsoreak dituzten gailuen kopurua izugarri handia da. Sentsoreak beraz, berariazkoak, merkeak eta txikiak dira, eta orain arteko lehenengo erabilpen nagusia, magnitude fisikoren bat neurtzea eta neurketa hauek zerbitzari zentralizatu batera bidaltzea izan da. Hau da, inguruan gertatzen direnak neurtu, eta zerbitzari jakin bati neurrien datuak aldiro aldiro edota atari baten baldintzapean igorri. Zerbitzariak logika aplikatu eta sistema osoa adimendun moduan jardungo du. Jokabide honetan, aurretik ezagunak diren entitateen arteko komunikazioen segurtasuna bermatzearen kexka, nahiz eta Internetetik pasatu, hein onargarri batean ebatzita dago gaur egun.

Baina adimendun ekosistema aurreratuak sentsoreengandik beste jokabide bat ere aurreikusten dute. Sentsoreek eurekin harremanak izateko moduko zerbitzuak ere eskaintzen dituzte. Erakunde baten prozesuetan, beste jatorri bateko erakundeekin elkarlanean, jokabide honen erabilpen nagusiak bi dira. Batetik, prozesuan parte hartzen duen erabiltzaileak (eta jabeak izan beharrik ez duenak) inguruarekin harremanak izan litzake, eta bere ekintzetan gailuak bere berezitasunetara egokitzearen beharrizana izan litzake. Bestetik, sentsoreen jarduera eta mantenimendua zaintzen duten teknikariek, beroriek egokitzeko zerbitzuen beharrizana izan dezakete.

Holako harremanak, sentsoreen eta erabiltzaileen kokalekua zehaztugabea izanik, kasu askotan Internet bidez eta zuzenak (*end-to-end*) izatea aurreikusten da. Hau da, sentsore txiki asko daude handik hemendik sistemaren adimena ahalbidetuz, eta harreman zuzenetarako zerbitzu ñimiñoak eskainiz. Batetik, zerbitzu zuzena, errazagoa eta eraginkorragoa dena, bestetik erronkak ere baditu. Izan ere, sentsoreak hain txikiak izanik, ezin dituzte gaur egungo protokolo eta mekanismo estandarak gauzatu. Beraz, sare mailatik eta aplikazio mailarainoko berariazko protokoloak sortzen ari dira. Tamalez, protokolo hauek arinak izatea dute helburu eta segurtasuna ez dute behar den moduan aztertu eta gauzatzen. Eta egon badaude berariazko sarbide kontrolerako ereduak baina baliabideen urritasuna dela eta, ez dira ez zorrotzak ez kudeagarriak. Are gehiago, Gartnerren arabera, erabilpen aurreratuetan inbertsioa gaur egun mugatzen duen traba nagusia segurtasunarekiko mesfidantza da.

Eta hauxe da erronka eta tesi honek landu duen gaia: batetik sentsoreak hain txikiak izanik, eta baliabideak hain urriak (10kB RAM, 100 kB Flash eta bateriak, sentsore txikienetarikoetan), eta bestetik Internet sarea hain zabala eta arriskutsua izanik, segurtasuna areagotuko duen sarbide zuzenaren kontrolerako eredu zorrotz, arin eta kudeagarri berri bat zehaztu eta bere erabilgarritasuna aztertu.

Horretarako, ikerkuntza helburuak zehaztu eta jarduera pausu ezberdinak eman ditugu. Lehenengo, orain arte aipatu diren adimendun ekosistema aurreratuetako segurtasuna orokorrean, eta sarbide kontrolean bereziki dauden beharrizanak, zailtasunak eta ebatzi gabe dauden arazoak aztertu ditugu.

Ondoren, sarbide kontrolen funtsa eta orain arteko ikerkuntzaren hedaduraren azterketa sakona egin da. Batetik, baliabideen urritasunik barik jarduten duten sarbide kontrol ereduak aztertu ditugu. Bestetik, orain arte bereziki proposatutako sarbide kontrol ereduak lehenago aztertutako beharrizanak eta zailtasunak zein heinean eta zelan betetzen dituzten aztertu dugu. Ondorioz, gaur egun ez dago sarbide kontrol eredurik (1) arina izateaz gain, hau da, baliabide urriko sentsoreetan egingarria, (2) zorrotza denik, hau da, politika aberatsa zehaztu eta betearazten duenik, ezta (3) kudeagarria denik ere ez, hau da, egoera aldakorretara politika estutuz egokitu daitekenik, edota hazteko gaitasuna duenik (erabilgarria azken finean).

Orduan, gure proposamenak berariazko sarbide kontrol eredu berri bat zehazten du. Batetik, politika zorrotzak zehazteko lengoaia berri bat proposatzen du. Gainera, zehaztutako politikak kodifikatzeko era berri eraginkorra ere proposatzen du. Bestetik, harreman seguru zuzena burutzeko, zuzeneko sesio ziurra gauzatzeko protokolo berri bat ere proposatzen du. Hidra izeneko protokolo hau, kontrola pausu bitan betearaztea ahalbidetzen duen arkitektura hibridoan oinarritzen da.

ARKITEKTURA

Zehaztutako arkitektura hibridoak, arkitektura zentralizatuen eta banatuen ezaugarriak uztartzen ditu bakoitzaren abantailak erabiltzeko asmoz. Izan ere, hiru entitate mota ezberdintzen dira: (1) erabiltzailea (*subject*) da, (2) sentsoreko (*resource*) zerbitzuak erabili nahi dituena, eta (3) zerbitzari bitartekari (*access control server*) baten laguntzarekin, sentsorearekin sesio zuzena gauzatzen duena.

Sentsoreak baliabide urrikoak dira, berriz, zerbitzaria ez, eta hau ezaugarri berezia da; azkenik, erabiltzaileak ez du zertan baliabide urriak izan beharrik.

Sesio ziurra gauzatzeko, zerbitzariaren bitartekaritza erabiltzeak, estandarrak erabili ahal izateaz gain, zerak ahalbidetzen ditu. Batetik, zerbitzarian baimena ematearen prozesuarekin loturiko eginkizun astun batzuk betetzen dira. Hau da, aurretiko identifikazioa eta autentifikazioa egiten dira, eta baita hasierako baimentzea ere. Horretarako identitateak, kredentzialak, eta politikak zehazteko eta era bateratuan eta eraginkorrean kudeatzeko funtzioak ditu. Gainera, Hidra protokoloan parte hartzen du sesio zuzena gauzatu ahal izateko. Azkenik, Hidraren eraginez, saiakera eta erabilpen guztien aztarnak hartu, bildu eta aztertu ere egiten ditu politikak egokitu eta berriro Hidra protokoloaren bitartez sentsoreei igorriz, adimena ahalbideratuz.

Bere aldetik, sentsoreak, Hidra protokoloa erabiliz, politika egokitua jaso eta autentifikazioaren ostean, bertako baldintzen araberako bigarren baimen zorrotza betearaziko du erabiltzailearekin sesio ziurra gauzatu aurretik. Edozelan ere, saiakeraren aztarnak zerbitzariari igorriko dizkio, eta baimendutako sesio ziurra gauzatzen den kasuetan, aurrerantzeko zerbitzuko eskaera guztiei baimenak betearazi eta aztarna moduan zerbitzariari igortzen dizkio.

Arkitektura honek, sentsoreen urritasunak gaindituz, baimen zorrotza betearaztea eta ikuskatzea ahalbidetzen ditu. Gainera, baimenik gabeko hainbat saiakera sentsoreraino heltzea ekidin, eta kritikoa den energia kontsumoa kontrolatzea ahalbidetzen ditu.

BAIMEN POLITIKAK ZEHAZTEKO LENGOAIA

Politika lengoaia aberats berri bat proposatzen dugu baimen politika zorrotzak zehaztu ahal izateko, baina sentsoreen urritasunak gaindituz. Ohikoa den moduan, baliabide, baldintza eta egoera ezberdinak, arau ezberdinen bitartez zehazten dira, eta beraz, definitutako politika elastikoa da. Gaitasun urriak dituzten sentsoreen arloan, berrikuntza bat, erkatze zuzenaz harago, bertoko baldintzak zehazteko funtzioen aberastasuna da.

Beste berrikuntza bat zera da, baldintzak aztertu ondorengo baimen erabakiaz gain, gainerako betebeharrak ere eragin daitezke. Honen bitartez, bapateko zorroztasunari, erabileraren kontrola gehitu dakioke. Hau da, betebeharrak, baldintzapean dauden erabilera kontadoreak eta egoera erregistroak eguneratu, edota baliabideak blokeatzeko zehaztu daitezke. Ez dago gaur egun, gaitasun urriak dituzten sentsoreetarako egokitua den eta halako aberastasuna ahalbidetzen duen politika lengoaiarik.

Halako aberastasuna ezinezkoa da, politika zehazten duen fitxategiaren luzera handiegia bihurtzen bada. Izan ere, gaitasun urriak dituzten sentsoreetan energia kontsumoan gehien eragiten duten eginkizunek komunikazioak dira. Eta komunikazioetan, gehien eragiten duena mezuen luzera da. Beraz, politikaren luzera derrigorrez kontutan hartu beharreko gaia da, politika Hidra protokoloko mezuetan txertatzen baita.

Beraz, beste berrikuntza garrantzitsu bat, gizakiak zehaztutako politika, sistemek erabiltzeko modura kodifikatzeko era da. Proposatutako kodifikazioak, politika zehazten duen bit katearen luzera zeharo laburtzen du. Proposatutako lengoaiarekin zehaztutako edozein testu formatu onartzen du, eta trinkotze maila oso altua du. Funtsa, politika lengoaiaren ezagutza eta elastikotasuna kudeatzen ahalbidetzen dituen bitak txertatzea dira.

Lortutako laburtzea, politikaren testuaren luzeraren araberakoa da: zenbat eta politika luzeagoa, laburtze indize handiagoa hain zuzen ere. Gaur egun erabiliak diren JSON eta CBOR kodifikazioekin egindako konparaketari adituz, lortutako luzerak ehuneko bosta eta hamarra inguru dira.

Beste alde batetik, badago baimen arauak sarbide kontrol listak (ACL) erabiliz zehazteko ohitura. Hala ere, estatikoa izateaz gain, ez da batere aberatsa eta beraz zorrotza, eta luzera aldetik, erabiltzaile eta zerbitzu kopuru batetik aurrera, guk proposatutako sarbide kontrol eredua arinagoa da.

HIDRA PROTOKOLOA

Proposaturiko arkitekturan, Hidra protokoloak, erabiltzailea eta sentsorearen arteko sesio ziurra bermatzen duen segurtasun atxikimendua ahalbidetzen du. Hau da, protokolo honen bitartez, elkar autentifikatu eta pausu biko baimenaren ondoren, bien arteko gako sekretua banatzen da.

Hidra, Ladonen oinarrituta dago, kriptografia simetrikoa (SKC) erabiltzen du, eta erlojuekiko menpekotasuna ekiditen du. Kerberos moduko tiketak erabiltzen ditu autentifikazioa eta behin-behineko baimenaren adierazle. Berrikuntza nagusia, zehaztutako hamaika mezuetariko jakin baten, egokitutako politika aberats bat txertatzea da. Beraz, segurtasun sesioa gauzatu aurretik, sentsoreak erabiltzailearengandik eskaera jasotzean, ordurako zerbitzariarengandik hartu duen politika betearazten du. Politika txertatze

honek eguneratze eta hazkundea ahalbidetzen ditu, kudeagarritasuna eta erabilgarritasuna sustatuz.

Bigarren berrikuntza nabarmena, saiakera guztien eta zerbitzu eskaera guztien "nork-zer-noiz-zenbat.ªztarnak mezu jakin baten zerbitzariari igorri ahal izatea da. Beraz, zerbitzariak, aztarnak aztertu ondoren, beharrizana ikusi ezkero, politika zehazten duen mezu berri bat ber-igorri diezaioke sentsoreari egokitutako politika eguneratuarekin, adimena sustatuz.

BALIOTZEA

Proposatutako sarbide kontrol eredu berriaren egingarritasuna eta egokitasuna baliotzeko bi ariketa burutu dira. Batetik, berezko segurtasuna aztertu da, eta bestetik, errendimenduan duen eragina aztertu da.

Segurtasuna aztertzeko, Hidrak autentifikazioa, baimen zorrotza, datu sekretuen konfidentzialtasuna eta osotasuna, eta kontularitza betetzen dituela aztertu dugu. Lehenengo eta behin, protokoloko mezuen berezko segurtasun ezaugarriak aztertu ditugu. Goraipatzekoa da mekanismo zehatzak erabili direla erasoekiko berezko segurtasuna sustatzeko, hala nola, igorlearen autentifikazioa, datu batzuen zifratzea, mezuen autentifikazio kodeak (MAC), haziak txertatzea eta zentzu bateko kode kateak.

Hala ere, bigarren azterketa formal bat ere burutu dugu. Azterketa honetan, Hidra AVISPA izeneko software tresna baten bitartez tentatu dugu. Horretarako, Hidraren HLPSL (*High-Level Protocol Specification Language*) eredua sortu dugu, hau da rolak, egoerak eta iragateak, sesioak eta segurtasun helburuak zehaztu ditugu. AVISPA-ren emaitza onek Hidraren segurtasuna bermatzen dute.

Beste alde batetik, Hidrak errendimenduan daukan eraginaren azterketa bi ikuspuntutatik burutu dugu, bata analitikoa eta bestea esperimentala. Kasu bietan, hiru parametro aztertu ditugu: Hidra bitartez segurtasun sesioa gauzatzeko behar den denbora, energia kontsumoa eta behar duen memoria. Azterketa sakonagoa egiteko asmoz, bai politikaren luzerak zein zifratze eta MAC abiadurak ere zelan eragiten duten aztertu dugu. Tamalez, ez dugu halako azterketa alderagarririk aurkitu Hidraren helburu berdintsuak dituzten protokoloekin konparatzeko.

Kasu bietan ere, kalkulatutako eta neurtutako emaitzak oso onargarriak dira, kasu larrienean ere, hau da, politika luzeenarekin eta baliabide gutxien dituen sentsore baten. Hain zuzen ere, denbora, zenbait erreferentzietan estandarizazio erakundeek eta autore nabarmenek gomendatutako balioak baino askoz txikiagoa da. Energia kontsumo handienaren baldintzetan ere, bateria arrunt birekin 4 miloi alditan baino gehiagotan erabili ahal izango litzateke Hidra protokoloa. Azkenik, kasurik txarrenean behar dituen RAM eta Flash memoria ere onargarriak dira.

Beraz, segurtasuna eta errendimenduaren azterketaren emaitzei adituta, Hidra protokoloa ziurra eta gaitasun urrien dituzten sentsoreetan ere egingarria dela esan daiteke.

KONKLUSIOAK

Tesi honetan azaltzen diren ikerketaren emaitzen ekarpenak honexek dira:

Lehenengo, adimendun ekosistema aurreratuak segurtasunarekiko eta zehatzago, sarbide kontrolarekiko dituen beharrizanen, zailtasunen eta erronken azterketa sakonaren emaitzak ditugu: zorroztasuna erabilgarritasuna batetik, eta egingarritasuna bestetik, aurkako indarrak dira batik bat.

Gero, sarbide kontrolen funtsa eta orain arteko ikerkuntza noraino heldu den aztertu ondoren, zera esan daiteke: gaur egun ez dago sarbide kontrol eredurik arina izateaz gain, zorrotza, kudeagarria eta hazgarria denik.

Ondorioz, guk proposatutako berariazko sarbide kontrol eredu berriaren ekarpenak honexek dira. Lehenengoa, politika zorrotzak zehazteko lengoaia aberatsa eta zehaztutako politikak kodifikatzeko eta trinkotzeko era eraginkorra da. Zorroztasuna eta egingarritasuna uztartzen dituzten bi ekarpen esanguratsu dira hauek.

Gero, Hidra izeneko protokoloa zehaztu dugu, erabiltzaileek eta sentsoreek zuzeneko segurtasun sesioak gauzatu ahal izateko. Hidrak, elkar autentifikatzeaz gain, baimena pausu bitan ahalbidetzen du, eta politika egokitua eta eguneratua sentsorean txertatzeko aukera ematen du. Era honetan, baldintza lokalak eta erabilera kontutan hartzen dituen politika betearazi ditzake sentsoreak, bai segurtasun atxikimendu aldian eta baita geroko zerbitzu aldian ere. Gainera Hidrak, aztarna guztien bilketa, azterketa eta erreakzioa ahalbidetzen ditu.

Horretarako, egingarritasunaren alde, proposatzen dugun arkitektura hibridoan, baimentze prozesu osoko eginkizunak banatu egiten ditugu. Arkitektura honetan sentsoreak funtsezko autentifikazioa, baimentzea eta kontularitza egiten ditu, eta berriz, zerbitzari bitartekari batek eginkizun osagarri guztiak burutzen ditu: autentifikazioa, behin-behineko baimentzea, politika egokitua txertatzea, eta kontularitza batik bat. Era honetan, estandarrekiko atxikimendua, eta identitateak, kredentzialak, eta politikak kudeatzeko era bateratu eta eraginkorra ahalbidetzen dira.

Berriro ere, bai Hidra eta baita arkitektura hibridoak, zorroztasuna eta egingarritasuna, eta gainera kudeagarritasuna eta erabilgarritasuna uztartzen dituen beste bi ekarpen esanguratsu dira.

Are gehiago, proposatutako sarbide kontrol eredu berriaren egingarritasuna eta egokitasuna baliotzeko bi ariketa burutu dira. Batetik, berezko segurtasunaren azterketak Hidrak ezarritako segurtasun helburuak betetzen dituela ondorioztatzen du. Bestetik, Hidra errendimenduarengan duen eraginaren

azterketaren ondorioz, gaitasun muga handienak dituzten sentsoreetan ere egingarria dela esan daiteke.

Ikerketaren ondoriozko aurkikuntzak eta proposamenak zabaltzearen alde, argitalpen internazionalak bai aldizkarietan, bai kongresuetan eta baita liburuetan burutu ditugu. Ariketa hauek gainera, ikerketaren bideratze eta emaitzen argitasunaren aldekoak izan dira guretzako.

Proposatutako gaiarekin zerikusia duten ikerketa eta garapenerako proiektu internazionaletan ere parte hartu eta hartzen jarraitzen dugu, badago eta zer ikertu oraindik. Batik bat, arrisku berrien azterketa, froga esperimentalak hardware, sistema eragile, berariazko protokolo estandar berriekin aztertzea eta alderatzea, sarearen eraginaren azterketan sakontzea, eta proposamenaren estandarizatzea dira batzuk.

RESUMEN

Ante la aparición de los escenarios inteligentes que habilita Internet of Things (IoT), comienzan a existir objetos de diferentes organizaciones accesibles a través de la red que ofrecen servicios con el fin de ajustarse a la coyuntura concreta. Tales ajustes permiten, por una parte, una mejor experiencia del usuario final y, por otra, una gestión dinámica en aras de una mayor productividad y eficiencia.

En tales entornos, los objetos inteligentes se despliegan de forma masiva y por tanto son baratos y, en consecuencia, son dispositivos de prestaciones limitadas en términos de capacidad de procesamiento, memoria y autonomía eléctrica. A su vez, son componentes críticos en la cadena de información que sustenta el proceso inteligente que habilitan. Por todo ello, la seguridad en general, y el control de acceso de grado fino, en particular, son requisitos obligatorios.

Sin embargo, tras un extenso análisis del estado del arte, se puede concluir que los modelos de control de acceso existentes y aplicables en dispositivos de prestaciones limitadas no cumplen con los requisitos de políticas expresivas de grado fino, ni con el principio que recomienda otorgar el mínimo de los permisos posibles.

Concretamente, en primer lugar, los controles de acceso tradicionales no son implementables en dispositivos de bajas prestaciones, pese a ser los más exhaustivos y flexibles. En segundo lugar, los nuevos controles de acceso propuestos para dispositivos de bajas prestaciones cumplen parcialmente con el requisito de grado fino y, además, no cubren la gama de dispositivos de mayor escasez de recursos (10 kB RAM, 100 kB Flash). Finalmente, los controles de acceso que actualmente se implementan en los dispositivos de mayor escasez de recursos se apoyan básicamente en la autenticación o, en su caso, las autorizaciones son de grado grueso, es decir, otorgan permisos en exceso, y además, escalan mal y no toman en consideración las condiciones de contexto locales del dispositivo.

Por tanto, persiste la necesidad de un modelo de control de acceso ligero extremo a extremo, que sea exhaustivo, es decir basado en políticas de grado fino y aplicable en escenarios abiertos orientados al servicio. Y ello porque tales escenarios integran cantidades ingentes de dispositivos que ofrecen servicios gestionables y que se implementan en dispositivos baratos y de prestaciones mínimas.

La contribución principal de esta tesis radica precisamente en la especificación de un modelo de control de acceso exhaustivo extremo a extremo sustentado en tres pilares. Primero, una arquitectura híbrida que combina las ventajas de las arquitecturas centralizadas y distribuidas y que posibilita una autorización en dos pasos.

Segundo, un lenguaje expresivo nuevo para definir políticas de autorización exhaustivas de grado fino y un método de codificación de políticas que reduce su longitud al mínimo, permitiendo que sea implementable incluso en los dispositivos de mínimas prestaciones. Este lenguaje permite definir políticas que consideran las condiciones de contexto locales del dispositivo, posibilitando así mismo la ejecución de acciones adicionales obligatorias asociadas a los permisos concedidos.

Finalmente, tercero, se propone un protocolo de seguridad llamado Hidra que permite el establecimiento de una asociación de seguridad extremo a extremo y que garantiza la autenticación mutua, la autorización exhaustiva de grado fino y el registro de actividades. Concretamente, Hidra permite la autorización en dos pasos, así como el provisionamiento dinámico de políticas ajustadas y exhaustivas en el dispositivo al que se pretende acceder.

La evaluación de la política y aplicación de los permisos se realiza en primera instancia en tiempo de establecimiento de la asociación de seguridad entre sujeto y dispositivo. Posteriormente, tal evaluación y aplicación se realiza también en cada uno de los accesos durante la vigencia de tal asociación en los que, además, se puede controlar el uso, el consumo y el comportamiento por parte del usuario.

El control de acceso propuesto cumple los requisitos de exhaustividad, factibilidad y dos dimensiones principales de la usabilidad, como son la escalabilidad y la posibilidad de ser gestionados dinámicamente. De hecho, la factibilidad es posible gracias (a) al factor de compresión tan alto del método de codificación propuesto, y (b) al diseño optimizado del protocolo Hidra basado en un esquema criptográfico de clave simétrica.

De este modo, el análisis de la factibilidad y adecuación del modelo de control de acceso propuesto viene determinado por la evaluación de la seguridad y el rendimiento del protocolo, tanto de forma analítica como experimental.

A saber, la validación de seguridad establece que Hidra cumple con los objetivos de seguridad de autenticación mutua robusta, autorización exhaustiva de grado fino, confidencialidad e integridad de los datos secretos y contabilidad. Tal evaluación analiza, en primer lugar, los aspectos específicos del diseño de Hidra que contribuyen a una mayor robustez frente a los eventuales ataques en red. Y en segundo lugar, la evaluación formal de la seguridad asistida por una herramienta software llamada AVISPA garantiza la ausencia de errores y la exactitud del diseño de Hidra.

Las evaluaciones del rendimiento, tanto analítico como experimental, analizan tres parámetros críticos como son el tiempo de respuesta, el consumo de energía y los requerimientos de memoria. Por un lado, la validación analítica supone una herramienta muy potente para evaluar cómo afectan diferentes parámetros al rendimiento del protocolo y en diferentes escenarios de uso. Por otra parte, la validación experimental permite probar que Hidra es realmente implementable y ejecutable en sensores reales, incluso cuando se trata de los dispositivos de mínimas prestaciones para extremar las condiciones de operación.

Tras el análisis, se confirma que la longitud de la política, que depende a su vez de la exhaustividad aplicada, es el factor clave para la factibilidad, ya que influye de forma directa y proporcional en los tres parámetros evaluados.

En cualquier caso, los resultados son muy positivos y se concluye que la combinación del lenguaje y el método de codificación permite definir políticas exhaustivas sin que su longitud crezca excesivamente. En particular, se demuestra que el factor de compresión del método de codificación propuesto es mucho mayor que el de los actualmente existentes.

Por tanto, se concluye que el control de acceso propuesto mantiene el equilibrio entre exhaustividad y factibilidad, y es el que posibilita mayor expresividad en las políticas comparado con los modelos usados actualmente. Además, el protocolo Hidra permite la provisión dinámica de políticas ajustadas y la contabilidad detallada de las actividades de acceso al dispositivo, lo que contribuye en su conjunto a una mayor seguridad de los dispositivos integrados en los escenarios inteligentes previstos, aun cuando sean de mínimas prestaciones posibles.

Finalmente, no se tiene constancia de una evaluación comparable del impacto de la expresividad de la política en el rendimiento y la factibilidad, por lo que, tanto el modelo de análisis como los resultados obtenidos, pueden ser considerados como una referencia válida para futuros análisis y comparativas.

That girl
Makes me wanna be a better man
Ye should she see fit
Gonna treat her like a real man can
She's fearless, she's free
Oh she is a real live wire.

— Better Man song by Paolo Nutini

ACKNOWLEDGMENTS

This thesis would not have been possible without the support through lessons learned, discoveries made, alternatives explored, and new plans set in motion of many appreciated people.

I owe my deepest gratitude to my friends and thesis supervisors Jasone Astorga and Eduardo Jacob for their invaluable wisdom, guidance, encouragements and dedication. Jasone eta Eduardo, eskerrik asko bihotzez. Jasone, you have been also extraordinarily gentle and supportive in some data processing steps. I extend my gratitude to Maider for so many good suggestions and assistance, eskerrik asko.

I would like also to express my gratitude to my colleagues at Nextel S.A. for their continuous inestimable discussions and support. Oscar, Manu, Pedro, Etxahun, Saioa, and Jordi, we have worked elbow to elbow as a complete team every day for a long time and you always had time for an extra question, thank you very much.

I am grateful also to the colleagues at the Department of Communications Engineering at the University of the Basque Country UPV/EHU, for their continuous endorsement.

I am lucky to have many more people around me that I will keep anonymous not to forget anyone, but they deserve my sincere acknowledgement. Firstly, they are people who have inspired me, who have risen my appetite for the challenges, who have motivated me out of my comfort area. I owe you my admiration and gratitude. Secondly, they are people that in this long period I relied on their complicity and comprehension both in the absences and in the discontinued opportunities for flushing my extra energy and doubts during a coffee, a wine, a beer, a dinner, a dance, a training session, a match, a ride, a race and so on.

I would like to show my greatest appreciation also to musicians in general and classic compositors in particular. They have been long hours of the best

music through the headphones enabling the isolation from the domestic battles. You will never be sufficiently paid.

Last but not least, I want to thank their continuous confidence to my family: etxekoak giñanak, ama Txaro, aitte Pedro Mari zana, Andikona eta Jon eta tartekoak; senide guztiak, Ramon eta Aintzane barne; eta etxekoak garanak. Specially my wife, Leire and children Paulo, Martina and Nikole. Without your immense backing, patience and relief, this thesis would not have materialized. Eskerrik asko bihotzez.

Contents

List of Figures

List of Tables

Listings

ACRONYMS

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
ABAC	Attribute-Based Access Control
ABE	Attribute Based Fine Grained Access Control
ACE	Authentication and Authorization for Constrained Environments
ACL	Access Control List
ACM	Access Control Matrix
ACCM	Accounting Manager
ACS	Access Control Server
AES	Advanced Encryption Standard
ANS	AutheNtication Server
APBR	Authorization Policy Binary Representation
API	Application Programming Interface
APPEL	A P3P Preference Exchange Language
AR	Access Rights
ARM	Advanced RISC Machine
ASL	Authorization Specification Language
AZS	AuthoriZation Server
A2C	Adaptive Access Control
BAN	Body Area Network
CA	Condition-Action paradigm
CA-BAC	Context Aware Based Access Control
CapBAC	Capability Based Access Control

CapBAC′	Capability Based Access Control adapted to IoT
CBOR	Concise Binary Object Representation
CDS	Constrained Device Sensor
CL-AtSe	Constraint Logic based Attack Searcher
CM	Credential Manager
CoAP	Constrained Application Protocol
COSE	CBOR Object Signing and Encryption protocol
CPS	Cyber-Physical System
CPU	Central Processing Unit
CWT	CBOR Web Token
DACM	Discretionary Access Control Model
DCapBAC	Distributed Capability Based Access Control
DFAC	Distributed Fine-Grained Access Control
DFG-AC	Distributed Fine-Grained Data Access Control for Distributed Sensor Networks
DoS	Denial of Service
DpACE	DTLS profile for authentication and authorization for constrained environments
DRM	Digital Right Management
DTLS	Datagram Transport Layer Security
EBNF	Extended Backus-Naur Form
ECA	Event-Condition-Action paradigm
ECC	Elliptic Curve Cryptography
ECDHE	ECC Diffie-Hellman Algorithm with Ephemeral Keys
ECDSA	Elliptic Curve Digital Signature
EC-BAC	Elliptic Curve Cryptography-Based Access Control
EEPROM	Electrically Erasable Programmable Read-Only Memory

ELAC	Easy and Lightweight Access Control
EPAL	Enterprise Privacy Authorization Language
E2E	End-to-End
FDAC	Fine-Grained Distributed Data Access Control
FIDO	Fast IDentity Online
GUI	Graphical User interface
HLPSL	High-Level Protocol Specification Language
HTTP	Hypertext Transfer Protocol
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
id	Identifier
IF	Intermediate Format
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol version 6
ITU-T	ITU Telecommunication Standardization Sector
JSON	JavaScript Object Notation
JSON′	Optimized JavaScript Object Notation
JWE	JSON Web Encryption
KDC	Key Distribution Center
LLN	Low-power and Lossy Network
LoWPAN	Low power Wireless Personal Area Networks
MAC	Message Authentication Code
MACM	Mandatory Access Control Model
MCU	Micro Controller Unit
MTU	Maximum Transmission Unit

OASIS	Organization for the Advancement of Structured Information Standards
OAuth	Open Authorization
OFMC	On-The-Fly-Model-Checker
OS	Operating System
OSCAR	Object-Based Security Architecture
OSI	Open System Interconnection
OSL	Obligation Specification Language
OWL	Web Ontology Language
OWL-Lite	Web Ontology Language Lite
PAN	Personal Area Network
PAP	Policy Administration Point
PCIM	Policy Core Information Model
PDM	Policy Domain Model
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
PKC	Public Key Cryptography
PSK	Pre-Shared Key
P3P	Platform for Privacy Preferences
RAM	Random Access Memory
RBAC	Role Based Access Control
RDF	Resource Description Framework
REL	Rights Expression Language
REST	Representational State Transfer
RFID	Radio Frequency Identification
RG	Research Goal

RISC	Reduced Instruction Set Computer
ROM	Read Only Memory
RPK	Raw Public Key
RPL	Routing Protocol for Low-power and Lossy Networks
RWX	Read Write Execute
SAML	Security Assertion Markup Language
SATMC	Boolean SATisfiability-based Model-Checker
SHA-256	Secure Hash Algorithm with 32-bit words
SKC	Symmetric Key Cryptography
SPAN	Security Protocol Animator for AVISPA
SRAM	Static Random Access Memory
STM32L	STMicroelectronics Ultra-low-power 32-bit MCUs
SWRL	Semantic Web Rule Language
TA4SP	Tree Automata based Automatic Approximations for the Analysis of Security Protocols
TCP	Transport Control Protocol
TGS	Ticket Granting Server
TGT	Ticket Granting Ticket
TLS	Transport Layer Security
UC	Use Case
UCON	Usage Based Access Control
UCON′	Usage Based Access Control adapted to IoT
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
USB	Universal Serial Bus
WSN	Wireless Sensor Networks
W3C	World Wide Web Consortium

XACML	eXtensible Access Control Markup Language
XACML′	eXtensible Access Control Markup Language adapted to IoT
XML	eXtensible Markup Language

Part I

INTRODUCTION

"Security is always excessive until it is not enough."

—- Robbie Sinclair

1 INTRODUCTION

This chapter firstly, conveys the context and the motivation of this thesis. In fact, forthcoming smart scenarios enabled by Internet of Things (IoT) envision objects that expose services that can adapt to user behavior or be managed with the goal of achieving higher productivity, often in multi-stakeholder applications. In such environments, smart things are cheap sensors (and actuators) and, therefore, Constrained Device Sensors (CDSs).

However, they are also critical components because of the importance of the provided information. Therefore, strong security in general and access control mechanisms in particular are required. However, existing feasible access control solutions do not cope well with the principle of least privilege, and they lack both expressiveness and manageability of the security policy to be enforced in the sensors and actuators. The main reason is that traditional access control models are not feasible in CDSs due to the severe resource constraints.

Once characterized the envisioned smart context and specified the unsolved security needs, this chapter conveys secondly the research goals of this thesis. Basically, they can be grouped in (1) the study of the access control requirements as well as the limitations to apply currently existing solutions; (2) the literature study to analyze the approach and the requirements coverage degree of the most relevant access control models; (3) the proposition of an innovative access control model; (4) the analysis of its suitability for the envisioned smart but constrained scenarios; and (5) the proper dissemination to the research community and the public in general.

In this introductory chapter, the research activities to reach the research goals are thirdly defined. Concretely, a deep state of the art analysis confirms the unsolved gap in terms of access control tightness and feasibility in the envisioned pervasive scenarios. Therefore, a new access control model is proposed, which conveys a hybrid architecture, a security policy language, a policy codification and a security protocol called Hidra for the establishment of an End-to-End (E2E) security association with a severely CDS.

The research activities follow with the validation of the proposed access control solution that conveys the security as well as the performance evaluation. Finally, the dissemination to the research community as well as the IoT solution providers and adopters in general, rounds up and enables invaluable feed back to the previous research activities.

Then, the thesis statement is summarized before the succinct description of the structure of the whole document.

1.1 CONTEXT: PROTECTION OF SENSORS ON CONSTRAINED DEVICES

This section conveys an overview of current security needs, concretely access control demands, on sensors implemented in CDSs that are accessible as things in an Internet Protocol version 6 (IPv6) network, i. e. integrated in IoT. Moreover, security concepts, features, approaches, and technologies are overviewed, analyzed, discussed and put into perspective to support the unsolved need and the appropriateness of the proposal in this thesis.

Actually, the IoT concept aims to connect anything with anyone, anytime, and anywhere, that is, global connectivity and global accessibility of things through the IPv6 Internet. It connects information technology things, e.g., sensors, actuators, Radio Frequency Identification (RFID) tags and readers, which might be embedded also in physical systems becoming Cyber-Physical Systems (CPSs), to enable interactions between the physical, data and virtual worlds.

Sensor networks integrated in IoT are envisioned to enhance the effectiveness and efficiency in several sectors, such as critical military surveillance applications, medicine, health-care, industry, energy, transport, traffic monitoring, emergency management and forest fire monitoring. Wireless Sensor Networks (WSN) technology has been intensively researched due to its high potential, and basically consists of a large number of distributed, autonomous, low-power, low-cost, small-sized devices, each with sensing, processing and communication capabilities.

Figure 1.1 shows an IoT schema that conveys different roles in various domains, therein operating, monitoring and controlling related business processes through pervasive computing applications. Traditionally, CDSs implement a producer behavior, publishing measurements and events to message brokers, as depicted with thick arrows. However, in more advanced IoT scenarios, CDSs behave as tiny information servers that can be addressed by their IPv6 address that is natively implemented as IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) [1].

Specifically, requesting clients, which are not expected to belong to the same domain, directly query the tiny CDS servers, establishing a secure E2E communication, as depicted with thin arrows. These services that are exposed through the IPv6 network, enable the usage, operation, maintenance and manageability of the CDSs over their entire life-cycle and protect the value stream of the connected objects. For example, an end user can utilize direct access to tune personal parameters, such as gender, age, and weight, in a constant health monitoring sensor.

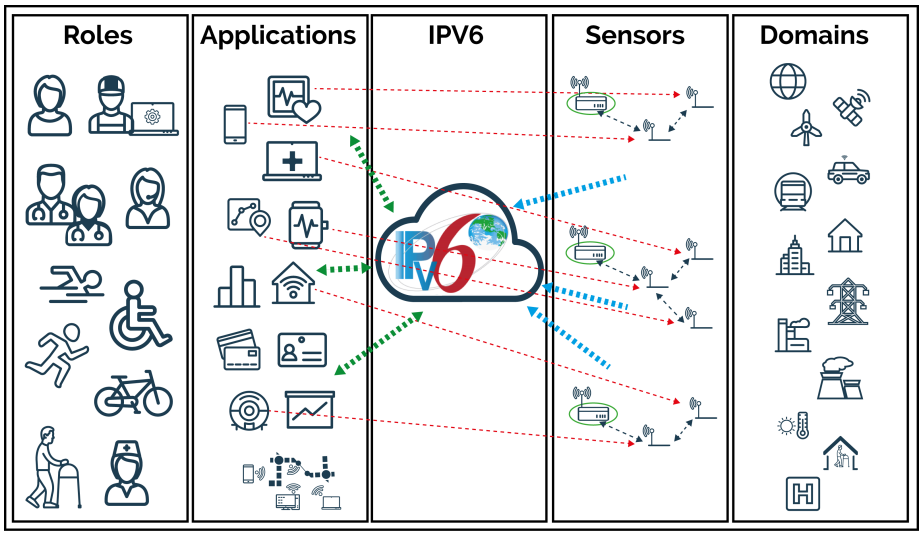

Figure 1.1: Scenario schema, where several stakeholders playing different roles access E2E IoT applications on different IoT domains through CDSs acting both as simple publishers (thick arrows) and as tiny E2E servers (thin arrows).

Hence the implementation of more ingenious and valuable applications need to tackle the insufficient security [2–4], which according to Gartner is dissuading potential investors from large scale deployments of IoT solutions [5].

Specifically, due to the global connectivity and the wireless nature of most communications at the edge, the things are significantly exposed to network threats. Concretely, CDSs are susceptible to many types of attacks through the network, which classified in passive or active attacks [6, 7], require proper security mechanisms.

In particular, research on security up to now has focused on network security involving key management, message authentication, intrusion detection, *etc* [8–10]. However, until recently low attention has been payed to fine-grained access control models [11].

Moreover, IoT integrating CDSs is a more demanding environment in terms of scalability and manageability as compared to traditional Internet services [12, 13]. In fact, substantial changes are identified in:

- Interaction patterns: short-lived, often casual and spontaneous interactions different to traditional systems.
- Context relevance: requests, data or authorization might depend on the local context.

Consequently, such new open scenarios require to tackle some security aspects not foreseen in the advent of the IoT [13, 14]. Besides the mobility and dynamic routing, service registering and discovering, sensors should deal with efficient, reliable, interoperable, scalable, flexible and manageable security mechanisms that should be designed and deployed to protect the right thing in the right way, where *one size fits all* is not a suitable strategy.

To that end, E2E traffic shall be secured by a properly authorized security association establishment between a subject and a CDS, which is an E2E connection that affords security services usually involving cryptographic mechanisms and a shared session key establishment. In these cases, the use of intermediary proxies is avoided because on the one hand, they are specific for each protocol or application and are not sufficiently flexible, whereas on the other hand, breaking the security association into two or more sub-transmissions might not be considered acceptable from a security point of view.

However, security in this terms is not a straightforward process since on one hand, the existence of billions of heterogeneous things challenges the identity and access control management. On the other hand, the global connectivity and the heterogeneity of the computational power and the communication protocols of the things, challenges the security protocols for the establishment of E2E secure communication channels to be lightweight and adaptive, and the cryptographic schemas and key management systems to be more efficient and optimal.

Given that, current thesis focuses on the access control and security protocol needed for the protection against the attacks aiming at illegitimate access to CDSs through the network.

Namely, application level access control in particular intercepts all access attempts to sensitive application resources and only allows those attempts that are explicitly authorized by the access control policy. Concretely, access control is the process of both mediating every request to resources and data maintained by a system that includes the security association establishment through a security protocol, and determining whether the request should be granted or denied [15].

In such complex space, shown in Figure 1.2, where IoT, WSNs and CPSs converge in the range of constrained devices, it is critical to consider also how the limitations on computational and energy power do impact on the operation and on the feasibility of any security mechanism in general, and access control model in particular.

Therefore, this section provides firstly, an overview of the IoT security in the envisioned scenarios, which presents some IoT related resource and network constraints; secondly, it describes how the currently standardized IoT protocol stack deals with security; thirdly it conveys the specific IoT

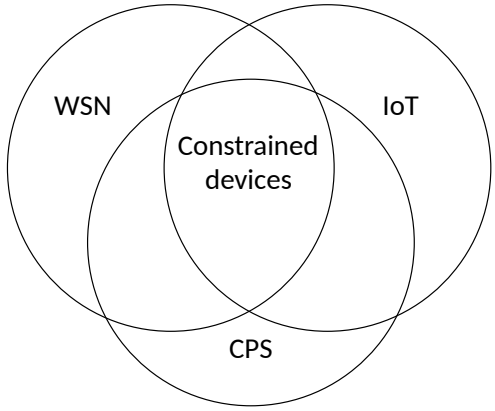

Figure 1.2: CDSs integrating sensing capabilities in IoT.

security challenges; and fourthly, it states the need of an innovative access control model and the focus of the current thesis.

1.1.1 *Constrained device classification*

Sensors and actuators integrated in CDSs can be implemented in constrained devices with strict resource restrictions such as limited computing capacity, little memory, insufficient network bandwidth, and often limited battery power. Depending on the dimension of such resources, diverse sizes of constrained devices can be distinguished, ranging from camera devices to the smallest networked sensor interacting with other *things* nearby.

Concretely, the range of constrained devices is defined by the Internet Engineering Task Force (IETF) [16]. Class 0 (C_0) is the lowest level, where devices have less than 10 kB and 100 kB of data and code memory respectively. From this lowest level, Class 1 (C_1) devices are about 10 kB of data and 100 kB of code, and class 2 (C_2) devices are up to 50 kB data and 250 kB code memory. These class N (C_N) devices are specifically implemented to fit to the requirements of different use-cases and applications. Besides, Moore's law [17] is foreseen to impact more on the price than on the resource capabilities [18, 19]. With respect to available power, mains-powered devices are notably distinguished from the ones powered by batteries or by using energy harvesting.

- C_0 devices generally cannot be managed or secured in the traditional sense. They can offer some specific tiny services through the network that require high optimization in order to be feasible, and the same happens with supported security functions. Samples of C_0 devices are networked sensors and actuators with specific purpose and powered

with batteries in massive deployments such as urban monitoring and light switching.

- C_1 devices are capable enough to use lightweight protocols such as Constrained Application Protocol (CoAP) over User Datagram Protocol (UDP). Therefore, they can act as fully developed peers into an Internet Protocol (IP) network supporting also some more general security functions. Samples of C_1 devices are networked sensors and actuators like fire/smoke detectors integrated in industrial control and large buildings, able to support some functions needed for its intended operation and management.

- C_2 devices are considered less constrained devices and they support most of the same protocol stacks as used in mobile devices such as smart phones. Samples of C_2 devices are networked sensors and actuators integrated in smart energy and building automation environments, able to support a range of services including some management ones.

- Devices with capabilities beyond C_2, nearer from non-constrained devices, are less demanding from a standards development point of view as they can largely use existing protocols unchanged, denoted in this document as traditional security protocols. Their principal constraint could be related to the location and the availability of mains-power or the use of batteries, tight to the energy consumption optimization.

In all cases, depending on the use-case and the operational scenario, all these devices still need to be assessed for the type of applications they will be running and the protocol functions they would need, and moreover from the manageability and security point of view.

Besides, the network where constrained devices work is usually also a constrained network. This implies low bandwidth, high packet loss, penalties for fragmentation due to large packets, limits on reachability over time and lack of advanced services such as IP multicast. Such networks conveying a variety of wireless links such as the low data rate Institute of Electrical and Electronics Engineers (IEEE) 802.15.4 [20] are also denoted by Low-power and Lossy Networks (LLNs) [21].

In any case, constrained devices C_0-C_2 share following limitations derived from resource scarcity:

- Complex authorization policies cannot be managed.

- Large number of secure connections cannot be managed.

- Deprived of user interface.

- Deprived of constant network connectivity.
- Time cannot be precisely measured.
- High power consumption of the wireless communications.
- Severely constrained storage space for security policies such as Access Control Lists (ACLs) in massive deployments.
- Required to save on cryptographic computations due to a high power consumption.

1.1.2 *IoT standardized protocol stack and enabled security*

Currently, security mechanisms and protocols are layered, in the sense that each OSI layer takes care of its own security needs. There are several standardization bodies such as the IEEE and the IETF contributing to the design of specific communication and security technologies for the interoperability of IoT distributed applications, since resource constraints in sensor nodes mean that standardized traditional security mechanisms with a large overhead of computation and communication are impractical to use in CDSs.

It is generally accepted a standardized protocol stack discussed in [22] and showed in Figure 1.3. Concretely, the protocols in the stack enable end-to-end Internet communications integrating constrained sensing devices operating in low-energy communication networks. However, these protocols have been designed considering the lightweight principles but the security principles have not been properly adopted.

At the physical and link layer IEEE 802.15.4 [23] specifies the mechanisms at the lowest OSI layers to enable the trade-off between energy-efficiency, range and data rate communications. This protocol sets a maximum of 102 bytes for the data field of higher layers.

This value is much lower than the Maximum Transmission Unit (MTU) of 1280 bytes required for IPv6, so 6LoWPAN [1, 20, 24] specifies the way to adapt the transmission of IPv6 packets over IEEE 802.15.4. Routing Protocol for Low-power and Lossy Networks (RPL) [25] enables the routing of IPv6 packets and the application-specific optimization of such routing.

At transport layer most of communications are state-less UDP, avoiding Transport Control Protocol (TCP)'s overhead, so there is no concept of a logical connection, acknowledgement of transmitted packets, retransmission of lost packets, nor flow control.

On top of UDP, at the application layer, the CoAP [26–28] enables request and response optimized communications using the key concepts of the web and restricting the Hypertext Transfer Protocol (HTTP) [29] to the minimum subset of features.

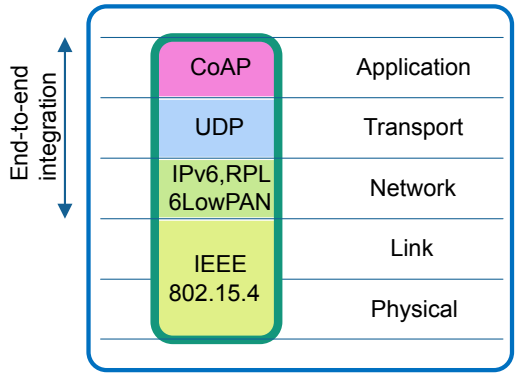

Figure 1.3: Communication protocols in the IoT.

In order to secure the E2E communications using such IoT protocol stack there are some mechanisms designed at each layer. Some of them are enabled directly by the protocol themselves and some other require the adoption of additional mechanisms. Hereinafter, a very brief look at layer per layer approach is explained [30].

In the lowest OSI layer, the IEEE 802.15.4-2011 standard specifies security services at the medium access control layer relying on the symmetric Advanced Encryption Standard (AES) supported by the hardware. Specifically, different security modes are supported by means of data encryption and message authentication codes. Moreover, ACL entries are supported for frame level access control enforcement.

However, specified link layer security mechanisms reduce significantly the data payload 102 bytes to down, the ACLs do not scale properly and there is no keying model specification nor message replay protection. Therefore, identified limitations might be overcome with the security mechanisms at other layers of the protocol stack, or with additional mechanisms proposed by the research community but not standardized yet [31, 32].

At the network layer, on one hand, although several vulnerabilities and requirements are identified, at the 6LoWPAN layer there is no specification for security mechanisms [33]. On the other hand, RPL defines three security modes, specifies secure versions of the routing control messages and supports key management. However, in the most secure mode, the authenticated mode, symmetric cryptography is discouraged by RPL specification and there is no clear specification of the asymmetric cryptography for the node authentication nor the key retrieval.

At the application layer CoAP provides a lightweight reliability mechanism and other than basic application data can be exchanged through *options*. These options model the behaviour of endpoints and are being researched by the community to extend the standard transport layer security

to enable some object security mechanisms as well. The resulting security approach [34] proposes three new options (1) to identify how security is applied, (2) to transport data for authentication and authorization of the CoAP client, and (3) to transport the security-related data to process cryptographically the CoAP message. This approach is rather granular but it also involves overheads and it is not standardized yet.

Given that, CoAP just specifies Datagram Transport Layer Security (DTLS) [35] to secure CoAP messages, so security is supported at the transport layer. In fact, DTLS specifies mechanisms to enable confidentiality, integrity, authentication, non-repudiation and protection against replay attacks for application layer using CoAP. DTLS, which in practice is an adapted Transport Layer Security (TLS) [36], requires a previous handshake between endpoints, since CoAP does not define any key management mechanisms.

Additionally, in DTLS, AES is adopted as the symmetric cryptographic algorithm, and Elliptic Curve Cryptography (ECC) is adopted to support authentication and key negotiation based on public key cryptography. Concretely, Elliptic Curve Digital Signature (ECDSA) enables endpoint authentication and ECC Diffie-Hellman Algorithm with Ephemeral Keys (ECDHE) to support key agreement between endpoints.

As a result, CoAP specifies four security modes depending on how authentication and key negotiation is performed through DTLS: (1) no security, (2) pre-shared symmetric keys, and Public Key Cryptography (PKC) based either on (3) raw public keys or (4) certificates. However, some drawbacks related with performance impact and scalability in constrained devices are circumvented through the development of tiny applications directly on top of UDP, since they are pending to be solved by the research community.

Concretely, the main issue is the impact of the handshake of the DTLS on the performance and the feasibility in CDSs, particularly the modes based on ECC PKC. Second is that DTLS handshake causes also fragmentation and the computational cost of the final *Finished* message is very high. ECC support is not broadly agreed in the research community and the support of X.509 certificates is pending of further research [30]. Additionally, E2E security is not always well suited if intermediary CoAP proxies are used. Finally, DTLS does not support group keying mechanisms to enable multicast communications.

The aforementioned security protocols and mechanisms contribute to security but they are not exempt from mentioned limitations. Security in sensor networks, therefore, remains as a challenger issue for broader adoption, and in particular access control, which is a critical security service that offers the appropriate access privileges to legitimate users and prevents illegitimate users from unauthorized access.

In order to overcome the scarcity of resources of CDSs and incompleteness of current standards, there is a proposal to evolve per layer security and

management to a cross-layer specification [37]. In fact, securing only the application layer does not protect CDSs from network attacks, while security mechanisms focused only at the network or link layer can not prevent possible inter-application security threats. For example, this approach stands for the standardization of the data format of the keying material to simplify cross-layer interactions. However, this approach has not been significantly seconded by the moment.

1.1.3 *Security challenges at IoT*

The mechanisms and protocols that enable the identity and access control, privacy, trust, governance and fault tolerance management, need also to tackle the specific challenges inherent to IoT: large scale, heterogeneity, complexity, exposure and resource constraints.

1. **Identity and authentication.** Besides the huge number of entities, since the interactions can be dynamic, the entities might not know each other in advance as in the case of vehicular networks circulating in sensored roads. Additionally, as in many scenarios instead of who, where and what are more relevant to be identified, so the entities might be identified by own or context attributes.

   Furthermore, the heterogeneity of the entities in IoT that can be computers, servers, application gateways, sensors, actuators, RFID tags, *etc.*, leads to the differentiation of three categories of identifiers: object identifiers, communication identifiers and application identifiers. Moreover, some entities might have multiple identities in different contexts and applications, or some users might rely their identity on devices named minimal entities that act and identify on behalf of the user [38].

   There are scenarios where things belong to a local spatial area, where local identity providers can manage the identities and even set trusted relationships with external entities for more agile inter-domain authentication processes. These relying identity providers enable to avoid the authentication logic in the CDSs, since the authentication can be based on proofs of identity when interacting with external entities. However, besides the absence of a unique central directory, different identity providers need to be dynamically integrated in a collaborative scenario. Moreover, traditional user-password authentication might not be suitable. Finally, in some scenarios a user might delegate credentials to some virtual entities under the concept of digital shadow [39].

2. **Access control.** Access control mechanisms that aim at being effective, scalable and lightweight, deal with security policies as well as the

permissions in all stages of their life cycle: assignation, provisioning, enforcement, maintenance and translations. Additionally, granularity on the permissions enabled by the expressiveness of the policy languages is crucial to adhere to the least privilege principle.

Moreover, location as well as some other context attributes become key conditions to be checked at enforcement time [40] in the accessed entity, in contrast to scenarios where access control logic might be externalized to trusted entities acting as token granting entities. Furthermore, some users might require to be able to delegate some permissions to other users or entities.

3. **Protocol and network security.** An E2E security association establishment to setup a secure communication channel requires a mutual authentication that requires credentials that might rely on shared keys or X.509 certificates. In scenarios where entities belong to a determined local area, Symmetric Key Cryptography (SKC) behaves optimally with preshared keys. However, when entities might connect with other unknown entities at any time, key distribution is a significant challenge [41].

   Furthermore, some challenges are derived from the limited computational resources of CDSs. Not all the security protocols nor cryptographic schemas are feasible in CDSs, and additionally, at the security association establishment time, some parameters need to be negotiated between E2E entities: the cryptographic algorithm, the strength of the key, and the security goals that can be integrity only or also confidentiality. Therefore, a tradeoff between compatibility and simplicity is required, where fast and compact cryptographic algorithms become crucial [42, 43].

4. **Privacy.** A data provider expects to be able to decide whether sharing or not a particular data set. In distributed IoT scenarios each entity should define the granularity of the generated and shared data, and enforce a proper access control policy on them. This entity-centric approach needs to be aligned with the user-centric approach that might interact with several CDSs around.

   In fact, each user might need proper and usable [44] interfaces to define the granularity and the access control policy on each CDS. This might be achieved relying on privacy-preserving distributed data mining algorithms [45], multiparty computation [46], or active isolated bundles containing data, metadata and application [47]. In any case, legal privacy regulations need to be mandatorily considered [48].

   There is another issue related with the potential entities that might track and profile users' activities without their consent. These misbe-

having environmental entities also might work collaboratively in the network, so user-centric approach might scan any active CDS prior to any operation to be aware at least of surrounding CDSs and eventually rely on the privacy coach concept [49].

5. **Trust and governance.** Trust between pair entities or user-entities is based on reputation calculus and sharing, but it is significantly challenged to enable user-managed circles of trust in scenarios where distributed autonomous networks are created and managed in the absence of a central systems [50]. Besides, other view is the trust on the system from the users' perspective, where surrounding network scan and inventorying mechanisms would support the awareness on their status and activity [51].

6. **Fault tolerance.** Things behaving as data providers might fault and stop working, so data consumers might rely on discovery services to pinpoint individual things or even network segments to guarantee the proper operation of the application service. Besides, some entities might send bogus data so receivers might rely on consistency checking mechanisms, reputation assessment, local clustering [52] and intrusion detection mechanisms. In fact, intrusion detection mechanisms might evolve from internal adversary detection to external malicious entity detection, which might also behave under a distributed attacker model [53].

Current thesis focuses mainly on the access control challenges in the establishment of a security association and further service access. I. e. access control and protocol security related challenges, but they are not easily decoupled from the rest, so it is interesting to be aware.

Finally, there are several strategies to deal with the challenges of the security mechanisms in the distributed IoT scenarios. One strategy is the setting of local groups such as personal area networks and the relying on trusted third parties such as identity providers most of the complexity in the identity and access control, privacy, trust, governance and fault tolerance management. Other strategies might focus on the secure interactions of human users with the surrounding IoT enabling concepts such as circles of trusts and user-centric access control.

1.1.4 *Limitations of current access control solutions for CDSs*

At the light of the aforementioned summarized overview, in the envisioned smart and open IoT scenarios, one of the essential security mechanisms for the security in general, and protection from unauthorized access or misuse in

particular, is the identity and access control management that is the subject of study in this thesis.

In these envisioned scenarios, the accuracy and correctness of the information exchanged with CDSs are crucial. Protecting this information requires the implementation of appropriate security mechanisms that include fine-grained access control mechanisms based on expressive policies and that can guarantee essential security properties such as confidentiality, integrity, availability, authenticity and non-repudiation [2, 3, 54].

However, implementing these appropriate security mechanisms in resource-constrained CDSs is not straightforward. Currently, one of the key challenges for enabling the broader adoption of smart things is the availability of feasible access control solutions.

Specifically, the proper setting of access controls should help prevent the disclosure of sensitive or restricted information that is not intended for public dissemination. In addition, access controls could be used to limit resource use in the event of a DoS attack against the CDS. Similarly, access controls could enforce separation of duty by ensuring server logs cannot be modified by CDS administrators and potentially ensure that the CDS process is only allowed to append to the log files.

In the context of the constrained devices required in large scale deployments, the access control must not only focus on the required security services, but also on how these services are realized in the overall system and how the security functionalities are executed overcoming such resource constraints.

How current access control models protect the confidentiality and the integrity of the data exchanged with constrained devices, as well as the authentication and authorization enforcement of any endpoint accessing data in the constrained device need to be deeply analyzed in Chapter 2.

Nevertheless, it can be anticipated that traditional access control models are not feasible in CDSs and currently feasible access control models tailored for IoT do not cope properly with the basic tightness and usability requirements [2–4, 11].

Current access control models need to be made much more flexible to make access decisions on the unexpected events, because it is hard to predefine all of the possibilities in an open scenario. A new access control model is needed to address higher reliability, scalability, availability and accountability to prevent unauthorized user access and allow authorized users data access in unexpected and unpredictable cases.

Therefore, there is a need for a new feasible access control model that supports enhanced fine-grained, dynamic and tight security policy enforcement in severely CDSs. After all, currently implemented static and coarsely grained policies to be enforced locally in the CDS are not well-suited for

service-oriented environments where information and management access is by nature dynamic and ad-hoc.

Consequently, there is a need for a new enlightened policy language that enables high expressiveness and consequently, enables the tightness of the enforcement and adherence to the least privilege principle. In fact, the latter is considered as the main contributor to the effectiveness, whereas the former sets the constraints to be faced from the efficiency point of view.

Accordingly, there is a need for a new security protocol that enables the establishment of an E2E security association, while supporting security provisioning and local context based enforcement in the CDSs. Last but not least, such security protocol should enable tracking and audit features.

1.2 RESEARCH GOALS

In order to tackle the unsolved security needs and challenges of the envisioned smart scenarios, this thesis sets the following Research Goals (RGs):

RG1. The study of the envisioned smart and pervasive scenarios and the related security needs and open issues.

RG2. A state of the art analysis of the existing access control models.

- The study of the access control foundations, the challenges to adapt them to the resource constrained scenarios and the specificity of the access control requirements in such scenarios.
- The study of retrospective access control models as well as security policy languages and their applicability to the envisioned scenarios once analyzed the constraints.
- The study of the IoT tailored access control approaches and how they cope with aimed security requirements.

RG3. The proposition of the specification of an innovative access control model, which conveys a hybrid architecture, a security policy language, a policy codification and a security protocol for the establishment of an E2E security association with a severely constrained device.

RG4. The analysis of the suitability of the access control model proposed in this thesis. This validation should be performed from both the security and performance points of view.

RG5. The dissemination of the significant findings and learned lessons to the research community as well as the IoT solution providers and adopters in general, to contrast approaches and get invaluable feed back to the previous research activities.

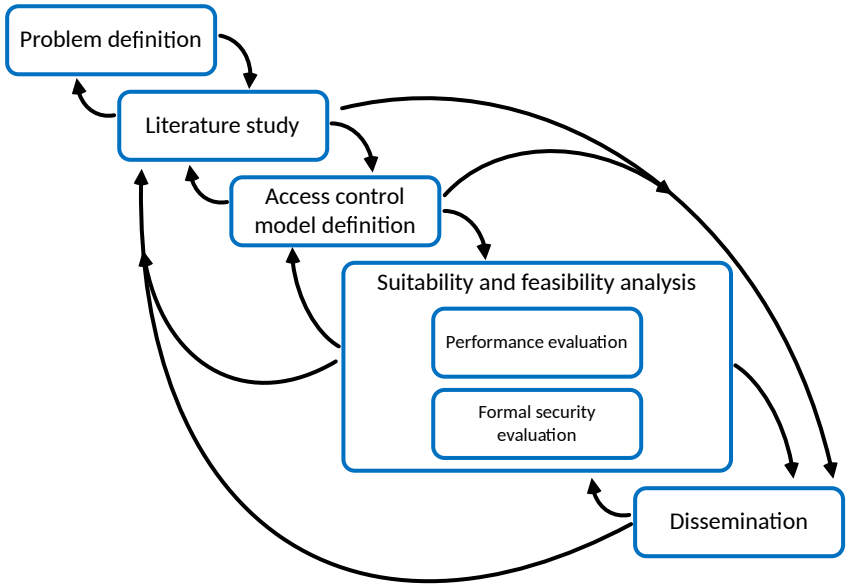

Figure 1.4: Cycle of research activities

1.3 RESEARCH ACTIVITIES

Aiming at the research goals achievement this thesis has defined the following research activities, showed in Figure 1.4.

The first main activity is the problem definition, which is conveyed in current introductory section. This activity is preceded and fed by the literature study, which also points out the unsolved gaps once the state of the art is analyzed.

Then, the innovation comes through the proposition of a cutting edge access control model that fulfils the security requirements and tackles with the challenges described during aforementioned activities.

This designing activity that conveys a hybrid architecture, a security policy language, a policy instance codification method and a security protocol for the establishment of an E2E security association, is fully dependant on the feasibility and suitability of the solution, which are analyzed and assessed during specific validation activities.

Finally, dissemination to the research community as well as the IoT solution providers and adopters in general, is conducted to both clarify main achievements and support further research activities.

All these activities result in remarkable feedback and advisory lessons that are applied backwards as shown in Figure 1.4, to make outcomes sounder and more profitable.

1.4 THESIS STATEMENT AND CONTRIBUTIONS

This thesis conveys:

> A new access control model that utilizes a hybrid architecture and a security policy language and codification that provides dynamic fine-grained policy enforcement in the sensors, which requires an efficient message exchange control called Hidra for the establishment of an E2E security association with a smart but severely constrained device.

To this end, current thesis has made the following contributions:

- A survey of the access control foundations and features.
- A state of the art analysis of the existing IoT tailored access control models.
- A cutting edge access control model for severely constrained C_0 and C_1 CDSs that conveys:
  - A new expressive access control policy language and a very efficient codification.
  - A new security protocol called Hidra for the establishment of an authorized E2E security association in a hybrid architecture, as well as for the dynamic provisioning of the appropriate policy and the accounting.
- A security validation modeled and performed with the assistance of a formal validation software tool.
- An analytical and experimental performance evaluation that in the absence of previous references might be valuable for further benchmarking.

1.5 THESIS ORGANIZATION

The contents of this thesis are structured as follows: firstly, a critical analysis of existing approaches related to the research goals of this thesis is conveyed in Chapter 2. Then, the proposed cutting edge access control model is specified in Chapter 3, which conveys a hybrid architecture, a security policy language and codification, and a security protocol called Hidra for the establishment of an E2E security association with severely constrained C_0

and C_1 CDSs. The feasibility and suitability of such access control model is assessed in Chapter 4, which consist of the security evaluation and both analytical and experimental performance evaluation of the proposed security protocol. Finally, Chapter 5 presents the conclusions on the obtained results, including the dissemination activities and pointing out the future work in this area.

Part II

STATE OF THE ART

"IoT without security = Internet of Threats."

— Stephane Nappo

Part VI

APPENDIX

APPENDIX A

A.1 HLPSL SPECIFICATION OF HIDRA

Listing A.1: Hidra HLPSL specification

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%
%% PROTOCOL*: Hidra
%% VARIANT: with ticket caching
%% PURPOSE: Strong mutual authentication
%%
%%      A := Authentication Server (ACS)
%%      C := Credential Manager (ACS)
%%      S := Subject (S)
%%      R := Resource (R)
%%      L := Log Manager (L)
%%
%% Phase 1 - Delegated authentication: obtaining a Ticket Granting Ticket (TGT):
%%
%%  S -> A: S,C,Lifetime1,N1
%%  A -> S: S,Tsc,{C,Ksc,Nsc,N1}_Ksa
%%
%%  where Tsc := {S,Ksc,Nsc}_Kca
%%
%% Phase 2 - Preliminary authorization: obtaining a Service Granting Ticket:
%%
%%  S -> C: R,Lifetime2,N2,Tsc,Asc
%%  C -> R: {S,R,Lifetime2,Nsr,{P}_Krc,Hn(Nrc)}_Krc
%%  R -> C: {S,R,Hn(Nrc)}_Krc
%%  C -> S: S,Tsr,{R,Ksr,Nsr,N2}_Ksc
%%
%%  where Hn:= is the n-th hash of the value in brackets
%%       Tsc := {S,Ksc,Nsc}_Kca
%%       Asc := {S,Hn(Nsc)}_Ksc
%%       Tsr := {S,Ksr,Nsr,Attrs,Attrc}_Krc
%%
%% Phase 3 - Locally authorized security association
%%
%%  S -> R: Tsr,Asr,N3
%%  R -> S: {Nsr,Subkey,N3}_Ksr
%%
%%  where Tsr := {S,Ksr,Nsr,Attrs,Attrc}_Krc
%%       Asr := {S,Nsr,Subkey}_Ksr
%%
%% Phase 4 - Access notification
%%
%%  R -> LM: R,{N5,IDpol,Lsr}_Krc
%%  LM -> R: R,N5,
%%
%%  where Lsr := {S,IDrr,IDra,IDge,IDri,IDob,Hn(N6)}_Krc
%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%
%% PROBLEMS: 8
%% CLASSIFICATION: G1, G2, G3, G6, G7, G8, G10, G12
%% ATTACKS: None
%% NOTES:
%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%
%%HLPSL:
%%

  role authenticationServer(
             A,S,C      : agent,
             Ksa,Kca    : symmetric_key,
             SND,RCV    : channel(dy))
```

```
  played_by A
  def=

    local State         : nat,
          N1            : text,
          Ksc           : symmetric_key,
          Lifetime1     : text,
          Nsc           : text

    const       sec_a_Ksc, sec_a_Nsc    : protocol_id,
                aksc    : protocol_id

    init  State := 0

    transition
      1. State  = 0     /\ RCV(S.C.Lifetime1'.N1') =|>
         State':= 1     /\ Ksc' := new()
                        /\ Nsc' := new()
                        /\ SND(S.{S.Ksc'.Nsc'}_Kca.{C.Ksc'.Nsc'.N1'}_Ksa)
                        /\ witness(A,S,aksc,Ksc'.N1')
                        /\ secret(Ksc',sec_a_Ksc,{A,S,C})
                        /\ secret(Nsc',sec_a_Nsc,{A,S,C})
  end role

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

  role credentialManager (
              C,R,S,A       : agent,
              Kca,Krc       : symmetric_key,
              SND,RCV       : channel(dy),
              Hash          : hash_func,
              F             : hash_func,
              MAC           : hash_func )
  played_by C
  def=

    local State         : nat,
          N2, N3        : text,
          Ksc, Ksr      : symmetric_key,
          Nsc, Nsr      : text,
          Lifetime2     : text,
          Rid           : text,
          L             : text set,
          H1, H2        : message,
          K3            : text,
          K0, K1, K2    : message,
          P             : text,
          Attrs         : text,
          Attrc         : text,
          Start         : bool

    const       sec_c_Ksc, sec_c_Ksr, sec_c_Nsc, sec_c_Nsr, sec_c_Nrc   : protocol_id,
                cksr, ckrc, ckrc1                                       : protocol_id,
                true, false                                             : bool

    init  State := 0 /\ L := {} /\ Start := true

    transition
      1. State  = 0     /\ RCV(R.Lifetime2'.N2'.{S.Ksc'.Nsc'}_Kca.{S.H1'}_Ksc')
                        /\ not(in(Nsc',L))
                        /\ H1'=Hash(Nsc')
                        /\ Start=true =|>
         State':= 1     /\ Start':=false
                        /\ L':=cons(Nsc',L)
                        /\ Nsr':= new()
                        /\ H2' := Hash(H1')
                        /\ K3' := new() /\ K2':= F(K3') /\ K1':= F(F(K3')) /\ K0':= F(F(F(K3')))
                        /\ SND(S.R.Nsr'.Lifetime2'.F(F(F(K3')).{P}_Krc).{MAC(S.Nsr'.Lifetime2'.F(F(F(K3')))).{P
                             }_Krc)}_Krc)
                        /\ witness(C,R,ckrc,Krc.F(F(F(K3'))))
                        /\ request(C,S,sksc,Ksc'.Nsc'.N2'.H1')
                        /\ secret(Ksc',sec_c_Ksc,{A,S,C})
                        /\ secret(Nsc',sec_c_Nsc,{A,S,C})

        2. State  = 1   /\ RCV (R.N3'.{MAC(R.N3')}_Krc) =|>
           State':= 2   /\ Ksr' := new()
                        /\ Rid' := new()
                        /\ SND(R.K1.{MAC(R.N3'.K1)}_Krc)
                        /\ SND(S.{S.Ksr'.Nsr.Attrs.Attrc}_Krc.{R.Ksr'.Nsr.N2}_Ksc)
                        /\ witness(C,R,ckrc1,Krc.K1)
                        /\ witness(C,S,cksr,Ksr'.N2)
                        /\ request(C,R,rkrc,Krc)
                        /\ secret(Ksc,sec_c_Ksc,{A,S,C})
                        /\ secret(Ksr',sec_c_Ksr,{C,S,R})
     end role
```

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

 role logManager (
             LM,R        : agent,
             Krc         : symmetric_key,
             SND,RCV     : channel(dy))
 played_by LM
 def=

   local State          : nat,
         IDpol          : text,
         Lsr : {agent.text.text.text.text.text.text}_symmetric_key,
         N5             : text,
         Start          : bool

   const       sec_lm_Krc        : protocol_id

   init   State := 0


   transition
       1.State   = 0     /\ RCV(R.{N5'.IDpol'.Lsr'}_Krc)=|>
         State':= 1      /\ SND(R.N5)

    end role

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

 role resource( R,S,C     : agent,
             Krc        : symmetric_key,
             SND, RCV : channel(dy),
             Hash           : hash_func,
             F          : hash_func,
             MAC        : hash_func)
 played_by R
 def=

   local       State                  : nat,
               Ksr, Subkey            : symmetric_key,
               Nsr, Nrc               : text,
               Lifetime2              : text,
               Rid                    : text,
               N3,N4                  : text,
               L                      : text set,
               H2, H3                 : message,
               K0, K1, K2             : message,
               K3                     : text,
               P                      : text,
               Attrs                  : text,
               Attrc                  : text,
               N5                     : text,
               IDpol                  : text,
               IDrr                   : text,
               IDra                   : text,
               IDge                   : text,
               IDri                   : text,
               IDob                   : text,
               N6                     : text

   const       sec_r_Nsr, sec_r_Ksr, sec_r_Nrc : protocol_id,
               rksr, rkrc                      : protocol_id

   init    State := 0 /\ L := {}

   transition
     1. State = 0    /\ RCV(S.R.Nsr'.Lifetime2'.F(F(F(K3'))).{P}_Krc).{MAC(S.Nsr'.Lifetime2'.F(F(F(K3')))).{P}_
          Krc)}_Krc)=|>
        State':= 1   /\ K0' := F(F(F(K3')))
                     /\ N3' := new()
                     /\ L' := cons(Nsr',L)
                     /\ SND(R.N3'.{MAC(R.N3')}_Krc)
                     /\ witness(R,C,rkrc,Krc)
                     /\ request(R,C,ckrc,Krc.F(F(F(K3'))))

       2. State   = 1    /\ RCV(R.K1'.{MAC(R.N3'.K1')}_Krc)
                         /\ K0=F(K1') =|>
          State':= 2     /\ request(R,C,ckrc1,Krc.K1')

       3. State = 2 /\ RCV({S.Ksr'.Nsr.Attrs.Attrc}_Krc.{S.Nsr.Subkey'}_Ksr'.N4')
                    /\ in(Nsr,L)=|>
          State':= 3   /\ SND({Nsr.Subkey'.N4'}_Ksr')
                     /\ L' := delete(Nsr,L)
                     /\ N5' := new()
                     /\ IDpol' := new()
```

```
                    /\ IDrr' := new()
                    /\ IDra' := new()
                    /\ IDge' := new()
                    /\ IDri' := new()
                    /\ IDob' := new()
                    /\ N6' := new()
                    /\ SND(R.{N5'.IDpol'.{S.IDrr'.IDra'.IDge'.IDri'.IDob'.Hash(N6')}_Krc}_Krc)
                    /\ witness(R,S,rksr,Ksr'.N4')
                    /\ request(R,S,sksr,Ksr'.Nsr)
                    /\ secret(Ksr',sec_r_Ksr,{C,S,R})

      4. State = 3 /\ RCV(R.N5)=|>
         State':= 4

  end role

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

  role subject ( S,C,R,A        : agent,
                 Ksa            : symmetric_key,
                 SND,RCV        : channel(dy),
                 Hash           : hash_func)
  played_by S
  def=

    local       State                   : nat,
                Ksr, Ksc, Subkey        : symmetric_key,
                Nsr, Nsc                : text,
                Lifetime1, Lifetime2    : text,
                Tsc: {agent.symmetric_key.text}_symmetric_key,
                Tsr: {agent.symmetric_key.text.text.text}_symmetric_key,
                N1, N2, N4              : text,
                L                       : text set,
                H1              : message

    const       sec_s_Ksc, sec_s_Ksr, sec_s_Nsc, sec_s_Nsr  : protocol_id,
                sksc, sksr                                  : protocol_id

    init   State := 0 /\ L := {}

    transition
      1. State  = 0     /\ RCV(start)  =|>
         State':= 1     /\ N1' := new()
                        /\ Lifetime1' := new()

      2. State  = 1     /\ RCV(S.Tsc'.{C.Ksc'.Nsc'.N1}_Ksa)
                        /\ not(in(Nsc',L))=|>
         State':= 2     /\ L':=cons(Nsc',L)
                        /\ H1' := Hash(Nsc')
                        /\ N2' := new()
                        /\ Lifetime2' := new()
                        /\ SND(R.Lifetime2'.N2'.Tsc'.{S.H1'}_Ksc')
                        /\ witness(S,C,sksc,Ksc'.Nsc'.N2'.H1')
                        /\ request(S,A,aksc,Ksc'.N1)
                        /\ secret(Ksc',sec_s_Ksc,{A,S,C})
                        /\ secret(Nsc',sec_s_Nsc,{A,S,C})

        2. State  = 1   /\ RCV(S.Tsc'.{C.Ksc'.Nsc'.N1}_Ksa)
                        /\ in(Nsc',L)=|>
         State':= 2     /\ L':=cons(Nsc',L)
                        /\ H1' := Hash(H1')
                        /\ N2' := new()
                        /\ Lifetime2' := new()
                        /\ SND(R.Lifetime2'.N2'.Tsc'.{S.H1'}_Ksc')
                        /\ witness(S,C,sksc,Ksc'.Nsc'.N2'.H1')
                        /\ request(S,A,aksc,Ksc'.N1)
                        /\ secret(Ksc',sec_s_Ksc,{A,S,C})
                        /\ secret(Nsc',sec_s_Nsc,{A,S,C})

      3. State  = 2     /\ RCV(S.Tsr'.{R.Ksr'.Nsr'.N2}_Ksc) =|>
         State':= 3     /\ Subkey' := new()
                        /\ N4' := new()
                        /\ SND(Tsr'.{S.Nsr'.Subkey'}_Ksr'.N4')
                        /\ witness(S,R,sksr,Ksr'.Nsr')
                        /\ request(S,C,cksr,Ksr'.N2)
                        /\ secret(Ksr',sec_s_Ksr,{C,S,R})

      4. State  = 3     /\ RCV({Nsr.Subkey.N4}_Ksr) =|>
         State':= 4     /\ request(S,R,rksr,Ksr.N4)

  end role

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

role session(
```

```
        A,C,S,R                : agent,
        Ksa,Krc,Kca            : symmetric_key,
        Hash                   : hash_func,
        F                      : hash_func,
        MAC                    : hash_func)
def=

  local
        SendS,ReceiveS           : channel (dy),
        SendR,ReceiveR           : channel (dy),
        SendC,ReceiveC           : channel (dy),
        SendA,ReceiveA           : channel (dy)

  composition
        subject(S,C,R,A,Ksa,SendS,ReceiveS,Hash)
    /\  resource(R,S,C,Krc,SendR,ReceiveR,Hash,F,MAC)
   /\ credentialManager(C,R,S,A,Kca,Krc,SendC,ReceiveC,Hash,F,MAC)
    /\  authenticationServer(A,S,C,Ksa,Kca,SendA,ReceiveA)

end role

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

role environment()
def=

  const
      a,c,s,r                          : agent,
      k_sa,k_rc,k_ca,k_ia,k_ic          : symmetric_key,
      h                                : hash_func,
      f                                : hash_func,
      mac                              : hash_func

  intruder_knowledge = {a,c,s,r,h,f,mac,k_ia}

  composition

        session(a,c,s,r,k_sa,k_rc,k_ca,h,f,mac)
        /\ session(a,c,i,r,k_ia,k_rc,k_ca,h,f,mac)

end role

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

goal

  %secrecy_of Ksc,Ksr, Nsc, Nrc and Nsr
  secrecy_of sec_a_Ksc, sec_c_Ksc, sec_s_Ksc, % address G10, G12
             sec_c_Ksr, sec_r_Ksr, sec_s_Ksr, % address G10, G12
             sec_a_Nsc, sec_c_Nsc, sec_s_Nsc, % address G12
             sec_r_Nrc, sec_c_Nrc % address G12

  %Subject authenticates AuthenticationServer on aksc
  authentication_on aksc % addresses G1, G3, G7 and G8
  %Subject authenticates ResourceManager on cksr
  authentication_on cksr % addresses G1, G3, G7 and G8
  %Subject authenticates Resource on rksr
  authentication_on rksr % addresses G1, G2, G3, G7 and G8
  %Resource authenticates Subject on sksr
  authentication_on sksr % addresses G1, G2, G3, G6, G7 and G8
  %ResourceManager authenticates Subject on sksc
  authentication_on sksc % addresses G1, G2, G3, G6, G7 and G8
  %ResourceManager authenticates Resource on rkrc
  authentication_on rkrc % addresses G1, G2, G3, G6, G7 and G8
  %Resource authenticates ResourceManager on ckrc
  authentication_on ckrc % addresses G1, G2, G3, G7 and G8
  %Resource authenticates ResourceManager on ckrc1
  authentication_on ckrc1 % addresses G1, G2, G3, G7 and G8

end goal

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

environment()
```

BIBLIOGRAPHY

[1] E. Kim, D. Kaspar, C. Gomez, and C. Bormann. *Problem Statement and Requirements for IPv6 over LowPower Wireless Personal Area Network (6LoWPAN) Routing*. RFC 6606. RFC Editor, May 2012. URL: https://www.rfc-editor.org/rfc/rfc6606.txt.

[2] Rodrigo Roman, Jianying Zhou, and Javier Lopez. «On the features and challenges of security and privacy in distributed internet of things.» In: *Computer Networks* 57.10 (2013). Towards a Science of Cyber SecuritySecurity and Identity Architecture for the Future Internet, pp. 2266 –2279. ISSN: 1389–1286. DOI: http://dx.doi.org/10.1016/j.comnet.2012.12.018.

[3] S. Sicari, A. Rizzardi, L.A. Grieco, and A. CoenPorisini. «Security, privacy and trust in Internet of Things: The road ahead.» In: *Computer Networks* 76 (2015), pp. 146 –164. ISSN: 1389–1286. DOI: http://dx.doi.org/10.1016/j.comnet.2014.11.008.

[4] Zheng Yan, Peng Zhang, and Athanasios V. Vasilakos. «A survey on trust management for Internet of Things.» In: *Journal of Network and Computer Applications* 42 (2014), pp. 120 –134. ISSN: 1084–8045. DOI: http://dx.doi.org/10.1016/j.jnca.2014.01.014.

[5] Janessa Rivera. *Survey Analysis: The Internet of Things Is a Revolution Waiting to Happen.* Feb. 2015. URL: http://www.gartner.com/newsroom/id/2977018.

[6] A. Rani and S. Kumar. «A survey of security in wireless sensor networks.» In: *2017 3rd International Conference on Computational Intelligence Communication Technology (CICT)*. Feb. 2017, pp. 1–5. DOI: 10.1109/CIACT.2017.7977334.

[7] Furrakh Shahzad, Maruf Pasha, and Arslan Ahmad. «A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures.» In: (Feb. 2017).

[8] Aditi Rani and Sanjeet Kumar. «A survey of security in wireless sensor networks.» In: *Computational Intelligence & Communication Technology (CICT), 2017 3rd International Conference on*. IEEE. 2017, pp. 1–5.

[9] Haowen Chan, Adrian Perrig, and Dawn Song. «Random key predistribution schemes for sensor networks.» In: *Security and Privacy, 2003. Proceedings. 2003 Symposium on*. IEEE. 2003, pp. 197–213.

[10] Sencun Zhu, Shouhuai Xu, S. Setia, and S. Jajodia. «LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks.» In: *Distributed Computing Systems Workshops, 2003. Proceedings. 23rd International Conference on*. May 2003, pp. 749–755. DOI: 10.1109/ICDCSW.2003.1203642.

[11] Haodong Wang and Qun Li. «Distributed user access control in sensor networks.» In: *Distributed Computing in Sensor Systems*. Springer, 2006, pp. 305–320.

[12] Ovidiu Vermesan, Peter Friess, Patrick Guillemin, Sergio Gusmeroli, Harald Sundmaeker, Alessandro Bassi, Ignacio Soler Jubert, Margaretha Mazura, Mark Harrison, Markus Eisenhauer, et al. «Internet of things strategic research roadmap.» In: *Internet of Things-Global Technological and Societal Trends* 1.2011 (2011), pp. 9–52.

[13] Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal, and Zied Chtourou. «A roadmap for security challenges in the Internet of Things.» In: *Digital Communications and Networks* (2017).

[14] Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad. «Proposed security model and threat taxonomy for the Internet of Things (IoT).» In: *International Conference on Network Security and Applications*. Springer. 2010, pp. 420–429.

[15] Pierangela Samarati and Sabrina Capitani de Vimercati. «Access Control: Policies, Models, and Mechanisms.» In: *Foundations of Security Analysis and Design: Tutorial Lectures*. Ed. by Riccardo Focardi and Roberto Gorrieri. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 137–196. ISBN: 978-3-540-45608-7. DOI: 10.1007/3-540-45608-2_3. URL: https://doi.org/10.1007/3-540-45608-2_3.

[16] C. Bormann, M. Ersue, and A. Keranen. *Terminology for Constrained-Node Networks*. RFC 7228. http://www.rfc-editor.org/rfc/rfc7228.txt. RFC Editor, May 2014.

[17] Robert R. Schaller. «Moore's Law: Past, Present, and Future.» In: *IEEE Spectr.* 34.6 (June 1997), pp. 52–59. ISSN: 0018–9235. DOI: 10.1109/6.591665. URL: http://dx.doi.org/10.1109/6.591665.

[18] Paolo Gargini. *ITRS Past, present and future*. URL: https://spcc2016.com/wp-content/uploads/2016/04/02-01-Gargini-ITRS-2.0-2.pdf.

[19] M. Mitchell Waldrop. *The chips are down for Moore's law*. http://www.nature.com/news/the-chips-are-down-for-moore-s-law-1.19338.

[20] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. *Transmission of IPv6 Packets over IEEE 802.15.4 Networks*. Tech. rep. RFC 4944. Internet Engineering Task Force, Sept. 2007.

[21] JP. Vasseur. *Terms Used in Routing for Low-Power and Lossy Networks*. RFC 7102. RFC Editor, Jan. 2014. URL: http://www.rfc-editor.org/rfc/rfc7102.txt.

[22] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler. «Standardized Protocol Stack for the Internet of (Important) Things.» In: *IEEE Communications Surveys Tutorials* 15.3 (Mar. 2013), pp. 1389–1406. ISSN: 1553–877X. DOI: 10.1109/SURV.2012.111412.00158.

[23] «IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).» In: *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)* (Sept. 2011), pp. 1–314. DOI: 10.1109/IEEESTD.2011.6012487.

[24] N. Kushalnagar, G. Montenegro, and C. Schumacher. *IPv6 over LowPower Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*. RFC 4919. RFC Editor, Aug. 2007. URL: http://www.rfc-editor.org/rfc/rfc4919.txt.

[25] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, JP. Vasseur, and R. Alexander. *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks*. RFC 6550. RFC Editor, Mar. 2012. URL: http://www.rfc-editor.org/rfc/rfc6550.txt.

[26] Z. Shelby, K. Hartke, and C. Bormann. *The Constrained Application Protocol (CoAP)*. RFC 7252. http://www.rfc-editor.org/rfc/rfc7252.txt. RFC Editor, June 2014.

[27] Matthias Kovatsch. «CoAP for the Web of Things: From Tiny Resource-constrained Devices to the Web Browser.» In: *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication*. UbiComp '13 Adjunct. Zurich, Switzerland: ACM, 2013, pp. 1495–1504. ISBN: 978-1-4503-2215-7. DOI: 10.1145/2494091.2497583. URL: http://doi.acm.org/10.1145/2494091.2497583.

[28] C. Bormann, A. P. Castellani, and Z. Shelby. «CoAP: An Application Protocol for Billions of Tiny Internet Nodes.» In: *IEEE Internet Computing* 16.2 (Mar. 2012), pp. 62–67. ISSN: 1089–7801. DOI: 10.1109/MIC.2012.29.

[29] R. Fielding and J. Reschke. *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*. RFC 7230. RFC Editor, June 2014. URL: http://www.rfc-editor.org/rfc/rfc7230.txt.

[30] J. Granjal, E. Monteiro, and J. Sá Silva. «Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues.» In: *IEEE Communications Surveys Tutorials* 17.3 (July 2015), pp. 1294–1312. ISSN: 1553–877X. DOI: 10.1109/COMST.2015.2388550.

[31] Yang Xiao, Hsiao-Hwa Chen, Bo Sun, Ruhai Wang, and Sakshi Sethi. «MAC security and security overhead analysis in the IEEE 802.15. 4 wireless sensor networks.» In: *EURASIP Journal on Wireless Communications and Networking* 2006.2 (2006), pp. 81–81.

[32] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva. «Security for the internet of things: a survey of existing protocols and open research issues.» In: *IEEE Communications Surveys & Tutorials* 17.3 (2015), pp. 1294–1312.

[33] Anass Rghioui, Mohammed Bouhorma, and Abderrahim Benslimane. «Analytical study of security aspects in 6LoWPAN networks.» In: *Information and Communication Technology for the Muslim World (ICT4M), 2013 5th International Conference on*. IEEE. 2013, pp. 1–5.

[34] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva. «Application-layer security for the WoT: extending CoAP to support endtoend message security for internet-integrated sensing applications.» In: *International Conference on Wired/Wireless Internet Communication*. Springer. 2013, pp. 140–153.

[35] E. Rescorla and N. Modadugu. *Datagram Transport Layer Security Version 1.2*. RFC 6347. RFC Editor, Jan. 2012. URL: http://www.rfc-editor.org/rfc/rfc6347.txt.

[36] T. Dierks and E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.1*. RFC 4346. http://www.rfc-editor.org/rfc/rfc4346.txt. RFC Editor, Apr. 2006. URL: http://www.rfc-editor.org/rfc/rfc4346.txt.

[37] Htoo Aung Maw, Hannan Xiao, Bruce Christianson, and James A Malcolm. «A survey of access control models in wireless sensor networks.» In: *Journal of Sensor and Actuator Networks* 3.2 (2014), pp. 150–180.

[38] Stefan G Weber, Leonardo A Martucci, Sebastian Ries, and Max Mühlhäuser. «Towards trustworthy identity and access management for the future internet.» In: *Proc. 4th International Workshop on Trustworthy Internet of People, Things & Services (IoPTS)*. Vol. 29. 2010.

[39] Amardeo C Sarma and João Girão. «Identities in the future internet of things.» In: *Wireless personal communications* 49.3 (2009), pp. 353–363.

[40] Guangdong Bai, Lin Yan, Liang Gu, Yao Guo, and Xiangqun Chen. «Context-aware usage control for web of things.» In: *Security and Communication Networks* 7.12 (2014), pp. 2696–2712.

[41] Rodrigo Roman, Cristina Alcaraz, Javier Lopez, and Nicolas Sklavos. «Key management systems for sensor networks in the context of the Internet of Things.» In: *Computers and Electrical Engineering* 37.2 (2011), pp. 147–159.

[42] Thomas Eisenbarth, Sandeep Kumar, Christof Paar, Axel Poschmann, and Leif Uhsadel. «A survey of lightweightcryptography implementations.» In: *IEEE Design and Test of Computers* 6 (2007), pp. 522–533.

[43] Mickaël Cazorla, Kevin Marquet, and Marine Minier. «Survey and benchmark of lightweight block ciphers for wireless sensor networks.» In: *Security and Cryptography (SECRYPT), 2013 International Conference on*. IEEE. 2013, pp. 1–6.

[44] Konstantin Beznosov, Philip Inglesant, Jorge Lobo, Rob Reeder, and Mary Ellen Zurko. «Usability Meets Access Control: Challenges and Research Opportunities.» In: *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies*. SACMAT '09. Stresa, Italy: ACM, 2009, pp. 73–74. ISBN: 978-1-60558-537-6. DOI: 10.1145/1542207.1542220. URL: http://doi.acm.org/10.1145/1542207.1542220.

[45] Charu C Aggarwal and S Yu Philip. «A general survey of privacy-preserving data mining models and algorithms.» In: *Privacy-preserving data mining*. Springer, 2008, pp. 11–52.

[46] Vladimir Oleshchuk. «Internet of things and privacy preserving technologies.» In: *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 2009. Wireless VITAE 2009. 1st International Conference on*. IEEE. 2009, pp. 336–340.

[47] Pelin Angin, Bharat Bhargava, Rohit Ranchal, Noopur Singh, Mark Linderman, Lotfi Ben Othmane, and Leszek Lilien. «An entity-centric approach for privacy and identity management in cloud computing.» In: *Reliable Distributed Systems, 2010 29th IEEE Symposium on*. IEEE. 2010, pp. 177–183.

[48] Rolf H Weber. «Internet of Things–New security and privacy challenges.» In: *Computer law and security review* 26.1 (2010), pp. 23–30.

[49] Gerben Broenink, Jaap-Henk Hoepman, Christian van't Hof, Rob Van Kranenburg, David Smits, and Tijmen Wisman. «The privacy coach: Supporting customer privacy in the internet of things.» In: *arXiv preprint arXiv:1001.4459* (2010).

[50] Jon Robinson, Ian Wakeman, Dan Chalmers, and Ben Horsfall. «Trust and the internet of things.» In: *Joint International Workshop on Trust in Location and Communications in Decentralised Computing (TruLoco'10), Morioka, Japan*. Citeseer. 2010.

[51] Christina Hochleitner, Cornelia Graf, Peter Wolkerstorfer, and Manfred Tscheligi. «uTRUSTit–Usable Trust in the Internet of Things.» In: *International Conference on Trust, Privacy and Security in Digital Business*. Springer. 2012, pp. 220–221.

[52] Thiago Teixeira, Sara Hachem, Valérie Issarny, and Nikolaos Georgantas. «Service oriented middleware for the internet of things: a perspective.» In: *European Conference on a Service-Based Internet*. Springer. 2011, pp. 220–229.

[53] Yichi Zhang, Lingfeng Wang, Weiqing Sun, Robert C Green II, and Mansoor Alam. «Distributed intrusion detection system in a multi-layer network architecture of smart grids.» In: *IEEE Transactions on Smart Grid* 2.4 (2011), pp. 796–808.

[54] Kim Thuat Nguyen, Maryline Laurent, and Nouha Oualha. «Survey on secure communication protocols for the Internet of Things.» In: *Ad Hoc Networks* 32 (2015). Internet of Things security and privacy: design methods and optimization, pp. 17 –31. ISSN: 1570-8705. DOI: 10.1016/j.adhoc.2015.01.006. URL: http://www.sciencedirect.com/science/article/pii/S1570870515000141.

[55] Joan Feigenbaum. *Towards an Infrastructure for Authorization*. 1998.

[56] Morris Sloman. «Policy driven management for distributed systems.» In: *Journal of Network and Systems Management* 2.4 (1994), pp. 333–360. ISSN: 1573-7705. DOI: 10.1007/BF02283186. URL: http://dx.doi.org/10.1007/BF02283186.

[57] Javier Lopez, Rolf Oppliger, and Günther Pernul. «Authentication and authorization infrastructures (AAIs): a comparative survey.» In: *Computers & Security* 23.7 (2004), pp. 578–590.

[58] Tom Goovaerts. «Distributed Authorization Middleware for Service Oriented Architectures (Gedistribueerde autorisatiemiddleware voor service georiënteerde architecturen).» In: (2011).

[59] Weili Han and Chang Lei. «A survey on policy languages in network and security management.» In: *Computer Networks* 56.1 (2012), pp. 477 –489. ISSN: 1389–1286. DOI: 10.1016/j.comnet.2011.09.014. URL: http://www.sciencedirect.com/science/article/pii/S1389128611003562.

[60] Amir Aryanpour, Song Y Yan, Scott Davies, and Andrew Harmellaw. «Towards Design an Interoperability Framework for Security Policy Languages.» In: *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). 2012, p. 1.

[61] Ravi S Sandhu and Pierangela Samarati. «Access control: principle and practice.» In: *IEEE communications magazine* 32.9 (1994), pp. 40–48.

[62] R. Levin, E. Cohen, W. Corwin, F. Pollack, and W. Wulf. «Policy-Mechanism Separation in Hydra.» In: *SIGOPS Oper. Syst. Rev.* 9.5 (May 1975), pp. 132–140. ISSN: 0163–5980. DOI: 10.1145/1067629.806531. URL: http://doi.acm.org/10.1145/1067629.806531.

[63] Michael Gegick and Sean Barnum. *LEast privilege*. URL: https://www.us-cert.gov/bsi/articles/knowledge/principles/least-privilege.

[64] Trent Jaeger. «Reference Monitor.» In: *Encyclopedia of Cryptography and Security (2nd Ed.)* 2011, pp. 1038–1040.

[65] James P. Anderson. *Computer security technology planning study*. Tech. rep. Air Force Electronic Systems Division, 1972.

[66] B. Moore. *Policy Core Information Model PCIM Extensions*. RFC 3460. RFC Editor, Jan. 2003.

[67] Bill Parducci. *eXtensible Access Control Markup Language (XACML) Version 3.0, Standard*. OASIS, 2013. URL: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

[68] A. Westerinen, J. Schnizlein, J. Strassner, M. Scherling, B. Quinn, S. Herzog, A. Huynh, M. Carlson, J. Perry, and S. Waldbusser. *Terminology for PolicyBased Management*. RFC 3198. RFC Editor, Nov. 2001.

[69] R. Yavatkar, D. Pendarakis, and R. Guerin. *A Framework for Policybased Admission Control*. RFC 2753. RFC Editor, Jan. 2000.

[70] Nicodemos Damianou. *A Policy Framework for Management of Distributed Systems*. Tech. rep. 2002.

[71] A. K. Bandara, E. C. Lupu, J. Moffett, and A. Russo. «A goal-based approach to policy refinement.» In: *Proceedings. Fifth IEEE International Workshop on Policies for Distributed Systems and Networks, 2004. POLICY 2004.* June 2004, pp. 229–239. DOI: 10.1109/POLICY.2004.1309175.

[72] «Protection. Operating System Review.» In: *SIGOPS Oper. Syst. Rev.* 8.1 (1974), pp. 18–24. ISSN: 0163–5980.

[73] G. Scott Graham and Peter J. Denning. «Protection: Principles and Practice.» In: *Proceedings of the May 16-18, 1972, Spring Joint Computer Conference*. AFIPS 1972 (Spring). Atlantic City, New Jersey: ACM, 1972, pp. 417–429. DOI: 10.1145/1478873.1478928. URL: http://doi.acm.org/10.1145/1478873.1478928.

[74] U. Dayal, E. Hanson, and J. Widom. *Active Database Systems*. Technical Report 1994-20. Stanford Infolab, 1994. URL: http://ilpubs.stanford.edu:8090/54/.

[75] Jan Chomicki, Jorge Lobo, and Shamim Naqvi. «Conflict resolution using logic programming.» In: *IEEE Transactions on Knowledge and Data Engineering* 15.1 (2003), pp. 244–249.

[76] Emil C Lupu and Morris Sloman. «Conflicts in policybased distributed systems management.» In: *IEEE Transactions on software engineering* 25.6 (1999), pp. 852–869.

[77] Jonathan D Moffett and Morris S Sloman. «Policy conflict analysis in distributed system management.» In: *Journal of Organizational Computing and Electronic Commerce* 4.1 (1994), pp. 1–22.

[78] M. Koch, L. V. Mancini, and F. ParisiPresicce. «On the Specification and Evolution of Access Control Policies.» In: *Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies*. SACMAT '01. Chantilly, Virginia, USA: ACM, 2001, pp. 121–130. ISBN: 1-58113-350-2. DOI: 10.1145/373256.373280. URL: http://doi.acm.org/10.1145/373256.373280.

[79] D. Agrawal, J. Giles, Kang-Won Lee, and J. Lobo. «Policy ratification.» In: *Sixth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'05)*. June 2005, pp. 223–232. DOI: 10.1109/POLICY.2005.25.

[80] Y. L. Traon, T. Mouelhi, and B. Baudry. «Testing Security Policies: Going Beyond Functional Testing.» In: *The 18th IEEE International Symposium on Software Reliability (ISSRE '07)*. Nov. 2007, pp. 93–102. DOI: 10.1109/ISSRE.2007.27.

[81] Evan Martin and Tao Xie. «A Fault Model and Mutation Testing of Access Control Policies.» In: *Proceedings of the 16th International Conference on World Wide Web*. WWW '07. Banff, Alberta, Canada: ACM, 2007, pp. 667–676. ISBN: 978-1-59593-654-7. DOI: 10.1145/1242572.1242663. URL: http://doi.acm.org/10.1145/1242572.1242663.

[82] Axiomatics. *Axiomatics policy server*. URL: http://www.axiomatics.com/products/axiomatics-policy-server.html.

[83] David Chadwick, Gansen Zhao, Sassa Otenko, Romain Laborde, Linying Su, and Tuan Anh Nguyen. «PERMIS: a modular authorization infrastructure.» In: *Concurrency and Computation: Practice and Experience* 20.11 (2008), pp. 1341–1357. ISSN: 1532–0634. DOI: 10.1002/cpe.1313. URL: http://dx.doi.org/10.1002/cpe.1313.

[84] EE Group et al. «JSR 220: Enterprise JavaBeansTM, Version 3.0 EJB Core Contracts and Requirements Version 3.0, Final Release.» In: *May* 28 (2006), pp. 60–66.

[85] Günter Karjoth. «Access control with IBM Tivoli access manager.» In: *ACM Transactions on Information and System Security (TISSEC)* 6.2 (2003), pp. 232–257.

[86] Oracle Coporation Bill Dettelback. 2008. URL: http://www.oracle.com/technetwork/testcontent/oes-entitlements-133195.pdf.

[87] Scott Cantor, John Kemp, Rob Philpott, Eve Maler, and OASIS. *Security assertions markup language, SAML 2.0*. http://saml.xml.org/saml-specifications. Mar. 2005.

[88] D. Hardt. *The OAuth 2.0 Authorization Framework*. RFC 6749. RFC Editor, Oct. 2012. URL: http://www.rfc-editor.org/rfc/rfc6749.txt.

[89] Shibboleth project Internet2. http://shibboleth.internet2.edu.

[90] Mary Shaw and David Garlan. *Software architecture: perspectives on an emerging discipline*. Vol. 1. Prentice Hall Englewood Cliffs, 1996.

[91] Konstantin Kosta Beznosov. «Flooding and recycling authorizations.» In: *Proceedings of the 2005 workshop on New security paradigms*. ACM. 2005, pp. 67–72.

[92] Qiang Wei. «Towards improving the availability and performance of enterprise authorization systems.» In: (2009).

[93] Qiang Wei, Matei Ripeanu, and Konstantin Beznosov. «Authorization using the publish-subscribe model.» In: *Parallel and Distributed Processing with Applications, 2008. ISPA'08. International Symposium on*. IEEE. 2008, pp. 53–62.

[94] H. Tschofenig, J. Arkko, D. Thaler, and D. McPherson. *Architectural Considerations in Smart Object Networking*. RFC 7452. RFC Editor, Mar. 2015.

[95] Jia Hao Kong, Li-Minn Ang, and Kah Phooi Seng. «A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments.» In: *Journal of Network and Computer Applications* 49 (2015), pp. 15–50.

[96] Darrel Hankerson, Alfred J. Menezes, and Scott Vanstone. *Guide to Elliptic Curve Cryptography*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003. ISBN: 038795273X.

[97] Peter A. Loscocco, Stephen D. Smalley, Patrick A. Muckelbauer, Ruth C. Taylor, S. Jeff Turner, and John F. Farrell. «The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments.» In: *In Proceedings of the 21st National Information Systems Security Conference*. 1998, pp. 303–314.

[98] Michael A Harrison, Walter L Ruzzo, and Jeffrey D Ullman. «Protection in operating systems.» In: *Communications of the ACM* 19.8 (1976), pp. 461–471.

[99] Ravi Sandhu, David Ferraiolo, and Richard Kuhn. «The NIST Model for Rolebased Access Control: Towards a Unified Standard.» In: *Proceedings of the Fifth ACM Workshop on Rolebased Access Control*. RBAC '00. Berlin, Germany: ACM, 2000, pp. 47–63. ISBN: 1-58113-259-X. DOI: 10.1145/344287.344301. URL: http://doi.acm.org/10.1145/344287.344301.

[100] Vincent C. Hu et al. *Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft)*. 2013.

[101] E. Yuan and J. Tong. «Attributed based access control (ABAC) for Web services.» In: *IEEE International Conference on Web Services (ICWS)*. Institute of Electrical and Electronics Engineers (IEEE), 2005. DOI: 10.1109/icws.2005.25. URL: http://dx.doi.org/10.1109/ICWS.2005.25.

[102] Manuel Hilty, Alexander Pretschner, David Basin, Christian Schaefer, and Thomas Walter. «A policy language for distributed usage control.» In: *European Symposium on Research in Computer Security*. Springer. 2007, pp. 531–546.

[103] Jaehong Park and Ravi Sandhu. «The UCONABC Usage Control Model.» In: *ACM Trans. Inf. Syst. Secur.* 7.1 (Feb. 2004), pp. 128–174. ISSN: 1094-9224. DOI: 10.1145/984334.984339. URL: http://doi.acm.org/10.1145/984334.984339.

[104] Zhang Guoping and Gong Wentao. «The research of access control based on UCON in the internet of things.» In: *Journal of Software* 6.4 (2011), pp. 724–731.

[105] Ecma International. *The JSON Data Interchange Format*. Standard ECMA-404. Oct. 2013.

[106] Nicodemos Damianou, Naranker Dulay, Emil Lupu, and Morris Sloman. «Policies for Distributed Systems and Networks: International Workshop, POLICY 2001 Bristol, UK, January 29–31, 2001 Proceedings.» In: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001. Chap. The Ponder Policy Specification Language, pp. 18–38. ISBN: 978-3-540-44569-2. DOI: 10.1007/3-540-44569-2_2. URL: http://dx.doi.org/10.1007/3-540-44569-2_2.

[107] L. Kagal, T. Finin, and Anupam Joshi. «A policy language for a pervasive computing environment.» In: *Policies for Distributed Systems and Networks, 2003. Proceedings. POLICY 2003. IEEE 4th International Workshop on*. June 2003, pp. 63–74. DOI: 10.1109/POLICY.2003.1206958.

[108] Tim Berners-Lee and Dan Connolly. *Notation3 (N3): A readable RDF syntax*. W3C Team Submission. W3C, Jan. 2008. URL: http://www.w3.org/TeamSubmission/n3/.

[109] Sushil Jajodia, Pierangela Samarati, and V. S. Subrahmanian. «A Logical Language for Expressing Authorizations.» In: *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 1997, pp. 31–42. ISBN: 0-8186-7828-3. URL: http://dblp.uni-trier.de/db/conf/sp/sp1997.html#JajodiaSS97.

[110] Lorrie Cranor, Marc Langheinrich, and Massimo Marchiori. *A P3P Preference Exchange Language 1.0 (APPEL 1.0)*. World Wide Web Consortium, Working Draft WDP3Ppreferences20020415. Apr. 2002.

[111] Paul Ashley, Satoshi Hada, Günter Karjoth, Calvin Powers, and Matthias Schunter. *Enterprise Privacy Authorization Language (EPAL)*. Tech. rep. Rüschlikon: IBM Research, 2003.

[112] Henry M. Levy. *CapabilityBased Computer Systems*. Newton, MA, USA: ButterworthHeinemann, 1984. ISBN: 0932376223.

[113] Steve Barker. «The next 700 access control models or a unifying meta-model?» In: *Proceedings of the 14th ACM symposium on Access control models and technologies*. ACM. 2009, pp. 187–196.

[114] Policy Languages Interest Group at W3C. *Review of Policy Languages and Frameworks*. https://www.w3.org/Policy/pling/wiki/PolicyLangReview.

[115] Sean Bechhofer, Frank van Harmelen, Jim Hendler, Ian Horrocks, Deborah L. McGuinness, Peter F. Patel-Schneider, and Lynn Andrea Stein. *OWL Web Ontology Language Reference*. Tech. rep. W3C, Feb. 2004. URL: http://www.w3.org/TR/owl-ref/.

[116] K. Selcuk Candan, Huan Liu, and Reshma Suvarna. «Resource Description Framework: Metadata and Its Applications.» In: *SIGKDD Explor. Newsl.* 3.1 (July 2001), pp. 6–19. ISSN: 1931-0145. DOI: 10.1145/507533.507536. URL: http://doi.acm.org/10.1145/507533.507536.

[117] Ian Horrocks, Peter F. Patel-Schneider, Harold Boley, Said Tabet, Benjamin Grosofand, and Mike Dean. *SWRL: A Semantic Web Rule Language Combining OWL and RuleML*. W3C. May 2004. URL: http://www.w3.org/Submission/SWRL/.

[118] specs@openid.net. *OpenID Authentication 2.0 - Final*. 2007. URL: http://openid.net/specs/openid-authentication-2_0.html.

[119] Dr. Rolf Lindemann, Davit Baghdasaryan, Eric Tiffany, and Fido Alliance. *FIDO UAF Protocol Specification v1.0*. https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-protocol-v1.0-ps-20141208.html. Dec. 2014.

[120] Sampath Srinivas, Dirk Balfanz, Eric Tiffany, Alexei Czeskis, and Fido Alliance. *Universal 2nd Factor U2F Overview*. https://fidoalliance.org/specs/fido-undefined-undefined-ps-20150514/fido-u2f-overview-v1.0-undefined-ps-20150514.html. May 2015.

[121] L. Seitz, G. Selander, and C. Gehrmann. «Authorization framework for the Internet-of-Things.» In: *2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*. June 2013, pp. 1–6. DOI: 10.1109/WoWMoM.2013.6583465.

[122] Ziyi Su and Frédérique Biennier. «On attribute-based usage control policy ratification for cooperative computing context.» In: *CoRR* abs/1305.1727 (2013). URL: http://arxiv.org/abs/1305.1727.

[123] Sergio Gusmeroli, Salvatore Piccione, and Domenico Rotondi. «A capability-based security approach to manage access control in the Internet of Things.» In: *Mathematical and Computer Modelling* 58 (2013). The Measurement of Undesirable Outputs: Models Development and Empirical Analyses and Advances in mobile, ubiquitous and cognitive computing, pp. 1189 –1205. ISSN: 0895-7177. DOI: http://dx.doi.org/10.1016/j.mcm.2013.02.006.

[124] José L Hernández-Ramos, Antonio J Jara, Leandro Marın, and Antonio F Skarmeta. «Distributed capability-based access control for the internet of things.» In: *Journal of Internet Services and Information Security (JISIS)* 3.3/4 (2013), pp. 1–16.

[125] Jose Luis Hernandez Ramos, Antonio J. Jara, Leandro Marin, and Antonio F. Skarmeta Gomez. «DCapBAC: embedding authorization logic into smart things through ECC optimizations.» In: *Int. J. Comput. Math.* 93 (2016), pp. 345–366.

[126] Ludwig Seitz, Goeran Selander, Erik Wahlstroem, Samuel Erdtman, and Hannes Tschofenig. *Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)*. Internet-Draft draft-ietf-ace-oauth-authz-11. IETF Secretariat, Mar. 2018. URL: `http://www.ietf.org/internet-drafts/draft-ietf-ace-oauth-authz-11.txt`.

[127] W. Denniss and J. Bradley. *OAuth 2.0 for Native Apps*. BCP 212. RFC Editor, Oct. 2017.

[128] C. Bormann and P. Hoffman. *Concise Binary Object Representation (CBOR)*. RFC 7049. RFC Editor, Oct. 2013.

[129] J. Schaad. *CBOR Object Signing and Encryption (COSE)*. RFC 8152. RFC Editor, July 2017.

[130] Stefanie Gerdes, Olaf Bergmann, Carsten Bormann, Goeran Selander, and Ludwig Seitz. *Datagram Transport Layer Security (DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE)*. Internet-Draft draft-ietf-ace-dtls-authorize-03. IETF Secretariat, Mar. 2018. URL: `http://www.ietf.org/internet-drafts/draft-ietf-ace-dtls-authorize-03.txt`.

[131] Michael Jones, Erik Wahlstroem, Samuel Erdtman, and Hannes Tschofenig. *CBOR Web Token (CWT)*. Internet-Draft draft-ietf-ace-cbor-web-token-15. IETF Secretariat, Mar. 2018. URL: `http://www.ietf.org/internet-drafts/draft-ietf-ace-cbor-web-token-15.txt`.

[132] P. Wouters, H. Tschofenig, J. Gilmore, S. Weiler, and T. Kivinen. *Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*. RFC 7250. RFC Editor, June 2014.

[133] P. Eronen and H. Tschofenig. *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*. RFC 4279. `http://www.rfc-editor.org/rfc/rfc4279.txt`. RFC Editor, Dec. 2005. URL: `http://www.rfc-editor.org/rfc/rfc4279.txt`.

[134] Olaf Bergmann. *Eclipse tinydtls*. `https://projects.eclipse.org/projects/iot.tinydtls`.

[135] Malisa Vucinic, Bernard Tourancheau, Franck Rousseau, Andrzej Duda, Laurent Damon, and Roberto Guizzetti. «OSCAR: Object security architecture for the Internet of Things.» In: *Ad Hoc Networks* 32 (2015). Internet of Things security and privacy: design methods and optimization, pp. 3 –16. ISSN: 1570-8705. DOI: /10.1016/j.adhoc.2014.12.005. URL: http://www.sciencedirect.com/science/article/pii/S1570870514003126.

[136] Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brünig, and Georg Carle. «DTLS Based Security and Two-way Authentication for the Internet of Things.» In: *Ad Hoc Netw.* 11.8 (Nov. 2013), pp. 2710–2723. ISSN: 1570-8705. DOI: 10.1016/j.adhoc.2013.05.003. URL: http://dx.doi.org/10.1016/j.adhoc.2013.05.003.

[137] Yanmin Zhu, Sye Loong Keoh, Morris Sloman, and Emil C Lupu. «A lightweight policy system for body sensor networks.» In: *IEEE Transactions on Network and Service Management* 6.3 (2009), pp. 137–148.

[138] N. Dulay, E. Lupu, M. Sloman, and N. Damianou. «A policy deployment model for the Ponder language.» In: *2001 IEEE/IFIP International Symposium on Integrated Network Management Proceedings. Integrated Network Management VII. Integrated Management Strategies for the New Millennium (Cat. No.01EX470)*. 2001, pp. 529–543. DOI: 10.1109/INM.2001.918064.

[139] Jasone Astorga, Eduardo Jacob, Maider Huarte, and Marivi Higuero. «Ladon: end to end authorisation support for resource deprived environments.» In: *IET Information Security* 6.2 (June 2012), pp. 93–101.

[140] Jasone Astorga, Nerea Toledo, Eduardo Jacob, and Marivi Higuero. «Taxonomy of Security Protocols for Wireless Sensor Communications.» In: *Security for Multihop Wireless Networks*. CRC Press, Taylor & Francis Group, USA, 2013.

[141] Oscar Garcia-Morchon and Klaus Wehrle. «Modular context-aware access control for medical sensor networks.» In: *Proceedings of the 15th ACM symposium on Access control models and technologies*. ACM. 2010, pp. 129–138.

[142] Nikos Fotiou, Theodore Kotsonis, Giannis F Marias, and George C Polyzos. «Access Control for the Internet of Things.» In: *Secure Internet of Things (SIoT), 2016 International Workshop on*. IEEE. 2016, pp. 29–38.

[143] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. «Attribute-based encryption for fine-grained access control of encrypted data.» In: *Proceedings of the 13th ACM conference on Computer and communications security*. Acm. 2006, pp. 89–98.

[144] John Bethencourt, Amit Sahai, and Brent Waters. «Ciphertext-policy attribute-based encryption.» In: *Security and Privacy, 2007. SP'07. IEEE Symposium on*. IEEE. 2007, pp. 321–334.

[145] Shucheng Yu, Kui Ren, and Wenjing Lou. «FDAC: Toward fine-grained distributed data access control in wireless sensor networks.» In: *IEEE Transactions on Parallel and Distributed Systems* 22.4 (2011), pp. 673–686.

[146] Sushmita Ruj, Amiya Nayak, and Ivan Stojmenovic. «Distributed fine-grained access control in wireless sensor networks.» In: *Parallel & Distributed Processing Symposium (IPDPS), 2011 IEEE International*. IEEE. 2011, pp. 352–362.

[147] Junbeom Hur. «Fine-grained data access control for distributed sensor networks.» In: *Wireless Networks* 17.5 (2011), pp. 1235–1249.

[148] Htoo Aung Maw, Hannan Xiao, and Bruce Christianson. «An adaptive access control model for medical data in wireless sensor networks.» In: *eHealth Networking, Applications & Services (Healthcom), 2013 IEEE 15th International Conference on*. IEEE. 2013, pp. 303–309.

[149] Chih-Chun Chang, Sead Muftic, and David J Nagel. «Measurement of energy costs of security in wireless sensor nodes.» In: *Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on*. IEEE. 2007, pp. 95–102.

[150] Haodong Wang, Bo Sheng, and Qun Li. «Elliptic curve cryptography-based access control in sensor networks.» In: *International Journal of Security and Networks* 1.3-4 (2006), pp. 127–137.

[151] Yun Zhou, Yanchao Zhang, and Yuguang Fang. «Access control in wireless sensor networks.» In: *Ad Hoc Networks* 5.1 (2007), pp. 3–13.

[152] Abdullah Al-Mahmud and Matei Ciobanu Morogan. «Identity-based authentication and access control in wireless sensor networks.» In: *International Journal of Computer Applications* 41.13 (2012).

[153] *IEEE 802.15.4 Standard: Wireless Medium Access (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal AreaNetworks (WPANs)*. Sept. 2006.

[154] Jennifer G. Steiner, Clifford Neuman, and Jeffrey I. Schiller. «Kerberos: An Authentication Service for Open Network Systems.» In: *IN USENIX CONFERENCE PROCEEDINGS*. 1988, pp. 191–202.

[155] Francois Carrez, Martin Bauer, Mathieu Boussard, and Nicola Bui. *Final architectural reference model for the IoT v3.0*. http://www.iot-a.eu/public/public-documents/d1.5/at_download/file. July 2013.

[156] Victor Shnayder, Mark Hempstead, Bor rong Chen, Geoff Werner Allen, and Matt Welsh. «Simulating the power consumption of large-scale sensor network applications.» In: *Proceedings of the 2nd international conference on Embedded networked sensor systems (SenSys '04)*. Baltimore, MD, USA: ACM, 2004, pp. 188–200.

[157] Richard E. Pattis. *EBNF: A Notation to Describe Syntax (PDF)*. http://www.cs.cmu.edu/ pattis/misc/ebnf.pdf.

[158] D. Dolev and A. Yao. «On the security of public key protocols.» In: *IEEE Transactions on Information Theory* 29.2 (1983), pp. 198–208.

[159] A. Armando et al. «The AVISPA tool for the automated validation of internet security protocols and applications.» In: *Proceedings of the 17th international conference on Computer Aided Verification (CAV'05)*. Edinburgh, Scotland, UK: SpringerVerlag, 2005, pp. 281–285.

[160] Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, J. Mantovani, S. Mödersheim, and L. Vigneron. «A High Level Protocol Specification Language for Industrial Security-Sensitive Protocols.» In: *Austrian Computer Society*. 2004, pp. 193–205.

[161] David Basin, Sebastian Mödersheim, and Luca Viganó. «OFMC: A symbolic model checker for security protocols.» In: *International Journal of Information Security* 4.3 (2005), pp. 181–208.

[162] Mathieu Turuani. «The CL-Atse Protocol Analyser.» In: *Term Rewriting and Applications*. Ed. by Frank Pfenning. Vol. 4098. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2006, pp. 277–286.

[163] Alessandro Armando and Luca Compagna. «SATMC: A SAT-Based Model Checker for Security Protocols.» In: *Logics in Artificial Intelligence*. Ed. by J. J. Alferes and J. Leite. Vol. 3229. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2004, pp. 730–733.

[164] Y. Boichut, P.-C. Héam, O. Kouchnarenko, and F. Oehl. «Improvements on the Genet and Klay Technique to Automatically Verify Security Protocols.» In: *Proceedings of International Workshop on Automated Verification of Infinite-State Systems (AVIS'2004), joint to ETAPS'04*. Barcelona, Spain, 2004, pp. 1–11.

[165] Thomas Genet. *A Short SPAN+AVISPA Tutorial*. Research Report. IRISA, Oct. 2015. URL: `https://hal.inria.fr/hal-01213074`.

[166] Mikko Kohvakka, Mauri Kuorilehto, Marko Hännikäinen, and Timo D. Hämäläinen. «Performance analysis of IEEE 802.15.4 and ZigBee for large-scale wireless sensor network applications.» In: *Proceedings of the 3rd ACM international workshop on Performance evaluation of wireless ad hoc, sensor and ubiquitous networks (PE-WASUN '06)*. Torromolinos, Spain: ACM, 2006, pp. 48–57.

[167] Pollaczek Khinchin. *The MG1 System, Pollaczek Khinchin theorem*. http://www.richardclegg.org/previous/networks2/Lecture9_06.pdf. 2005.

[168] Chih-Chun Chang, David J. Nagel, and Sead Muftic. «Assessment of Energy Consumption in Wireless Sensor Networks: A Case Study for Security Algorithms.» In: *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference* 0 (2007), pp. 1–6. DOI: http://doi.ieeecomputersociety.org/10.1109/MOBHOC.2007.4428758.

[169] Shammi Didla, Aaron Ault, and Saurabh Bagchi. «Optimizing AES for Embedded Devices and Wireless Sensor Networks.» In: *Proceedings of the 4th International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities*. TridentCom '08. Innsbruck, Austria: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008, 4:1–4:10. ISBN: 978-963-9799-24-0. URL: http://dl.acm.org/citation.cfm?id=1390576.1390581.

[170] Wei Dai. *Cryptopp library speed benchmark*. http://www.cryptopp.com/benchmarks-amd64.html. 2009.

[171] *MEMSIC's IRIS mote (XM2110CA) datasheet*. http://www.memsic.com/userfiles/files/Datasheets/WSN/IRIS_Datasheet.pdf.

[172] ITU. *Network performance objectives for IP based services*. Tech. rep. ITU-T rec. Y.1541. ITU, Dec. 2011.

[173] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. V. Moreno. «A decentralized approach for security and privacy challenges in the Internet of Things.» In: *Internet of Things (WF-IoT), 2014 IEEE World Forum on*. Mar. 2014, pp. 67–72. DOI: 10.1109/WF-IoT.2014.6803122.

[174] Williams Stallings and Thomas Case. «Business Data Communications: Infrastructure, Networking, and Security.» In: 7th ed. draft-ersue-constrained-mgmt-03. Pearson Education Limited, 2013. Chap. 2, pp. 57–84.

[175] P. Gaur and M. P. Tahiliani. «Operating Systems for IoT Devices: A Critical Survey.» In: *2015 IEEE Region 10 Symposium*. May 2015, pp. 33–36. DOI: 10.1109/TENSYMP.2015.17.

[176] Eclipse Foundation Ian Skerrett. *IoT developer survey results, 2017*. https://es.slideshare.net/IanSkerrett/iot-developer-survey-2017.

[177] A. Dunkels, B. Gronvall, and T. Voigt. «Contiki - a lightweight and flexible operating system for tiny networked sensors.» In: *29th Annual IEEE International Conference on Local Computer Networks*. Nov. 2004, pp. 455–462. DOI: 10.1109/LCN.2004.38.

[178] MEMSIC's TelosB mote (TPR2420CA) datasheet, http://www.memsic.com/products/wireless-sensor-networks/wireless-modules.html.

[179] *Zolertia Z1 datasheet*. http://zolertia.sourceforge.net/wiki/images/e/e8/Z1_RevC_Datasheet.pdf.

[180] *Wismote datasheet*. http://www.arago-systems.com/images/stories/WiSMote/Doc/wismote.pdf.

[181] Stoian Ivanov Kokke Matteo Brichese. *Tiny-AES128-c libraries*. Tiny AES128 in C. URL: https://github.com/kokke/tiny-AES128-C.

[182] Mikel Uriarte Itzazelaia, Jasone Astorga, Eduardo Jacob, Maider Huarte, and Pedro Romaña. «Feasibility Assessment of a Fine-Grained Access Control Model on Resource Constrained Sensors.» In: *Sensors* 18.2 (Feb. 2018), p. 575. ISSN: 1424-8220. DOI: 10.3390/s18020575. URL: http://dx.doi.org/10.3390/s18020575.

[183] M. Uriarte, J. Astorga, E. Jacob, M. Huarte, and M. Carnerero. «Expressive policy based access control for resource-constrained devices.» In: *IEEE Access* PP.99 (2017), pp. 1–1. DOI: 10.1109/ACCESS.2017.2730958.

[184] Jose Ramon Gisbert, C Palau, Mikel Uriarte, Gonzalo Prieto, José Antonio Palazón, Manuel Esteve, Oscar López, Javier Correas, M Carmen Lucas-Estañ, Pablo Giménez, et al. «Integrated system for control and monitoring industrial wireless networks for labor risk prevention.» In: *Journal of Network and Computer Applications* 39 (2014), pp. 233–252.

[185] Mikel Uriarte, Jasone Astorga, Eduardo Jacob, Maider Huarte, and Manuel Carnerero. «Feasbility assessment of a fine-grained access control model on resource constrained sensors.» In: *Proceedings of the XIII Jornadas de Ingeniería Telemática (JITEL 2017)*. Valencia, Spain, 2017.

[186] Madhusanka Liyanage, Ijaz Ahmed, Mika Ylianttila, Jesus Llorente Santos, Raimo Kantola, Oscar Lopez Perez, Mikel Uriarte Itzazelaia, Edgardo Montes de Oca, Asier Valtierra, and Carlos Jimenez. «Security for future software defined mobile networks.» In: *Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on*. IEEE. 2015, pp. 256–264.

[187] Mikel Uriarte, Óscar Lázaro, Alicia Gonzalez, Ivan Prada, Oscar López, Jordi Blasi, Eneko Olivares, and Carlos E Palau. «Usable Access Control Enabled by Sensing Enterprise Architectures.» In: *IWEI Workshops*. 2015.

[188] Jens Ziegler, Robert Buchmann, Markus Graube, Jan Hladik, Tobias Münch, Patricia Ortiz, Johannes Pfeffer, Florian Schneider, Mikel Uriarte, Dimitris Karagiannis, et al. «Implementation and Operation of Collaborative Manufacturing Networks.» In: *Working Conference on Virtual Enterprises*. Springer. 2014, pp. 197–208.

[189] Markus Graube, Patricia Ortiz, Manuel Carnerero, Oscar Lázaro, Mikel Uriarte, and Leon Urbas. «Flexibility vs. security in linked enterprise data access control graphs.» In: *Information Assurance and Security (IAS), 2013 9th International Conference on*. IEEE. 2013, pp. 13–18.

[190] Patricia Ortiz, Oscar Lázaro, Mikel Uriarte, and Manuel Carnerero. «Enhanced multi-domain access control for secure mobile collaboration through linked data cloud in manufacturing.» In: *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a*. IEEE. 2013, pp. 1–9.

[191] Mikel Uriarte, Oscar López, Jordi Blasi, Oscar Lázaro, Alicia González, Iván Prada, Eneko Olivares, Carlos E Palau, Miguel A Portugués, and Alejandro García. «Sensing enabled capabilities for access control management.» In: *Integration, Interconnection, and Interoperability of IoT Systems*. Springer, 2018, pp. 149–167.