UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

Definition of a Methodology for the Security Evaluation of Internet of Things Devices

Definición de una Metodología para la Evaluación de Seguridad de Dispositivos del Internet de las Cosas.

Dña. Sara Nieves Matheu García

2020

Universidad de Murcia

Facultad de Informática

Definición de una Metodología para la Evaluación de Seguridad de Dispositivos del Internet de las Cosas.

Tesis Doctoral

Presentada por:
Sara Nieves Matheu García

Supervisada por:
Dr. Antonio Fernando Skarmeta Gómez
Dr. José Luis Hernández Ramos

Murcia, Junio de 2020

University of Murcia

Faculty of Computer Science

Definition of a Methodology for the Security Evaluation of Internet of Things Devices

Ph.D. Thesis

Authored by:
Sara Nieves Matheu García

Supervised by:
Dr. Antonio Fernando Skarmeta Gómez
Dr. José Luis Hernández Ramos

Murcia, June 2020

A aquéllos que nos dejaron por el camino:
mi abuelo Paco, mi abuela Cari y Ceni.

Agradecimientos

Detrás de una tesis doctoral nunca hay una única persona, hay unos directores, un grupo de investigación, unos compañeros, una familia y muchísima gente que de una manera u otra ha contribuido a que decidieras continuar por este camino.

Por eso, quiero darles las gracias a mis dos maravillosos directores de tesis. A Antonio, que me acogió en su grupo de investigación cuando intentaba conseguir una beca predoctoral y que me ha enseñado tanto no solo a nivel académico y profesional, sino también personal. Siempre ha tenido mucha más confianza en mí que la que yo suelo tener y lo ha demostrado de muchísimas maneras, entre ellas permitiéndome ser partícipe de los trabajos que se desarrollan en el ECSO y en los diferentes proyectos de investigación que lleva. Para mi es todo un ejemplo a seguir de perseverancia, trabajo duro y de éxito, un verdadero "manager of the universe". Y por supuesto a José Luis, que ha sido mi incansable compañero de investigación estos años y que espero que continúe así por muchos más, pues es toda una fuente de conocimiento, de preguntas que te hacen pensar y de buenas ideas. No conozco persona más perfeccionista que él, y lo ha demostrado continuamente en las revisiones exhaustivas de todas las publicaciones. Realmente esta tesis no habría sido posible sin su inestimable ayuda y guía. Le deseo toda la suerte del mundo con el camino que quiera tomar. Gracias también a Ioannis, que me permitió realizar la estancia de investigación en una ciudad maravillosa, como es Roma, y que me ayudó en todos los problemas que tuve allí, que no fueron pocos.

Tengo que darles las gracias a mis padres, a mi tía y a mi novio por todo el apoyo que me han dado siempre, a pesar de los nervios, de las derrotas y del estrés. Daba igual lo que hiciera, la decisión que tomara o el camino que siguiese, siempre estaban allí para ayudarme y animarme.

Gracias a mis compañeros de investigación, en especial a Jorge, Alejandro, Salva, Juan Antonio, Gianmarco, Raúl, Abbas y Elizabeta por todos los buenos momentos y las interesantes discusiones y publicaciones que han surgido, y a sobre todo a Dan, que a pesar del trabajo que tenga encima, sabes que siempre está dispuesto a ayudar. Gracias a Rafa, que junto a Dan fue el que me inició en este maravilloso mundo de la investigación. Espero que nunca pierdas esa mente inquieta y esa chispa que te hace trasmitir la pasión que tienes por tu trabajo cuando das clase, eres toda una inspiración. Gracias a Paco Céspedes, que ya en bachillerato consiguió meterme el gusanillo por las matemáticas y la informática. En general, gracias a todos los profesores que me han permitido llegar a donde estoy gracias a sus enseñanzas.

"La felicidad no es una estación de llegada, sino un modo de viajar". M. Runbeck

Contents

List of Figures

List of Tables

Abbreviations

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
AAA	Authentication, Authorization and Accounting
ACE	Access Control Entry
ACL	Access Control List
AIF	Authorization Information Format
AIOTI	Alliance for the Internet of Things Innovation
CAP	Cybersecurity Assurance Program
CBOR	Concise Binary Object Representation
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CNSS	Committee on National Security Systems
CNSSI	CNSS Instruction
CoAP	Constrained Application Protocol
COSE	CBOR Object Signing and Encryption
CPA	Commercial Product Assurance
CSPN	Certification de Sécurité de Premier Niveau
CVSS	Common Vulnerability Score System
CWSS	Common Weakness Scoring System
CWT	CBOR Web Token
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DDoS	Distributed Denial Of Service
DoS	Denial Of Service
DSL	Domain Specific Language
DTLS	Datagram Transport Layer Security
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EC	European Commission
ECSO	European Cyber Security Organization
EDHOC	Ephemeral Diffie-Hellman Over COSE
eIDAS	electronic IDentification, Authentication and trust Services
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
EU	European Union
GDPR	General Data Protection Regulation
GPS	Global Positioning System
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers

IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
JWA	JSON Web Algorithms
JWK	JSON Web Key
LLDP	Link Layer Discovery Protocol
M2M	Machine to Machine
MBT	Model Based Testing
MitM	Man in the Middle
MS	Member State
MSPL	Medium-level Security Policy Language
MUD	Manufacturer Usage Description
NFC	Near Field Communication
NFV	Network Function Virtualization
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NTBD	National Thing Behavior Database
NVD	National Vulnerability Database
OCL	Object Constraint Language
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PANA	Protocol for carrying Authentication for Network Access
PCIM	Policy Core Information Model
PDF	Portable Document Format
PP	Protection profile
PSD	Payment Services Directive
PSK	Pre-Shared Key
QoS	Quality of Service
QR code	Quick Response code
RADIUS	Remote Authentication Dial-In User Service
SAST	Static Application Security Testing
SCAP	Security Content Automation Protocol
SDN	Software Defined Network
SME	Small and medium-sized enterprises
SUIT	Software Updates for Internet of Things
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TTCN3	Testing and Test Control Notation Version 3
UDP	User Datagram Protocol
UL	Underwriters Laboratories
UML	Unified Modeling Language
URL	Uniform Resource Locator
WG	Working Group
XACML	eXtensible Access Control Markup Language
XCCDF	Extensible Configuration Checklist Description Format
XML	Extensible Markup Language
YANG	Yet Another Next Generation

Capítulo 1

Resumen

1.1. Motivación

En los últimos años, la tecnología ha avanzado a pasos agigantados cambiando nuestra percepción del mundo y la manera en la que realizamos acciones cotidianas. Uno de los paradigmas que más impacto ha tenido en nuestro día a día es el Internet de las Cosas (IoT), el cual ha permitido conectar a Internet dispositivos cotidianos con el objetivo de recopilar y compartir información. Así, disponemos de neveras inteligentes capaces de obtener información sobre los alimentos que faltan, gestionar la lista de la compra e incluso realizar dicha compra comunicándose con el supermercado, o cafeteras que se conectan con nuestro móvil y se activan cuando suena la alarma. Este ecosistema de dispositivos no sólo ha traído enormes beneficios al entorno de domótica, sino que ha supuesto un increíble avance en la industria, facilitando por ejemplo los procesos de monitorización de la cadena de suministro para garantizar la calidad de los productos. Este término, que fue acuñado por Kevin Ashton en 1999 [6], se ha ido desarrollando gracias a tecnologías paralelas como la conexión inalámbrica o la inminente llegada del 5G[1], permitiendo gestionar la información de una manera más eficiente y facilitando el continuo intercambio de información. Mientras que en 2019 el número de dispositivos IoT era de aproximadamente 26.66 billones, en los próximos años esta tendencia seguirá al alza, con una estimación de 74.44 billones de dispositivos en 2025, como se puede ver en la Figura 1.1[2].

Una de las principales características de estos dispositivos es la baja capacidad de cómputo de la que disponen, en pos de una mayor duración de la batería que permita el funcionamiento continuo del dispositivo. Sin embargo, dicha capacidad de cómputo, unida a los bajos costes, ha hecho que aspectos fundamentales como la seguridad y la privacidad no sean tenidos en cuenta adecuadamente, llevando a una situación en la que un atacante dispone de una enorme red de dispositivos interconectados totalmente desprotegidos. Este hecho queda patente en el gran incremento de ataques que han sufrido estos dispositivos, desde juguetes hasta dispositivos médicos necesarios para el mantenimiento de una vida humana[3]. Uno de los ataques con mayor impacto fue Mirai, en Octubre de 2016[4], donde se comprometieron millones de dispositivos IoT (e.g., cámaras o grabadoras digitales de vídeo) para ejecutar un ataque de denegación de servicio distribuido (DDoS) contra grandes plataformas como Spotify o Amazon. Esto provocó la interrupción de los servicios y por tanto grandes pérdidas monetarias.

[1] https://www.3gpp.org/release-17

[2] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[3] https://www.finance-monthly.com/2019/09/the-worst-and-weirdest-iot-hacks-of-all-times/

[4] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

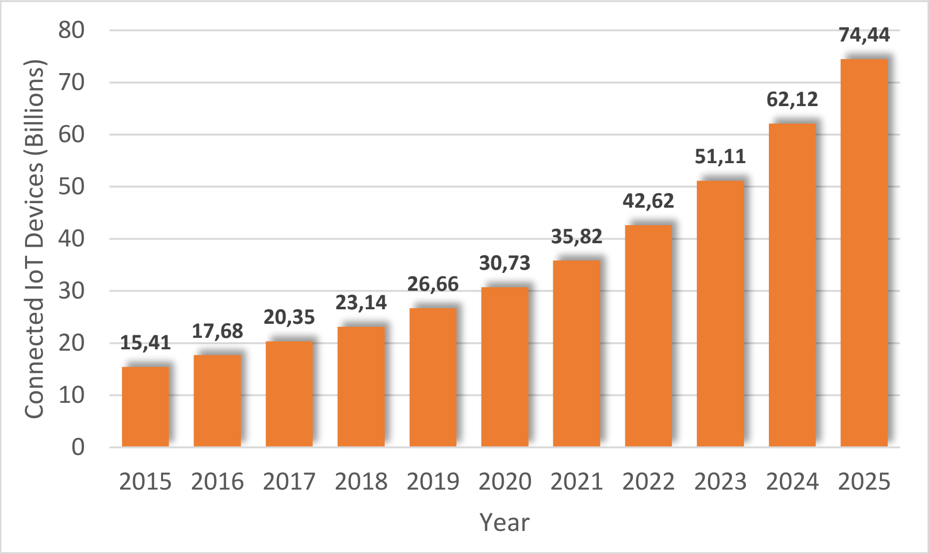


Figura 1.1: Dispositivos IoT conectados: histórico y previsión.

Este ataque se ha ido desarrollando, creando una gran cantidad de variaciones. El hecho preocupante es que ya en el año 2018, el 20 % de las compañías reportaron ataques IoT en los últimos tres años, según el estudio realizado por Gartner[5].

Esta situación, que tiende a agravarse por momentos, subraya la importancia de diseñar mecanismos de protección adecuados para los dispositivos IoT. Una de las iniciativas europeas más ambiciosas para abordar las preocupaciones existentes sobre ciberseguridad, es el establecimiento de un marco de certificación. En este sentido, la Unión Europea aprobó (EU) el 27 de Junio de 2019 la *Regulación 2019/881 del Parlamento Europeo y del Consejo del 17 de Abril de 2019 sobre la Agencia Europea de Ciberseguridad (ENISA) y la certificación de seguridad de la tecnología de la información y las comunicaciones* (Cybersecurity Act), el cual establece a ENISA como el punto central para la construcción de un framework de certificación europeo [70]. El principal objetivo de este framework sería garantizar una seguridad básica para cualquier componente de tecnologías de la información y las comunicaciones (ICT) (incluyendo dispositivos IoT) y comunicar al usuario final la seguridad del dispositivo que está comprando, facilitando la comparación de dispositivos similares. Otras iniciativas paralelas, como la Organización Europea de Ciberseguridad (ECSO), que agrupa empresas, centros de investigación y universidades, propone un meta esquema de certificación de ciberseguridad [146] a través de un grupo de trabajo especialmente dedicado a certificación. En Estados Unidos, esta iniciativa viene liderada por el Instituto Nacional de Estándares y Tecnología (NIST) [144] y, en Japón, el gobierno gestiona el desarrollo de un framework de ciberseguridad para dar guías sobre la implementación de la ciberseguridad [18].

Sin embargo la creación de un framework de certificación no es una tarea fácil, especialmente en un contexto como el de IoT. Ya de por sí, la gran variedad de métricas, estándares de seguridad y esquemas de certificación hacen difícil la selección y comparación de los niveles de seguridad. Esto es especialmente difícil cuando los esquemas pertenecen a países diferentes con diferentes regulaciones y leyes, perjudicando a los fabricantes de dispositivos, que necesitan certificarse con varios esquemas para poder vender sus productos en varios países, con el consecuente desembolso monetario. Los costes de la certificación, unidos a los altos tiempos de preparación, ejecución y espera de los resultados, hacen inviable su aplicación en dispositivos de bajo coste, como son los dispositivos IoT. Otro gran reto

[5] https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018

es la alta dinamicidad que presentan este tipo de dispositivos tan versátiles, capaces de cambiar de entorno operacional y sujetos a una plétora de nuevas amenazas cada día. La certificación tradicional, que suele ser estática y que no considera ningún proceso de monitorización posterior, no puede hacer frente a esta dinamicidad. Se necesitan mecanismos ágiles y automáticos, que permitan la repetición de la evaluación de seguridad de manera rápida y a bajo coste cuando se detecta un posible cambio de seguridad, ya sea debido a una nueva vulnerabilidad o debido a una actualización del firmware. Además, esta dinamicidad requiere una etiqueta de seguridad que muestre la seguridad del producto en tiempo real de una manera que cualquier usuario no experto pueda entenderlo, similarmente a como se hace con las etiquetas energéticas, pero de una forma más dinámica (e.g., con herramientas como el código de respuesta rápida (QR) o la tecnología inalámbrica de corto alcance (NFC)).

En resumen, un framework de certificación debería cumplir las siguientes características:

- Armonización de los esquemas de certificación y estándares de seguridad existentes para facilitar la comparación y unificar los criterios de evaluación.
- Uso de estándares para definir los procesos de la certificación de seguridad, ya que aunque muchos de estos estándares tienen sus debilidades, el framework debería hacer uso de sus puntos fuertes y de su consenso entre la comunidad científica.
- Consideración de vulnerabilidades en todas las capas de la pila de protocolos y en todos los componentes del sistema, incluyendo el análisis de las dependencias y de los efectos cascada.
- Escalabilidad y automaticidad para permitir una recertificación rápida y a bajo coste que lidie con la dinamicidad de la seguridad ante una nueva vulnerabilidad o actualización.
- Ligero, requiriendo la mínima documentación formal posible para entenderlo y aplicarlo, de coste asumible para la empresa, y rápido, sin que afecte al lanzamiento del producto al mercado.
- Etiqueta de seguridad visual y dinámica que recoja los resultados de la evaluación, que aporte información suficiente pero de una manera visual, sencilla y clara que pueda ser entendible por una persona no experta.
- Consideración del contexto del dispositivo o sistema durante la evaluación para facilitar la comparación, ya que un dispositivo IoT puede desplegarse en diferentes contextos con diferentes requisitos de seguridad.
- Uso de métricas objetivas, que no dependan del evaluador y por tanto favorezcan la reproducibilidad de la evaluación. Además, se deberían evitar métricas difíciles de calcular como la probabilidad de explotación de una vulnerabilidad.

1.2. Objetivos y Metodología

Como respuesta a los problemas analizados en la sección anterior, se planteó esta tesis colaborando en el contexto del proyecto Europeo H2020 ARMOUR[6], con el objetivo de diseñar una metodología de evaluación de la seguridad enfocada a dispositivos IoT. Dicha metodología está orientada a servir como base para un futuro framework de certificación, ayudando a definir e instanciar los procesos relacionados con la evaluación de la seguridad. La metodología se ha diseñado combinando valoración de riesgos y tests para la evaluación objetiva del riesgo y la seguridad. En una segunda parte, dicha metodología se ha instanciado a través de tecnologías y mecanismos que permiten automatizar el proceso, de manera que así se pueda facilitar la escalabilidad y la recertificación, lidiando con la alta dinamicidad de los entornos IoT. Finalmente, y con el objetivo de llevar los resultados de la evaluación a la fase de operación del dispositivo, se ha propuesto un mecanismo de mitigación basado en perfiles de comportamiento, de manera que se pueda reducir la superficie de ataque del dispositivo

[6] https://www.armour-project.eu/

IoT. La implementación de dicho mecanismo se ha integrado con los resultados del proyecto Europeo H2020 ANASTACIA[7]. La evaluación de seguridad propuesta ha sido validada en varios escenarios y considerando diferentes protocolos. Así, se han fijado los siguientes objetivos para el desarrollo de esta tesis:

- Objetivo 1: Análisis de los requisitos de evaluación de seguridad en dispositivos IoT.
- Objetivo 2: Análisis del estado del arte actual en materia de certificación de seguridad, evaluación de seguridad, técnicas de testeo, y de las principales iniciativas de organismos europeos y de estandarización.
- Objetivo 3: Propuesta de una metodología de evaluación de la seguridad para dispositivos IoT, de manera que se tengan en cuenta los requisitos analizados en el Objetivo 1.
- Objetivo 4: Análisis de las principales herramientas y técnicas de evaluación del riesgo, y de diseño y ejecución de tests de seguridad.
- Objetivo 5: Propuesta de instanciación de la metodología diseñada en el Objetivo 2, de manera que se tengan en cuenta los requisitos analizados en el Objetivo 1.
- Objetivo 6: Validación y evaluación de la propuesta en varios escenarios IoT.
- Objetivo 7: Integración de perfiles de comportamiento, en particular del estándar Manufacturer Usage Description (MUD [53]), en la metodología, de manera que se puedan utilizar los resultados de la evaluación de seguridad para mitigar ataques durante la fase de operación del dispositivo.
- Objetivo 8: Validación y evaluación de la propuesta de mitigación en entornos IoT para demostrar su factibilidad.

Dichos objetivos han ido guiando la metodología y el desarrollo de la investigación realizada en esta tesis. Las primeras etapas, dedicadas a analizar qué propiedades de los dispositivos IoT dificultan su evaluación de seguridad y cuáles son las carencias en los actuales esquemas de certificación y evaluación de la seguridad, han sido cruciales para determinar el camino a seguir durante el diseño de la metodología. A su vez, la participación en grupos europeos como el ECSO y el analisis de las iniciativas llevadas a cabo por la Comisión Europea (EC), ENISA, la industria y la comunidad científica, ha permitido alinear nuestros esfuerzos con lo que se está haciendo en materia de certificación en seguridad en el mundo y en especial, en Europa. Además, para el diseño de la metodología, nos hemos basado en estándares como el del Instituto Europeo de Estándares de Telecomunicaciones (ETSI), el ETSI EG 203 251 [54], que ya propone el uso de los tests para incrementar la fiabilidad de la evaluación de la seguridad. El análisis de los mecanismos de certificación y evaluación de la seguridad actuales puso de manifiesto sus carencias, especialmente las relacionadas con la dinamicidad de la seguridad. Así, la instanciación de la metodología fue realizada teniendo en cuenta este hecho, de manera que se permitiera una reevaluación rápida. Finalmente, para la instanciación de la fase de mitigación de la metodología, se utilizó el estándar MUD como mecanismo para definir perfiles de comportamiento que permitieran reducir la superficie de ataque durante la fase de operación del dispositivo. Dicha integración no sólo supuso la extracción de resultados útiles para la mitigación, sino también la extensión del MUD y su obtención y aplicación durante la instalación del dispositivo. El diseño, instanciación, despliegue y evaluación de la metodología de evaluación de seguridad, así como las mitigaciones, suponen el fruto de la investigación realizada en esta tesis, que será explicada más detalladamente en la siguiente sección.

[7] http://www.anastacia-h2020.eu/

Tabla 1.1: Principales resultados de la tesis

Resultado	Objetivos	Publicaciones
R1.Análisis de las propiedades necesarias para la evaluación de seguridad en entornos IoT, y análisis de las carencias encontradas en los sistemas de certificación y evaluación de seguridad actuales.	1, 2	[86] [3]
R2.Diseño de una metodología de evaluación de la seguridad para IoT basada en estándares actuales, combinando evaluación del riesgo y tests de seguridad con el objetivo de evaluar la seguridad de una manera objetiva.	3	[86] [158] [134] [87] [3]
R3.Implementación de la metodología de evaluación de la seguridad para IoT mediante técnicas y herramientas apropiadas para el contexto IoT que favorezcan la automatización de la evaluación de la seguridad con el objetivo de lidiar con la dinamicidad de la seguridad, la escalabilidad y la recertificación.	4, 5	[134] [87] [158] [31]
R4. Integración de los resultados de la metodología de evaluación con la creación de un perfil de comportamiento extendido del dispositivo (partiendo del estándar MUD), que ayude a configurar su seguridad durante la fase de instalación, asi como la monitorización de comportamientos sospechosos.	7,8	[31] [10]
R5. Integración de la gestión del MUD en la fase de instalación del dispositivo, de manera que se instalen las políticas de seguridad antes de que el dispositivo pueda acceder a los recursos de la red y se reduzca así la superficie de ataque	7,8	[30] [10]
R6.Validación y evaluación de las soluciones propuestas sobre diferentes escenarios y protocolos IoT con el objetivo de verificar su viabilidad	6, 8	[30] [158] [134] [31] [39]

1.3. Resultados

La consecución de los diferentes objetivos de esta tesis ha dado lugar a diversas publicaciones científicas en revistas, conferencias y capítulos de libros que pueden consultarse al final del Capítulo 5. Los principales resultados obtenidos, así como su relación con los objetivos planteados se recogen en la Tabla 1.1. Además, durante la tesis se ha participado en diferentes proyectos de investigación (e.g., ARMOUR, CybserSec4Europe[8]) y en iniciativas europeas relacionadas con la certificación en seguridad, lideradas por entidades como EC o ECSO.

Es importante mencionar que esta tesis se ha presentado en la modalidad por compendio, por lo que los detalles de los resultados se encuentran en las cuatro publicaciones principales que la comprenden. No obstante, a continuación se explican a alto nivel y de manera resumida los principales resultados de cada uno de los artículos del compendio.

1.3.1. Toward a Cybersecurity Certification Framework for the Internet of Things

La primera publicación del compendio [86] analiza en detalle las principales características de los dispositivos IoT que dificultan la evaluación de la seguridad (**R1**). Mientras que por un lado, la gran heterogeneidad de dispositivos complica las comparaciones objetivas en materia de seguridad, por otro lado, la alta dinamicidad a la que están sometidos este tipo de dispositivos, hacen necesario que la evaluación de la seguridad tenga en cuenta el entorno cambiante en el que opera, ya sea debido a una

[8] https://cybersec4europe.eu/

actualización o al descubrimiento de una nueva vulnerabilidad. De esa manera, se hace un análisis de los desafíos que tiene el diseño de un framework de certificación de seguridad para IoT. Este análisis no sólo tiene en cuenta las propiedades analizadas y los esquemas de certificación actuales, sino que también recoge las inquietudes de industria, organismos reguladores y organismos estandarizadores, ya que durante la tesis se ha podido tener contacto con varias de estas entidades. Entre los desafíos de la certificación, destaca la alta variedad de estándares de seguridad y esquemas, que hacen difícil la homogeneización de criterios de evaluación y la comparación entre ellos, así como el uso de métricas que pueden depender del criterio del evaluador. Sin embargo, a pesar de dichas debilidades, el framework debería hacer uso de los puntos fuertes de los estándares existentes y aprovecharse de su aceptación en la comunidad. El proceso de certificación debería ser sencillo, requiriendo la mínima documentación formal posible para entenderlo y aplicarlo y no demasiado caro. Esto es especialmente importante en el entorno IoT, donde el coste de los dispositivos es tan bajo que una certificación que incremente demasiado su coste sería inviable, y donde un retraso excesivo en el lanzamiento del producto al mercado puede derivar en pérdidas económicas para el fabricante. Aunque para evaluar la seguridad se suele tener en cuenta las vulnerabilidades ya conocidas del dispositivo que se está evaluando, en el contexto IoT no hay ninguna base de datos de vulnerabilidades específica. No obstante, cada vez más vulnerabilidades de estos dispositivos son añadidas a la base de vulnerabilidades de referencia, la base de datos nacional de vulnerabilidades (NVD) de Estados Unidos. El contexto donde opere el dispositivo, así como sus componentes y dependencias, y las vulnerabilidades en las diferentes capas de la pila de protocolos, deberían tenerse en cuenta para una correcta evaluación de la seguridad. Sin embargo, hoy por hoy, el mayor problema es la dinamicidad, ya que aunque un dispositivo haya sido certificado como seguro, esto puede cambiar rápidamente, no sólo por una nueva vulnerabilidad, sino por una actualización o un parche. Este hecho, unido a que la cantidad de dispositivos IoT no deja de crecer, hace necesaria una solución escalable y automatizada que permita una recertificación rápida y a bajo coste. Por último, como resultado del proceso de certificación, es necesaria la creación de una etiqueta que aporte información suficiente de una manera visual, sencilla y clara, para que pueda ser interpretada por una persona no experta.

Como una propuesta para lidiar con dichos retos, el artículo propone la metodología de evaluación de seguridad diseñada en la tesis (**R2**), con el objetivo de que pueda servir como base para la certificación. En particular, dicha metodología se basa en el estándar ETSI EG 203 251 [54], en el cual se plantean dos visiones diferentes: una en la que la evaluación del riesgo es asistida por tests, y otra en la que los tests son dirigidos por la evaluación del riesgo. Dichas visiones fueron combinadas y se añadieron aspectos adicionales inherentes a la certificación, como es el concepto de etiquetado.

1.3.2. Risk-based Automated Assessment and Testing for the Cybersecurity Certification and Labelling of IoT Devices

La segunda publicación [87] detalla la metodología de evaluación de la seguridad desarrollada en esta tesis (**R2**) y la instanciación propuesta (**R3**). La metodología toma como punto de partida un conjunto de cinco vulnerabilidades generales (falta de autenticación, falta de autorización, falta de confidencialidad, falta de integridad y falta de disponibilidad), así como vulnerabilidades más específicas que pueden ser obtenidas de bases de datos de vulnerabilidades conocidas. Con el objetivo de tener en cuenta el contexto en el que se va a desplegar el dispositivo, la metodología hace uso del concepto de perfiles de protección, término tomado del estándar de certificación Common Criteria (CC) [151], los cuales reflejan el nivel de riesgo aceptado para cada propiedad y en cada contexto. Esto es debido a que, por ejemplo, la disponibilidad puede ser crucial en un dispositivo sanitario, mientras que en un entorno demótico, no lo es tanto. La principal ventaja de la metodología es el uso del testeo para evaluar el riesgo, en lugar de basarse en listas de criterios que pueden ser interpretadas. La instanciación propuesta para dicha metodología se basa en el uso de tests basados en modelos (MBT) [116], una técnica en la que el sistema objetivo se modela a alto nivel y a partir de ese modelo se generan los tests de una manera automática. Para enlazar los tests a alto nivel con el sistema real se requiere de una interfaz (adaptador) que, una vez implementada, facilita la reejecución y modificación de los tests, agilizando los procesos de reevaluación. Para la ejecución de los tests se propone el uso de TITAN[9], una herramienta que utiliza el lenguaje Testing and Test Control Notation Versión 3 (TTCN3)[10] y sirve para automatizar la ejecución de dichos tests y la obtención de los resultados. Los resultados y las métricas obtenidas de los tests son utilizados junto al estándar Common Vulnerability Score System (CVSS) [43] para obtener un valor numérico del riesgo de cada vulnerabilidad general. El riesgo obtenido se compara con los perfiles disponibles y se representMSPLa en la etiqueta, un diagrama de araña basado en un pentágono, donde los vértices representan las vulnerabilidades y las aristas los perfiles obtenidos. Para lidiar con la dinamicidad de la etiqueta se propone el uso de QR o NFC. Dicha metodología instanciada es usada para evaluar la seguridad de una libreria que implementa el protocolo Datagram Transport Layer Security (DTLS) [163] sobre dispositivos IoT a través de la plataforma FIT IoT Lab[11], que permite llevar a cabo tests sobre dispositivos IoT en escenarios a gran escala de manera remota (**R6**).

1.3.3. Extending MUD Profiles Through an Automated IoT Security Testing Methodology

La tercera publicación [31] se centra en la fase de mitigación de la metodología de evaluación de la seguridad diseñada anteriormente. Para ello, se propone el uso de perfiles de comportamiento, capaces de especificar el comportamiento normal del dispositivo, ya sea para monitorizar comportamientos sospechosos o para aplicar políticas de seguridad que restrinjan el comportamiento del dispositivo a lo esperado, de manera que se reduzca la superficie de ataque. En particular, se usa el estándar MUD, el cual hace uso de listas de control de acceso (ACL) para especificar el comportamiento de un dispositivo a nivel de red. Dicho perfil es definido durante la fase de producción del dispositivo y aporta información relevante durante su fase de operación. El MUD hace uso de términos de alto nivel que permiten definir varios comportamientos de forma compacta; por ejemplo, para indicar que un dispositivo sólo puede hablar con dispositivos del mismo fabricante, se puede usar *same manufacturer*. De esta manera, el MUD abstrae de toda información que depende del escenario donde se instalará, como direcciones IP. Sin embargo, la expresividad del MUD está limitada a ciertos aspectos de red (puertos, protocolos Transmission Control Protocol (TCP) [9] o User Datagram Protocol (UDP) [8] y control de acceso de red), con lo cual aspectos de grano más fino, o referentes a otras capas de la pila TCP/IP, no tienen cabida. En este artículo, proponemos la generación de un MUD extendido a partir de los resultados de la evaluación de seguridad. De esta manera, el MUD es capaz de representar información de seguridad relevante para su configuración como el tamaño de las claves, los algoritmos criptográficos que debe usar, e incluso las conexiones máximas que es capaz de soportar para evitar un ataque de denegación de servicio (DoS) (**R4**). Dicha extensión plantea el desafío de cómo implementar las políticas extendidas en la red de despliegue del dispositivo, especialmente las relacionadas con la autorización de acceso a recursos. Los artículos de investigación hacen uso de la tecnología de redes definidas por software (SDN) para implementar las políticas de acceso a nivel de red. Sin embargo, esta tecnología no permite la implementación de las restricciones de acceso a nivel de aplicación. Por ello (**R5**), en el artículo se propone el uso del estándar eXtensible Access Control Markup Language (XACML), que permite automatizar el proceso de evaluacion de autorizacion usando un efoque basado en politicas y el uso de Concise Binary Object Representation (CBOR) [61] Web Tokens (CWT), integrando Authorization Information Format (AIF) [35]. Los tokens CWT utilizan la notación CBOR, que reduce el tamaño de dicho token y facilita su uso en entornos IoT. De esta manera, cuando el dispositivo quiere acceder a cierto recurso, debe solicitar un token de acceso, que será entregado o denegado dependiendo de las políticas de acceso del MUD extendido. En caso de que el token sea entregado, cuando el dispositivo acceda al recurso, deberá adjuntar el token como prueba de su autorización. Tanto la metodología de evaluación, como la generación del MUD, se evalúan en un escenario IoT con dispositivos reales (**R6**) que tienen implementado el protocolo Ephemeral Diffie-Hellman Over CBOR Object Signing and

[9] http://www.ttcn-3.org/index.php/tools/16-tools-noncom/112-non-comm-titan

[10] http://www.ttcn-3.org/

[11] https://www.iot-lab.info/

Encryption (EDHOC) [52].

1.3.4. Enforcing Behavioral Profiles Through Software Defined Networks in the Industrial Internet of Things

La cuarta y última publicación del compendio [30] se enfoca en la implementación de las políticas del estándar MUD (**R5**) durante la fase de instalación del dispositivo en la red (*bootstrapping* [33]). El estándar MUD define el formato basado en ACL y la arquitectura necesaria para su almacenamiento, obtención, traducción e implementación, pero no especifica los mecanismos y técnicas que se deben seguir para la ejecución segura de dichos procesos. Con el objetivo de cubrir estas necesidades, en este artículo se propone la integración de dichos procesos en el bootstrapping. En particular, la obtención del MUD se integra en el protocolo extensible de autenticación (EAP) [34], enviando el Localizador de Recursos Uniforme (URL) para obtener el MUD en un atributo del mensaje del protocolo de Autenticación, Autorización y Contabilidad (AAA) [72]. De esta manera, la obtención del MUD ocurre cuando el dispositivo ya ha sido autenticado en la red. Cuando la URL se recibe, la entidad principal de la arquitectura MUD, el MUD Manager, se encarga de obtenerlo del servidor del fabricante, así como la firma para verificar su integridad. Para la implementación de las políticas del MUD, se propone una arquitectura para traducir las políticas del MUD a reglas que puedan ser implementadas por los switches SDN. Dicha arquitectura está basada en los componentes del proyecto H2020 ANASTACIA. Así, las políticas MUD son traducidas al lenguaje intermedio de políticas de seguridad (MSPL) [75] que es el que se gestiona internamente en la arquitectura. Para la implementación de dichas políticas, se selecciona un lenguaje al que traducir las políticas MSPL, que en este caso es OpenFlow [74].

En el artículo se propone un caso de uso basado en gemelos digitales, una técnica que consiste en tener una copia virtual de un dispositivo, capaz de emular su comportamiento [5]. En el caso de uso, los gemelos digitales son utilizados para monitorizar la implementación de las políticas del MUD, de manera que la configuración se instale en los gemelos antes que en la red real para detectar posibles inconsistencias entre las políticas del MUD y las políticas ya definidas en la red, y aplicar así mecanismos de resolución de conflictos. De esta manera, las políticas que se instalen en la red real, ya habrán sido probadas y cualquier problema se habrá resuelto, por lo que las operaciones no se verán afectadas.

Finalmente, la arquitectura y los procesos propuestos se han evaluado sobre un escenario con dispositivos IoT reales, analizando la sobrecarga del proceso completo de gestión del MUD con respecto a un mecanismo de bootstrapping usual basado en EAP sobre Protocol for carrying Authentication for Network Access (PANA) [73]. También se estudian cuáles son las fases más restrictivas en materia de tiempo (**R6**) para verificar su viabilidad.

1.4. Conclusiones y Trabajos Futuros

El desarrollo de un framework de certificación es una iniciativa ambiciosa que ha generado un gran interés en todo el mundo, tanto en industria y en investigación, como en organizaciones estandarizadoras y reguladoras. Mientras que en Estados Unidos esta iniciativa está liderada por el NIST, en Europa, tras la aprobación del Cybsersecurity Act, ENISA ha adoptado el rol de liderar la creación de dicho framework. Diferentes retos alientan y, a la vez, frenan el desarrollo del framework de certificación, especialmente en el contexto del IoT. Por un lado, la gran variedad de esquemas de certificación, estándares de seguridad y dispositivos hacen difícil la tarea de comparar y establecer los criterios básicos de seguridad. Esto queda acentuado por el hecho de que los actuales esquemas de certificación de seguridad utilizan métricas subjetivas que pueden interpretarse de manera diversa por diferentes expertos. Además, un mismo dispositivo IoT puede operar en contextos muy diferentes que requieren niveles de seguridad adecuados a dichos entonos, como por ejemplo salud e industria. Por otro lado, la gran cantidad de ataques, vulnerabilidades y amenazas a los que se ven sometidos cada día este tipo de dispositivos deriva no sólo en cambios continuos en la seguridad, sino que involucran a su vez actualizaciones y parches que igualmente afectan a la seguridad certificada con anterioridad. Este hecho no es tenido en cuenta por los esquemas actuales de certificación de seguridad, que certifican de manera estática una versión concreta de un dispositivo, y ésta queda anulada cuando hay un cambio de seguridad. En este caso, se requiere una nueva y completa certificación, con el correspondiente desembolso monetario y gasto de tiempo.

Aunque el establecimiento de dicho framework de certificación aún requiere una coordinación conjunta de todas las partes implicadas, la metodología de evaluación de la seguridad para IoT propuesta en esta tesis está orientada a servir como base para futuras aproximaciones de dicho framework de certificación. Para ello, la metodología se basa en la combinación de la evaluación del riesgo y de tests de seguridad con el objetivo de medir de forma objetiva la seguridad de un dispositivo IoT. Además, dicha metodología ha sido instanciada a través de técnicas que permiten la automatización de los tests, facilitando posteriores reevaluaciones. Para ello, se ha utilizado la metodología MBT, la cual permite generar tests automáticamente a partir de un modelo a alto nivel. Los resultados de los tests alimentan la evaluación del riesgo con el objetivo de medir empírica y objetivamente el riesgo asociado a cada vulnerabilidad. Como resultado de la metodología, se ha propuesto una etiqueta visual y dinámica que lidie con los cambios constantes de seguridad. Finalmente, la tesis ha culminado con el uso de los ficheros MUD como herramienta de mitigación preventiva antes de que el dispositivo tenga acceso a la red. Para ello, se ha propuesto una extensión del estándar MUD, permitiendo la definición de información de seguridad derivada de la evaluación previa, y se ha integrado la gestión y la implementación de las políticas de seguridad del MUD en el bootstrapping del dispositivo. Esta propuesta no sólo permite reducir la superficie de ataque del dispositivo y de la red, sino que también permitiría utilizar el fichero MUD como herramienta para monitorizar comportamientos sospechosos dentro de la red.

Esta tesis abre la puerta a diversas vías de trabajo futuro, algunas de las cuales ya están siendo desarrolladas. En particular, la metodología va a ser extendida de manera que considere también aspectos relacionados con la privacidad, más allá de la seguridad. Además, la metodología se centra en un único dispositivo IoT, por lo que también se va a desarrollar una instanciación más adecuada para sistemas complejos, donde se tengan en cuenta las dependencias entre vulnerabilidades y los efectos cascada. Ligado con esto, se va a analizar la aplicabilidad de la metodología sobre diferentes entornos de especial relevancia, como son los vehículos automáticos y el 5G, enmarcado en proyectos Europeos H2020 como INSPIRE-5Gplus[12]. Para ello, también se hace necesario el análisis de la seguridad de sistemas complejos, por lo que se baraja el uso de árboles de vulnerabilidades y del fichero MUD como mecanismo de creación del grafo de red, de manera que sirva para analizar dichas dependencias. A la hora de formalizar las relaciones entre propiedades y componentes, se está analizando dentro del proyecto H2020 CyberSec4Europe la posibilidad de combinar la metodología con el framework de seguridad desarrollado por el NIST [144].

Relacionado con el MUD, se ha aceptado a fecha de escritura de esta tesis un artículo donde ya se continúa el trabajo realizado [10]. Específicamente, se propone una extensión completa del MUD mediante MSPL para capturar otros tipos de políticas de seguridad, ya sea privacidad, autenticación, autorización, control de acceso o protección del canal. También se proponen mecanismos para realizar la implementación de las nuevas políticas, extendiendo de manera natural el trabajo previo mediante SDNs, tokens CWT y blockchain. En paralelo se está trabajando en colaboración con los autores del draft *Automated IoT Security* [7] para gestionar la seguridad de un dispositivo IoT de manera automatizada durante todo su ciclo de vida, y se está desarrollando una segunda versión más detallada. Específicamente, se está trabajando en la instanciación de los diferentes procesos de gestión de la seguridad (e.g., la evaluación del riesgo, la obtención de información de seguridad de fuentes externas, la monitorización del dispositivo y la configuración de la seguridad).

[12] https://5g-ppp.eu/inspire-5gplus/

Chapter 2

Abstract

2.1. Motivation

In recent years, technology has advanced by leaps and bounds changing our perception of the world and the way we carry out daily actions. One of the paradigms that most impacted in our daily life is the Internet of Things (IoT), which allows quotidian devices to be connected to the Internet with the aim of collecting and sharing information. Thus, we have smart refrigerators that can obtain information about the missing food, manage the shopping list and even shop, or coffee machines connected to our mobile phone that are activated when the alarm rings. This ecosystem of devices has not only brought enormous benefits to the home automation environment, but has also led to an incredible advance in the industry, facilitating, for example, supply chain monitoring processes to guarantee the quality of products. This term, which was coined by Kevin Ashton in 1999 [6], has been further developed thanks to different technologies such as wireless connection or the upcoming 5G era[1], in order to manage data more efficiently and to foster a continuous exchange of information. While in 2019 there were approximately 26.66 billion of IoT devices, in the coming years this trend will continue to rise, with an amount of 74.44 billion devices in 2025, as shown in Figure 2.1[2].

One of the main features of these devices is the low computing capability to increase the battery life that allows the continuous operation of the device. However, this computing capability, together with the low costs, have made that essential aspects, such as security and privacy, are not considered properly, leading to a situation in which an attacker is able to harm a lot of unprotected and interconnected devices. The consequences can be observed in the high increase of the attacks against these devices, from toys to medical devices[3]. In particular, one of the most well-known attacks was the Mirai IoT Botnet, in October 2016[4], when millions of IoT devices (e.g., cameras or digital video recorders) were compromised with the aim of executing a distributed denial of service (DDoS) attack against platforms such as Spotify or Amazon. This caused the interruption of services and therefore significant monetary losses. This attack has been evolved through a large number of variations. Indeed, the 20% of companies reported IoT attacks in the last three years, according to the study performed by Gartner in 2018[5].

[1] https://www.3gpp.org/release-17

[2] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[3] https://www.finance-monthly.com/2019/09/the-worst-and-weirdest-iot-hacks-of-all-times/

[4] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[5] https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018

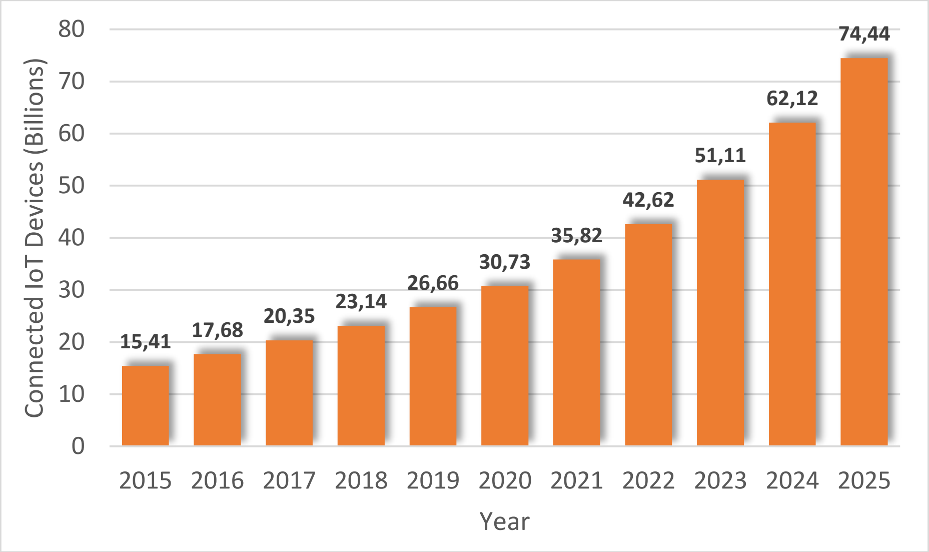


Figure 2.1: Connected IoT Devices: historical and prevision.

This situation highlights the importance of designing adequate protection mechanisms for IoT devices. One of the most ambitious European initiatives to address existing cybersecurity concerns is the establishment of a cybersecurity certification framework. Indeed, the European Union (EU) approved the 27th of June 2019 the *Regulation 2019/881 of the European Parliament and of the Council of April 17 2019 on the European Union Agency for Cybersecurity (ENISA) and on information and communications technology cybersecurity certification* (Cybersecurity Act), which establishes ENISA as the central point for the development of a European cybersecurity certification framework [70]. The main objective of this framework is to guarantee a minimum security level for Information and Communications Technology (ICT) components (including IoT devices), and to communicate the security level of the product to end users, in order to facilitate the comparison of similar devices. Other initiatives, such as the European Cyber Security Organization (ECSO), which encompasses companies, research centers and universities, proposes a meta-scheme for cybersecurity certification [146] through a working group specially focused on certification aspects. In United States, this initiative is led by the National Institute of Standards and Technology (NIST) [144] and, in Japan, the government is managing the development of a cybersecurity framework to give guidance on the implementation of cybersecurity [18].

However, the development of a cybersecurity certification framework is not an easy task, especially in a context like the IoT. The wide variety of metrics, security standards and certification schemes makes difficult the comparison of different security levels. This is especially challenging when such schemes belong to different countries with different regulations and laws. As a consequence, device manufacturers need to certify their devices against several schemes to sell their products in different countries, with the associated monetary investment. The cost of the certification process, together with the effort required for the preparation and execution, make its application unfeasible for low-cost devices. Another significant challenge is the high dynamism inherent to these devices, which can change their operational environment, and could be affected by a plethora of new threats every day. Traditional certification approaches, which are usually static and do not consider any monitoring process, cannot cope with this dynamism. Thus, agile and automated mechanisms are needed to allow a new security evaluation process in a lightweight and cost-effective way when a security change is detected, due to a new vulnerability or a firmware update. In addition, this dynamism also requires a dynamic security label to maintain the security level of the product up-to-date (e.g., with technologies such as Quick Response (QR) codes or Near Field Communication (NFC)), so that non-expert users could understand the label's content, in a similar way to current European energy labels.

Based on previous aspects, a cybersecurity certification framework should have the following properties:

- Harmonization of existing certification schemes and security standards to facilitate the comparison, and to unify the evaluation criteria.
- Usage of standards to define the security certification processes. Although many of these standards have weak points, the framework should take their strengths, and the terminology agreed by the scientific community.
- Consideration of vulnerabilities at all the protocol stack layers as well as the vulnerabilities of all the system components, including an analysis of dependencies and cascading effects.
- Scalable and automated processes to allow a fast and cost-effective re-certification to deal with the security dynamism in case of a new vulnerability or update.
- Lightweight, requiring only the minimum formal documentation to understand and apply it, affordable for the company, and efficient, to avoid affecting the market release of the product.
- Visual and dynamic security label to reflect (in a non-ambiguous but simple way) the result of the evaluation, so it could be understood by a non-expert user.
- Integration of the device context in the security evaluation to facilitate the comparison, since an IoT device can be deployed in different contexts with different security requirements.
- Usage of objective metrics, which do not depend on the security expert, to favor the reproducibility of the evaluation. Metrics that are difficult to calculate, such as the likelihood of exploitation of a vulnerability, should be avoided.

2.2. Goals and Methodology

The previous set of challenges and requirements stimulated the development of this thesis, which has been developed in collaboration with the European project H2020 ARMOUR[6], with the aim of designing a security evaluation methodology for IoT devices. It is intended to serve as a basis for a future certification framework by defining and instantiating the processes related to the security evaluation. The methodology was designed by combining security risk assessment and security testing for an objective risk evaluation. In a second part, the methodology was instantiated through technologies and mechanisms that allow the automation of the processes, facilitating the re-certification, and therefore, dealing with the high dynamism of IoT environments. Finally, we proposed a mitigation mechanism based on behavioral profiles, so that the attack surface of the IoT device can be reduced. The main purpose of this approach is to bring the results of the evaluation to the operation phase of the device. The implementation of this mechanism has been integrated with the results of the European project H2020 ANASTACIA[7]. Finally, the proposed security evaluation methodology has been validated in several scenarios by considering different protocols. Thus, the following objectives have been set for the development of this thesis:

- Objective 1: Analysis of the security evaluation requirements in IoT devices.
- Objective 2: Analysis of the current state of the art regarding security certification, security assessment and testing techniques, and the main European and standardization initiatives.

[6] https://www.armour-project.eu/

[7] http://www.anastacia-h2020.eu/

- Objective 3: Proposal of a security evaluation methodology for IoT devices, taking into account the requirements analyzed in Objective 1.
- Objective 4: Analysis of the main tools and techniques for risk assessment, test design and test execution.
- Objective 5: Proposal for an instantiation of the methodology designed in Objective 2, taking into account the requirements analyzed in Objective 1.
- Objective 6: Validation and evaluation of the proposal in different IoT scenarios.
- Objective 7: Integration of security behavioral profiles, specifically the Manufacturer Usage Description standard (MUD [53]), in the methodology, so that the security evaluation results could be used to mitigate attacks during the devices operation phase.
- Objective 8: Validation and evaluation of the mitigation proposal in IoT environments to demonstrate its feasibility.

These objectives have guided the methodology and the development of the research carried out in this thesis. The first stages were dedicated to analyze which properties of IoT devices hinder the security evaluation process, and the deficiencies of current security evaluation and certification schemes. This process was crucial for determining the way forward during the design of the security evaluation methodology. The participation in EU initiatives, such as ECSO, and the analysis of the efforts carried out by the European Commission (EC), ENISA, the industry and the scientific community, has allowed to align the efforts of the thesis with ongoing institutional efforts in security certification. Furthermore, the proposed methodology is based on standards such as the one from the European Telecommunications Standards Institute (ETSI), the ETSI EG 203 251 [54], which already proposes the use of security tests to increase the reliability of the security risk assessment. The analysis of the current security evaluation and certification mechanisms revealed their shortcomings, especially those related to the dynamic nature of security. Thus, the instantiation of the methodology was carried out taking into account this fact to allow an efficient and automated security re-evaluation. Finally, the MUD standard was used for the instantiation of the methodologys mitigation phase as a mechanism to define behavioral profiles that allow reducing the attack surface during the device's operation phase. The integration with the behavioral profiles was intended to produce useful results for mitigation purposes. Furthermore, we proposed an extension of the MUD standard, as well as an approach to manage the obtaining and enforcement of the MUD security policies during the installation phase of the device. The design, instantiation, deployment and evaluation of the security evaluation methodology, as well as the mitigation phase, are the result of the research carried out in this thesis, which will be explained with more details in the following section.

2.3. Results

The achievement of the different objectives of this thesis has derived in several scientific publications in magazines, journals, conferences and book chapters that can be reviewed at the end of Chapter 5. The main results, as well as their relationship with the already mentioned objectives, are shown in Table 2.1. Furthermore, the thesis has been developed under the umbrella of different research projects (e.g., ARMOUR or CybserSec4Europe[8]), also collaborating in European initiatives related to cybersecurity certification that are led by entities such as the EC or ECSO.

It is worth noting that this thesis has been presented by the compendium modality, so the details of the results are found in the four main publications that comprise it. However, the details of each article are briefly explained below.

[8] https://cybersec4europe.eu/

Table 2.1: Main thesis results

Result	**Objectives**	**Publications**
R1.Analysis of the properties for the security evaluation in the IoT context, and analysis of the deficiencies of current security evaluation and certification schemes.	1, 2	[86] [3]
R2.Design of a security evaluation methodology for IoT based on current standards, combining risk assessment and security testing for an objective security evaluation.	3	[86] [158] [134] [87] [3]
R3.Implementation of the security evaluation methodology for IoT through suitable techniques and tools for this paradigm, to design an automated security assessment, in order to address dynamism, scalability and re-certification aspects.	4, 5	[134] [87] [158] [31]
R4. Integration of the results provided by the security evaluation methodology with the generation of an extended behavioral profile of the device (based on the MUD standard). This approach is intended to help in the security configuration of the device's installation phase, as well as to monitor suspicious behaviors.	7,8	[31] [10]
R5.Integration of the MUD management in the device's installation phase, so that security restrictions are installed before the device can access the network to reduce the attack surface.	7,8	[30] [10]
R6.Validation and evaluation of the proposed solutions in different IoT scenarios and protocols in order to verify their feasibility.	6, 8	[30] [158] [134] [31] [39]

2.3.1. Toward a Cybersecurity Certification Framework for the Internet of Things

The first publication of the compendium [86] details the main properties of IoT devices that complicate the security evaluation process (**R1**). On the one hand, the inherent heterogeneity of IoT devices hinder objective security comparisons. On the other hand, the high dynamism of such devices requires to take into account the evolving environment in which they operate (e.g., due to an update or the discovery of a new vulnerability). This way, the article presents an analysis of the main challenges associated to the definition of a cybersecurity certification framework for IoT. This analysis takes into account current certification schemes, and includes the concerns of industry and regulatory and standardization bodies, which have been contacted during the thesis. Among the challenges of certification, we highlight the high variety of security standards and schemes, which hinder the comparison of evaluation criteria, as well as the usage of subjective metrics that may depend on the experts' criteria. However, despite the weak points, the certification framework should make use of the strengths of existing standards and take advantage of the aspects agreed by the research community. The certification process should be simple and cost-effective, requiring as little formal documentation as possible to apply it. This is especially important in the IoT environment, where the cost of devices is so low that a costly security certification would be unfeasible. Furthermore, an excessive delay in the market release of the product could lead to monetary losses for the manufacturer. Although cybersecurity certification usually takes the security vulnerabilities of the evaluated device at a starting point, there is no specific vulnerability database for IoT. Nonetheless, more and more vulnerabilities from these devices are being added to the well-known National Vulnerability Database (NVD). The context in which the device operates, as well as its components and dependencies, and vulnerabilities at different network layers, should be also taken into account for a comprehensive security evaluation. However, the main current challenge is the security dynamism, since a device can be certified as secure but this condition could change quickly, not only due to a new vulnerability, but also due to an update or patch. This aspect, together with the fact that the number of IoT devices continues to grow, require a scalable and automated solution that allows a fast and cost-effective re-certification. Finally, as a result of the certification process, it is necessary to create a label that provides sufficient information in a visual, simple and clear way, so that it can be understood by a non-expert user.

To deal with some of these challenges, the article proposes the security evaluation methodology designed in this thesis (**R2**), with the aim to serve as a basis for cybersecurity certification. In particular, this methodology is based on the ETSI standard EG 203 251 [54], in which two different views are proposed: one in which security risk assessment is assisted by security testing, and another one in which security testing is driven by security risk assessment. These two visions were combined into a single one and additional aspects inherent to cybersecurity certification were added, such as the concept of labeling.

2.3.2. Risk-based Automated Assessment and Testing for the Cybersecurity Certification and Labelling of IoT Devices

The second publication [87] details the security evaluation methodology for IoT developed in this thesis (**R2**), and the proposed instantiation (**R3**). The methodology takes as a starting point a set of five general vulnerabilities (lack of authentication, lack of authorization, lack of confidentiality, lack of integrity and lack of availability), as well as specific vulnerabilities that can be obtained from vulnerability databases. To take into account the context in which the device will be deployed, the methodology uses the concept of protection profile, which is a term used by the Common Criteria (CC) [151] certification standard to reflect the acceptable level of risk for each security property and for each context. For example, availability can be crucial in a health device, but not in a house automation environment. The main advantage of the methodology is the usage of security testing to assess the risk, instead of relying on checklists that could be interpreted. The proposed instantiation for the evaluation methodology is based on the usage of Model-Based Testing (MBT) [116], in which the system is modeled at a high level, and tests are generated in an automatic way from that model. To link the high level tests with the real system, it is necessary an interface (adapter) that facilitates the re-execution and modification of the tests, so that the re-evaluation processes could be more efficient. For the test execution, we employ TITAN[9], a tool that integrates the Testing and Test Control Notation language Version 3 (TTCN3)[10] to automate the tests execution and the obtaining of the corresponding results. These results, and the metrics derived from the tests, are integrated with the Common Vulnerability Score System (CVSS) [43] standard to obtain a numerical value of the risk for each general vulnerability. This risk is compared with the available protection profiles and it is represented on the label, which is a pentagonal radar chart, in which the vertices represent the vulnerabilities and the obtained profiles are identified by the edges. To deal with the security dynamism, we propose the usage of QR codes or NFC. The instantiated methodology is used to evaluate the security provided by a library implementing the Datagram Transport Layer Security (DTLS) [163] protocol over IoT devices by using the FIT IoT Lab [11] platform, which allows remote IoT device testing in large-scale scenarios (**R6**).

2.3.3. Extending MUD Profiles Through an Automated IoT Security Testing Methodology

The third publication [31] focuses on the mitigation phase of the designed security evaluation methodology. For this purpose, the usage of behavioral profiles is proposed, which provide a way of specifying the normal behavior of the device. This can be used to monitor suspicious behaviors, as well as to enforce security policies that restrict the behavior of the device to what is expected, so that the attack surface is reduced. In particular, we use the MUD standard, which details the behavior of a device at the network level through Access Control Lists (ACLs). The profile is defined during the device's manufacturing phase and provides relevant security information to be considered during its operation. The MUD uses high-level terms that allow defining several behaviors in a compact way. For

[9] http://www.ttcn-3.org/index.php/tools/16-tools-noncom/112-non-comm-titan

[10] http://www.ttcn-3.org/

[11] https://www.iot-lab.info/

example, to indicate that a device can only communicate with devices from the same manufacturer, it is possible to use the term *same manufacturer*. This way, the MUD abstracts from all the information that depends on the domain in which the device will be installed, such as IP addresses. However, the expressiveness of the MUD model is limited to certain network aspects (ports, Transmission Control Protocol (TCP) [9] or User Datagram Protocol (UDP) [8] and network access control), and therefore, more fine-grained security aspects or related to other protocol stack's layers cannot be described. In this article, we propose the generation of an extended MUD file from the results of the security evaluation. This way, the MUD can represent information such as the key size or cryptographic algorithms to be used, and even the maximum number of connections that the device is capable of supporting to avoid a denial of service (DoS) attack (**R4**). The proposed MUD extension poses the challenge of how to implement the extended policies in the device's deployment network, especially those related to authorization access over resources. In general, current research works propose the enforcement of MUD access control policies by using Software Defined Networking (SDN). However, this technology does not allow the enforcement of access control policies at application level. For this reason (**R5**), this article proposes the usage of the eXtensible Access Control Markup Language (XACML) standard, which automates the authorization access evaluation process by using a policy-based approach, and the usage of the Concise Binary Object Representation (CBOR) [61] Web Tokens (CWT), which integrate the Authorization Information Format (AIF) [35]. CWT tokens use CBOR notation, which reduces the token size and is suitable for IoT environments. Thus, when the device wants to access a certain resource, it has to request an access token, which will be granted or denied depending on the access policies of the extended MUD. In case the token is granted, when the device accesses the resource, it has to attach the token as an authorization proof. Both the evaluation methodology and the generation of the extended MUD are evaluated in an IoT scenario with real devices (**R6**) that implement the Ephemeral Diffie-Hellman Over CBOR Object Signing and Encryption (EDHOC) [52] protocol.

2.3.4. Enforcing Behavioral Profiles Through Software Defined Networks in the Industrial Internet of Things

The last publication [30] of the compendium focuses on the MUD policies enforcement (**R5**) during the device installation phase (*bootstrapping* [33]). The MUD standard defines an ACLs-based format and a general architecture for the storage, obtaining, translation and enforcement of MUD files, but it does not describes specific mechanisms and techniques for this purpose. In order to cover these needs, this article proposes the integration of these processes in the bootstrapping phase. In particular, the MUD obtaining is integrated in the Extensible Authentication Protocol (EAP) [34], sending the Uniform Resource Locator (URL) to obtain the MUD file in a messages attribute of the Authentication, Authorization and Accounting protocol (AAA) [72]. This way, the MUD is obtained when the device has already been authenticated in the network. When the URL is received, the main entity of the MUD architecture, the MUD Manager, is responsible for obtaining the MUD file from the manufacturer's server, as well as the signature to verify its integrity. For the enforcement of MUD policies, an architecture is proposed to translate the MUD policies into rules that can be implemented in the SDN switches. This architecture is based on the components of the H2020 ANASTACIA project. Thus, MUD policies are translated to an intermediate policy language, the Medium-level Security Policy Language (MSPL) [75], which is the language managed internally in the architecture. When the MUD policies have to be enforced, a specific language is selected to translate the MSPL policies, which in this case, are implemented using OpenFlow [74].

The article proposes a use case based on digital twins, a technique that consists of a virtual copy of the device to emulate its behavior [5]. In the use case, digital twins are used to monitor the implementation of MUD policies, so that the configuration is installed on the twins rather than on the real network to detect possible inconsistencies between the MUD policies and the policies already defined in the network. This way, the policies that are installed in the real network will have already been tested and any problem will have been resolved, so that the normal operation of the network will not be affected.

Finally, the proposed architecture and processes have been evaluated on a scenario with real IoT devices to analyze the overhead of the complete MUD management process with respect to a usual bootstrapping based on the EAP protocol over the Protocol for carrying Authentication for Network Access (PANA) standard [73]. The most restrictive time phases are also analyzed (**R6**) to verify the feasibility of the solution.

2.4. Conclusions and Future Work

The development of a cybersecurity certification framework is an ambitious initiative that has generated a high interest worldwide, both in industry and research, as well as standardization and regulatory bodies. While in the United States this initiative is led by the NIST, in Europe, after the approval of the Cybsersecurity Act, ENISA has adopted the role of leading the development of such framework. Different challenges encourage and hinder the development of the certification framework, especially in the context of the IoT. On the one hand, the wide variety of certification schemes, security standards and devices harden the comparison and establishment of basic security criteria. This is accentuated by the fact that current security certification schemes use subjective metrics that can be interpreted in a different way by experts. Furthermore, the same IoT device can operate in very different contexts that require a different security level, such as health and industry. On the other hand, the large number of attacks, vulnerabilities and threats associated to IoT devices leads to continuous changes in their security level, and could involve frequent updates and patches that affect the security level previously certified. This fact is not taken into account by current security certification schemes, which statically certify a specific version of a device and this is revoked when there is a security change. Therefore, a new and complete certification process is required, with the associated time and monetary costs.

Although the establishment of a cybersecurity certification framework still requires a joint coordination of all the stakeholders, the IoT security evaluation methodology proposed in this thesis is intended to serve as a basis for future approaches to such certification framework. Towards this end, the methodology combines security risk assessment and security testing in order to objectively measure the security level of an IoT device. Furthermore, the methodology has been instantiated through techniques and tools that allow the automation of the security testing, facilitating subsequent re-evaluations. In particular, the usage of the MBT technique is proposed to generate security tests from a high-level model in an automated way. The results of the tests feed the risk assessment process in order to empirically and objectively measure the risk associated with each vulnerability. As a result of the security evaluation methodology, a dynamic and visual label has been proposed to deal with potential security changes. Finally, the thesis has culminated with the usage of MUD files as a preventive mitigation tool before the device has access to the network. We proposed an extension of the MUD standard, allowing the definition of security information derived from the previous evaluation, and we integrated the management and enforcement of the MUD security policies in the device's bootstrapping. This proposal not only reduces the attack surface of the device, but also allows the MUD file to be used as a tool to monitor suspicious behaviors within the network.

This thesis opens the door to different research lines, some of which are already being explored. In particular, the methodology will be extended to consider aspects related to privacy, beyond security issues. In addition, the methodology focuses on a single IoT device, so we will explore mechanisms to evaluate more complex systems by considering the dependencies between vulnerabilities and cascade effects. Related to this aspect, we will analyze the applicability of the methodology to different environments of significant relevance, such as smart vehicles and 5G, in the scope of European H2020 projects such as INSPIRE-5Gplus [12]. Towards this end, it is also necessary to analyze the security level of complex systems, so we will analyze the use of vulnerability trees and the usage of the MUD file as a mechanism for creating the network graph, so that it can be used to analyze these dependencies. Regarding the formalization of the relationships between properties and components, we consider

[12] https://5g-ppp.eu/inspire-5gplus/

the possibility of combining the proposed methodology with the security framework developed by NIST [144], which is being analyzed within the H2020 CyberSec4Europe project.

Regarding the MUD standard, an article has been accepted at the date of writing this thesis, where the work carried out [10] has been continued. Specifically, a more complete extension of the MUD model is proposed by integrating the MSPL language to capture additional types of security policies (e.g., privacy, authentication, authorization, access control or channel protection). We also proposed mechanisms to carry out the enforcement of the new policies by extending the previous work through SDNs, CWT tokens and blockchain. In addition, we are currently collaborating with the authors of the IETF draft *Automated IoT Security* [7] to automatically manage the security of an IoT device throughout its life cycle. Indeed, we are working on a more detailed version of the draft. Specifically, the research is focused on instantiating the different security management processes for IoT, including risk assessment, monitoring and security configuration.

Chapter 3

Introduction

In the race for the connectivity, we have more and more devices that are connected to the Internet, invading our daily life. This fact has been specially emphasized since the appearance of the IoT, a term that was coined by Kevin Ashton to reflect a way of improving the process of gathering information from the real world, where machines, instead of people, get the information [6]. This is the case, for example, of a fridge that detects the food expiration date and alerts the user by sending her a text message to the mobile phone, or a smart house where different devices can be controlled by the user's voice. Alarms, cameras, home appliances, sensors, Global Positioning Systems (GPS), wearable and physical devices are connected over the world composing the so-called IoT. These devices are intended to improve both the people's daily life and the business environment, by gathering and sharing a massive amount of data ubiquitously. Furthermore, the advent of the 5G technology represents a turning point in the IoT paradigm, improving the connection speed and allowing the exchange of more data in less time. Whereas in 2019 the number of connected devices reached the 26.66 billions, some predictions expect a high growth in the next years, reaching the 74.44 billions of devices in 2025[1].

However, the adoption of the IoT paradigm is obstructed by security and privacy. Some of the main security issues are authentication, access control, attack detection, encryption, integrity and the standardization of the mechanisms employed to protect the device [4]. In 2016, Gartner's survey already pointed security as a key barrier for the 32% of the IT leaders surveyed[2], and a survey performed by the Mobile Ecosystem Forum shows that security and privacy, specially in the home domain, represent the most significant concerns[3]. Only in the first half of 2019, Kaspersky detected more than 100 million IoT attacks[4]. One of the more recent (December 2019) and well-known attacks was performed over a surveillance camera installed in children's room. The hacker acceded to the camera and he was able to see and talk to the children, pretending he was Santa Claus[5]. That was not the first time that connected toys were the target of an attack. A high number of modern toys record the children's voice and their responses for further analysis. This fact harms children's privacy and exposes their responses to hackers interested in obtaining personal information from children, as happened with the VTech company in 2015[6]. Furthermore, in October 2016, the Mirai attack had a significant

[1] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] https://www.gartner.com/smarterwithgartner/the-iot-effect-opportunities-and-challenges-2/

[3] https://www.mobileecosystemforum.com/2016/04/07/trust-related-concerns-hamper-consumer-adoption-iot/

[4] https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019

[5] https://www.bbc.com/news/technology-50760103

[6] https://www.theguardian.com/technology/2015/nov/30/vtech-toys-hack-private-data-parents-children

impact worldwide, in which a network of millions of IoT devices (e.g., webcams) was used to trigger a DDoS attack against big platforms such as Twitter, Github, Amazon or Spotify, taking advantage of by default users and passwords. It caused the interruption of these services for hours, with high monetary loses. In these attacks, the hacked IoT devices are enrolled into a botnet in order to perform other attacks. Based on the Mirai IoT Botnet, different variations have been implemented (e.g., Torii, Hajime or BrickerBot) [76]. The worrying fact is that 20% of the companies adopting an IoT solution have reported a security incident in the last three years, as described in 2018 by Gartner[7].

In this context, there is a need to foster initiatives addressing cybersecurity concerns in an increasingly connected society. Such efforts should be driven by legislative instruments to govern the development of new technological advances [2]. Indeed, at the EU level, the *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on the European Union Agency for Cybersecurity (ENISA) and on information and communications technology cybersecurity certification (Cybersecurity Act)* [70] was approved the 27th June 2019. The Cybersecurity Act, in addition to the General Data Protection Regulation (GDPR) [71] and the Network and Information Security (NIS) directive [19] conform the three main pillars of the EU perspective on cybersecurity. The objectives of the Cybersecurity Act are manifold. On the one hand, ENISA is established as a key point toward the creation and maintenance of a European cybersecurity certification framework. Cybersecurity certification is defined by the U.S. Committee on National Security Systems (CNSS) [51] as a "*Comprehensive evaluation of an information system component that establishes the extent to which a particular design and implementation meets a set of specified security requirements*". In this regard, cybersecurity certification provides a way to increase the trustworthiness and confidence on the security level of a product, which is essential to promote the adoption of current technologies associated to the IoT paradigm. On the other hand, the Cybersecurity Act establishes a regulatory framework, which details the security requirements that EU products and services will have to meet in order to obtain a cybersecurity certificate. As a consequence, it is expected a reduction of the existing market fragmentation in terms of cybersecurity certification schemes. There are other initiatives that are also focused on cybersecurity certification aspects. In Europe, the ECSO, which embraces companies, research centers and universities, is supporting the implementation of the cybersecurity certification framework through a specific working group (WG1: Standardization, certification, labeling, and supply chain management). Indeed, they are working towards the definition of a cybersecurity certification meta-scheme [146]. Beyond the EU, the NIST created in 2014 a Cybersecurity Framework (NIST CPS framework) [144] to provide guidelines to support the management of cybersecurity risks. This framework was based on the Executive Order 13636, "Improving Critical Infrastructure Cybersecurity"[8], and was updated in 2018 to address security requirements in emerging scenarios [143]. Subsequent NIST publications, such as the NIST 800-37-R2 "Risk Management Framework for Information Systems and Organizations" [97], have been aligned to the framework. In Japan, the government developed in 2019 the "Cyber/Physical Security Framework", which provides some security guidelines to protect the industrial society [18]. All these initiatives agree on the importance of cybersecurity certification as a tool to evaluate and compare the security of different products, and therefore, to increase the end user's trust in a hyper-connected society.

In spite of these initiatives, the IoT ecosystem poses several challenges in terms of cybersecurity certification, and specifically, for cybersecurity evaluation. The wide variety of devices and products as well as certification schemes and methodologies, derives on a heterogeneous environment that hardens the objective security level comparison. This problem is exacerbated by out-of-date certificates that are unable to deal with security changes. The dynamism inherent to IoT devices (e.g., security and configuration changes, new vulnerabilities, updates and patches) makes necessary an agile and dynamic certification scheme to manage the security level of a product throughout its life cycle. Furthermore, the certification results should be reflected in a visual and up-to-date way to be understood by non-expert users (e.g., through a cybersecurity label). Finally, the cybersecurity certification scheme

[7] https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018

[8] https://www.dhs.gov/publication/eo-13636-ppd-21-fact-sheet

must cope with the market requirements, providing an agile and cost effective evaluation with the aim of not delaying the market release of the product and still providing a profit margin. In this regard, automated and scalable approaches are crucial to ensure a wide adoption. To overcome these challenges, this thesis presents an IoT cybersecurity evaluation methodology for cybersecurity certification based on International Organization for Standardization (ISO) 31000[9] and ISO 29119[10] standards by combining security risk assessment and security testing as the two main blocks for security evaluation. The design, instantiation and evaluation of the methodology make use of different technologies and approaches for security testing and risk assessment adapted to the IoT landscape. This work has been mainly performed under the umbrella of different EU research initiatives, such as the European H2020 ARMOUR and CyberSec4Europe projects.

The structure of this chapter is as follows: Section 3.1 details and extends the main challenges associated to the definition of a cybersecurity certification scheme. We emphasize the problems associated to the IoT paradigm and provide some guidelines based on such analysis. The related work associated with the main building blocks of the methodology, that is, security risk assessment, security testing and treatment, is presented in Section 3.2. Sections 3.3 and 3.4 present the proposed cybersecurity evaluation methodology, along with the proposed instantiation and the security strategies derived from it. Finally, Section 3.5 provides an overview of the main conclusions derived from this thesis.

3.1. Cybersecurity Certification Challenges

This section analyses and describes the main challenges of cybersecurity certification, with the focus on cybersecurity evaluation aspects and the application on IoT scenarios. This analysis is based on the inputs of several cybersecurity organizations, such as ENISA[11], ECSO[12], the Alliance for Internet of Things Innovation (AIOTI)[13] and DIGITALEUROPE[14], which encompasses the European Industry.

3.1.1. Harmonization

One of the main challenges associated to cybersecurity certification is the wide variety of standards and schemes that currently coexist, as described in an ECSO report [147]. The heterogeneity of cybersecurity certification schemes for products, systems, domains, solutions, services and industries derives on a heterogeneous and confusing landscape of solutions. Therefore, it is quite unclear which security aspects are considered to obtain an adequate security level for a specific context or technology. In this situation, comparability is unfeasible because each scheme uses its own metrics and processes to evaluate a product, specially when products are certified under different national schemes. Furthermore, in some cases, the security standards being used for certification are overlapped, so that confusion is increased.

ENISA already remarked the need for the harmonization of cybersecurity certification to increase the European market competitiveness [152]. Some main concepts linked to the cybersecurity process should be harmonized, such as the stakeholders involved during the process and their roles, or the Evaluation Assurance Levels (EALs), which indicate the depth and rigor of the certification process. Although this effort is led by ENISA, the certification meta-scheme developed by ECSO [146] represents an important initiative towards the aggregation of several certification schemes under a common umbrella.

Currently, the most recognized agreement for certification aspects is linked to the well-known cybersecurity certification standard Common Criteria (CC) [151], in particular, the Common Criteria

[9] https://www.iso.org/iso-31000-risk-management.html
[10] https://www.iso.org/standard/56736.html
[11] https://www.enisa.europa.eu/
[12] https://www.ecs-org.eu/
[13] https://aioti.eu/
[14] http://www.digitaleurope.org/

Recognition Arrangement (CCRA)[15]. However, although this arrangement encompasses a large number of EU Member States (MS) (17 at the date of writing this thesis), some of them are still not part of it.

3.1.2. Standardization

Another important point is to consider current cybersecurity standards, schemes and regulations (e.g., Payment Services Directive (PSD2), electronic identification, authentication and trust services (eIDAS) regulation, GDPR or the NIS directive) as well as best practices and recommendations. Despite their limitations, cybersecurity certification schemes should avoid reinventing the wheel and the overlapping among each other [149]. In this regard, they should be based on essential concepts, terms and operational aspects of well-established schemes (e.g., CC) to foster harmonization and common understanding.

Moreover, the standards for cybersecurity certification should be open and transparent to foster interoperability. Furthermore, missing standards and gaps should be carefully identified before the approval of a cybersecurity certification scheme, as they constitute its basis. This is specially important in the case of emerging technologies associated to IoT or 5G, which are currently evolving [17].

3.1.3. Composition and Aggregation

The cybersecurity certification of complex systems has attracted an increasing interest. Indeed, a single system could be composed of several components performing different functionality. From a certification perspective, it should be possible to reuse the cybersecurity certificates of such components for the cybersecurity certification of the system as a whole. Whereas it is clear that reusing the certificates helps to a more cost-effective certification of the system, some questions arise related to the certification information to be shared, and how it should be disseminated. Specifically, a trade-off should be established between the visibility of the cybersecurity certification data (processes, tests, vulnerabilities, risk level, etc.) and the right of the certification body to protect such data. A certification body could claim that too much visibility of these processes could benefit competing certification bodies. In order to facilitate composition, it is necessary not only the certification information of the system software and hardware components, but also the interactions between them and the system [149]. This is also crucial to detect cascade effects and assess the real security level of the system. In this regard, a European database containing all the information related with cybersecurity certification (e.g., test reports, risk level) would help to come up with a more harmonized cybersecurity certification composition approach. Furthermore, this database could also provide transparency by giving details about the certification process itself.

Also, security composition could be related to the aggregation of vulnerabilities from different layers of the TCP/IP stack. The security certification process should consider the protocol stack to cover vulnerabilities at different layers and provide a complete security evaluation of the product. In fact, the EU RASEN project [140] described a mechanism to aggregate risks from different layers. However, the certification of certain aspects (e.g., physical threats) could be challenging, especially when considering automation aspects.

3.1.4. Scalability, Dynamism and Automation

Cybersecurity is itself a dynamic concept. Indeed, at the end of the cybersecurity certification process, a product can be certified as secure, but this condition could change during its life cycle. Cybersecurity re-certification may be needed because of the certificate expiration, so that a complete re-certification is required, or because of a security change, which could require a partial re-certification. Security changes can be caused by a new discovered vulnerability, or an update/patch that applies to the certified product.

[15] https://www.commoncriteriaportal.org/files/operatingprocedures/cc-recarrange.pdf

However, cybersecurity certification is usually executed over a static security configuration, and any change on the security level of the product implies the invalidation of the certificate. Although more cybersecurity certification schemes consider partial re-certification processes (e.g., Certification de sécurité de premier niveau (CSPN) [142] or the Commercial Product Assurance (CPA) [145]), in most cases, the certification process has to be completely repeated (e.g., in CC, in which even a minor change invalidates the certificate). This situation is specially relevant in the IoT paradigm, in which devices need to be frequently updated,

Indeed, a lightweight re-certification scheme could help to deal with this problem, by using a cost-effective security re-evaluation process. Furthermore, it should take into account the update of the cybersecurity label and certificate to maintain the security level up-to-date. It is also important to analyze when the re-certification process is needed, and which security changes could trigger it. In this regard, complementary approaches are needed to support post-market security monitoring (e.g., by analyzing traffic data) to detect new vulnerabilities that could trigger the re-certification process. Sharing the collected data is also necessary to alert other manufacturers and certification bodies about zero-days threats and enable them to take the proper actions (e.g., a patch) as soon as possible [149]. Furthermore, the use of automated procedures and tools for a fast certification process is also necessary to ensure both the re-certification and the scalability of the process itself. In this regard, technologies and techniques that allow generating tests automatically (e.g., MBT) or the automatic execution of the tests (e.g., TITAN[16]) could help to achieve this goal.

3.1.5. Cost-effective and Lightweight

The cost associated to the cybersecurity certification process is an important barrier for its adoption [29]. On the one hand, the cybersecurity certification could require monetary costs related to the payment to a certification body issuing the certificate, or the testing laboratory being involved in the process. Furthermore, the process can involve qualified personnel to implement the measures required to obtain the certification. In companies with low monetary benefits, cybersecurity certification is not even considered, and for small and medium sized enterprises (SMEs), certification costs may not be affordable. Indeed, an ENISA's survey [16] shows that 52% of the SMEs estimate that the initial cybersecurity certification costs are between 10,000 and 100,000 euros. In fact, 31% of such SMEs prefer self-assessment, and only the 25% rely on a third party certification. On the other hand, the cybersecurity certification process involves a high time consumption, including the preparation for the certification process itself until the results are obtained. This could imply a delay in the market release of the product, with the corresponding monetary losses. The already mentioned ENISA's survey [16] reflects that 60% of the surveyed entities identify the duration of the process as a key barrier for cybersecurity certification. This fact is accentuated due to the complexity of current security certification schemes, which usually require too formal documentation. For the CC certification, the elaboration of the documentation required for security evaluation can take an average time of six months [147]. Therefore, a common language and process would help to have a better understanding, as many companies are not familiar with the processes and documentation needed for each certification scheme.

Based on this, the cybersecurity certification process should be cost-effective and lightweight to foster its adoption, facing the trade-off between the certification assurance level and the costs for the companies, specially for SMEs and startups. It could also help to deal with security changes, by providing a faster and affordable re-certification process.

3.1.6. User Friendly Label

A common problem is the transparency of the cybersecurity certification process, as the end user is often not aware of the processes behind it. Furthermore, because of the complexity of the process, end users are not able to compare the certification results of different products. In order

[16] http://www.ttcn-3.org/index.php/tools/16-tools-noncom/112-non-comm-titan

to address this challenge, a cybersecurity label should provide a simplified view of the cybersecurity certification process to concisely represent the results [149]. Indeed, Bosch [81] already pointed out the need of having a label to provide an understandable and comparable representation of cybersecurity certification results without being swamped by technical details. In this regard, the design of this cybersecurity label has to face an important trade-off. On the one hand, it has to represent the information in a simple and visual way, hiding the complexity of the process. On the other hand, it has to give a complete and non-ambiguous representation of the process results. This is quite challenging; indeed, compared to the European energy efficiency label (which measures a physical magnitude), security aspects are more complex.

Furthermore, as discussed in Section 3.1.4, a cybersecurity certification scheme should manage the security changes over the life cycle of the product [153]. A certified device may be subject to new vulnerabilities or threats, as well as updates and patches that could affect the security level that was previously certified. Therefore, the cybersecurity certification label should reflect the dynamic aspects of the IoT domain. As pointed out by ECSO [146], the cybersecurity certification label should dynamically represent the current security level of the certified product. In this regard, the label could integrate Machine to Machine (M2M) technologies such as NFC or QR codes, which can be easily generated and updated in case of a security change. Furthermore, a dynamic tag could provide the users with additional security information about the product via a smartphone [150]. Other devices could also make use of the electronic information to validate the cybersecurity certificate and even to isolate the device in case its security is compromised.

3.1.7. Context Dependent

The context in which the device will operate during its life cycle, or the nature of the data to be managed, are important factors that determine the security level required in those contexts. For example, while data integrity in a home automation context is relatively important, the health environment could pose additional requirements, because it could have an effect on a person' health status. Furthermore, privacy aspects are also crucial to avoid potential damages derived from the leakage of such information.

Based on these aspects, the cybersecurity certification process must take into account the operational context of the device that must be integrated in the evaluation process, and consequently, reflected in the cybersecurity evaluation. However, this is specially challenging because the context could be unknown when the cybersecurity certification process is performed. Furthermore, IoT devices could have high mobility, so their context could change during their life cycle. In addition, such devices could operate with data of different sensitivity degrees, requiring different treatments to ensure their protection (e.g., temperature data or health status of a patient). In this regard, tools such as the CC security profiles, could help to establish a minimum security level required for a specific context and device.

3.1.8. Objective and Repeatable

Currently, there is no consensus on the guidelines and security requirements that should be mandatory as a cybersecurity certification baseline [149]. Also, there is a lack of consensus regarding the security metrics, which are employed to assess the security level based on the previous security requirements and guidelines. Furthermore, such metrics are usually qualitative, and computed through the evaluation of statements that could lead to a subjective interpretation. Some of the metrics are also difficult to be calculated in an objective way, due to its complexity, as reported in [148]. Indeed some approaches, such as the Common Weakness Scoring System (CWSS) [141], advocate the omission of metrics like likelihood, because they require additional data from the system to be calculated properly. This situation derives on a heterogeneous environment in which cybersecurity certification results may vary depending on how and who evaluates the product.

Based on these aspects, an objective security evaluation and repeatable cybersecurity certification process would increase the trustworthiness on the process and facilitate the comparability. Furthermore, an objective and repeatable process helps to deal with the security dynamism, as the stakeholders could reevaluate the product internally to verify if the security requirements and guidelines are still fulfilled.

These challenges have driven the development of this thesis. While some of them require the collaboration and cooperation between different stakeholders (e.g., manufacturers and regulatory institutions), other aspects need to be addressed by automated mechanisms and tools to foster the adoption of cybersecurity certification processes. For this purpose, the proposed security evaluation methodology for IoT is intended to serve as a basis for future developments of an IoT security certification framework and to give some guidelines on how to address the analyzed challenges through specific mechanisms and techniques for security evaluation. The next section analyzes these mechanisms in the context of the current state of the art, considering the three main pillars of the proposed evaluation methodology: security risk assessment, security testing and risk treatment.

3.2. Related Work

As described in the previous section, we consider security testing, risk assessment and treatment as the main building blocks for cybersecurity evaluation, which are explicitly considered by the ETSI approach [38]. The proposed instantiation is based on different technologies and tools to address some of the main challenges discussed in Section 3.1, but other approaches are also possible to instantiate such methodology. Based on these aspects, this section analyses the different existing approaches and current efforts associated to these key processes.

3.2.1. Security Risk Assessment

Security risk assessment is defined by the CNSS Instruction (CNSSI) 4009 [51] as "*the process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur*". Thus, we consider a risk assessment methodology to determine the risk of a vulnerability, weakness or threat to measure the security level of a certain device, component or system.

Currently, there are several standardized risk assessment schemes to quantify the risk associated to a certain vulnerability. CWSS [141] defines three categories of metrics that are used to calculate the risk (between 0 and 100): the Base Finding, which integrates the weakness's risk; Attack Surface, which integrates the attacker perspective; and Environmental, which integrates information about the context. Furthermore, CWSS can be used with the Common Weakness Risk Analysis Framework (CWRAF) [164] to capture weaknesses associated to a specific business domain. However, some of the CWSS metrics, such as likelihood, are difficult to be calculated [15]. This fact has been taken into account in similar approaches, such as CVSS [42], which advocates for the elimination of such metrics. CVSS also uses three groups of metrics, with a similar meaning: Base, Temporal and Environmental. Furthermore it is a widely used approach, for example in the Common Vulnerabilities and Exposures (CVE)[17], as well as in the NVD that was created by the NIST. A different approach is the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [139], which focuses on operational risk and security practices, not on technological aspects. However, OCTAVE is based on a complex documentation that makes its application difficult and time-consuming. In this regard, there is a more lightweight approach called OCTAVE-S [161]. Other well-known approaches are the DREAD scheme [138] from Microsoft or the OWASP Risk Rating Methodology [162], which is more focused on web applications.

[17] https://cve.mitre.org/

However, these schemes cannot be directly applied to the IoT domain, and therefore need to be adapted to capture all the features of this paradigm, including the high dynamism, as well as scalability and heterogeneity requirements. Furthermore, the metrics of such schemes are still subjective and based on qualitative values. In this regard, there is a high number of research proposals that try to cope with these challenges by adapting existing schemes to the IoT context. For example, CVSS has been adapted to asses the Bluetooth technology [136] by integrating additional security aspects, as well as to the industrial IoT [129], and even the smart home [128] domain. DREAD has been adapted to IoT scenarios to classify and evaluate threats [137] and to specific domains, such as the smart metering [132] or the e-health [126]. OCTAVE has also been applied to the smart home domain [135]. There are also works that instead of limiting the risk assessment to a single scheme, are based on a combination of them. The framework developed in [131] combines CVSS, STRIDE[18] and DREAD schemes, and the authors in [80] use the Microsoft SDL tool and STRIDE for modelling purposes, and CVSS, Open Web Application Security Project (OWASP)[19], HEAVENS [119] and EVITA [120] to assess the risks.

Other works are based on new risk assessment approaches. For example, based on game theory, authors in [133] propose a security framework for e-health to predict and react against attacks, [130] uses an attack tree to measure risks in social IoT. Moreover, graphs and trees are highly used mechanisms to determine the risk of a scenario. In [127], authors use bipartite graphs to address attack propagation. Furthermore, the proposed framework in [124] uses attack trees to model attacks and quantify the risk, and authors in [157] use graphs in the power supply context. Additionally, the research proposed by [123] develops a dynamic risk assessment strategy based on the captured network packets. Finally, authors in [125] propose a risk assessment scheme using an analytic hierarchy process.

As previously described, there is a plethora of works related to risk assessment for IoT scenarios. However, the proposals are usually linked to a specific context and fail to deal with some of the mentioned challenges in Section 3.1, such as the current subjectivity of the evaluation, which makes comparison difficult to be accomplished. The security evaluation methodology proposed in this thesis establishes CVSS as the basis standard for the risk assessment process instantiation, due to its simplicity and wide recognition. To deal with the objectivity challenge of the evaluation, the metrics of the CVSS formula are obtained directly and empirically from the security tests.

3.2.2. Security Testing

Following the definition of CNSSI-4009, "*Security Testing is the process to determine that an information system protects data and maintains functionality as intended*". Security testing is considered one of the key elements for evaluating the security of a Target of Evaluation (TOE). It allows both the validation of certain security properties as well as the discovery of security threats that were not previously considered. Thus, security testing represents an essential process to improve the users' trust in an ICT system. In this regard, there is a high variety of testing strategies and tools that can be used during the different phases of the software development life cycle [118] [98] [66].

One of the most popular techniques is the *penetration testing* [90], in which the TOE is attacked by simulating real world attacks to discover security flaws that an attacker could use to compromise the target. Depending on the available information about the TOE, penetration testing can be based on black-box techniques if the information about the TOE is limited; or white-box, in which the attacker knows the internal details of the TOE. Furthermore, intermediate approaches are also possible. Although it is often performed manually, there are several tools available to automate the penetration testing process, such as vulnerability or port scanners [111]. Current literature shows a plethora of examples of the applicability of penetration testing to the IoT paradigm. In the smart home domain, authors of [27] propose the usage of phantom devices to detect security flaws, whereas in the work proposed by [25], the traffic interception is automated to detect Man in the Middle (MitM) attacks. In specially sensitive domains, such as toys [95] [1], wearable devices [94] or IP cameras [102], the

[18] https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[19] https://www.owasp.org/index.php/OWASP$_{R}isk_{R}ating_{M}ethodology$

penetration testing studies highlight the lack of security and privacy best practices. Some research papers are focused on testing IoT protocols (e.g., IPv6 over Low power Wireless Personal Area Networks (6LoWPAN)) [92] [106] against DoS attacks through the usage of penetration testing tools such as Metasploit [93]. Other authors focus on penetration testing tools and strategies that could be applied to the IoT domain in general. This is the case of [159], which proposes a vulnerability scanner for IoT security testing based on the search engine Shodan [96]. Another approach is represented by the PENTOS tool, which is proposed in [60] to automatically obtain devices' information, in order to execute penetration testing attacks.

Related with penetration, *fuzzing testing* aims to stress the TOE by introducing non-valid data inputs (data fuzzing testing [99]) or behaviors (behavioral fuzzing testing [110]). This can be the case of modifying the message sequence of a protocol. This testing approach benefits from the automation of the existing tools that help to generate random data based on different fuzzers. This approach is widely used to stress IoT protocols [154] [104] [103] by generating invalid messages but also invalid message sequences. This is the case of protocols such as the Constrained Application Protocol (CoAP) [50], Zigbee [28] or 6LoWPAN [155]. However, other applications are also possible, for example to discover memory corruption vulnerabilities [100] or to discover compatibility and performance issues [26].

One of the most simplest strategies for security testing is the *code review*, which is a white testing approach based on finding vulnerabilities in the source code of the TOE. This can be performed manually by an expert or automated through the use of Static Application Security Testing (SAST) [112]. In this case, the tool automatically analyses the source code and reports potential security flaws as well as recommendations to fix them. Although this technique has a really low false negative rate, it is limited to predefined vulnerabilities, and therefore it cannot discover zero-days vulnerabilities, as for example, penetration testing. In IoT, SAST is usually employed to find vulnerabilities in the embedded firmware [23] [24].

To deal with potential security changes, *regression testing* [113] is focused on verifying that any change performed over the TOE does not derive on side effects for the security and functionality of the whole system. As in the previous approach, this technique can be executed manually or using tools to automate the process, as in [82]. Depending on the methodology to select the tests to be re-executed, regression testing strategies can be classified into *test all*, when all the tests are executed, *minimization*, if some tests are removed according to certain criteria, *prioritization*, if the tests are ordered by their importance, or *selection*, if only a subset of the tests are executed.

Finally, *model-based testing* (MBT) [117] is based on the test generation from a high-level model that can represent the TOE and its interactions (behavioral MBT), its environment, or the attacker (attack pattern MBT [114]). This is a key point in the IoT context, as the model can represent any TOE independently of its underlying technology. The definition of the model can be performed using several languages such as formal (e.g., UML), proprietary [115] or Domain Specific Languages (DSL) [68]. Although MBT has been usually linked to functional testing, its usage has been extended to the security context [158], under the name of MBT security testing (MBST) [116]. One of the main features of this technique is the need of an adapter to link the high level model and tests with the real implementation of the TOE. Indeed, the implementation of such adapter represents the most time consuming process of MBT. However, this fact is counteracted by the possibility of generating the tests automatically from the high level model, reducing considerably the implementation time. Indeed, there is a high number of tools that help to automate the test generation [67], such as CertifyIt [91] or MISTA[20]). MBT has been strongly considered in the IoT domain beyond the already mentioned ARMOUR project. In particular, it has been applied to the aircraft domain using DSL to detect injection attacks [68] and to specific protocols (e.g., CoAP [101]), by combining MBT with the automated execution of tests through TTCN3. A similar approach is used in [160]. Following an attack pattern MBT approach, authors in [105] evaluate the security of a real smart meter scenario by modeling the attacker behavior. Furthermore, [107] combines MBT with a service-oriented solution to test IoT systems in the European platform FIWARE[21]. Finally, authors in [14] analyze the coverage of the MBT technique.

[20] http://cs.boisestate.edu/ dxu/research/MBT.html

[21] https://www.fiware.org/

Whereas penetration testing continues leading the testing strategies to evaluate the security of a system, MBT represents a promising approach for the security testing in the IoT domain, due to the possibility of automating the generation of the tests, and therefore, dealing with security changes and scalability aspects [62]. The automation of the test generation and execution, and the simplicity of modeling the TOE at a high level, are the main reasons to consider MBT for the instantiation of the security testing process. Although the implementation of an *adapter* is required, further modifications and repetitions of the tests do not require significant changes of the adapter. However, there is no a silver bullet approach, and an IoT security testing approach could embrace different techniques to deal with the security evaluation challenges during the whole life cycle of a certain device.

3.2.3. Risk Treatment

According to ISO 3100, *"Risk treatment is a risk modification process. It involves selecting and implementing one or more treatment options. Once a treatment has been implemented, it becomes a control or it modifies existing controls".* There are different treatment options proposed by the ISO 3100: avoiding, reducing or retaining the risk, removing the source of risk, modifying the consequences or the likelihood, sharing the risk with others, or even increasing the risk to pursue an objective.

Our treatment instantiation benefits from the security evaluation processes to reduce the risk when the device is installed in the network, in order adjust the device functionality to its intended behavior. In this regard, behavioral profiles, which allow the specification of such intended behavior, are a key mechanism to effectively protect a system by reducing the attack surface, and to detect potential attacks by monitoring the device behavior [22].

Policy-based approaches (e.g., the Policy Core Information Model (PCIM) [20] standard from the Internet Engineering Task Force (IETF)) have been considered traditionally to specify the network behavior of a device, providing a description of the communications allowed to/from a device. Other similar approaches are proposed in [48] and [59], which define a policy enforcement framework to restrict the network communications. Authors also discuss how the network behavior of an IoT device is easily predictable. A more recent standard is the Yet Another Next Generation (YANG) [65] Data Model for Network ACLs [65], which is integrated by the MUD standard [53] to provide manufacturers a way to define and share the network behavior of a device from the manufacturing phase.

MUD is strongly considered by organizations over the world, such as the NIST [47] [46], which has considered the MUD for the creation of a National Thing Behavior Database (NTBD)[22] or other IETF WGs such as the Software Updates for Internet of Things (SUIT) WG, which has recently published a mechanism to align its efforts with the MUD approach [13]. The MUD standard allows the manufacturer to describe the expected network behavior of devices in a scalable and formal way. To this end, the MUD model considers high-level terms to compact the definition of several security policies into a single statement. For example, the high term *same manufacturer* indicates that the security policy applies to all the devices of the same manufacturer, avoiding the manual definition of a security policy per each device, to enhance flexibility and scalability. It also provides mechanisms to extend the MUD model, so manufacturers could express other conditions that are not contemplated in the standardized MUD data model (e.g., Quality of Service (QoS)). The MUD standard has received a significant acceptance degree by scientific community and industry because of the benefits in terms of flexibility and scalability to reduce the attack surface of IoT devices. Because of these aspects, the instantiation of the risk treatment process of the proposed tethodology is based on the MUD standard.

However, the MUD model does not provide mechanisms to describe more fine grained aspects and additional security restrictions beyond the network layer. Furthermore, the MUD standard does not give any indication on how to perform the enforcement of the policies. In this regard, some research papers [63] [58] propose the usage of the SDN paradigm to enforce such restrictions. Furthermore, this integration is supported by the NIST[23]. Authors in [78] also consider an SDN-based framework to enforce network restrictions and mitigate spoofing attacks in smart homes. In addition, [12] describes

[22] https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot

[23] https://github.com/usnistgov/nist-mud

the integration of MUD with a Network Function Virtualization (NFV) approach, which required the extension of the MUD model. However, none of the proposals provide details on how to translate the MUD restrictions and results regarding the evaluation performance. Another challenge related with the MUD standard is the generation of the behavioral profile in an automated way. To cope with this aspect, most of research works use the network traffic to generate the MUD file. Authors in [89] generate the MUD file from the network traffic to protect IoT devices against DDoS attacks. In [57], the authors automate the generation of the MUD from the network traffic by proposing a tool called MUDgee[24]. They have published the profiles generated with this tool[25]. The same authors [79] also use the MUD file to monitor the profiles and detect potential attacks. In addition, a similar approach is proposed in [11]. Our proposal is complementary to these approaches. Indeed, we assume the existence of an already generated MUD file, which is extended from the security testing report, in order to describe additional security aspects, such as the key length, authorization over resources, or cipher-suites. However, as the proposed MUD extension also adds additional restrictions, the enforcement of such restrictions has required additional mechanisms beyond the use of SDNs. Towards this end, we have used a combination of a policy-based approach (XACML) and a capability-based approach to grant authorization tokens. Furthermore, we have integrated the management of the MUD profiles with the bootstrapping of the device, so that the network components can obtain and enforce the MUD restrictions before the device joins the network.

3.2.4. Gap Analysis

Currently, there is not *silver bullet* certification scheme dealing with the challenges associated to the IoT paradigm. The IoT poses specific problems that have to be addressed through the current schemes by adapting the certification process accordingly. However, the fragmented landscape of technologies and protocols and the heterogeneity of IoT devices, products and components make difficult the comparison and the establishment of a common evaluation basis. The problem is exacerbated by current cybersecurity certification and risk assessment schemes that base their security evaluation on security statements or checklists, deriving on subjective interpretations by a security expert. In addition, some of the most well-known schemes are also focused on a specific context (e.g., OWASP, which is focused on web applications), contain metrics difficult to be calculated such as the likelihood (e.g., CWSS) or are proprietary schemes with metrics not approved by the community (e.g., Underwriters Laboratories (UL) Cybersecurity Assurance Program (CAP)). In this regard, the security evaluation methodology proposed in this thesis deals with this challenge by combining security risk assessment and security testing, so that security tests are used to improve the risk assessment, providing empirical and objective metrics to evaluate the associated risk. Furthermore, we also ensure the repeatably of the process. Although composition and aggregation challenges are considered as future work, we are already working on the analysis of dependencies and composition of evaluations through the usage of vulnerability trees.

Moreover, the scale of IoT requires lightweight and flexible approaches to provide an effective and efficient certification approach throughout the life cycle of a device. However, current schemes fail to deal with the security changes that continuously occur during the life cycle. In case of a security change (e.g., due a new vulnerability, update or patch), the certificate is revoked and a complete certification process has to be performed. As an example, a CC certification can take between 6 and 12 months and the cost of the certificate is about 250.000 dollars. In order to deal with scalability and dynamism aspects, the proposed methodology is instantiated through techniques and tools that favor the automation of the evaluation processes. In particular, we use MBT to automatically derive the security tests from a high level model of the TOE, and the execution of the tests is also automated through tools such as JUnit or TITAN. In contrast to checklist approaches, which are performed manually, the automation of the evaluation processes facilitates a cost-effective evaluation, which helps

[24] https://github.com/ayyoob/mudgee

[25] https://iotanalytics.unsw.edu.au/mud/

to increase the certification adoption, as well as the reevaluation process, dealing with the security dynamism.

As previously discussed, the context in which the device operates is an important parameter to be taken into account to foster the comparability between different devices, and to guarantee that the security level is enough for a particular context. The proposed evaluation methodology takes the notion of Protection Profiles (PP) from the CC standard to integrate the context of the device in the security evaluation. These profiles are meant to specify the security requirements for each context. This way, we reflect the differences between the security level required in each context. This aspects enhances comparability of devices that could operate in several contexts.

The evaluation methodology is based on existing standards, following the recommendations we gave in the previous sections to favor the acceptance of the proposal by the scientific community. In particular, the integration between risk assessment and security testing is based on the ETSI EG 203 251 [54], ISO 31000[26] and ISO 29119[27] standards. Nevertheless, we also use additional standards for the instantiation of the methodology, such as CVSS for the risk assessment, MUD for the treatment and CC for the integration of the device's context in the security evaluation. It is worth noting that we also use essential concepts and terms from the widely accepted CC standard, such as PPs, EALs or TOE, to foster the homogenization of the certification process.

At the end of the evaluation process, the proposed methodology generates a cybersecurity label. The label has been designed as a radar chart to be visual and easy to understand for non-expert users. The main idea behind the label is the concept of *more area, more risk*, providing a visual representation of the security level of a product. Furthermore, the label includes a QR code to provide an up-to-date security level, and to give access to additional details of the security evaluation performed over the device. This information can be useful for experts users and to facilitate the composition of certificates for evaluating more complex systems.

Next section describes with details the methodology proposed in this thesis for the security evaluation of IoT devices, which is intended to serve as a basis for the cybersecurity certification. As discussed, the methodology aims to cope with most of the gaps previously discussed, such as the dynamism, the standardization, the context dependency, the need for a visual and dynamic label, and the requirements for an objective and repeatable evaluation process.

3.3. A Risk-based Framework for Automated Cybersecurity Evaluation

The cybersecurity evaluation framework proposed in this thesis was partially developed in the scope of the EU ARMOUR H2020 project, and described in several research publications (e.g., [86] and [87]). It is based on the two ETSI approaches described in [54], which are based on the ISO 31000 standard for *Risk Management* and the ISO 29119 standard for *Security Testing.* These approaches were initially developed in the EU FP7 RASEN project [140] and later standardized by ETSI. Indeed, ETSI describes two approaches to combine *security risk assessment* and *security testing* to improve the security evaluation: a risk-based security testing approach, in which risk assessment is used to improve the security testing; and a test-based risk assessment approach, in which the risk assessment is improved by the security testing process. However, the ETSI approach does not describe potential solutions to integrate both flows or how such processes could be performed.

Indeed, these flows (security testing and security risk assessment) have been further considered in current literature as essential processes for cybersecurity evaluation. Indeed, ECSO considered them as key elements for cybersecurity certification: " ... *It would be convenient to consider a security testing methodology (to) help in [...] the process of updating the certificate in a fast, easy and inexpensive manner. When doing an update or patch, security tests can be executed to assist*

[26] https://www.iso.org/iso-31000-risk-management.html

[27] http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/67/56736.html

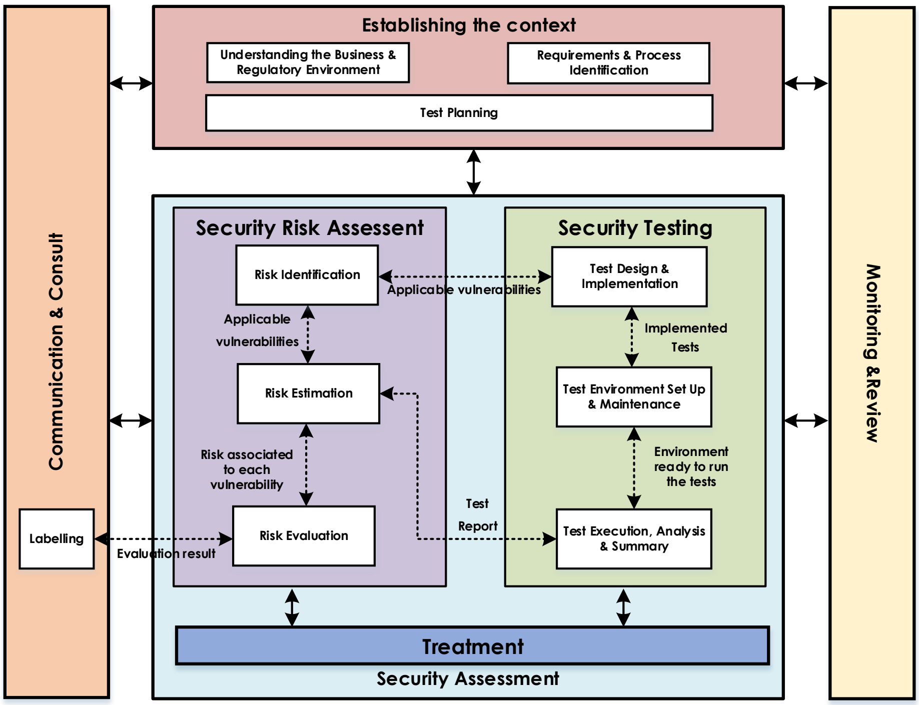

Establishing the context
Understanding the Business & Regulatory Environment
Requirements & Process Identification
Test Planning
Communication & Consult
Monitoring &Review
Security Risk Assesent
Security Testing
Risk Identification
Applicable vulnerabilities
Test Design & Implementation
Applicable vulnerabilities
Implemented Tests
Risk Estimation
Test Environment Set Up & Maintenance
Risk associated to each vulnerability
Environment ready to run the tests
Test Report
Labelling
Evaluation result
Risk Evaluation
Test Execution, Analysis & Summary
Treatment
Security Assessment

Figure 3.1: Proposed methodology for cybersecurity evaluation based on the ETSI risk-based security assessment and testing methodologies [38]

reassessment processes...” [146]. As shown in Figure 3.1, the ETSI approach also considers a previous process called *establishing the context* to analyze the context in which the security is being evaluated (e.g., regulation and business aspects), as well as the test planning (objective, scope, testing technique, etc.). Additional processes named *communicate and consult*, and *monitoring and review* support security risk assessment and testing processes, to react and control the information derived from the overall assessment process. Finally, the *treatment* activity is meant to provide security countermeasures to deal with the vulnerabilities and the risk values obtained through the assessment process.

The proposed security evaluation methodology combines both ETSI approaches, building a framework on top of the two main streams of this proposal: security testing to identify security flaws, and security risk assessment to measure the associated risk by considering legal and business issues. Moreover, the proposed methodology considers additional activities inherent to cybersecurity certification, such as *labeling* (included in the communicate and consult process). As described in the previous section, labeling aspects are considered by regulatory and security organizations, and they are also mentioned in the ECSO meta-scheme [146]. Figure 3.1 shows the integrated vision of the discussed ETSI approaches, as well as the additional aspects considered in the proposal.

According to Figure 3.1, the *establishing the context* process, which integrates the sub-activities from the two ETSI approaches, encompasses the *understanding the business and regulatory environment* and the *requirements and process identification* activities. These activities are meant to analyze the context in which the TOE (e.g., a device) will be operating, and the security requirements of that context. It also includes the *test planning* activity, which comes from the risk-based testing approach. This activity is meant to establish the test strategy by defining the test phases, technologies and procedures that will be used during the *security testing* process.

The *security assessment* process represents the core of the methodology, integrating the *security risk assessment* and the *security testing. Security risk assessment* aims to measure and quantify the security level of the TOE through certain security metrics. This process includes the following activities:

- *Risk Identification*, which identifies potential risks, causes and consequences based on the expert's opinions, historical data, theoretical analysis and stakeholders' needs. Based on the test-based risk assessment approach, *risk identification* is improved by *security testing* by identifying vulnerabilities or particularly critical areas through the use of tools and techniques such as network discovering or vulnerabilities scanners.

- *Risk Estimation*, which determines and quantifies the risk level of the TOE based on the identified risks and vulnerabilities. As the risk estimation is usually a complex, imprecise and subjective activity (it often relies on expert judge), the test-based risk security assessment approach tries to improve the objectivity and trustworthiness of the measurements by using the security testing results (test report) to adjust the risk values.

- *Risk Evaluation*, which compares the risk level obtained during the risk estimation to determine if the risk is acceptable based on certain criteria.

In a similar way, *security testing* process, which aims to detect security failures, comprises three activities:

- *Test design and implementation*, which specifies, designs, implements and derives test cases based on the identified risks. As a result, the tests cases are implemented and assembled to test procedures. Here, *security risk assessment* could provide additional information about the identified risks to systematically determine and prioritize the tests (risk-based security testing approach).

- *Test environment setup and maintenance*, which is meant to set up the scenario in which the tests will be executed (e.g., through the configuration of devices).

- *Test Execution, Analysis and Summary*, which is meant to execute the implemented tests in the scenario. It also includes the systematic analysis and summary of the test results. In case a re-assessment is required (e.g., due to an update or patch), *security risk assessment* could help to prioritize the execution of the tests based on their likelihood of discovering security flaws (risk-based security testing approach).

Both ETSI flows share an additional activity as part of the security assessment process: the *treatment.* This process is intended to provide mitigation and countermeasures to the security flaws discovered during the security evaluation. Some of the actions considered in current standards (e.g. ISO 31000), and oriented to mitigate the risk, are the reduction of the risk through countermeasures, or to divert the risk from one asset to another. The main purpose of this is to distribute the risk within the system or even avoid the risk by stopping the activity, in case it is required.

In addition to the *establishing the context* and *security assessment* processes, the ETSI proposal considers two activities to manage the security information flows during the TOE's life cycle. In particular, they are intended to set up the management perspective by continuously reacting, controlling and improving all the security evaluation process. On the one hand, the *monitoring and review* process obtains information from external sources that could be relevant for the evaluation process (e.g., a new vulnerability or a new regulation). On the other hand, the *communicate and consult* process is aimed to disseminate the information related with the internal process and the security level achieved. As part of this process, we have considered the *labeling* activity, which is meant to create a visual and simple security label with the security evaluation results.

Based on the proposed methodology derived from both ETSI approaches, Section 3.4 proposes an instantiation of the main building blocks through different tools and technologies. Indeed, it is meant to set up the basis for the creation of a lightweight and efficient IoT cybersecurity evaluation and certification, coping with some of the gaps analyzed in Section 3.1.

Table 3.1: General vulnerabilities for the security evaluation process

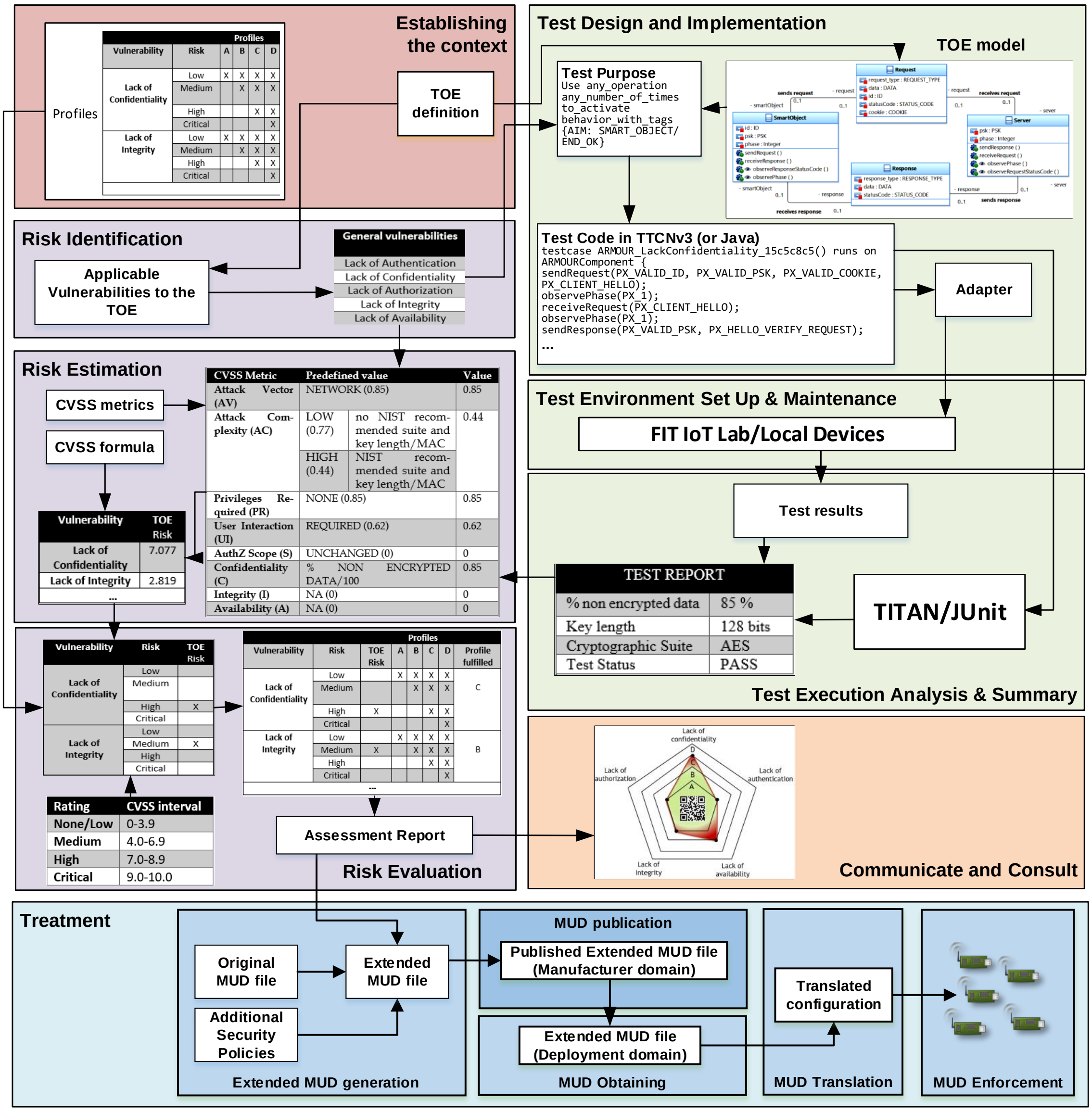
Vulnerability	**Description**
Lack of confidentiality	Transmitted data should be read only by legitimate endpoints.
Lack of integrity	Transmitted data should not suffer modifications during transmission, and in case it happens, any change should be detected.
Lack of availability	Exceptions, errors and overloads should be controlled to avoid faults that affect the endpoints.
Lack of authentication	The endpoints should be legitimate.
Lack of authorization	Endpoint services should be accessible only to endpoints who have the right to access them.

3.4. Framework Instantiation for Evaluating IoT Cybersecurity

This section presents the proposed instantiation based on the methodology described in Section 3.3 and developed in the research articles [87] and [86], which explain the application of the methodology instantiation to two specific security protocols: EDHOC [52] and DTLS [163]. Furthermore, the instantiation has been partially developed in the scope of the EU H2020 ARMOUR project. The approach is meant to address some of the gaps previously described. On the one hand, the methodology based on the ETSI approach provides a common and high-level framework to evaluate and manage the security level of the TOE during its life cycle. It should be noted that, while the instantiation of the monitoring process is not addressed (indeed, it is part of our future work), it is meant to provide a continuous information entry point about new vulnerabilities, updates, patches or any other relevant security information that could affect to the risk level of the TOE. If required, the monitoring process could trigger automatically the security assessment process to perform a re-certification. As a result, the security level is updated in the label and certificate through the *communicate and consult* process. On the other hand, the instantiation is intended to automate as much as possible the process of the security evaluation by using suitable mechanisms and tools to deal with the security dynamism inherent to IoT scenarios. In this regard, the automation of the security evaluation allows the update of the security label and certificate in a lightweight and cost-effective way, reducing the complexity of the certification process. Finally, the context is integrated in the security evaluation process through the so-called protection profiles, which reflect the security level necessary for a specific context and TOE. This aspect is intended to foster the comparability between security aspects of different contexts, which usually require different security levels.

As already mentioned, the security evaluation proposal intends to evaluate the security level of a certain TOE. Although the TOE is defined by CC as *a set of software, firmware and/or hardware possibly accompanied by guidance*, we also consider its configuration (i.e., a specific protocol, libraries, cryptographic parameters, etc.) as part of the TOE, as well as the context in which it is intended to operate. Also, it is important to mention that the security evaluation approach takes as starting point a set of applicable vulnerabilities against which the TOE will be evaluated. These vulnerabilities can be extracted from public vulnerabilities databases, such as the NVD, and/or from a more generic set, as considered by the oneM2M initiative [21]. Then, the resulting set of specific vulnerabilities is mapped to five general security vulnerabilities described in Table 3.1, which are used to evalute the TOE's security level. Indeed, a detailed mapping of the oneM2M vulnerabilities can be found in [87]. These general vulnerabilities have been extracted from existing literature [121] [122] [165] to provide a simplified view of the security aspects. Furthermore, the mapping of such vulnerability to the five general vulnerabilities is intended to facilitate the visualization of the results in a multi-dimensional security label, in order to measure the risk associated to the lack of a certain security property.

Figure 3.2 shows an overview of the proposed instantiation, which will be further explained in the next subsections, as well as the tools and mechanisms employed for each process. As already



Test Purpose

```
Use any_operation
any_number_of_times
to_activate
behavior_with_tags
{AIM: SMART_OBJECT/
END_OK}
```

Test Code in TTCNv3 (or Java)

```
testcase ARMOUR_LackConfidentiality_15c5c8c5() runs on
ARMOURComponent {
sendRequest(PX_VALID_ID, PX_VALID_PSK, PX_VALID_COOKIE,
PX_CLIENT_HELLO);
observePhase(PX_1);
receiveRequest(PX_CLIENT_HELLO);
observePhase(PX_1);
sendResponse(PX_VALID_PSK, PX_HELLO_VERIFY_REQUEST);
...
```

Vulnerability	Risk	Profiles A	B	C	D
Lack of Confidentiality	Low	X	X	X	X
	Medium		X	X	X
	High			X	X
	Critical				X
Lack of Integrity	Low	X	X	X	X
	Medium		X	X	X
	High			X	X
	Critical				X

General vulnerabilities
Lack of Authentication
Lack of Confidentiality
Lack of Authorization
Lack of Integrity
Lack of Availability

CVSS Metric	Predefined value		Value
Attack Vector (AV)	NETWORK (0.85)		0.85
Attack Complexity (AC)	LOW (0.77)	no NIST recommended suite and key length/MAC	0.44
	HIGH (0.44)	NIST recommended suite and key length/MAC	
Privileges Required (PR)	NONE (0.85)		0.85
User Interaction (UI)	REQUIRED (0.62)		0.62
AuthZ Scope (S)	UNCHANGED (0)		0
Confidentiality (C)	% NON ENCRYPTED DATA/100		0.85
Integrity (I)	NA (0)		0
Availability (A)	NA (0)		0

Vulnerability	TOE Risk
Lack of Confidentiality	7.077
Lack of Integrity	2.819
...	

TEST REPORT	
% non encrypted data	85 %
Key length	128 bits
Cryptographic Suite	AES
Test Status	PASS

Vulnerability	Risk	TOE Risk
Lack of Confidentiality	Low	
	Medium	
	High	X
	Critical	
Lack of Integrity	Low	
	Medium	X
	High	
	Critical	

Vulnerability	Risk	TOE Risk	Profiles A	B	C	D	Profile fulfilled
Lack of Confidentiality	Low		X	X	X	X	C
	Medium			X	X	X	
	High	X			X	X	
	Critical					X	
Lack of Integrity	Low		X	X	X	X	B
	Medium	X		X	X	X	
	High				X	X	
	Critical					X	
...							

Rating	CVSS interval
None/Low	0-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Figure 3.2: Proposed instantiation of the methodology for cybersecurity evaluation

mentioned, it is worth noting that the instantiation of the monitoring process is considered as part of our future work in this area.

3.4.1. Combining Security Risk Assessment and Security Testing

The first phase of the process, called *establishing the context*, is composed by three different activities to set up the security evaluation and certification process by gathering information related with the TOE's context. Firstly, the *understanding the business and regulatory environment* analyses the security level required in a particular domain (e.g., health, industry, military, etc.), and the regulation and directives that have to be met (e.g., GDPR). These requirements are processed to create sets of baseline requirements for different levels, linked to the domain and the nature of the data being managed. From the identified requirements, the *requirements and process identification* will define a set of security profiles (A, B, C, D) similarly to the European energy labels [85] to indicate the acceptable risk level (low, medium, high and critical) for each general vulnerability to obtain the associate profile in a specific domain. An example of profile definition can be found at the beginning of Figure 3.2. For that domain, if the TOE obtains a high risk for the lack of confidentiality, it will only be able to obtain profiles C or D. This way, the context is integrated in the security evaluation process by means of the security profiles, coping with one of the challenges previously mentioned. Finally, the *test planning* activity, analyses the security requirements of the TOE and establishes a testing strategy according to them. This process can also interact with the *communicate and consult* and *monitoring and review* processes, in order to update the security profiles according to the current regulation and the evolving requirements of the different domains.

The second and main process of the evaluation methodology, *security assessment*, is intended to be instantiated through automated tools and methodologies for the security test generation and execution. The main purpose is to automate as much as possible the *security testing* and *security risk assessment* processes to address the requirements associated to frequent security changes. Whereas security testing aims to develop a test suite to validate and obtain information about the TOE security, risk assessment is intended to measure the risk associated to the TOE based on the information obtained from such tests. The risk value is used to select the profile fulfilled by the TOE that is defined in the previous *establishing the context* phase. It is worth noting that this thesis presents a concrete instantiation of the security evaluation methodology, but other instantiation approaches (based on different tools and mechanisms) are also possible.

As a first step, the *risk identification* activity analyses and selects the vulnerabilities applicable to the TOE. The set of TOE-specific vulnerabilities (e.g., obtained from a vulnerability database or any other external source) are mapped to the five general ones to aggregate their risk measurements at the end of the process. The main goal is to obtain a unified risk value for each general vulnerability. The selected vulnerabilities drive the security test definition, and identify the elements to create a high-level model of the TOE.

Then, the *test design and implementation* is focused on the development of a test suite, and it is automated following the MBT approach, which generates automatically the test suite from a high level-model of the TOE and a series of test purposes [109]. This approach is well-known because of its benefits for systematic compliance testing [108]. Our approach makes use of a subset of the Unified Modeling Language (UML) class diagrams [117] to model the architectural components of the TOE scenario (e.g., endpoints, messages, attackers, etc.), and the relationships between them. Furthermore, we use the Object Constraint Language (OCL) [156] to specify the TOE's behavior (e.g., its operations). Figure 3.2 shows the TOE model (an scenario implementing the DTLS protocol) composed by two endpoints, *smart object* and *server*, and two message entities, *request* and response. The test purposes are defined through the tool CertifyIt [91] by referring to the high-level model components and operations. As shown in Figure 3.2, there is no need for a complete definition of the tests. Instead, we can define tags in the OCL behavioral specification of the operations (e.g., *SMART_OBJECT/END_OK*) and use them in the test purposes to indicate that we want to reach a specific point of the scenario execution (e.g., a successful DTLS exchange). This way, CertifyIt generates all the intermediate steps to complete the test, so it requires less time to define the security tests. The tool allows exporting the high-level tests in several languages such as Extensible Markup Language (XML), Portable Document Format (PDF), JUnit, and TTCN3. In particular, we use TTCN3 [87] and JUnit [86]. Whereas TTCN3 offers a standardized testing language to automatically execute the tests, JUnit presents a well-known approach based on the Java programming language. CertifyIt also produces a series of interfaces, named *adapters*, to link such tests with the real implementation of the TOE. Therefore, the adapter has to be implemented to link the high-level operations with the real operations associated to the TOE. Although this represents the most time-consuming activity of the process, once the adapter is implemented, the addition of new tests and vulnerabilities sightly affects it. This aspect is crucial to deal with the security dynamism and the potential need of a re-evaluation process in IoT scenarios.

The *test environment set up and maintenance* sets up the execution environment of the test suite. This thesis uses physical local devices in [86] as execution environment, as well as the large-scale infrastructure FIT IoT-Lab platform[28] (with about 200 nodes) in [87]. In both cases, this activity involves selecting the physical devices and uploading the code.

After the tests are implemented, they are executed during the *test execution, analysis and summary*. If the tests were exported in JUnit, they can be executed in a Java platform (e.g., ECLIPSE), whereas if the tests were generated in TTCN3, they can be executed in a compilation and execution environment named TITAN. Both approaches are used to send different test commands to the real TOE through the adapter to execute the tests. At the end of the process, the test report collects the information obtained from the tests (e.g., if the test failed or passed, errors, sniffer information, etc.). Towards this end, a standardized, flexible and expressive format is key to guarantee the homogenization of the results, which are generated from different assessment approaches, in order to facilitate the comparison among them. For this purpose, we propose the use of the Extensible Configuration Checklist Description Format (XCCDF) [37], which is a standardized format defined by the NIST as part of the Security Content Automation Protocol (SCAP) [41]. XCCDF is based on XML to describe security checklists, configuration and benchmarks, allowing the representation of the assessment results. Furthermore, although this is out of the scope of this thesis, XCCDF can also be used to automate the checklist verification through the Open Vulnerability and Assessment Language (OVAL) [40]. Despite the limitations of XCCDF, specially in the IoT domain [69], SCAP is evolving towards a new version with a special focus on the IoT environment support [49].

The test report is used as input for the *risk estimation*. The information collected from the tests is mapped to the CVSS [42] metrics to obtain a numerical risk value. An example of this mapping is shown in Figure 3.2 (e.g., the percentage of non-encrypted data is mapped to the confidentiality metric). A more detailed explanation of this mapping can be found in [87]. CVSS is a risk assessment standard widely used in vulnerability databases such as the NVD. The CVSS metrics are combined in a formula to obtain the risk associated to a vulnerability. By integrating the tests results in the risk calculation, the measurement is performed in an objective and empirical way.

Finally, the *risk evaluation* compares the risk obtained in each general vulnerability with the profiles available for the TOE. Figure 3.2 shows the comparison for the lack of confidentiality and integrity. In this case, the TOE obtained a high risk in confidentiality, which fulfills profiles C and D. This process is repeated for each general vulnerability to obtain a security profile for each of them.

As a result of the security evaluation process, a cybersecurity label is generated. The label integrates the information about the context in which the TOE has been certified by means of the security profiles and the risk obtained for each vulnerability. Also, it indicates the rigor and depth of the security evaluation by using the EALs, which are specified by CC. The label has been designed as a pentagonal radar diagram to support the visualization of the security dimensions (i.e., the five general vulnerabilities) and to provide a visual representation that could be understood by non-expert users. The intersection of the vulnerabilities with the different profiles creates an area that represents the risk, with the meaning of *the more area, the more risk*. Figure 3.2 shows an example of the proposed label, which follows ECSO recommendations by integrating a QR-code to deal with future updates of the label.

3.4.2. Treatment Through the Usage of MUD Files

The proposed security evaluation measures the security level associated to a specific TOE, and it is also intended to identify the main security gaps that could be addressed to increase the TOE's security level. In this regard, the *treatment* process has been instantiated as a preventive mechanism to protect both the TOE and the network in which it operates, since the device associated to that TOE is installed in the network (*bootstrapping process*). Toward this end, we propose the use of behavioral profiles that describe the expected behavior of a device during its operational phase. In particular, we use the IETF MUD standard [53], which provides a data model so that manufacturers could represent

[28] https://www.iot-lab.info/

the allowed/denied communications from/to their devices in a scalable and flexible format. The MUD architecture is composed by four main components:

- Thing or Device, which is in charge of sending a MUD URL to indicate where its MUD file is stored.
- Router or Switch to which the device is connected.
- MUD Manager, the main entity to manage MUD files, which is in charge of the processes required for obtaining and enforcing the different security restrictions described in a MUD file.
- MUD File Server, which hosts the MUD files of a particular manufacturer.

Whereas in this thesis MUD files are mainly used to configure the device before it joins the network, MUD restrictions could be also used to monitor the device's behavior to find suspicious behaviors or ongoing attacks.

The MUD standard has attracted the attention of several standardization organizations such as the NIST in U.S., which envisages the MUD as a potential approach to protect IoT devices from DoS attacks [47] [46]. Furthermore, the NIST proposes the usage of this standard for the creation of a vulnerability behavior database[29].

A manufacturer can use the MUD standard to specify the allowed accesses to specific cloud services, between devices of the same manufacturer or devices being managed by the same controller. For this purpose, the MUD data model considers specific high-level terms. The approach also allows the specification of protocols and ports for the communications, and it provides mechanisms to extend the MUD model, so manufacturers could express other conditions that are not contemplated in the standardized MUD data model (e.g., QoS). However, beyond network aspects, the current specification does not provide the possibility of defining more fine-grained security aspects, such as cryptographic algorithms or specific key lengths to be used. Also, although the standard describes an approach to define the network behavioral profile of a device, it does not specifies how to perform the enforcement of such security policies. However, the use of standard technologies for the enforcement process is crucial to increase the usage and deployment of the MUD standard.

To cope with such issues, this thesis proposes the extension of the MUD model to add more fine-grained security details, and additional aspects beyond network access control, such as resource authorization. As shown in Figure 3.2, the extended MUD file is generated (*Extended MUD generation* phase) from the security assessment process. Then, such file is published in the MUD File Server (*MUD publishing* phase). The extended MUD file is obtained (*MUD obtaining* phase) during the bootstrapping, and translated and enforced in the deployment network in which the device will be operating (*MUD translation and enforcement phases*). The description and proposed instantiation of these phases will be described in the next subsections.

Extended MUD Generation and Publication

In this section, we describe the proposed extension for the MUD model to identify and describe a broader range of security aspects. The main purpose is to protect IoT devices through security features, which are described in the manufacturing phase, and the security evaluation results. Toward this end, we generate the extended MUD file by using the original MUD file (i.e., based on the standard MUD model) associated to the device, as well as the assessment report, which was obtained during the security assessment process. This is shown in the *Extended MUD generation* phase of Figure 3.2. Therefore, the proposed extension integrates the results of the evaluation process in the MUD file to create a more expressive MUD model. The extended MUD describes additional security aspects (e.g., cryptographic algorithms and cipher-suites) to allow/deny a communication. Furthermore, beyond network configuration, the extended model also provides mechanisms to control the access to specific resources hosted by a certain device.

[29] https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot

The MUD model defines the network restrictions by using policies or ACLs. Some examples could be “allow communication between devices of the same manufacturer” or “deny the access from any device through a specific port”. In particular, the model is based on the YANG standard and JavaScript Object Notation (JSON) [64] for serialization purposes. A standard MUD file uses two main containers: “mud” and “acls”. The first one describes aspects related with the MUD file itself, such as the MUD URL (“mud-url”) to identify the MUD file’s location, the generation date (“lastupdate”) or the expiration date (“cache-validity”). This container also includes a reference to the name of the ACLs restricting the communication from/to the device. The ACLs are defined in the second main container, “acls”, and they are classified according to the nature of the restrictions (“to-device-policy” and “from-device-policy”). The YANG model is augmented in the MUD standard to add more expressive and high-level terms such as “manufacturer” and “same-manufacturer”, which allow the definition of a high number of restrictions by using a single statement. Other terms, such as ‘controller” or “local-networks”, make reference to typical network components without the need of using an IP address, in order to abstract the MUD specification from the network implementation details.

Listing 3.1: Proposed MUD extension

```
module: ietf-access-control-list
   +--rw access-lists
      +--rw acl* [name]
      |  +--rw name
      |  +--rw type?
      |  +--rw aces
      |  +--rw ace* [name]
      |     +--rw name
      |     +--rw matches
      |     |  +--rw mud
      |     |  |  +--rw manufacturer?
      |     |  |  +--rw same-manufacturer?
      |     |  |  +--rw model?
      |     |  |  +--rw local-networks?
      |     |  |  +--rw controller?
      |     |  |  +--rw my-controller?
      |     |  +--rw direction-initiated?
      |     |  +--rw eth?
      |     |  +--rw ipv4?
      |     |  +--rw ipv6?
      |     |  |  +--rw dscp?
      |     |  |  +--rw ecn?
      |     |  |  +--rw length?
      |     |  |  +--rw ttl?
      |     |  |  +--rw protocol?
      |     |  |  +--rw (destination-network)?
      |     |  |  +--rw (source-network)?
      |     |  |  +--rw flow-label?
      |     |  +--rw tcp?
      |     |  +--rw udp?
      |     |  |  +--rw length?
      |     |  |  +--rw source-port
      |     |  |  +--rw destination-port
      |     |  |  +--rw application-protocol?
      |     |  +--rw icmp?
      |     |  +--rw [application-protocol-name]?*
      |     |  |  +--rw application-protocol?
      |     |  |  +--rw num-connections?
      |     |  |     +--rw operator
      |     |  |     +--rw value
      |     |  |  +--rw keys?
      |     |  |     +--rw alg*
      |     |  |     +--rw crv?*
      |     |  |     +--rw key_ops*
      |     |  |  +--rw resource?*
      |     |  |     +--rw url*
      |     |  |     +--rw ace* [name]*
      |     |  |        +--rw name
      |     |  |        +--rw matches
      |     |  |        |  +--rw action
      |     |  |        |  +--rw ...
      |     |  |        +--rw actions
      |     |  |        +--rw statistics
      |     |  +--rw egress-interface?

      |     |  +--rw ingress-interface?

      |     +--rw actions
      |     |  +--rw forwarding
      |     |  +--rw logging?
      |     +--rw statistics
      +--rw attachment-points
```

In particular, we extend the “acl” container by adding additional terms and fields, which are highlighted (in bold) in Listing 3.1. For the sake of clarity, some fields have been omitted in the listing. A complete scheme of the original MUD model can be found in [65]. We followed a similar approach to the original MUD model to integrate the new fields. Specifically, the block concerning the network-layer protocol (e.g., IPv4/IPv6) has a reference to the transport-layer protocol (e.g., TCP or UDP) through the "protocol" field. This protocol is further detailed in a particular block to describe the allowed/denied communications, and additional information (e.g., port numbers). We follow this embedded scheme by adding an additional field named "application-protocol" (line 34 of Listing 3.1), which references the application-layer protocol. As several application layer protocols can be used, this field can be repeated, in case it is required. The restrictions associated to an application-layer protocol are detailed in a different block (lines 36-46).

As part of the "application-protocol" block, we have defined three main properties. The first one, "num-connections" (line 38), is intended to restrict the number of simultaneous connections that the device could support before collapsing. It has an "operator" to indicate *equal, less than or grater than* (as described in [65]), and the "value" itself. It should be noted that this field is directly obtained from the availability tests of the security assessment process. The second property, "keys" (line 41), is related to the cryptographic parameters of the protocol. Specifically, it makes reference to the name of the cryptographic algorithm ("alg") following the JSON Web Algorithms (JWA) [55] standard; the intended use of the key ("key_ops"), based on the JSON Web Key (JWK) [56] standard; and the curve ("crv") in case of using elliptic curve cryptography. Finally, the third property, "resources" (line 45), restricts the access to certain resources hosted or accessed by the device. Specifically, this block includes the URL to the resource ("url"), which can be repeated for each resource, and the Access Control Entry (ACE) restrictions applicable to each of them ("ace"). The ACE data model has been extended by allowing the use of the MUD high-level terms (e.g., same manufacturer, controller, etc.). Furthermore, we define an additional field, "action", to detail the specific allowed/denied action (e.g., POST, PUT, GET) for each resource. We developed an example of MUD generation that is applied to the EDHOC protocol in [31].

As already mentioned, the extension of the MUD model is intended to describe more fine-grained security aspects, such as cryptographic details, as well as additional aspects to network-layer restrictions, such as resource authorization. It should be noted that the MUD standard does not describe the processes required for the enforcement of security restrictions. Furthermore, as previously described, we added a set of additional restrictions. Therefore, there is a need to define an approach dealing with this aspect that is addressed in the next section.

Extended MUD Obtaining, Translation and Enforcement

The proposed architecture and the main interactions between the components to manage the extended MUD files are described in Figure 3.3. In particular, we integrated the MUD management aspects with the bootstrapping process of the device, in which it is authenticated to access a network. This way, the restrictions described in the MUD file will be enforced before the device is able to interact with other network components, in order to reduce the attack surface. We also leverage the potential integration of the MUD standard with the Software-Defined Networking (SDN) paradigm for the automated and dynamic enforcement of the security restrictions, as we discussed in Section 3.2. Therefore, the architecture proposed in Figure 3.3 combines the standardized MUD architecture with the SDN paradigm and the bootstrapping process.

The *device authentication* represents the first phase of the bootstrapping process. For this purpose, we use a lightweight approach based on the EAP [34] protocol and the AAA Framework [72]. EAP represents a flexible authentication approach that allows several authentication mechanisms or *EAP methods* (e.g., EAP-PSK based on pre-shared keys or EAP-TLS based on Transport Layer Security). In particular, we use the EAP-PSK method, which does not require public key cryptography but pre-shared keys (PSK), and therefore, it is suitable for constrained scenarios. As shown in Figure 3.3, the EAP session is established between the EAP Peer and the EAP Server through the Authentication Agent acting as an intermediate entity. During the authentication phase, the EAP peer and EAP server exchange several messages with the aim of authenticating both endpoints. On the one hand, for the transport of the EAP messages between the EAP peer and the authentication agent, we use the

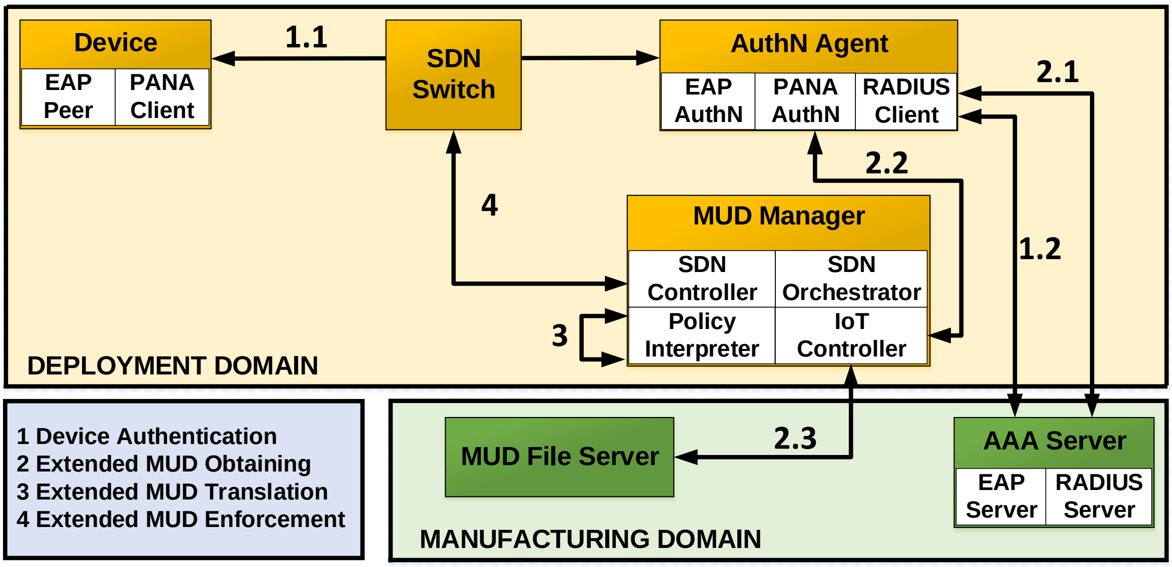


Figure 3.3: Proposed architecture for the extended MUD management

Protocol for Carrying Authentication for Network Access (PANA) [73], which is a widely used protocol in IoT scenarios (e.g., in ZigBee IP [84] or in the ETSI M2M [83]). PANA involves two main roles, the PANA client and the PANA authenticator. However, other alternatives may be possible [33]. On the other hand, the authentication agent and the EAP server use the well-known Remote Authentication Dial In User Service (RADIUS) protocol [32], which defines the roles of RADIUS client and server.

During the *MUD obtaining* phase, the device communicates the location of the MUD file, by using the MUD URL parameter. In this regard, the MUD standard [53] proposes several mechanisms: the Dynamic Host Configuration Protocol (DHCP) [45], the Link Layer Discovery Protocol (LLDP) [77], and the Institute of Electrical and Electronics Engineers (IEEE) 802.1AR standard [44] to embed the MUD URL in an X.509 certificate. However, the standard leaves the door open to the usage of other mechanisms, specially in very constrained scenarios. In our approach, we embed the MUD URL in the last message of the authentication process. In particular, we use the "vendor-specific" attribute of the RADIUS protocol that includes the EAP Success message. When the authentication agent receives the MUD URL, following the process described by the standard specification [53], it is forwarded to the MUD Manager. Then, the MUD manager (acting as IoT Controller) will request the MUD file from the MUD file Server, which is located in the manufacturer domain. Furthermore, the MUD manager will also obtain the MUD signature to verify the integrity of the MUD file.

Once the MUD file has been obtained by the MUD Manager, it has to be translated and enforced by different network components. Our proposal is based on the SDN approach proposed in the scope of the EU H2020 ANASTACIA project. Toward this end, the restrictions of the MUD file are translated (*MUD translation* phase) to an intermediate policy language called MSPL [75], which represents the information in an enforcement-agnostic way. The translation of the MUD file is orchestrated by the SDN Orchestrator and executed by the Policy Interpreter (see Figure 3.3). It should be noted that further information (e.g., IP addresses) could be required to translate the MUD high-level terms such as "manufacturer" or "controller".

During the *MUD enforcement*, the SDN Orchestrator decides the suitable mechanism to enforce the security policies. For the network constraints, the intermediate MSPL language is translated into the corresponding flow rules (MSPL translation). We use the well-known OpenFlow protocol [74] to enable the SDN controller to install and configure the SDN flows in the SDN switches. Once the configuration is completely installed, the bootstrapping finishes, and therefore, the device can perform the usual operations within the network (e.g., communicate with another device or access to a resource).

For the enforcement of the resource authorization, we propose the usage of authorization tokens and the XACML[30] standard. XACML defines an attribute-based access control policy language and a processing model to evaluate the access requests according to the rules, which in this case, are defined in the MUD file. Therefore, when a device wants to access a resource, it needs an authorization token. The request is evaluated against the authorization policies and based on them, the token is granted or not. The authorization restrictions defined on the MUD are translated into XACML rules, and used to authorize or deny the generation of the token. If the token is granted, the device can use this token as an authorization proof to access such resource. To deal with constrained scenarios, we also propose the usage of CBOR [61] to encode the tokens, similarly to the CWT standard [36]. In addition, we combine CWT and AIF [35] to create a token representation based on the notions of capability-based access control [88]. The implementation of this part was considered as future work and it has been published at the date of finishing this thesis [10]. The results concerning the SDN implementation and its integration with the bootstrapping phase can be found in [30].

3.5. Lessons Learned and Conclusions

The continuously growth of the IoT paradigm has brought enormous benefits to everyone's lives. However, these benefits are overshadowed by the high number of security issues to which these devices are exposed. In this regard, cybersecurity and regulatory organizations consider the development of cybersecurity certification approaches as a key component for a more trustworthy digital landscape. Indeed, the definition of a cybersecurity certification framework is intended to provide a reliable and transparent representation of the security level associated to any ICT product or component. At EU level, this initiative is led by ENISA after the adoption of the Cybersecurity Act regulation in 2019.

However, the task of developing a cybersecurity certification framework needs to cope with significant challenges, specially in the case of emerging scenarios, such as the IoT paradigm. Indeed, the high heterogeneity degree of existing IoT devices and systems hinders the realization of a cost-effective, automated and scalable security evaluation process. One of the main challenges is the security dynamism, due to the continuous updates and patches that are required by such devices, and the zero-day threats to which they are exposed. Thus, a scalable, automated and dynamic security evaluation approach, is crucial to make the cybersecurity certification viable for IoT scenarios.

In this regard, this thesis proposes a methodology for evaluating IoT security that copes with a large set of the challenges previously described. The methodology is based on different processes standardized by ETSI, and combines security risk assessment and testing to realize an objective security evaluation process, whose results can be compared. In addition, the methodology takes into account specific aspects of cybersecurity certification, such as the creation of a visual cybersecurity label that reflects the security level of a certain device or product, as it is currently considered by the energy domain. Furthermore, the proposed methodology defines several mechanisms to deal with the risk treatment process during the deployment of a new IoT device in a certain network.

The methodology has been instantiated through techniques and tools to foster the automation of the different processes. Toward this end, MBT techniques have been employed to automatically derive tests from a high-level model of a certain TOE. Such tests are also executed automatically by tools such as JUnit or TITAN. To give a numerical value to the risk level, test results are integrated with the metrics of the CVSS standard. Furthermore, the context in which the TOE will operate has been taken into account through profiles that reflect the security level required in a specific context. Finally, the treatment process makes use of the MUD standard to specify the recommended security restrictions at network level to protect the device during its operation phase. The MUD management has been integrated with the bootstrapping phase of the device to obtain the MUD file and enforce the restrictions using SDNs before the device can operate in the network. Therefore, such process is

[30] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

intended to reduce the attack surface of the device and the network itself. Furthermore, we extended the MUD model to include security aspects beyond network access control, through the integration of the security evaluation results. Consequently, the expressiveness of the MUD standard is further enhanced.

The proposed methodology is intended to serve as a basis for future cybersecurity certification approaches to cope with some of the cybersecurity certification challenges. As a future work, we plan to extend the proposed methodology by integrating monitoring techniques that could automatically trigger a security re-evaluation process. Furthermore, we will analyze the use of graph techniques to represent the relationship among different IoT devices or systems, and their vulnerabilities. Indeed, we are already working on these aspects in the scope of several European H2020 projects to further contribute to the development of a holistic security evaluation methodology.

Chapter 4

Publications composing the PhD Thesis

4.1. Toward a Cybersecurity Certification Framework for the Internet of Things

Title	Toward a Cybersecurity Certification Framework for the Internet of Things
Authors	Sara Nieves Matheu-Garcia and José Luis Hernández-Ramos and Antonio Skarmeta-Gómez
Type	Journal
Journal	IEEE Security and Privacy
Impact factor (2018)	1.596
Publisher	IEEE
Pages	66–76
Volume	17
Issue	3
Year	2019
Month	May
ISSN	1540-7993
DOI	`http://dx.doi.org/10.1109/MSEC.2019.2904475`
URL	`https://ieeexplore.ieee.org/document/8713275`
State	Published
Author's contribution	The PhD student, Sara Nieves Matheu García, is the main author of the paper

Journal details: IEEE Security and Privacy
ISSN: 1540-7993
Publisher: IEEE
Impact factor (2018): 1.596
Website: `https://ieeexplore.ieee.org/xpl/aboutJournal.jsp?punumber=8013`

Authors – Personal details	
Name	**Sara Nieves Matheu García**
Position	PhD student of the Department of Information and Communications Engineering
University	University of Murcia
Name	**Dr. José Luis Hernández Ramos**
Position	Postdoctoral Researcher
Research Centre	European Commission Joint Research Centre in Ispra (Italy)
Name	**Dr. Antonio F. Skarmeta Gómez**
Position	Professor of the Department of Information and Communications Engineering
University	University of Murcia

Abstract

Although the development of a cybersecurity certification framework is an ambitious effort, the dynamic and heterogeneous nature of the Internet of Things makes its realization challenging from technical and legal perspectives. This work proposes a framework based on technologies currently employed in European initiatives to promote a more harmonious vision of this effort.

4.2. Risk-based Automated Assessment and Testing for the Cybersecurity Certification and Labelling of IoT Devices

Title	Risk-based Automated Assessment and Testing for the Cybersecurity Certification and Labelling of IoT Devices
Authors	Sara Nieves Matheu-Garcia and José Luis Hernández-Ramos and Antonio Skarmeta-Gómez and Gianmarco Baldini
Type	Journal
Journal	Computer Standards and Interfaces
Impact factor (2018)	2.441
Publisher	Elsevier
Pages	64–83
Volume	62
Year	2019
Month	February
ISSN	0920-5489
DOI	`http://dx.doi.org/10.1016/j.csi.2018.08.003`
URL	`https://www.sciencedirect.com/science/article/pii/S0920548918301375`
State	Published
Author's contribution	The PhD student, Sara Nieves Matheu García, is the main author of the paper

Journal details: Computer Standards and Interfaces
ISSN: 0920-5489
Publisher: Elsevier
Impact factor (2019): 2.441
Website: `https://www.elsevier.com/locate/csi`

Authors – Personal details	
Name	**Sara Nieves Matheu García**
Position	PhD student of the Department of Information and Communications Engineering
University	University of Murcia
Name	**Dr. José Luis Hernández Ramos**
Position	Postdoctoral Researcher
Research Centre	European Commission Joint Research Centre in Ispra (Italy)
Name	**Dr. Antonio F. Skarmeta Gómez**
Position	Professor of the Department of Information and Communications Engineering
University	University of Murcia
Name	**Dr. Gianmarco Baldini**
Position	Senior Researcher
Research Centre	European Commission Joint Research Centre in Ispra (Italy)

Abstract

Nowadays, security aspects represent one of the most significant barriers for the adoption of large-scale Internet of Things (IoT) deployments. In this sense, being able to certify and communicate the security level of a certain device is crucial for their acceptance. Towards this end, we propose a security certification methodology designed for IoT to empower different stakeholders with the ability to assess security solutions for large-scale IoT deployments in an automated way. It also supports transparency on the IoT security level to the consumers because the methodology provides a label as one of the main results of the certification process. The certification approach represents an instantiation of the Risk-based Security Assessment and Testing methodologies presented by ETSI based on the ISO 31000 and ISO 29119, and it is built on top of different technologies and approaches for security testing and risk assessment adapted to the IoT landscape. As a proof of concept, the proposed methodology is applied to one of the scenarios proposed in the scope of the Horizon 2020 ARMOUR project for assessing the fulfillment of several security properties of IoT devices.

4.3. Extending MUD Profiles Through an Automated IoT Security Testing Methodology

Title	Extending MUD Profiles Through an Automated IoT Security Testing Methodology
Authors	Sara Nieves Matheu-Garcia and José Luis Hernández-Ramos Salvador Pérez-Franco and Antonio Skarmeta-Gómez
Type	Journal
Journal	IEEE Access
Impact factor (2018)	4.098
Publisher	IEEE
Pages	149444 - 149463
Volume	7
Year	2019
Month	October
ISSN	2169-3536
DOI	`http://dx.doi.org/10.1109/ACCESS.2019.2947157`
URL	`https://ieeexplore.ieee.org/abstract/document/8867876`
State	Published
Author's contribution	The PhD student, Sara Nieves Matheu García, is the main author of the paper

Journal details: IEEE Access
ISSN: 2169-3536
Publisher: IEEE
Impact factor (2018): 4.098
Website: `https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639`

Authors – Personal details	
Name	**Sara Nieves Matheu García**
Position	PhD student of the Department of Information and Communications Engineering
University	University of Murcia
Name	**Dr. José Luis Hernández Ramos**
Position	Postdoctoral Researcher
Research Centre	European Commission Joint Research Centre in Ispra (Italy)
Name	**Salvador Pérez Franco**
Position	PhD student of the Department of Information and Communications Engineering
University	University of Murcia
Name	**Dr. Antonio F. Skarmeta Gómez**
Position	Professor of the Department of Information and Communications Engineering
University	University of Murcia

Abstract

Defining the intended behaviour of IoT devices is considered as a key aspect to detect and mitigate potential security attacks. In this direction, the Manufacturer Usage Description (MUD) has been recently standardised to reduce the attack surface of a certain device through the definition of access control policies. However, the semantic model is only intended to provide network level restrictions for the communication of such device. In order to increase the expressiveness of this approach, we propose the use of an automated IoT security testing methodology, so that testing results are used to generate augmented MUD profiles, in which additional security aspects are considered. For the enforcement of these profiles, we propose the use of different access control technologies addressing application layer security concerns. Furthermore, the methodology is based on the use of Model-Based Testing (MBT) techniques to automate the generation, design and implementation of security tests. Then, we describe the application of the resulting approach to the Elliptic Curve Diffie-Hellman over COSE (EDHOC) protocol, which represents a standardisation effort to build a lightweight authenticated key exchange protocol for IoT constrained scenarios.

4.4. Enforcing Behavioral Profiles through Software-Defined Networks in the Industrial Internet of Things

Title	Enforcing Behavioral Profiles through Software-Defined Networks in the Industrial Internet of Things
Authors	Sara Nieves Matheu-Garcia and Alejandro Molina-Zarca and José Luis Hernández-Ramos and Jorge Bernal-Bernabé and Antonio Skarmeta-Gómez
Type	Journal
Journal	Applied Sciences
Impact factor (2018)	2.217
Publisher	MDPI
Article Number	4576
Number of pages	21
Volume	9
Issue	21
Year	2019
Month	October
ISSN	2076-3417
DOI	`https://doi.org/10.3390/app9214576`
URL	`https://www.mdpi.com/2076-3417/9/21/4576`
State	Published
Author's contribution	The PhD student, Sara Nieves Matheu García, is the main author of the paper

Journal details: Applied Sciences, Special Issue "Software Defined Networks in IoT Environments"

ISSN: 2076-3417
Publisher: MDPI
Impact factor (2018): 2.217
Website: `https://www.mdpi.com/journal/applsci`

Authors – Personal details	
Name	**Sara Nieves Matheu García**
Position	PhD student of the Department of Information and Communications Engineering
University	University of Murcia
Name	**Alejandro Molina Zarca**
Position	PhD student of the Department of Information and Communications Engineering
University	University of Murcia
Name	**Dr. José Luis Hernández Ramos**
Position	Postdoctoral Researcher
Research Centre	European Commission Joint Research Centre in Ispra (Italy)
Name	**Dr. Jorge Bernal Bernabe**
Position	Researcher of the Department of Information and Communications Engineering
University	University of Murcia
Name	**Dr. Antonio F. Skarmeta Gómez**
Position	Professor of the Department of Information and Communications Engineering
University	University of Murcia

Abstract

The fourth industrial revolution is being mainly driven by the integration of Internet of Things (IoT) technologies to support the development lifecycle of systems and products. Despite the well-known advantages for the industry, an increasingly pervasive industrial ecosystem could make such devices an attractive target for potential attackers. Recently, the Manufacturer Usage Description (MUD) standard enables manufacturers to specify the intended use of their devices, thereby restricting the attack surface of a certain system. In this direction, we propose a mechanism to manage securely the obtaining and enforcement of MUD policies through the use of a Software-Defined Network (SDN) architecture. We analyze the applicability and advantages of the use of MUD in industrial environments based on our proposed solution, and provide an exhaustive performance evaluation of the required processes.

Chapter 5

References

[1] P. Kasinathan, C. Pastrone, M. A. Spirito, M. Vinkovits, N. O. T. J. L. Shachar Siboni, Asaf Shabtai, and Y. Elovici, "Advanced Security Testbed Framework for Wearable IoT Devices," in *IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, vol. 16, 2016.

[2] J. L. Hernandez-Ramos, D. Geneiatakis, I. Kounelis, G. Steri, and I. Nai Fovino, "Toward a Data-Driven Society: A Technological Perspective on the Development of Cybersecurity and Data-Protection Policies," *IEEE Security Privacy*, vol. 18, no. 1, pp. 28–38, Jan. 2020, conference Name: IEEE Security Privacy.

[3] S. N. Matheu and A. F. Skarmeta, "Cybersecurity Certification in IoT Environments," in *Security Risk Management for the Internet of Things: Technologies and Techniques for IoT Security, Privacy and Data Protection.* John Soldatos, River Publishers, 2020, pp. 178–195.

[4] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Computer Networks*, vol. 144, pp. 17–39, Oct. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128618305243

[5] S. P. A. Datta, "Emergence of Digital Twins - Is this the march of reason?" 2017.

[6] Kevin Ashton, "That 'Internet of Things' Thing," 2009, library Catalog: www.rfidjournal.com. [Online]. Available: https://www.rfidjournal.com/that-internet-of-things-thing

[7] O. Garcia-Morchon and T. Dahm, "Automated IoT Security," 2019, library Catalog: tools.ietf.org. [Online]. Available: https://tools.ietf.org/html/draft-garciamorchon-t2trg-automated-iot-security-01

[8] J. Postel, "User Datagram Protocol," 1980, library Catalog: tools.ietf.org. [Online]. Available: https://tools.ietf.org/html/rfc768

[9] ——, "Transmission Control Protocol," 1981, library Catalog: tools.ietf.org. [Online]. Available: https://tools.ietf.org/html/rfc793

[10] S. N. Matheu, A. Robles Enciso, A. Molina Zarca, D. Garcia-Carrillo, J. L. Hernández-Ramos, J. Bernal Bernabe, and A. F. Skarmeta, "Security Architecture for Defining and Enforcing Security Profiles in DLT/SDN-Based IoT Systems," *Sensors*, vol. 20, no. 7, p. 1882, Jan.

2020, number: 7 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1424-8220/20/7/1882

[11] A. Sivanathan, "IoT Behavioral Monitoring via Network Traffic Analysis," *arXiv:2001.10632 [cs]*, Jan. 2020, arXiv: 2001.10632. [Online]. Available: http://arxiv.org/abs/2001.10632

[12] Y. Afek, A. Bremler-Barr, D. Hay, R. Goldschmidt, L. Shafir, G. Abraham, and A. Shalev, "NFV-based IoT Security for Home Networks using MUD," *arXiv:1911.00253 [cs]*, Nov. 2019, arXiv: 1911.00253. [Online]. Available: http://arxiv.org/abs/1911.00253

[13] B. Moran and H. Tschofenig, "Strong Assertions of IoT Network Access Requirements," 2020, library Catalog: tools.ietf.org. [Online]. Available: https://tools.ietf.org/html/draft-moran-suit-mud-00

[14] F. R. Garcia, B. Marin, and S. A. Banados, "Visualization of MBT testing coverage," in *2019 13th International Conference on Research Challenges in Information Science (RCIS)*. Brussels, Belgium: IEEE, May 2019, pp. 1–2. [Online]. Available: https://ieeexplore.ieee.org/document/8877033/

[15] J. R. C. Nurse, S. Creese, and D. De Roure, "Security Risk Assessment in Internet of Things Systems," *IT Professional*, vol. 19, no. 5, pp. 20–26, 2017, arXiv: 1811.03290. [Online]. Available: http://arxiv.org/abs/1811.03290

[16] ENISA, "Considerations on ICT security certification in EU - Survey Report," 2017. [Online]. Available: https://www.enisa.europa.eu/publications/certification_survey

[17] Cyberwatching, "Cybersecurity standard gap analysis," 2019. [Online]. Available: https://www.trust-itservices.com/sites/default/files/Cybersecurity%20standard%20gap%20analysis.pdf

[18] Cyber Security Division Commerce and Information Policy Bureau Ministry of Economy, Trade and Industry, "The Cyber Physical Security Framework," 2019.

[19] European Commission, "DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS directive)," 2016. [Online]. Available: http://link.springer.com/10.1007/978-1-137-54482-7_33

[20] E. Ellesson, J. Strassner, B. Moore, and A. Westerinen, "Policy Core Information Model – Version 1 Specification," 2001. [Online]. Available: https://tools.ietf.org/html/rfc3060

[21] oneM2M, "Technical report TR-0008," 2018. [Online]. Available: http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf

[22] H. Habibi Gharakheili, A. Sivanathan, A. Hamza, and V. Sivaraman, "Network Level Security for the Internet of Things: Opportunities and Challenges," *Computer*, vol. 52, no. 8, pp. 58–62, Aug. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8780392/

[23] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti, "A Large-Scale Analysis of the Security of Embedded Firmwares," 2014, pp. 95–110. [Online]. Available: https://www.usenix.org/node/184450

[24] K. Cheng, Q. Li, L. Wang, Q. Chen, Y. Zheng, L. Sun, and Z. Liang, "DTaint - Detecting the Taint-Style Vulnerability in Embedded Device Firmware," in *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Jun. 2018, pp. 430–441, iSSN: 2158-3927.

[25] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, “SoK - Security Evaluation of Home-Based IoT Deployments,” in *2019 IEEE Symposium on Security and Privacy (SP).* San Francisco, CA, USA: IEEE, May 2019, pp. 1362–1380. [Online]. Available: https://ieeexplore.ieee.org/document/8835392/

[26] Y. Zheng, A. Davanian, H. Yin, C. Song, H. Zhu, and L. Sun, “FIRM-AFL - High-Throughput Greybox Fuzzing of IoT Firmware via Augmented Process Emulation,” 2019, pp. 1099–1114. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/zheng

[27] W. Zhou, Y. Jia, Y. Yao, L. Zhu, L. Guan, Y. Mao, P. Liu, and Y. Zhang, “Discovering and Understanding the Security Hazards in the Interactions between IoT Devices, Mobile Apps, and Clouds on Smart Home Platforms,” 2019, pp. 1133–1150. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/zhou

[28] B. Cui, S. Liang, S. Chen, B. Zhao, and X. Liang, “A Novel Fuzzing Method for Zigbee Based on Finite State Machine,” *International Journal of Distributed Sensor Networks*, vol. 10, no. 1, p. 762891, Jan. 2014. [Online]. Available: https://doi.org/10.1155/2014/762891

[29] P. Cihon, G. M. Gutierrez, S. Kee, M. J. Kleinaltenkamp, T. Voigt, and A. Rosato, “Why Certify? Increasingadoption of the proposed EU Cybersecurity Certification Framework.” Sophia Antipolis, France: Cambridge Judge Business School, 2018. [Online]. Available: https://docbox.etsi.org/Workshop/2018/201806_ETSISECURITYWEEK/IoTSecurity/00POSTERS/Cambridge%20EU%20Cybersecurity%20Certification%20Report.pdf

[30] S. N. Matheu García, A. Molina Zarca, J. L. Hernández-Ramos, J. B. Bernabé, and A. S. Gómez, “Enforcing Behavioral Profiles through Software-Defined Networks in the Industrial Internet of Things,” *Applied Sciences*, vol. 9, no. 21, p. 4576, Jan. 2019. [Online]. Available: https://www.mdpi.com/2076-3417/9/21/4576

[31] S. N. Matheu, J. L. Hernandez-Ramos, S. Perez, and A. F. Skarmeta, “Extending MUD profiles through an Automated IoT Security Testing Methodology,” *IEEE Access*, pp. 1–20, 2019.

[32] B. Aboba and P. R. Calhoun, “RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP),” 2003. [Online]. Available: https://tools.ietf.org/html/rfc3579

[33] B. Sarikaya, M. Sethi, and D. Garcia-Carillo, “Secure IoT Bootstrapping: A Survey,” 2018. [Online]. Available: https://tools.ietf.org/id/draft-sarikaya-t2trg-sbootstrapping-05.html

[34] B. Aboba, D. Simon, and P. Eronen, “Extensible Authentication Protocol (EAP) Key Management Framework,” 2008. [Online]. Available: https://tools.ietf.org/html/rfc5247

[35] Carsten Bormann, “An Authorization Information Format (AIF) for ACE,” 2019. [Online]. Available: https://tools.ietf.org/html/draft-bormann-core-ace-aif-06

[36] S. Erdtman, E. Wahlstroem, H. Tschofenig, and M. Jones, “CBOR Web Token (CWT),” 2018. [Online]. Available: https://tools.ietf.org/html/rfc8392

[37] NIST, “Extensible Configuration Checklist Description Format (XCCDF) - Security Content Automation Protocol,” Dec. 2016. [Online]. Available: https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/xccdf/

[38] ETSI, “ETSI EG 203 251: Methods for Testing & Specification; Risk-based Security Assessment and Testing Methodologies,” 2015. [Online]. Available: https://www.etsi.org/deliver/etsi_eg/203200_203299/203251/01.01.01_50/eg_203251v010101m.pdf

[39] S. N. Matheu, S. Perez, Hernandez-Ramos, and A. F. Skarmeta, “On the automation of security testing for IoT constrained scenarios,” in *20th World Conference on Information Security Applications (WISA)*, Jeju, Korea, 2019, (to appear).

[40] MITRE, “OVAL - Open Vulnerability and Assessment Language,” 2016. [Online]. Available: https://oval.mitre.org/

[41] NIST, “SCAP 1.3 - Security Content Automation Protocol,” 2016. [Online]. Available: https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Releases/SCAP-1-3

[42] FIRST, “Common Vulnerability Score System (CVSS) v3,” 2015. [Online]. Available: https://www.first.org/cvss/cvss-v30-specification-v1.8.pdf

[43] ——, “Common Vulnerabilities Scoring System (CVSS),” 2014. [Online]. Available: https://www.first.org/cvss

[44] IEEE, “802.1AR - Secure Device Identity,” 2018. [Online]. Available: https://1.ieee802.org/security/802-1ar/

[45] R. Droms, “Dynamic Host Configuration Protocol (RFC 2131),” 1997. [Online]. Available: https://tools.ietf.org/html/rfc2131

[46] T. Polk, M. Souppaya, and W. C. Barker, “Mitigating IoT-Based Automated Distributed Threats,” 2017. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/iot-ddos-project-description-draft.pdf

[47] Jeffrey Voas, Rick Kuhn, Phillip Laplante, and Sophia Applebaum, “NISTIR 8222: Internet of Things (IoT) Trust Concerns,” 2018. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8222/draft

[48] I. Molloy and H. Huang, “Standardizing IoT Network Security Policy Enforcement,” in *Workshop on Decentralized IoT Security and Standards*, 2018. [Online]. Available: http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/07/diss2018_7_Barrera_paper.pdf

[49] D. A. Waltermire and J. Fitzgerald-McKay, “Transitioning to the Security Content Automation Protocol (SCAP) Version 2,” Sep. 2018. [Online]. Available: https://www.nist.gov/publications/transitioning-scap-version-2

[50] B. Melo, P. L. Geus, and A. A. Gregio, “Robustness Testing of CoAP Server-side Implementations through Black-box Fuzzing Techniques,” in *Brazilian Symposium on Information Security and Computer Systems*, Brazil, 2017, pp. 533–540. [Online]. Available: https://pdfs.semanticscholar.org/487b/7a45bc5962fd2cdf65da2caa05fcaef64591.pdf

[51] CNSSI, “CNSSI No. 4009: Committee on National Security Systems (CNSS) Glossary,” 2015. [Online]. Available: https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf

[52] G. Selander, J. Mattsson, and F. Palombini, “Ephemeral Diffie-Hellman Over COSE (EDHOC),” 2019. [Online]. Available: https://tools.ietf.org/id/draft-selander-ace-cose-ecdhe-13.html

[53] E. Lear, D. Romascanu, and R. Droms, “Manufacturer Usage Description Specification (RFC 8520),” 2019. [Online]. Available: https://tools.ietf.org/html/rfc8520

[54] ETSI, *ETSI ES 201 873-1 : Methods for Testing and Specification (MTS). The Testing and Test Control Notation version 3; Part 1: TTCN-3 Core Language*, 2015. [Online]. Available: https://www.etsi.org/deliver/etsi_es/201800_201899/20187301/04.10.01_60/es_20187301v041001p.pdf

[55] Michael Jones, “JSON Web Algorithms (JWA) (RFC7518),” 2015. [Online]. Available: https://tools.ietf.org/html/rfc7518

[56] ——, “JSON Web Key (JWK) (RFC7517),” 2015. [Online]. Available: https://tools.ietf.org/html/rfc7517

[57] A. Hamza, D. Ranathunga, H. H. Gharakheili, M. Roughan, and V. Sivaraman, “Clear as MUD: Generating, Validating and Applying IoT Behaviorial Profiles (Technical Report),” Apr. 2018, arXiv: 1804.04358. [Online]. Available: http://arxiv.org/abs/1804.04358

[58] M. Ranganathan, “Soft MUD: Implementing Manufacturer Usage Descriptions on OpenFlow SDN Switches,” in *International Conference on Networks (ICN)*, Mar. 2019.

[59] D. Barrera, I. Molloy, and H. Huang, “IDIoT - Securing the Internet of Things like it’s 1994,” Dec. 2017, arXiv: 1712.03623. [Online]. Available: http://arxiv.org/abs/1712.03623

[60] V. Visoottiviseth, P. Akarasiriwong, S. Chaiyasart, and S. Chotivatunyu, “PENTOS - Penetration testing tool for Internet of Thing devices,” in *TENCON 2017 - 2017 IEEE Region 10 Conference*, Penang, Nov. 2017, pp. 2279–2284. [Online]. Available: http://ieeexplore.ieee.org/document/8228241/

[61] C. Bormann and P. Hoffman, “Concise Binary Object Representation (CBOR) (RFC7049),” 2013. [Online]. Available: https://tools.ietf.org/html/rfc7049

[62] G. Bernabeu, E. Jaffuel, B. Legeard, and F. Peureux, “MBT for global platform compliance testing: Experience report and lessons learned,” in *25th IEEE International Symposium on Software Reliability Engineering Workshops*, Naples, Italy, 2014.

[63] A. Hamza, H. H. Gharakheili, T. A. Benson, and V. Sivaraman, “Detecting Volumetric Attacks on IoT Devices via SDN-Based Monitoring of MUD Activity,” in *Symposium on SDN Research (SOSR)*, California, USA, 2019, pp. 36–48.

[64] T. Bray, “The JavaScript Object Notation (JSON) Data Interchange Format (RFC8259),” 2017. [Online]. Available: https://tools.ietf.org/html/rfc8259

[65] M. Jethanandani, D. Blair, L. Huang, and S. Agarwal, “YANG Data Model for Network Access Control Lists (RFC8519),” 2019. [Online]. Available: https://tools.ietf.org/html/rfc8519

[66] B. Potter and G. McGraw, “Software security testing,” *IEEE Security Privacy*, vol. 2, no. 5, pp. 81–85, Sep. 2004.

[67] W. Li, F. Le Gall, and N. Spaseski, “A Survey on Model-Based Testing Tools for Test Case Generation,” in *Tools and Methods of Program Analysis*, V. Itsykson, A. Scedrov, and V. Zakharov, Eds., vol. 779. Cham: Springer International Publishing, 2018, pp. 77–89.

[68] A. Cretin, B. Legeard, F. Peureux, and A. Vernotte, “Increasing the Resilience of ATC systems against False Data Injection Attacks using DSL-based Testing,” in *Doctoral Symposium ICRAT*, 2018.

[69] J. Lubell and T. Zimmerman, “Challenges to automating security configuration checklists in manufacturing environments,” in *Critical Infrastructure Protection XI*, ser. IFIP Advances in Information and Communication Technology, M. Rice and S. Shenoi, Eds. Springer International Publishing, 2017, pp. 225–241.

[70] E. Parliament, “REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act),” 2019.

[71] European Parliament, “REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),” 2016. [Online]. Available: https://eugdpr.org/

[72] J. Vollbrecht, M. Holdrege, C. Laat, P. Calhoun, L. Gommans, S. Farrell, B. d. Bruijn, G. Gross, and D. Spence, “AAA Authorization Framework (RFC 2904),” 2000.

[73] Y. Ohba, B. Patil, D. Forsberg, H. Tschofenig, and A. E. Yegin, “Protocol for Carrying Authentication for Network Access (RFC 5191),” 2008.

[74] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, “OpenFlow - enabling innovation in campus networks,” *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, p. 69, 2008.

[75] A. M. Zarca, J. B. Bernabe, R. Trapero, D. Rivera, J. Villalobos, A. Skarmeta, S. Bianchi, A. Zafeiropoulos, and P. Gouvas, “Security Management Architecture for NFV/SDN-aware IoT Systems,” *IEEE Internet of Things Journal*, 2019.

[76] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and Other Botnets,” *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[77] IEEE, “IEEE Standard for Local and metropolitan area networks - Station and Media Access Control Connectivity Discovery,” *IEEE Std 802.1AB-2016*, pp. 1–146, 2016.

[78] M. Al-Shaboti, I. Welch, A. Chen, and M. A. Mahmood, “Towards Secure Smart Home IoT - Manufacturer and User Network Access Control Framework,” in *IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, 2018, pp. 892–899.

[79] A. Hamza, D. Ranathunga, H. H. Gharakheili, T. A. Benson, M. Roughan, and V. Sivaraman, “Verifying and Monitoring IoTs Network Behavior using MUD Profiles,” *arXiv:1902.02484 [cs]*, Feb. 2019. [Online]. Available: http://arxiv.org/abs/1902.02484

[80] S. P. Kadhirvelan and A. Soderberg-Rivkin, “Threat Modelling and Risk Assessment Within Vehicular Systems,” Ph.D. dissertation, University of Gothenburg, 2014. [Online]. Available: http://publications.lib.chalmers.se/records/fulltext/202917/202917.pdf

[81] J. Hubner and M. Lastovka, “BOSCH Political Viewpoint. Security in IoT.” 2017.

[82] E. Fourneret, F. Bouquet, Frederic Dadeau, and Stephane Debricon, “Selective Test Generation Method for Evolving Critical Systems,” in *2011 IEEE Fourth International Conference on Software Testing, Verification and Validation Workshops.* Berlin, Germany: IEEE, Mar. 2011, pp. 125–134. [Online]. Available: http://ieeexplore.ieee.org/document/5954401/

[83] ETSI, “ETSI TS 102 690: Machine-to-Machine communications (M2M);Functional architecture,” 2013. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102600_102699/102690/02.01.01_60/ts_102690v020101p.pdf

[84] ZigBee Alliance, “ZigBee IP Specification,” 2013. [Online]. Available: http://www.sandelman.ca/tmp/6tisch/13002r01ZB_Marketing-ZigBee_IP_Specification_Public_Download.pdf

[85] European Commission, “Directive 2010/30/EU on the indication by labelling and standard product information of the consumption of energy and other resources by energy-related products,” 2010. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32010L0030

[86] S. N. Matheu, J. L. Hernandez-Ramos, and A. F. Skarmeta, "Toward a Cybersecurity Certification Framework for the Internet of Things," *IEEE Security Privacy*, vol. 17, no. 3, pp. 66–76, May 2019.

[87] S. N. Matheu-Garcia, J. L. Hernandez-Ramos, A. F. Skarmeta, and G. Baldini, "Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices," *Computer Standards & Interfaces*, vol. 62, pp. 64–83, Feb. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0920548918301375?via%3Dihub

[88] J. L. Hernandez-Ramos, A. J. Jara, L. Marin, and A. F. S. Gomez, "DCapBAC - embedding authorization logic into smart things through ECC optimizations," *International Journal of Computer Mathematics*, vol. 93, no. 2, pp. 345–366, Feb. 2016. [Online]. Available: https://doi.org/10.1080/00207160.2014.915316

[89] Caspar Schutijser, "Towards automated DDoS abuse protection using MUD device profiles," Ph.D. dissertation, University of Twente, 2018. [Online]. Available: https://www.sidnlabs.nl/downloads/theses/towards_automated_ddos_abuse_protection_cschutijser.pdf

[90] M. Bishop, "About Penetration Testing," *IEEE Security & Privacy Magazine*, vol. 5, no. 6, pp. 84–87, Nov. 2007. [Online]. Available: http://ieeexplore.ieee.org/document/4402456/

[91] B. Legeard and A. Bouzy, "Smartesting CertifyIt: Model-Based Testing for Enterprise IT," in *2013 IEEE Sixth International Conference on Software Testing, Verification and Validation*. Luxembourg, Luxembourg: IEEE, Mar. 2013, pp. 391–397. [Online]. Available: http://ieeexplore.ieee.org/document/6569752/

[92] G. Mulligan, "The 6LoWPAN Architecture," in *Proceedings of the 4th Workshop on Embedded Networked Sensors*, ser. EmNets '07. New York, NY, USA: ACM, 2007, pp. 78–82. [Online]. Available: http://doi.acm.org/10.1145/1278972.1278992

[93] D. Maynor, *Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research*. Elsevier, Apr. 2011, google-Books-ID: JWgNVFtbWJ4C.

[94] S. Hiremath, G. Yang, and K. Mankodiya, "Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare," in *2014 4th International Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH)*, Nov. 2014, pp. 304–307.

[95] E. Taylor and K. Michael, "Smart Toys that are the Stuff of Nightmares," *IEEE Technology and Society Magazine*, vol. 35, no. 1, pp. 8–10, Mar. 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7430049/

[96] R. Bodenheim, J. Butts, S. Dunlap, and B. Mullins, "Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices," *International Journal of Critical Infrastructure Protection*, vol. 7, no. 2, pp. 114–123, Jun. 2014. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1874548214000213

[97] NIST, "Risk Management Framework for Information Systems and Organizations," 2018. [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-draft-fpd.pdf

[98] J. P. Dias, F. Couto, A. C. Paiva, and H. S. Ferreira, "A Brief Overview of Existing Tools for Testing the Internet-of-Things," in *2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*. Vasteras: IEEE, Apr. 2018, pp. 104–109. [Online]. Available: https://ieeexplore.ieee.org/document/8411738/

[99] C. Chen, B. Cui, J. Ma, R. Wu, J. Guo, and W. Liu, "A systematic review of fuzzing techniques," *Computers & Security*, vol. 75, pp. 118–137, Jun. 2018. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404818300658

[100] J. Chen, W. Diaoy, Q. Zhaoz, C. Zuoz, Z. Linz, X. Wangx, W. C. Lau, M. Sun, R. Yang, and K. Zhang, "IoTFuzzer - Discovering Memory Corruptions in IoT Through App-based Fuzzing," in *Network and Distributed System Security Symposium*, 2018.

[101] N. Chen, C. Viho, A. Baire, X. Huang, and J. Zha, "Ensuring Interoperability for the Internet of Things: Experience with CoAP Protocol Testing," *Journal for Control, Measurement, Electronics, Computing and Communications*, vol. 6, pp. 448–458, 2012.

[102] K. J. W. Bjørneset, "Testing Security for Internet of Things. Survey on Vulnerabilities in IP Cameras," PhD Thesis, University of Oslo, 2017. [Online]. Available: https://www.mn.uio.no/ifi/english/research/groups/psy/completedmasters/2017/Kim_Jonatan_Wessel_Bjorneset/kim_jonatan_wessel_bjorneset_testing_security_for_internet_of_things_a_survey_on_vulnerabilities_in_ip_cameras.pdf

[103] S. Sorsa, "Protocol fuzz testing as a part of secure software development life cycle," Ph.D. dissertation, Tampere University of Technology, 2018. [Online]. Available: https://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/25667/Sorsa.pdf?sequence=3

[104] T. L. Munea, I. Luk Kim, and T. Shon, "Design and Implementation of Fuzzing Framework Based on IoT Applications," *Wireless Personal Communications*, vol. 93, no. 2, pp. 365–382, Mar. 2017. [Online]. Available: http://link.springer.com/10.1007/s11277-016-3322-9

[105] F. M. Tabrizi and K. Pattabiraman, "Formal security analysis of smart embedded systems," in *Proceedings of the 32nd Annual Conference on Computer Security Applications - ACSAC '16*. Los Angeles, California: ACM Press, 2016, pp. 1–15. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2991079.2991085

[106] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," in *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. Lyon, France: IEEE, Oct. 2013, pp. 600–607. [Online]. Available: http://ieeexplore.ieee.org/document/6673419/

[107] A. Ahmad, F. Bouquet, E. Fourneret, F. L. Gall, and B. Legeard, "Model-Based Testing as a Service for IoT Platforms," in *International Symposium on Leveraging Applications of Formal Methods*, 2016, pp. 727–742.

[108] J. Botella, F. Bouquet, J.-F. Capuron, F. Lebeau, B. Legeard, and F. Schadle, "Model-Based Testing of Cryptographic Components - Lessons Learned from Experience," in *2013 IEEE Sixth International Conference on Software Testing, Verification and Validation*. Luxembourg, Luxembourg: IEEE, Mar. 2013, pp. 192–201. [Online]. Available: http://ieeexplore.ieee.org/document/6569731/

[109] J. Bozic and F. Wotawa, "Model-based Testing - From Safety to Security," in *STV Bozic, Wotawa*, 2012, pp. 9–16.

[110] M. Schneider, J. Grossmann, I. Schieferdecker, and A. Pietschker, "Online Model-Based Behavioral Fuzzing," in *2013 IEEE Sixth International Conference on Software Testing, Verification and Validation Workshops*. Luxembourg, Luxembourg: IEEE, Mar. 2013, pp. 469–475. [Online]. Available: http://ieeexplore.ieee.org/document/6571672/

[111] J. Bau, E. Bursztein, D. Gupta, and J. Mitchell, "State of the Art: Automated Black-Box Web Application Vulnerability Testing," in *2010 IEEE Symposium on Security*

and Privacy. Oakland, CA, USA: IEEE, 2010, pp. 332–345. [Online]. Available: http://ieeexplore.ieee.org/document/5504795/

[112] N. Ayewah, D. Hovemeyer, J. D. Morgenthaler, J. Penix, and W. Pugh, "Using Static Analysis to Find Bugs," *IEEE Software*, vol. 25, no. 5, pp. 22–29, Sep. 2008. [Online]. Available: http://ieeexplore.ieee.org/document/4602670/

[113] S. Yoo and M. Harman, "Regression testing minimization, selection and prioritization: a survey," *Software Testing, Verification and Reliability*, vol. 22, no. 2, pp. 67–120, Mar. 2012. [Online]. Available: http://doi.wiley.com/10.1002/stv.430

[114] J. Bozic and F. Wotawa, "Security Testing Based on Attack Patterns," in *2014 IEEE Seventh International Conference on Software Testing, Verification and Validation Workshops.* OH, USA: IEEE, Mar. 2014, pp. 4–11. [Online]. Available: http://ieeexplore.ieee.org/document/6825631/

[115] D. Xu, M. Tu, M. Sanford, L. Thomas, D. Woodraska, and W. Xu, "Automated Security Test Generation with Formal Threat Models," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, pp. 526–540, Jul. 2012. [Online]. Available: http://ieeexplore.ieee.org/document/6155723/

[116] M. Felderer, B. Agreiter, P. Zech, and R. Breu, "A Classification for Model-Based Security Testing," Oct. 2011, pp. 109–114. [Online]. Available: https://www.thinkmind.org/index.php?view=article&articleid=valid_2011_5_10_40020

[117] F. Bouquet, C. Grandpierre, B. Legeard, F. Peureux, N. Vacelet, and M. Utting, "A subset of precise UML for model-based testing," in *Proceedings of the 3rd international workshop on Advances in model-based testing - A-MOST '07.* London, United Kingdom: ACM Press, 2007, pp. 95–104. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1291535.1291545

[118] M. Felderer, M. Büchler, M. Johns, A. D. Brucker, R. Breu, and A. Pretschner, "Chapter One - Security Testing: A Survey," in *Advances in Computers.* Elsevier, 2015, vol. 101, pp. 1–51. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0065245815000649

[119] L. Aljoscha and M. Islam, "HEAling Vulnerabilities to ENhance Software Security and Safety – Project Proposal (HAVENS)," 2016. [Online]. Available: http://autosec.se/wp-content/uploads/2018/03/HEAVENS_D2_v2.0.pdf

[120] EVITA, *E-Safety Vehicle Intrusion Protected Applications*, 2008. [Online]. Available: https://www.evita-project.org/

[121] K. Moore, R. Barnes, and H. Tschofenig, "Best Current Practices for Securing Internet of Things (IoT) Devices," 2016. [Online]. Available: https://tools.ietf.org/html/draft-moore-iot-security-bcp-00

[122] M. Abomhara and G. M. Koien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65–88, 2015. [Online]. Available: http://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

[123] C. Liu, Y. Zhang, J. Zeng, L. Peng, and R. Chen, "Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology," in *2012 8th International Conference on Natural Computation.* Chongqing, Sichuan, China: IEEE, May 2012, pp. 874–878. [Online]. Available: http://ieeexplore.ieee.org/document/6234533/

[124] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini, "A risk assessment methodology for the Internet of Things," *Computer Communications*, vol. 129, pp. 67–79, Sep. 2018. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0140366418303487

[125] F. Alsubaei, A. Abuhussein, and S. Shiva, “Quantifying security and privacy in Internet of Things solutions,” in *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium.* Taipei: IEEE, Apr. 2018, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/8406318/

[126] M. Cagnazzo, M. Hertlein, T. Holz, and N. Pohlmann, “Threat modeling for mobile health systems,” in *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW).* Barcelona: IEEE, Apr. 2018, pp. 314–319. [Online]. Available: https://ieeexplore.ieee.org/document/8369033/

[127] V. L. Shivraj, M. A. Rajan, and P. Balamuralidhar, “A graph theory based generic risk assessment framework for internet of things (IoT),” in *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS).* Bhubaneswar: IEEE, Dec. 2017, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/8384121/

[128] C. Wongvises, A. Khurat, D. Fall, and S. Kashihara, “Fault tree analysis-based risk quantification of smart homes,” in *2017 2nd International Conference on Information Technology (INCIT).* Nakhonpathom: IEEE, Nov. 2017, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/8257865/

[129] H. Wang, Z. Chen, J. Zhao, X. Di, and D. Liu, “A Vulnerability Assessment Method in Industrial Internet of Things Based on Attack Graph and Maximum Flow,” *IEEE Access*, vol. 6, pp. 8599–8609, 2018. [Online]. Available: http://ieeexplore.ieee.org/document/8290918/

[130] S. Lee, S. Kim, K. Choi, and T. Shon, “Game theory-based Security Vulnerability Quantification for Social Internet of Things,” *Future Generation Computer Systems*, vol. 82, pp. 752–760, May 2018. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167739X17308440

[131] A. B. Garcia, R. F. Babiceanu, and R. Seker, “Trustworthiness requirements and models for aviation and aerospace systems,” in *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS).* Herndon, VA: IEEE, Apr. 2018, pp. 1–16. [Online]. Available: https://ieeexplore.ieee.org/document/8384911/

[132] S. Cleemput, “Secure and privacy-friendly smart electricity metering,” PhD Thesis, Arenberg doctoral school. Faculty of Engineering Science, 2018. [Online]. Available: https://www.esat.kuleuven.be/cosic/publications/thesis-303.pdf

[133] H. Abie and I. Balasingham, “Risk-Based Adaptive Security for Smart IoT in eHealth,” in *Proceedings of the 7th International Conference on Body Area Networks.* Oslo, Norway: ACM, 2012. [Online]. Available: http://eudl.eu/doi/10.4108/icst.bodynets.2012.250235

[134] S. N. Matheu-Garcia, J. L. Hernandez-Ramos, and A. F. Skarmeta, “Test-based risk assessment and security certification proposal for the Internet of Things,” in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT).* Singapore: IEEE, Feb. 2018, pp. 641–646. [Online]. Available: https://ieeexplore.ieee.org/document/8355193/

[135] B. Ali and A. Awad, “Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes,” *Sensors*, vol. 18, no. 3, p. 817, Mar. 2018. [Online]. Available: http://www.mdpi.com/1424-8220/18/3/817

[136] Y. Qu and P. Chan, “Assessing Vulnerabilities in Bluetooth Low Energy (BLE) Wireless Network Based IoT Systems,” in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS).* New York, NY, USA: IEEE, Apr. 2016, pp. 42–48. [Online]. Available: http://ieeexplore.ieee.org/document/7502262/

[137] H. Sandor and G. Sebestyen-Pal, “Optimal security design in the Internet of Things,” in *2017 5th International Symposium on Digital Forensic and Security (ISDFS)*. Tirgu Mures, Romania: IEEE, Apr. 2017, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/7916496/

[138] Microsoft, “DREAD scheme,” 2010. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)#dread

[139] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process,” CERT, Tech. Rep., 2007. [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

[140] RASEN project, “D3.2.3. Techniques for Compositional Test-Based Security Risk Assessment v.3,” 2015. [Online]. Available: http://www.rasenproject.eu/downloads/985/

[141] MITRE, “CWE - Common Weakness Scoring System (CWSS),” 2014. [Online]. Available: https://cwe.mitre.org/cwss/cwss_v1.0.1.html

[142] ANSSI, “Certification de sécurité de premier niveau (CSPN),” 2008. [Online]. Available: https://www.ssi.gouv.fr/administration/produits-certifies/cspn/

[143] NIST, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” National Institute of Standards and Technology, Tech. Rep., 2018. [Online]. Available: https://doi.org/10.6028%2Fnist.cswp.04162018

[144] ——, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0,” Feb. 2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[145] CESG, “The Commercial Product Assurance (CPA) build standard,” 2014. [Online]. Available: https://www.ncsc.gov.uk/content/files/protected_files/document_files/The%20CPA%20Build%20Standard%201.3.pdf

[146] ECSO, “A Meta-Scheme Approach v1.0,” 2017. [Online]. Available: http://www.ecs-org.eu/documents/uploads/european-cyber-security-certification-a-meta-scheme-approach.pdf

[147] ——, “State of the Art Syllabus v2,” 2017. [Online]. Available: http://www.ecs-org.eu/documents/uploads/updated-sota.pdf

[148] J. Hearn, “Does the common criteria paradigm have a future?” *IEEE Security & Privacy Magazine*, vol. 2, no. 1, pp. 64–65, Jan. 2004. [Online]. Available: http://ieeexplore.ieee.org/document/1264857/

[149] AIOTI, “Report on Workshop on Security and Privacy in the Hyper-Connected World,” 2016. [Online]. Available: https://goo.gl/KeKqbs

[150] ——, “Report on Workshop on Security & Privacy in IoT,” 2017. [Online]. Available: https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf

[151] CCRA, “Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model.” 2017. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[152] H. Baars, R. Lassche, R. Massink, and H. Pille, “Smart grid security certification in Europe. Challenges and recommendations,” 2014. [Online]. Available: https://www.enisa.europa.eu/publications/smart-grid-security-certification-in-europe/at_download/fullReport

[153] R. Anderson and S. Fuloria, “Certification and evaluation: A security economics perspective,” in *2009 IEEE Conference on Emerging Technologies & Factory Automation.* Palma de Mallorca, Spain: IEEE, Sep. 2009, pp. 1–7. [Online]. Available: http://ieeexplore.ieee.org/document/5347129/

[154] P. Anantharaman, M. Locasto, G. F. Ciocarlie, and U. Lindqvist, “Building Hardened Internet-of-Things Clients with Language-Theoretic Security,” in *2017 IEEE Security and Privacy Workshops (SPW).* San Jose, CA: IEEE, May 2017, pp. 120–126. [Online]. Available: http://ieeexplore.ieee.org/document/8227297/

[155] A. Lahmadi, C. Brandin, and O. Festor, “A Testing Framework for Discovering Vulnerabilities in 6LoWPAN Networks,” in *2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems.* Hangzhou, Zhejiang, China: IEEE, May 2012, pp. 335–340. [Online]. Available: http://ieeexplore.ieee.org/document/6227765/

[156] J. Cabot and M. Gogolla, “Object Constraint Language (OCL): A Definitive Guide,” in *Proceedings of the 12th international conference on Formal Methods for the Design of Computer, Communication, and Software Systems: formal methods for model-driven engineering*, 2017. [Online]. Available: https://www.researchgate.net/publication/262330177_Object_Constraint_Language_OCL_A_Definitive_Guide

[157] G. George and S. M. Thampi, “A Graph-Based Security Framework for Securing Industrial IoT Networks From Vulnerability Exploitations,” *IEEE Access*, vol. 6, pp. 43 586 – 43 601, 2018.

[158] A. Ahmad, G. Baldini, P. Cousin, S. N. Matheu, A. Skarmeta, E. Fourneret, and B. Legeard, “Cognitive Hyperconnected Digital Transformation: Internet of Things Intelligence Evolution,” ser. River Publishers Series in Communications. River Publishers, 2017, pp. 189–220. [Online]. Available: https://books.google.es/books?id=nPIxDwAAQBAJ

[159] H. Al-Alami, A. Hadi, and H. Al-Bahadili, “Vulnerability scanning of IoT devices in Jordan using Shodan,” in *2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes and Systems (IT-DREPS)*, 2017.

[160] R. Tonjes, E. S. Reetz, K. Moessner, and P. Barnaghi, “A Test-driven Approach for Life Cycle Management of Internet of Things enabled Services,” in *Future Network and Mobile*, 2012. [Online]. Available: http://info.ee.surrey.ac.uk/Personal/P.Barnaghi/doc/IoTest-Paper.pdf

[161] C. J. Alberts, A. J. Dorofee, J. F. Stevens, and C. Woody, “OCTAVE-S Implementation Guide, Version 1,” Tech. Rep., 2005. [Online]. Available: https://resources.sei.cmu.edu/asset_files/Handbook/2005_002_001_14273.pdf

[162] OWASP, *OWASP Application Security Verification Standard (ASVS) Project.* [Online]. Available: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

[163] E. Rescorla and N. Modadugu, *Datagram Transport Layer Security Version 1.2*, 2012, published: RFC 6347. [Online]. Available: https://tools.ietf.org/html/rfc6347

[164] MITRE, *Common Weakness Risk Analysis Framework (CWRAF).* [Online]. Available: https://cwe.mitre.org/cwraf/

[165] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, “Internet of Things security: A survey,” *Journal of Network and Computer Applications*, vol. 88, pp. 10 – 28, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804517301455

Publications

[P1] A. Ahmad, G. Baldini, P. Cousin, S. N. Matheu, A. Skarmeta, E. Fourneret and B. Legeard, “Large Scale IoT Security Testing Benchmarking and Certification” in Cognitive Hyperconnected Digital Transformation. *River Publishers* **2017**, 189–220. ISBN:978-87-93609-11-2.

[P2] S.N. Matheu García, J.L. Hernández Ramos, A. Skarmeta, “Proposal of Certification and Benchmarking for the Internet of Things”. *ETSI IoT Week* **2017**. Available online: https://www.researchgate.net/publication/320672978_Proposal_of_Certification_and_Benchmarking_for_the_Internet_of_Things_-_ETSI_IoT_Week_2017.

[P3] S. Pérez, J.L. Hernández-Ramos, S.N. Matheu-García, D. Rotondi, A. Skarmeta, L. Straniero, D. Pedone, “A Lightweight and Flexible Encryption Scheme to Protect Sensitive Data in Smart Building Scenarios”. *IEEE Access* **2018**, *6*, 11738–11750. doi:10.1109/ACCESS.2018.2801383.

[P4] S.N. Matheu García, J.L. Hernández Ramos, A. Skarmeta, “Test-Based Risk Assessment and Security Certification Proposal for the Internet of Things”. *IEEE 4th World Forum on Internet of Things (WF-IoT)* **2018**, 641–646. doi:10.1109/WF-IoT.2018.8355193.

[P5] S.N. Matheu García, J.L. Hernández Ramos, A. Skarmeta, “Toward a Cybersecurity Certification Framework for the Internet of Things”. *IEEE Security Privacy* **2019**, *17, 3* , 66–76. doi:10.1109/MSEC.2019.2904475.

[P6] S.N. Matheu García, J.L. Hernández Ramos, A. Skarmeta, G. Baldini, “Risk-Based Automated Assessment and Testing for the Cybersecurity Certification and Labelling of IoT Devices”. *Computer Standards and Interfaces* **2019**, *62* , 64–83. doi:10.1016/j.csi.2018.08.003.

[P7] S.N. Matheu García, A. Molina Zarca, J.L. Hernández Ramos, J.B. Bernabé, A. Skarmeta, “Enforcing Behavioral Profiles through Software-Defined Networks in the Industrial Internet of Things”. *Appl. Sci.* **2019**, *9*, 4576. doi:10.3390/app9214576.

[P8] S.N. Matheu, J.L. Hernández Ramos, S. Perez, A. Skarmeta, “Extending MUD profiles through an Automated IoT Security Testing Methodology”. *IEEE Access* **2019**, *7*, 149444–149463. doi:10.1109/ACCESS.2019.2947157.

[P9] R. Neisse, J.L. Hernández-Ramos, S.N. Matheu, G. Baldini, A. Skarmeta, “Toward a Blockchain-Based Platform to Manage Cybersecurity Certification of IoT Devices”. *IEEE Conference on Standards for Communications and Networking (CSCN)* **2019**, 1–6. doi:10.1109/CSCN.2019.8931384.

[P10] G. Baldini, J.L. Hernández-Ramos, G. Steri, S.N. Matheu, “Zone Keys Trust Management in Vehicular Networks Based on Blockchain”. *Global IoT Summit (GIoTS)* **2019**, 1–6. doi:10.1109/GIOTS.2019.8766375.

[P11] S.N. Matheu, S. Pérez, J.L. Hernández-Ramos, A. Skarmeta, “On the Automation of Security Testing for IoT Constrained Scenarios”. *20th World Conference on Information Security Applications (WISA)* **2019**, *LNCS 11897*, 286-298. doi:https://doi.org/10.1007/978-3-030-39303-8_22.

[P12] S.N. Matheu García, A. Robles Enciso, A. Molina Zarca, D. García Carrillo, J.L. Hernández Ramos, J.B. Bernabé, A. Skarmeta, "Security Architecture for Defining and Enforcing Security Profiles in DLT/SDN-Based IoT Systems". *Sensors* **2020**, *29, 7* , 1882. doi:10.3390/s20071882.

[P13] S. N. Matheu and A. Skarmeta, "Cybersecurity Certification in IoT Environments" in Security Risk Management for the Internet of Things: Technologies and Techniques for IoT Security, Privacy and Data Protection. *Edited by John Soldatos, River Publishers* **2020**, 178–195. doi:10.1561/9781680836837.ch10.