1

Introducing the Challenges in Cybersecurity and Privacy: The European Research Landscape

Jorge Bernal Bernabe and Antonio Skarmeta

Department of Information and Communications Engineering,
University of Murcia, Murcia, Spain
E-mail: jorgebernal@um.es; skarmeta@um.es

The continuous, rapid and widespread usage of ICT systems, the constrained and large-scale nature of certain related networks such as IoT (Internet of Things), the autonomous nature of upcoming systems, as well as the new cyber-threats appearing from new disruptive technologies, are given rise to new kind of cyberattacks and security issues. In this sense, this book chapter categorises and presents 10 current main cybersecurity and privacy research challenges, as well as 14 European research projects in the scope of cybersecurity and privacy, analysed further throughout this book, that are addressing these challenges.

1.1 Introduction

The widespread usage and development of ICT systems is leading to new kind of cyber-threats. Cyberattacks are continuously emerging and evolving, exploiting disruptive systems and technologies such as Cyber Physical Systems (CPS)/IoT, virtual technologies, clouds, mobile systems/networks, autonomous systems (e.g. drones, vehicles). Cyber attackers are continuously improving their techniques to come up with stealth and sophisticated attacks, especially against IoT, since these environments suffer additional vulnerabilities due to their constrained capabilities, their unattended nature

and the usage of potential untrustworthiness components. Similarly, identity-theft, fraud, personal data leakages, and other related cyber-crimes are continuously evolving, causing important damages and privacy problems for European citizens in both virtual and physical scenarios.

In this evolving cyber-threat landscape, we have identified 10 main cybersecurity and privacy research challenges (described in Section 2 of this chapter):

1. Interoperable and scalable security management in heterogeneous ecosystems
2. Autonomic security orchestration and enforcement in softwarized and virtualized IoT/CPS systems and mobile environments
3. Cognitive detection and mitigation of evolving new kind of cyber-threats
4. Dynamic Risk assessment and evaluation of cybersecurity, trustworthiness levels, privacy and legal compliance of ICT systems
5. Digital Forensics handling, security intelligent and incident information exchange
6. Cybersecurity and privacy tools for end-users and SMEs. The usability and human factor challenges
7. Reliable and privacy-preserving physical and virtual identity management
8. Efficient and secure cryptographic mechanisms to strengthen confidentiality and privacy
9. Global trust management of eID and related services
10. Privacy assessment, run-time evaluation of the quality of security and privacy risks

To meet those challenges, new holistic approaches, methodologies, techniques and tools are needed to prevent and mitigate cyberattacks by employing novel cyber-situational awareness frameworks, risk analysis and modelling tools, threat intelligent systems, cyber-threat information sharing methods, advanced big-data analysis techniques as well as new solutions that can exploit the benefits brought from latest technologies such as SDN/NFV and Cloud systems. In addition, novel privacy-preserving techniques, and crypto-privacy mechanisms, identity and eID management systems, trust services, and recommendations are needed to protect citizens' privacy while keeping usability levels.

The European Commission is addressing the aforementioned challenges through different means, including the Horizon 2020 Research and

Innovation program, thereby financing innovative research projects that can cope with the increasing cyberthreat landscape.

In this sense, the cybersecurity strategy of the European Union is summarized in 5 strategic priorities "An Open, Safe and Secure Cyberspace" [1]

- *Achieving Cyber resilience;*
- *Reducing cybercrime;*
- *Developing a cyber defense policy and capabilities related to the Common Security and Defense Policy (CSDP);*
- *Developing the industrial and technological resources for cybersecurity;*
- *Establishing a coherent international cyberspace policy for the European Union that promoted core EU values.*

Namely, the European program H2020-EU.3.7 [2] – "Secure societies – Protecting freedom and security of Europe and its citizens", budget with 1694.60 million, is addressing those cybersecurity and privacy challenges. The general objective in that program is "*to foster secure European societies in a context of unprecedented transformations and growing global interdependencies and threats, while strengthening the European culture of freedom and justice*."

Thus, the H2020-EU.3.7 program is addressing the global challenge about *"undertaking the research and innovation activities needed to protect our citizens, society and economy as well as our infrastructures and services, our prosperity, political stability and wellbeing."* Namely, this programme [3] aims:

- *"to enhance the resilience of our society against natural and man-made disasters, ranging from the development of new crisis management tools to communication interoperability, and to develop novel solutions for the protection of critical infrastructure;*
- *to fight crime and terrorism ranging from new forensic tools to protection against explosives;*
- *to improve border security, ranging from improved maritime border protection to supply chain security and to support the Union's external security policies including through conflict prevention and peace building;*
- *and to provide enhanced cybersecurity, ranging from secure information sharing to new assurance models."*

In this context, this book presents and analyses 14 cybersecurity and privacy-related EU projects founded by this H2020 program, encompassing: ANASTACIA, SAINT, FORTIKA, CYBECO, SISSDEN, CIPSEC, CS-AWARE. RED-Alert, Truessec.eu. ARIES, LIGHTest, CREDENTIAL, FutureTrust. For further information about other H2020 EU projects funded under this H2020-EU.3.7 the reader is refereed to [2].

Each chapter in the book is dedicated to a different funded European Research project and includes the project's overviews, objectives, and the particular research challenges, among the ones identified above, that they are facing. In addition, each EU research project in his corresponding chapter describes its research achievements on security and privacy, as well as the techniques, outcomes, and evaluations accomplished in the scope of the corresponding EU project.

The idea of this book was originated after a successful clustering workshop entitled "*European projects Clustering workshop On Cybersecurity and Privacy (ECoSP 2018)*" [4] collocated in ARES Conference – 13th International Conference on Availability, Reliability and Security, where the EU projects analyzed in this book were presented and the attenders exchanged their views about the European research landscape on Security and privacy.

The rest of this chapter is structured as follows. Section 2 presents the main security and privacy research challenges. Section 3 is devoted to the introduction of the main H2020 EU projects covered in this book, and the main challenges, among the ones identified in Section 2, that each project is facing. Section 4 concludes this chapter.

1.2 Cybersecurity and Privacy Research Challenges

The Ponemon Institute in a recent study [23], identified the Cyber threats with the greatest risk: Cyber warfare or cyber terrorism, Breaches involving high-value information, Nation-state attackers, Breaches that damage critical infrastructure, Breaches that disrupt business and IT processes, Emergence of cyber syndicates, Stealth and sophistication of cyber attackers, Emergence of hacktivism, Breaches involving large volumes of data, Malicious or criminal insiders, Negligent or incompetent employees. The study highlights that Cyber warfare and cyber terrorism and breaches involving high-value information will have the greatest impact on organizations over the next three years.

These cyber-threats are especially notorious and dangerous when affecting IoT and CPS, where massive heterogenous, and potentially

constrained, things are being added to the network, meaning additional potential vulnerabilities. In this regard, Roman et al. [19] identified the main "Challenges of Security & Privacy in Distributed Internet of Things". Namely, they provided and analysis of attacker models and threats and identified 7 main challenges in the design and deployment of the security mechanisms, including: Identity and Authentication, Access control, Protocol and Network Security, Privacy, Trust management, Governance, Fault tolerance.

Additionally, recently [22] identified the security and privacy threats in IoT at different network layers, including the major security vulnerabilities. In that paper authors highlighted the main aspects of the IoT ecosystem, such as, having legacy systems running in these platforms, the large number of devices, dynamicity, constrained nature, which are provoking new kind of threats. Likewise, [25] reviewed the IoT cybersecurity research, highlighting the data handling issues, standardization aspects, and research trends when IoT meets Cloud Computing and 5G technologies. Other research trends (Fault Tolerance Mechanism, Self-Management, IoT Forensics, Blokchain Embedded Cybersecurity Design) are also studied.

Besides, Backes et al. [24] identified their 8 most important challenges in IT security research. Including, (1) Security for Autonomous Systems, (2) Security in Spite of Untrustworthy Components, (3) Security Commensurate with Risk, (4) Privacy for Big Data, (5) Economic Aspects of IT Security, (6) Behaviour-related and Human Aspects of IT Security (7) Security of Cryptographic Systems against Powerful Attacks, (8) Detection and Reaction.

The characterization presented herein includes most of those security research challenges but, unlike their work, we use another perspective and for us some of their research challenges (such as economic aspects) are out of our main challenges, as they are not such important in our classification.

The main cybersecurity and privacy research challenges identified are described below. It should be noted that order of challenges does not have any relation with the order of importance or impact of the challenges.

1.2.1 Main Cybersecurity Research Challenges

1. **Interoperable and scalable security management in heterogeneous ecosystems**
   Security Management in fragmentated and heterogeneous domains is still nowadays an open research challenge. This issue is exacerbated in CPS/IoT deployments which are comprised of heterogenous disparate

kind of devices and networks protocols/systems. Security management requires a holistic approach to deal with new types of wireless network technologies (e.g. 5G), potentially constrained networks (e.g. LPWANs), protocols and systems, that need to face the management of large and scalable deployments in any segment of network: RAN, Edge, Fog or Core segments.

The definition of security management policies to deal with heterogeneity and interoperability across domains, systems and networks, introduces several challenges related to the employed security models, the language and the level of abstraction required to govern the systems. In this regard, interoperability and contextual aspects in policies, particularities of managed systems domains, policy conflicts and resolution as well as dependencies in policies, are open research challenges that need to be solved. The policies should encompass not only security/privacy policies, but also QoS/SLA policies, network management policies (e.g. slicing, traffic filtering), operational and orchestration policies.

2. **Autonomic security orchestration and enforcement in softwarized and virtualized IoT/CPS systems and mobile networks**
   - *Holistic security orchestration*: New autonomic and context-awareness security orchestrators are needed, which can choregraph and enforce quickly and dynamically the proper defence mechanism (proactively or as countermeasure), according to the circumstances, in SDN/NFV-enabled systems. The orchestration will need to face the challenge to interface with diverse, heterogeneous and distributed IoT controllers, NFV-MANO (Management and Orchestration) orchestrators, Fog-Edge entities, SDN controllers, thereby enforcing dynamically the security enablers in the network/systems.
   - *Virtualized and Softwarized security management*: current defences of network operators and companies are mainly based on hardware appliances. Naturally, the hardware appliances have fixed location that must be chosen by the ISP smartly. These hardware appliances can be deployed on-premises or outsourced, and the packets/flows are redirected to these hardware appliances. Using the virtualization enabled by SDN and NFV allows a quick instantiation of VMs in the adequate location. Indeed, the lack of elasticity can be easily handled by Security Virtual Network Function (VNF) functions that can be chained and placed on-demand according to the incoming attacks.

However, it is challenging to manage the orchestration and placement of multiple VNFs on an NFV Infrastructure at large scale, either at the core of at the edge of the network, while dealing with scalability and security issues and additional threats that raise from the fact of using a virtualized environment.

- *Selection of the adequate mitigation plan*: and fast enforcement of the defined policies are challenging processes that require a lot of efforts and time. The orchestration and the enforcement of the adequate countermeasures in a short time, and without affecting the Quality of Service (QoS), introduce several challenges that must be duly considered. Also, the definition and enforcement of mitigation plans while reducing the deployment cost and by taking into account the limitations in existing infrastructure clouds, the system/network status and are open research questions that needs to be addressed.
- *Lightweight Security enablers and protocols for IoT/CPS systems*: Traditional security enablers and protocols, encompassing Authentication, Authorization and Accounting (AAA), Channel protection protocols, network filtering, deep packet inspection, intrusion detection..., need to be evolved and adapted to be able to be enforced and managed properly in softwarized and virtualized networks (SDN/NFV) and CPS/IoT systems. In addition, these security enablers and protocols need to be redesigned to cope with the constrained nature of distributed IoT networks, that requires lightweight crypto-protocols and solutions to be enforced in constrained (battery, memory, cpu) devices and networks.
- *Security in 5G mMTC and mobile networks*: 5G mMTC (massive Machine-type Communications) is the key technology needed to scale up the internet of thing (IoT). However, this 5G large-scale management and orchestration raises new cybersecurity threats which requires novel security solutions, as analysed in [26]. 5G imports vulnerabilities and threats coming from cloud computing, virtualization and SDN/NFV technologies. Thus, it is a research challenge to deal with information transmission management, secure communication channels, new security interfaces for AAA to deal with Non-Access Spectrum (NAS) signalling, roaming security, and cope with diverse network-based mobile security threats and attacks (e.g. saturation attacks, penetration attacks, identity thief, Man-in-the-middle, scanning attaks, Hijacking, DoS attacks, Signaling storms).

3. Cognitive detection and mitigation of evolving new kind of cyber-threats

- *Dealing with evolving kind of cyberattacks*: The identification of novel types of attacks not yet identified before (e.g. unknown zero-day attacks), that can exploit IoT networks, CPS (and the consequent protection approaches to provide advanced security from last generation threats) is a key research challenge. This new kind of attacks need to be addressed following a global approach through both, signature-based and anomaly-based detection techniques, by using artificial intelligence and Big Data analysis approaches. In the cyber physical world, the attacker's goal is to disrupt both the normal operations of the CPS, e.g. sensor readings, safety limits violation, status reports, safety compliance violation etc. and communication flows among devices. The continued rise of cyber-attacks together with the evolving skills of the attackers, and inefficiency of the traditional security algorithms to defend against advanced and sophisticated attacks such as DDoS, slow DoS and zero-day, demand the development of novel defence and resilient detection techniques.
- *Monitoring in heterogenous ICT systems*. Cybersecurity handling, especially in Critical systems, Cyber Physical Systems and IoT networks introduces challenges due the restrictions and constrained nature of these kind of devices and networks. New tools, for network scanning (including encrypted traffic), analysis of digital forensics and pen testing as well as innovative algorithms and techniques (e.g. machine learning) are needed to perform security analysis.
- *Real-time incident detection and analysis*: Incident analysis should be supported by risk models that follows a multidimensional approach, performing evaluation of incidents that combines several factors (such as, for instance, incident severity, criticality of assets affected, global risk associated to the incident or cost of potential mitigations among others) to decide, if needed, dynamically the most convenient mitigation plan to enforce. It should cover, threat analysis, data fusion and correlation from different sources different types of events to detect hidden relations and thus identify potential threats.
- *Cyber situational-awareness, self-learning and dynamic reaction for self-healing, self-repair and self-protection capabilities*: Management and Control systems as well as Autonomous systems, such as for instance, drones, smart objects, self-driving cars, robots, etc, will need

to perform self-learning to make proper intelligent decisions based on current real-time situation. However, those autonomous systems could be manipulated when sensing the external world, and therefore, assessing the quality of the potential sensed environment is a challenge. In addition, upcoming cybersecurity frameworks and systems should face the challenge of countering dynamically cyberattacks according to contextual and evolving conditions, thereby providing self-healing, self-repair and self-protection capabilities. This will allow to diagnose and enforce proper defence mechanism and mitigate threats autonomously.

- *Cognitive big data analysis of systems/networks, services, social networks and cybersecurity intelligence information to counter cyber-threats*: To meet this challenge an interdisciplinary approach should be followed, performing cognitive science, communications, computational linguistics, discourse processing, language studies and social psychology. Upcoming cybersecurity solutions should meet the challenge of combing diverse technologies, such for instance, IA algorithms, Machine Learning (ML), CEP (Complex Event Processing), SNA (Social Network Analysis) and NLP (Natural Language processing) to assess systems data/events, social features in communications used by terrorist organizations, in order to increase security levels and counter cyber-threats.

4. **Dynamic risk assessment and evaluation of cybersecurity, trustworthiness levels and legal compliance of ICT systems**
   New models are needed to quantify in real time, according to the context, the trustworthiness, of new kind of devices-system-networks, compute the risk associated to an ICT system and evaluate the security and privacy legal compliance. Risk evaluation should be performed through an interdisciplinary approach including not only technological, but also legal and socio-ethical perspectives. Relevant metrics need to be established for cybersecurity economic analysis, cybersecurity and cybercrime market. The risk evaluation should consider automated analysis, for behavioural, social analysis, cybersecurity risk and cost assessment. In this regard, another challenge is to make this risk analysis usable and easy interpretable for administrators and stakeholders, through short and long terms actions and recommendations.

   Another related challenge is to kept users informed about the trustworthiness levels of their application and servers, according to multi

factor criteria, encompassing sociocultural, legal, ethical, technological and business while paying due attention to the protection of Human Rights. Proper recommendations about certification and labelling of ICT products and services should be automatically inferred, that will foster trust among citizens that use them.

5. **Digital forensics handling, security intelligence and incident information exchange**
   An important cybersecurity challenge is to improve levels of collaboration between cooperative and regulatory approaches for information sharing in order to enhance cybersecurity and mitigate the risk and the impact of cyber-attacks. In this regard, new standards, models, protocols are needed to achieve interoperability for effective collaboration between operational teams including Law Enforcement Agencies, CSIRTs, Organization, through automated exchange of cybercrime data, including source Open Source Intelligence (OSINT) data sources, thereby allowing sharing the own system cyber-situational awareness information with the external entities in an effective way. In addition, another challenge is to perform automatic application and enforcement of data sharing in an interoperable manner that can feed the incident analysis, which ultimately, can help in the cybersecurity decision support making.

6. **Cybersecurity and privacy tools for end-users and SMEs. The usability and human factor challenges**
   Individuals, SMEs, local administrators and related end-users are overwhelmed with the complexity of cybersecurity and privacy aspects, which obstructs proper decision making and digital technology usage. These kinds of users cannot dedicate enough effort and resources to invest in security personnel and cybersecurity products or services. User-friendly and automated cybersecurity unified tools need to implemented targeting (potential inexpert) final users, so that they can face cybersecurity threats and manage properly security configurations. The human factor is one of the most problems when it comes to security management, as it can easily generate new security gaps. Most of the cyber-attacks such as ramsonware, physing, identity chief, etc, are originated by the end-user. Thus, the human factor needs to be handled by cybersecurity frameworks and tools in order to increase system resilience against end-users' and operators' errors.

1.2.2 Privacy and Trust Related Research Challenges

7. **Reliable and privacy-preserving physical and virtual identity management**
   Identity management Systems require new security and privacy mechanisms that can holistically manage user's/object's privacy, ID-proofing techniques based on multiple biometrics, strong authentication, usage of breeder documents (e.g. eID, ePassports), while ensuring privacy-by-default, unlikability, anonymity, federation support, non-reputation and self-sovereign IdM management. The challenge is to manage properly those features for mobile, online or physical/face-to face scenarios, while maintaining usability and compliance with regulation e.g. GDPR (General Data Protection Regulations)[GDPR] and eIDAS [21]. This will allow ultimately to reduce identity-theft and related cybercrimes.

   In this context, another challenge arises from the extension of global identity management and AAA to *anything* deployments, managing efficiently identities and access control of new kinds of autonomous Systems, such as, IoT smart objects, self-driving cars, robots, humanoids, drones, etc. that requires new evolved algorithms, protocols and systems.

8. **Efficient and secure cryptographic mechanisms to strengthen confidentiality and privacy**
   - *Confidentiality and privacy in distributed systems*: End-to-end encryption of shared data, in transit and in rest, while maintaining usability and efficiency on the end-user side is an open research challenge that still needs to be covered effectively to protect user's privacy. In this sense, new techniques, algorithms and protocols, e.g. those based on proxy re-encryption, are needed to reinforce security/privacy while outsourcing the computation to Cloud wallets to minimize user's risks in protecting crypto-material. In addition, new crypto-privacy techniques are needed to guarantee authenticity on the data through novel signatures schemes.
   - *Data anonymization and secure data sharing*: All exchanged data should be encrypted, without intermediate entities such as proxies or cloud-providers being able to access the user's data. Data minimization and privacy-by-default properties, above all, in emerging distributed deployments needs to be guaranteed. Thus, novel crypto-privacy protocols, mechanism and systems, such as those based

on Zero-knowledge proofs, are needed to ensure anonymity, minimal disclosure of personal information, above all in public Clouds, ledgers and mobiles, while ensuring the user's rights laid out in GDPR.

- *Big data privacy*: Data analytics raises new concerns about privacy preservation, as the possible dynamic combination of large data coming from diverse sources can undermine anonymity, pseudonimity properties that can be given for granted in a single domain. This challenge is especially relevant in critical sectors (eHealth, eBanking), distributed systems that will handle massive user data, e.g. blockchains, ledgers, and social networks. Therefore, new technologies to enforce efficient privacy protection are needed, as a response of a new collaborative privacy-assessment mechanisms.
- *Crypto-resilience to brute-force attacks*: Quantum computing technology is making possible new risks and threats, as most of current encryption and signature algorithms will not be fully secure against brute-force attacks perpetrated by quantum computers. In this sense, new cryptographic algorithms are needed to be resilient to brute-force attacks using quantum computing.

9. **Global trust management of eID and related services**
There is a need of a Global, trusted, open and scalable infrastructure where authorities can publish their trust information to certify trustworthy electronic identities, so that rest of stakeholders, including public sector, private companies, and citizens can verify automatically trust in electronic transactions, while hiding the complexity of dealing with heterogenous formats and protocols.

   This challenging Global Trust System should deal with issues such as unified data model, rights delegation, trust policy language, claims discovery to make the system interoperable accessible for everyone, while facilitating, at the same time, the use of eID and electronic signature technology in real world applications. This global trust management infrastructure should leverage the eIDAS trust scheme laid out in Regulation (EU) N°910/2014 [21], extending the European Trust Service Status List (TSL) infrastructure towards a "Global Trust List".

10. **Privacy assessment, run-time evaluation of the quality of security and privacy risks** There is a need of evaluation tools and methods to assess whether an application or a service is compliant with privacy and personal data protection principles, as well as quantitative and qualitative run-time evaluation of the quality of security and privacy risks.

In this sense, novel Dynamic Security and Privacy Seals (DSPS) are needed to increase trust in the system, by combining ISO, legal norms and security and privacy standards with deep technical monitoring integration, in order to provide a user-friendly and synthetic view of the overall system trust ability. In this regard, it is challenging to integrate and enhance the alerts generated by the underlying systems with direct technical and organizational feedback from the end-user. These novel kinds of seals would come up with legally valid and non-repudiable proof of compliance of the system with legal or contractual security-privacy requirements, which can be easily managed and visualized by the user.

1.3 H2020 Projects Facing the Challenges

1.3.1 Cybersecurity Related Projects Addressing the Challenges

- **ANASTACIA** [5] (Chapter 02): ANASTACIA is researching, developing and demonstrating a holistic solution enabling trust and security by-design for Cyber Physical Systems (CPS) based on IoT and Cloud architectures. ANASTACIA cybersecurity framework provides self-protection, self-healing and self-repair capabilities through novel enablers and components. The framework dynamically orchestrates and deploys security policies and actions that can be instantiated on local agents. Thus, security is enforced in different kinds of devices and heterogeneous networks, e.g. IoT – or SDN/NFV – based networks. The framework has been designed in full compliance to SDN/NFV standards as specified by ETSI NFV and OFN SDN, respectively. Therefore, Anastacia is addressing challenges #1, #2, #3 and #4 enumerated in Section 2.1
- **SAINT** [6] (Chapter 03): "SAINT analyses and identifies incentives to improve levels of collaboration between cooperative and regulatory approaches to information sharing. SAINT is designing new methodologies for the development of an ongoing and searchable public database of cybersecurity indicators and open source intelligence. Comparative analysis of cyber-crime victims and stakeholders within a framework of qualitative social science methodologies deliver valuable evidences and advance knowledge on privacy issues and deep web practices. SAINT defines innovative models, algorithms and automated framework for cost-benefit analysis and estimation of tangible and intangible costs

for optimal risk and investment incentives". Thus, SAINT is mainly focusing on challenge #5 enumerated in Section 2.1.

- **FORTIKA** [7] (Chapter 04): "The project is designing and implementing a security 'seal' specially devised for small and medium-sized companies that will strengthen trust and facilitate further adoption of digital technologies. The project is implementing robust, resilient and effective cybersecurity solutions to be customized for each individual enterprise's evolving needs and can also speedily adapt/respond to the changing cyber threat landscape". Therefore, FORTIKA is mainly focusing on challenges #2 and #6 of those described in Section 2.1.
- **CYBECO** [8] (Chapter 05): "CYBECO focuses on two mains aspects to deal with cyber-insurance from a Behavioural Choice Perspective: (1) including cyber threat behaviour through adversarial risk analysis to support insurance companies in estimating risks and setting premiums and (2) using behavioural experiments to improve IT owners' cybersecurity decisions. Therefore, CYBECO facilitates risk-based cybersecurity investments supporting insurers in their cyber offerings through a risk management modelling framework and tool." Therefore, SAINT is mainly focusing on challenge #4 of Section 2.1.
- **SISSDEN** [9] (Chapter 06): "SISSDEN is intended to improve the cyber security through development of situational awareness and sharing of actionable information. The passive threat data collection mechanism is complemented by behavioural analysis of malware and multiple external data sources. Actionable information produced by SISSDEN provides no-cost victim notification and remediation via organizations such as CERTs, ISPs, hosting providers and LEAs such as EC3. The main goal of the project is the creation of multiple high-quality feeds of actionable security information that can be used for remediation purposes and for proactive tightening of computer defences. This is achieved through the development and deployment of a distributed sensor network based on state-of-the-art honeypot and darknet technologies, the creation of a high-throughput data processing centre, and provisioning of in-depth analytics, metrics and reference datasets of the collected data." Therefore, SISSDEN is mainly focusing on challenge #5 of Section 2.1.
- **CIPSEC** [10] (Chapter 07): "CIPSEC aims to create a unified security framework that orchestrates state-of-the-art heterogeneous security products to offer high levels of protection in IT (information technology)

and OT (operational technology) departments of CIs, also offering a complete security ecosystem of additional services. These services include vulnerability tests and recommendations, key personnel training courses, public-private partnerships (PPPs), forensics analysis, standardization activities and analysis against cascading effects." CIPSEC is mainly focusing on challenge #3, #4 and #5 of Section 2.1.

- **CS-AWARE** [11] (Chapter 08): CS-AWARE aims to increase the automation of cybersecurity awareness approaches, by collecting cybersecurity relevant information from sources both inside and outside of monitored local public administrations (LPA) systems, performing advanced big data analysis to set this information in context for detecting and classifying threats and to detect relevant mitigation or prevention strategies. CS-AWARE aims to advance the function of a classical decision support system by enabling supervised system self-healing in cases where clear mitigation or prevention strategies for a specific threat could be detected. CS-AWARE is built around this concept and relies on cybersecurity information being shared by relevant authorities in order to enhance awareness capabilities. At the same time, CS-AWARE enables system operators to share incidents with relevant authorities to help protect the larger community from similar incidents. CS-AWARE is mainly focusing on challenge #5 of Section 2.1.
- **RED-Alert** [12] (Chapter 09): "RED-Alert has built a complete software toolkit to support LEAs in the fight against the use of social media by terrorist organizations for conducting online propaganda, fundraising, recruitment and mobilization of members, planning and coordination of actions, as well as data manipulation and misinformation. The project aims to cover a wide range of social media channels used by terrorist groups to disseminate their content which will be analysed by the RED-Alert solution to support LEAs to take coordinated action in real time but having as a primordial condition preserving the privacy of citizens." RED-Alert is mainly focusing on challenge #3 of Section 2.1.
- **Truessec.eu** [13] (Chapter 10): "The main goal of TRUESSEC project is to foster trust and confidence in new and emerging ICT products and services throughout Europe by encouraging the use of assurance and certification processes that consider multidisciplinary aspects such as sociocultural, legal, ethical, technological and business while paying due attention to the protection of Human Rights." Therefore, TRUESSEC is mainly addressing challenge #4.

Table 1.1 Main cybersecurity research challenges and related EU project's

Challenge ID	Name	EU projects addressing the challenge
1	Interoperable and scalable security management in heterogeneous ecosystems	ANASTACIA
2	Autonomic Security orchestration and enforcement in softwarized and virtualized IoT/CPS systems and mobile environments	ANASTACIA, FORTIKA, CIPSEC
3	Cognitive detection and mitigation of evolving new kind of cyber-threats	ANASTACIA, CIPSEC, CS-AWARE, RED-ALERT
4	Dynamic Risk assessment and evaluation of cybersecurity, trustworthiness levels, privacy and legal compliance of ICT systems	CYBECO, CIPSEC, TRUESSEC, ANASTACIA
5	Digital Forensics handling, security intelligent and incident information exchange	SIESSDEN, SAINT, CIPSEC, CS-AWARE
6	Cybersecurity and privacy tools for end-users and SMEs. The usability and human factor challenges	FORTIKA

Table 1.1 recaps the main cybersecurity research challenges presented in Section 1.2.1 and links them with the EU project's, presented in this section, that are addressing those challenges.

1.3.2 H2020 Projects Addressing the Privacy and Trust Related Challenges

- **ARIES** [14] (Chapter 11): Aries aims to set up a reliable identity ecosystem encompassing technologies, processes and security features that ensure highest levels of quality in secure credentials for highly secure and privacy-respecting physical and virtual identity management processes with the specific aim to tangibly achieve a reduction in levels of identity fraud, theft, wrong identity and associated crimes. The ecosystem is strengthening the link between physical documents linked to the biometric identity and the digital (online and mobile) identity.
- **LIGHTest** [15] (Chapter 12): LIGHTest project aims to set-up a global trust infrastructure where authorities can publish their trust information. Thus, member states can use infrastructure to publish lists of qualified trust services, while private companies can establish trust in different sectors, such as, inter-banking, international trade, shipping, business reputation and credit rating. Then, different entities can query this trust

information to verify trust in simple signed documents or multi-faceted complex transactions.

- **CREDENTIAL** [16] (Chapter 13): CREDENTIAL project has developed a cloud-based service for identity provisioning and data sharing. On the one hand, it offers high confidentiality and privacy guarantees to the data owner, while, on the other hand, it offers high authenticity guarantees to the receiver. CREDENTIAL integrates advanced cryptographic mechanisms into standardized authentication protocols. The solution has proved high user convenience, strong security, and practical efficiency.
- **FutureTrust** [17] (Chapter 14): The FutureTrust project aims to develop a comprehensive Open Source validation service as well as a scalable preservation service for electronic signatures and will provide components for the eID-based application for qualified certificates across borders, and for the trustworthy creation of remote signatures and seals in a mobile environment. Furthermore, the FutureTrust project extends and generalize existing trust management concepts to build a "Global Trust List", which allows to maintain trust anchors and metadata for trust services and eID related services around the globe.
- **LEPS** [18] (Chapter 15): LEPS project aims to "validate and facilitate the connectivity options to recently established eIDAS ecosystem, which provides this trusted environment with legal, organisational and technical guarantees already in place. Strategies have been devised to reduce SP implementation costs for this connectivity to eIDAS technical infrastructure". The project has implemented integrated and validated the solution in Pilots of two EU countries.

Table 1.2 summarizes the main privacy-related research challenges presented in Section 1.2.2 and links them with the EU project's, presented in this section, that are addressing those challenges.

Table 1.2 Main Privacy related research challenges and related EU projects

Challenge ID	Name	EU projects addressing the challenge
7	Reliable and privacy-preserving physical and virtual identity management	ARIES, LEPS
8	Efficient and secure cryptographic mechanisms to strengthen confidentiality and privacy	CREDENTIAL
9	Global trust management of eID and related services	LIGHTest, Future Trust
10	Privacy assessment, run-time evaluation of the quality of security and privacy risks	ANASTACIA

1.4 Conclusion

This chapter has identified and introduced the 10 main cybersecurity and privacy research challenges presented and addressed in this book by 14 European research projects. Some of the challenges revolve around the autonomic cybersecurity management, orchestration and enforcement in heterogeneous and virtualized CPS/IoT and mobile ecosystems. The challenges identified cognitive detection and mitigation of evolving new kind of cyber-threats; the dynamic risk assessment and evaluation of cybersecurity, trustworthiness levels, privacy and legal compliance of ICT systems; the digital Forensics handling; the security intelligent and incident information exchange; and cybersecurity and privacy tools and the associated usability and human factor. Regarding privacy and trust related challenges, we have identified four main global ones, encompassing the reliable and privacy-preserving identity management, efficient and secure cryptographic mechanisms, Global trust management and privacy assessment.

In addition, the chapter has introduced the 14 EU projects analysed in the book and the main challenges the are addressing. ANASTACIA, SAINT, FORTIKA, CYBECO, SISSDEN, CIPSEC, CS-AWARE. RED-Alert, Truessec.eu. ARIES, LIGHTest, CREDENTIAL, FutureTrust.

The rest of the book is intended to present each of those 14 EU projects, which are described in a different book chapter. Each chapter includes the project's overviews and objectives, the particular challenges they are covering, research achievements on security and privacy, as well as the techniques, outcomes, and evaluations accomplished in the scope of the EU project.

Acknowlegdements

This work has been supported by a postdoctoral INCIBE grant "Ayudas para la Excelencia de los Equipos de Investigación Avanzada en Ciberseguridad" Program, with Code INCIBEI-2015-27363. This book chapter has also received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 700085 (ARIES project).

References

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. (2013). Available at from: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

[2] H2020-EU.3.7. – Secure societies – Protecting freedom and security of Europe and its citizens. https://cordis.europa.eu/programme/rcn/664463/en

[3] Secure societies – Protecting freedom and security of Europe and its citizens Last accessed 10/04/1 from: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens

[4] European projects Clustering workshop On Cybersecurity and Privacy (ECoSP 2018) https://2018.ares-conference.eu/workshops/ecosp-2018/. held in conjunction with the 13th International Conference on Availability, Reliability and Security (ARES 2018 – http://www.ares-conference.eu)

[5] ANASTACIA (Advanced Networked Agents for Security and Trust Assessment in CPS / IOT Architectures) H2020 EU project, Grant Agreement No. 731558 http://anastacia-h2020.eu/

[6] SAINT (Systemic Analyzer In Network Threats) H2020 EU project, Grant Agreement No. 740829 https://project-saint.eu/

[7] FORTIKA (Cyber Security Accelerator for trusted SMEs IT Ecosystem) H2020 EU project, Grant Agreement No. 740690. http://fortika-project.eu/

[8] CYBECO (Supporting Cyberinsurance from a Behavioural Choice Perspective) H2020 EU project, Grant Agreement No. 740920. https://www.cybeco.eu/

[9] SISSDEN (Secure Information Sharing Sensor Delivery Event Network) H2020 EU project, grant Agreement No. 700176. https://sissden.eu/

[10] CIPSEC (Enhancing Critical Infrastructure Protection with innovative SECurity framework) H2020 EU project, Grant Agreement No. 700378 http://www.cipsec.eu/

[11] CS-AWARE (A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced

big data analysis) H2020 EU project, Grant Agreement No. 740723. https://cs-aware.eu/
[12] RED-Alert (Real-time Early Detection and Alert System) H2020 EU project, Grant Agreement No. 740688 http://redalertproject.eu/
[13] Truessec.eu (TRUst-Enhancing certified Solutions for SEcurity and protection of Citizens' rights in digital Europe) H2020 EU project, Grant Agreement No. 731711 http://truessec.eu/
[14] Aries (ReliAble euRopean Identity EcoSystem), H2020 EU Project Grant Agreement No. 700085 https://www.aries-project.eu/
[15] LIGHTest (Lightweight Infrastructure for Global Heterogeneous Trust management in support of an open Ecosystem of Stakeholders and Trust schemes), H2020 EU Project Grant Agreement No. 700321, https://www.lightest.eu/
[16] CREDENTIAL (Secure Cloud Identity Wallet), H2020 EU project, Grant Agreement No. 653454, https://credential.eu/
[17] FutureTrust (Future Trust Services for Trustworthy Global Transactions), H2020 EU project, Grant Agreement No. 700542 https://www.futuretrust.eu/
[18] LEPS (Leveraging eID in the Private Sector), European Union's Connecting Europe Facility, Grant Agreement No. INEA/OEF/ICT/A2016/1271348. http://www.leps-project.eu/
[19] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279.
[20] Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, 104(9), 1727–1765.
[21] European Parliament, 'Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC', European Parliament, Brussels, Belgium, Regulation 910/2014, 2014.
[22] Ziegler, S., Crettaz, C., Kim, E., Skarmeta, A., Bernabe, J. B., Trapero, R., & Bianchi, S. (2019). Privacy and Security Threats on the Internet of Things. In *Internet of Things Security and Data Protection* (pp. 9–43). Springer, Cham.
[23] Megatreds (2018). "Study on global megatrends in cybersecurity, ponemon institute research report", Research report, February 2018.

[24] Backes, M., Buxmann, P., Eckert, C., Holz, T., Müller-Quade, J., Raabe, O., & Waidner, M. (2016). *Key Challenges in IT Security Research*. Discussion Paper for the Dialogue on IT Security 2016, SecUnity, https://it-security-map. eu.

[25] Lu, Y., Da Xu, L. Internet of Things (IoT) cybersecurity research: a review of current research topics. *IEEE Internet of Things Journal*, 2018.

[26] Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2017, September). 5G security: Analysis of threats and solutions. In *2017 IEEE Conference on Standards for Communications and Networking (CSCN)* (pp. 193–199). IEEE.