Defining security requirements with Common Criteria: applications, adoptions, and challenges

Nan Sun[a,b,*], Chang-Tsun Li[a], Hin Chan[d], Ba Dung Le[b,c], MD Zahidul Islam[c], Leo Yu Zhang[a], MD Rafiqul Islam[c], Warren Armstrong[e]

[a]*School of Information Technology, Deakin University, Waurn Ponds, Victoria, Australia*
[b]*Cyber Security Cooperative Research Centre, Joondalup, Western Australia, Australia*
[c]*School of Computing, Mathematics and Engineering, Charles Sturt University, Wagga Wagga, New South Wales, Australia*
[d]*Australia Cyber Security Centre, Canberra, Australian Capital Territory, Australia*
[e]*QuintessenceLabs Pty Ltd, Canberra, Australian Capital Territory, Australia*

Abstract

Advances of emerging Information and Communications Technology (ICT) technologies push the boundaries of what is possible and open up new markets for innovative ICT products and services. The adoption of ICT products and systems with security properties depends on consumers' confidence and markets' trust in the security functionalities and whether the assurance measures applied to these products meet the inherent security requirements. Such confidence and trust are primarily gained through the rigorous development of security requirements, validation criteria, evaluation, and certification. Common Criteria for Information Technology Security Evaluation (often referred to as Common Criteria or CC) is an international standard (ISO/IEC 15408) for cyber security certification. In this paper, we conduct a systematic review of the CC standards and its adoptions. Adoption barriers of the CC are also investigated based on the analysis of current trends in security evaluation. Specifically, we share the experiences and lessons gained through the recent *Development of Australian Cyber Criteria Assessment (DACCA)* project that promotes the CC among stakeholders in ICT security products related to specification, development, evaluation, certification and approval, procurement, and deployment. Best practices on developing Protection Profiles, recommendations, and future directions for trusted cybersecurity advancement are presented.

Keywords: Common Criteria, Protection Profile, Cyber Security, Trusted System, Security Standard and Certification

1. Introduction

Statistics from the Australian Cyber Security Centre's (ACSC) Annual Cyber Threat Report [23] show a sharp upwards trend in the number of cyber security incidents. Cyber security issues are becoming a day-to-day struggle across both private and public sectors. The ever-increasing number of cyber attacks and security incidents continues to deepen concerns over data breaches, physical system damage, economic loss, reputation harm, and even compromise of national security [124]. Given these acute concerns, the security requirement definition and certification process for Information and Communication Technology (ICT) products are of paramount importance. With a robust security infrastructure in place, hacking and other forms of cyber attacks can be prevented and mitigated to some extent [89]. Furthermore, security vulnerabilities often slip into ICT products during the development and implementation stages. With the more widespread use of ICT products, it is imperative to have in place a rigorous security evaluation process to ensure the products' security performance and the enforcement of protection policies.

In recent years, the interest in trusted systems that enforce a given set of attributes to a stated degree of assurance has reemerged [117]. Enhancing the trust and confidence users have in ICT products is of great significance in the area of cybersecurity, which can be gained through setting security standards, and using independent assessment against the standards [107]. Setting standards is challenging in every industry as it not only requires a set of objective standards but also involves strong third-party intervention. The Common Criteria for Information Technology Security Evaluation (often referred to as Common Criteria or CC) is an international standard (ISO/IEC 15408) for achieving cyber security certification. It is inherited from ICT security assurance, through a rigorous verification process, which is conducted on a case-by-case basis [31]. With the strict, standardized and repeatable methodology, the CC provides assurance for implementing, evaluating and operating a security product at the level that is commensurate with the operational environments.

Under the CC, vendors list the intended security functional requirements (SFRs) within a Security Target (ST) [31]. Since new products are constantly being developed and every product is designed and developed differently, Protection Profiles (PPs) have been created for common products, such as databases, operating systems and smart cards [32]. Generally, PPs define a set of security requirements and objectives for a specific category of products or systems. In addition, PPs can serve as a benchmark in terms of product security. Once validated by competent and licensed laboratories [39], a certificate is issued by the certification authority and recognized by CC signatory countries.

Since the Common Criteria standard emerged in the 1990s, there have been 17 Certificate Authorizing Participants (including Australia) and 14 Certificate Consuming Participants signed up to the Common Criteria Recognition Arrangement (CCRA) [30]. If an ICT security product is successfully evaluated, the product will be certified by the certification authority of a CCRA signatory country and listed on the Certified Products List at the Common Criteria Portal [37]. The certification helps consumers to determine whether the products meet their security requirement, which also boosts the competitiveness of the products through comparing with similar products on the market.

Contributions of this paper: In this paper, we aim to provide a coherent and comprehensive picture of current efforts on cyber Common Criteria development in Australia and internationally. Specifically, through the collaboration with Australian Certification Authority of the Australian Cyber Security Centre, QuintessenceLabs and cyber security researchers in academia, the lessons and best practice relevant to defining security requirements with the PP development are summarized and shared in this paper. The target audiences of the paper are researchers in academia, security policy-makers, industrial practitioners, and end users in the public and private sectors who are interested in the specification, development, evaluation, certification, procurement, and operation of ICT products with security properties. In summary, the contributions of this work are as follows.

- A systematic review of Common Criteria and its applications are demonstrated based on literature review and our own experience gained through the recent *Development of Australian Cyber Criteria Assessment (DACCA)* project [1].

- An in-depth and comprehensive analysis of current trends in Common Criteria adoption is carried out. Based on the identified challenges of CC adoption, the adoption barriers of Common Criteria internationally and nationally are analyzed.

- Practices, recommendations and future directions derived from the analysis and solutions to address identified challenges in the development of Protection Profiles are presented. These efforts pave the way for the widespread adoption of Common Criteria assessment.

Comparison with related works: There are limited review works that explore security requirements for ICT products and services. The latest work in [89] provided an overview of cyber security certification for the Internet of Things (IoT). In [89], Matheu et al. analyzed the various cybersecurity certification schemes and the potential challenges in applying them to the IoT ecosystem. They also studied current

---

[1]https://cybersecuritycrc.org.au/development-australian-cyber-criteria-assessment

efforts in risk assessment and testing processes and [89] made significant contributions to the deployment of an IoT cybersecurity certification framework. However, this work [89] focused specifically on IoT products and covered a broad range of certification standards without an in-depth discussion of the CC methodology and adoption. From the perspective of security testing and risk assessment in the IoT, previous works [19] [46] [78] reviewed the key building blocks for the cyber security certification process. Besides security certification in IoT, Leszczyna et al. [82] conducted a comprehensive survey on smart grid standards that deal with cybersecurity issues and provided valuable insight into security related standards. The work in [82] covered 36 cybersecurity-related and 12 privacy-related standards. However, similar to [89], insightful analysis on the CC is lacking. In addition, Kara et al. [70] reviewed the CC in a specific field, which stressed CC's application in secure software development. When it comes to the significance of the CC , Matheu et al. [89] acknowledged the CC as the most widely deployed and adopted cyber security certification standard in the field of IoT. Albeit the fact that Russia is neither a Certificate Authorizing Participant nor a Certificate Consuming Participant of the CC, the history, structure, and features of the CC used in the Russian scheme are presented in [12] and [13], which manifest the importance of the CC. In addition, China is not a CCRA signatory country but has the adoption of the CC called GB/T 18336 [65]. To the best of our knowledge, this paper is the first comprehensive survey on the Common Criteria for Information Communications Technology Security Evaluation with regard to its applications, adoptions and related challenges.

Roadmap: The rest of the paper is organized as follows. We start with introducing the methodology and applications of Common Criteria towards security assurance for ICT product evaluation in Section 2. Section 3 presents our comprehensive literature review with respect to the Common Criteria adoption trend, adoption barriers, and its impact. Section 4 discusses the challenges in PP development and our experience gained from the development of a Protection Profile for encryption key management. In addition, the best practices and future directions that support CC approaches are shared based on the identified challenges. Section 5 concludes this review paper.

2. Common criteria methodology

This section aims to introduce the Common Criteria methodology and its applications for evaluating ICT products. The analysis is based on Protection Profiles and Certified Products listed on the CC portal, research papers and technical reports from various organizations including governments, vendors and other CC participants. In addition, potential categories of CC applications on emerging technologies are proposed.

2.1. Driving security assurance through Security Targets and Protection Profiles

The CC is the driving force for the widest available mutual recognition of secure ICT products. In this subsection, we demonstrate how to drive security assurance through Security Targets and Protection Profiles with the CC standards. Firstly, definitions on key CC concepts are identified and specified. Secondly, we introduce the methodology of the CC through presenting the rationales and relationships among the core building blocks in the CC. Thirdly, we emphasize that the CC is risk based by illustrating how the CC works to reduce and minimize risks and threats, so as to raise users' confidence on the security performance of ICT products.

2.1.1. Background and definitions on key Common Criteria concepts

The CC was developed to certify that products and systems meet pre-defined security requirements [62]. Through a set of specifications and guidelines designed to evaluate information security products and systems, the products that have undergone successful testing and evaluation are awarded the CC certification [117].

The history of the CC: In 1994, the CC was developed by the governments of the US, Canada, Germany, France, the UK, and the Netherlands [62]. The CC is the unified standards of the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), the United States Trusted Computer System Evaluation Criteria (TCSEC), and the European Information Technology Security Evaluation Criteria (ITSEC) [101]. The consolidation of these security standards helps to avoid the repetitive work on evaluation of similar

Table 1: Security Assurance Requirements	
Class	Class name
APE	Protection Profile Evaluation
ASE	Security Target Evaluation
ADV	Development
AGD	Guidance Documents
ALC	Life-Cycle Support
ATE	Tests
AVA	Vulnerability Assessment
ACO	Composition

Table 2: Security Functional Requirements	
Class	Class name
FAU	Security Audit
FCO	Communication
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPR	Privacy
FPT	Protection of the TOE Security Functionality
FRU	Resource Utilization
FTA	TOE Access
FTP	Trusted Path/Channels

products and systems of the same type and also addresses the application in prevailing international markets. By March 2021, the Common Criteria Recognition Arrangement (CCRA) consists of 31 governmental organizations, including 17 certificate authorizing nations and 14 certificate consuming nations [34]. The CCRA aims to conduct evaluations to high and consistent standards, improve the availability of Certified Products, and eliminate the duplication and improve efficiency of evaluations and processes [34]. The CCRA maintains the CC portal's Certified Products List (CPL) [37] that lists all CC Certified Products completed by all certificate authorizing nations.

Key CC concepts: The part of the product or system that is the subject of the evaluation is called the Target of Evaluation (TOE). To define a standard set of security requirements for a particular class of related products, the Protection Profile (PP) is usually developed by a user or user group [62]. A PP serves as a reusable template of security requirements to support the definition of functional standards, and also as a guide for formulating product development or procurement specifications. A PP is an implementation-independent set of security requirements for a particular technology that enables repeatable evaluations. To enhance the consistency of testing, some PPs are augmented with the specification of testing activities. Depending on the TOE, multiple profiles can be used at once based on the particular technology that the TOE is to be certified. If a vendor has an ICT product that they would like to be evaluated and certified under the CC standards, they must complete a Security Target (ST) description. The ST is the document provided by the vendor to identify the security features of the TOE [31]. In addition, the ST includes the evaluation of any potential security risks by defining the security functional and assurance measures that the TOE should offer to meet the CC requirements.

As shown in Table 1, eight categories of Security Assurance Requirements (SARs) are identified by the CC to be used as the basis for gaining confidence that claimed security measures are implemented correctly. The CC defines eleven categories of Security Functional Requirements (SFRs) in relation to desirable security functionalities to provide a standard way of expressing the requirements for a TOE, as summarized in Table 2. The Evaluation Assurance Levels (EAL) define how the product is tested and how thoroughly the product is evaluated. The EAL levels are scaled from EAL1 (the lowest) to EAL7 (the highest) [31]. The EAL number does not measure the security of the product or system itself. It states at what level the product or system was tested. A higher EAL level reflects added assurance requirements that must be met to achieve CC certification [33]. Although the product or system that will be certified must fulfill the exact *assurance* requirements to achieve a specific EAL level, they do not have to fulfill the exact *functional* requirements (i.e., security features). Therefore, the product or system with a higher EAL level does not necessarily mean more secure in the particular application than the one with a lower EAL level. If two products contain the same and necessary *security features* in the ST, then a higher EAL level indicates the product is more secure.

How are products tested: For evaluation against a PP that specifies testing activities, the vendor should complete a self-assessment on compliance with the PP. For EAL-based evaluation, the vendor's testing
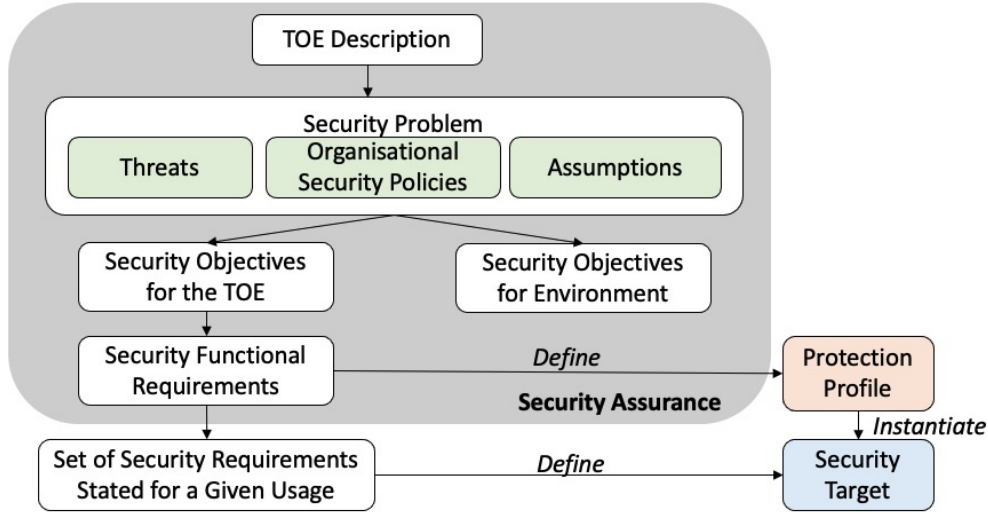
Figure 1: Methodology of Common Criteria

would serve as an input to the evaluator's testing [31]. The tests are carried out under laboratory conditions to validate the security features of the product and to evaluate how the product satisfies the requirements listed in the ST [39]. If the validation and evaluation are successful, the product will be awarded a CC certificate and listed on the CC portal [38]. From the consumer's point of view, the CC certification ensures consumers that they can trust the products they are investing in conform to the vendor's claims and can offer reliable security protection for their operational environment. For the vendors, the CC certification boosts the competitiveness of their products when the consumers compare similar products on the market. The advantage of using the CC is that products can be evaluated once and sold in multiple nations. The CCRA ensures that the same criteria and testing methodology are applied to the products against the same criteria in different accredited laboratories, regardless of their geographic location or national affiliation. For governments, besides supporting procurement, the CC certification also increases the transparency of ICT products' security features, facilitating the supervision and surveillance of the market.

2.1.2. Methodology of Common Criteria

We explain CC methodology by introducing the core building blocks of the CC, including TOE description, security problem definition, security objectives, and security requirements. The relationships between these core building blocks are depicted in Figure 1.

- **TOE description:** The first step is to define the usage and major security features of the TOE, to give end-users a general idea of its capabilities, usage, and whether the TOE meets their security needs [31].

- **Security problems:** In line with the description of the TOE, the security problems will be defined in three aspects: threats, organizational security policies, and assumptions [31]. Firstly, a threat consists of adversarial actions performed by a threat agent on an asset. The actions affect one or more properties of the asset from which that asset derives its value. One example of a threat is "An attacker may attempt to intercept communications from the TOE". Secondly, organizational security policies are security rules, procedures, or guidelines imposed by an actual or hypothetical organization in the operational environment, which can be applied to the TOE and/or its operational environment. An example of organizational security policies on the auditing activities is "Audit logs will be archived every seven days". Lastly, assumptions can be made about the operational environment, including the physical setting (e.g., "the TOE is located in a secure area, which will prevent unauthorized physical

access"), personnel skills and behaviour (e.g., "operators of the TOE are appropriately trained"), and connectivity (e.g., "the TOE will not be connected to an insecure network").

- **Security objectives:** The security objectives are the intended solution expressed as a concise and abstract response to the security problems. The security objectives serve three purposes: (1) provide a high level solution to the security problems; (2) divide the solution into those objectives to be satisfied by the TOE, and those objectives to be satisfied by the environment; (3) demonstrate that these part-wise solutions can form a complete solution to the security problem. Security objectives for the TOE consist of the objectives that the TOE should achieve to solve security problems. For example, a high level objective such as "the TOE shall keep confidential the content of all files transmitted between it and a server" addresses the security problems caused by unauthorized monitoring of network traffic. The security objectives for the operational environment include statements that describe the goals that the environment should achieve. For example, "the operational environment shall ensure that all human TOE users receive appropriate training before working with the TOE" provides the procedural measures to assist the TOE in correctly providing its security functionalities from the perspective of the operational environment.

- **Security Functional Requirements (SFRs):** The SFRs are a translation of the security objectives for the TOE [32]. The SFRs provide a more detailed and complete translation to make sure that the security objectives can be completely addressed. Specifically, the SFRs are independent of any specific technical implementation. Hence, the CC requires the translation from security objectives to the SFRs to be conducted with standardized language. The advantages and reasons for the standardized language requirements are twofold. One is to provide an exact description instead of natural language of what is the functionality to be evaluated. Another advantage is to allow comparison among products of the same class that will be evaluated. The standardized language enforces the use of the same terminology and concepts that contributes to easy comparison. The CC supports the standardized translation by providing predefined security functional requirements, operations, and dependencies. It is worth mentioning that the SFRs are only for the TOE. The operational environment is not evaluated, and therefore a description aimed at the evaluation of the operational environment is not required [32]. The parts of the operational environment may be evaluated in another independent evaluation. For instance, an operating system as a TOE may require a firewall to be present in its operational environment. The current evaluation focuses on the operating system TOE only, and another evaluation can be applied to the firewall subsequently.

- **Security Assurance Requirements (SARs):** Different from the SFRs, the SARs describe the measures taken during the process of development and evaluation of ICT products to assure compliance with the security functionalities [33]. The pre-packaged set of security assurance requirements are defined in the CC as summarized in Table 1 and specified from EAL1 to EAL7. For certain PPs, the EAL specification is optional, which indicates the PP can specify a customized set of assurance components (i.e., no EAL). The recent trend on PP development includes assurance activities for each SFR by specifying detailed actions in the supporting documents for the evaluator to perform [38]. It is noted that assumptions which are always made by the TOE on the operational environment. Security objectives for the TOE do not trace back to assumptions, and they are not evaluated but need to be understood and upheld.

To sum up based on the above blocks in Figure 1, a Protection Profile defines the security requirements of a technology type while a Security Target describes how the TOE meets the defined requirements. The TOE physical environment, security requirements and the purpose of the TOE, which is relevant to the product type and the intended use, are included in the PP [89]. The goal of the CC methodology is to achieve an internationally recognized evaluation benchmark for ICT security. As shown in Figure 1, a PP is a CC requirement specification for a specific technology. In the context of a dedicated use-case, a set of security requirements stated for a given usage are extracted to instantiate an ST and determine the TOE [61].
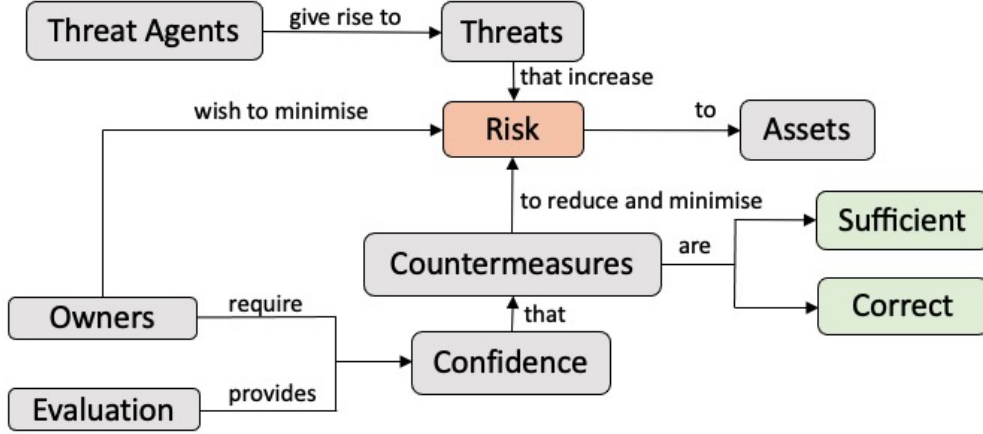
Figure 2: CC is risk-based

2.1.3. CC is risk based

The CC process is useful as a guide for the development, evaluation and/or procurement of ICT products with security functionality [33]. Typically, from the perspective of risk control and management, the CC is risk-based, as illustrated in Figure 2. On one hand, under the CC methodology, security is concerned with protecting assets that refer to entities that the owners of a system places value upon, including hardware, software, data, and transmission link. On the basis of the impact of the threats on the assets and the likelihood of the threats being exploited, threats rise the risks to the assets. The owners impose ICT and non-ICT countermeasures that seek to reduce and minimize the risk to assets. On the other hand, the CC evaluation provides the confidence to achieve the protection goals of ICT security with confidentiality, integrity, availability, authenticity, and non-repudiation [131], which is also needed by vendors and purchasers. Sufficient and correct countermeasures, which are achieved by conforming to CC requirements, will minimize the risks to the assets. Hence, trust under risk is achieved through the evaluation of ICT security assessment according to the CC.

2.2. Common Criteria applications: current categories and future developments

In this subsection, we provide the analysis on CC applications by reviewing current efforts. In addition, we propose future developments for the applications of CC based on emerging technologies and compliance requirements with emerging privacy legislations.

2.2.1. Existing categories of Certified Products and applications

We firstly review and summarize the existing Certified Products and applications under the CC by category. The Certified Products and Protection Profiles endorsed on the CC Portal [38] by December 2021, research papers, and technical reports on Common Criteria are included in the review.

- **Access control devices and systems:** Functioning within the framework of the security system, access control devices and systems ensure only authorized persons can access the system [16]. Usually, an access control system is a software-based application that provides an interface for authorized users to pass through an interface integrated into the system. The access control devices are the physical hardware that an access control system requires to enforce the functional rules. Under the category of access control devices and systems, the CC portal [38] contains PPs for the evaluation of Single Sign On (SSO) and enterprise management access control. The archived PP list on the CC portal [38] lists the 11 PPs for firewalls, intrusion detection systems and the US Government Authorization server for basic robustness environments, which are for reference only and are not to be used as a basis for new evaluations. Twenty-five products are certified under the access control devices and systems category.

7

- **Biometric systems and devices:** Biometrics is one of the most robust and reliable approaches for human identification in the physical and cyber spaces [64]. Tremendous advances in sensor technologies and data processing techniques lead to the strengthening of traditional biometric technologies (e.g., fingerprint, face, voice, iris, etc.) and the emergence of new technologies (e.g., DNA analysis, biometric payment cards, etc.). However, vulnerabilities and threats will inevitably occur, highlighting the significance of evaluating the security of biometric systems and devices [3]. The Protection Profiles for fingerprint spoof detection based on organizational security policies and biometric verification mechanisms are listed on the CC portal [38]. So far, there are no Certified Products under this category. Tekampe et al. [126] offered guidance for the evaluators of biometric system, vendors, and certifiers of biometric systems and devices according to the CC for security evaluation, which is a valuable input for further standardization activities.

- **Boundary protection devices and systems:** Boundary protection monitors and controls communications at the external boundary of the system to prevent and detect malicious and other unauthorized communication [76]. Boundary protection can be achieved through firewalls, routers, gateways, proxies, and encrypted tunnels [1]. Practical design, installation, configuration, and maintenance of the boundary protection devices and systems are critical tasks in providing effective cyber security. In summary, there are a total of 46 Certified Products and 42 PPs listed on the CC portal in this domain, including several personal firewalls. One example of PPs in this category is the collaborative Protection Profile (cPP) Module for Stateful Traffic Filter Firewalls.

- **Data protection:** Data protection refers to the rules, safeguards, and practices put in place to protect data and ensure that users remain in control of the data [20]. As the extent and potential value of data increases, the data protection regulation is significant for users to protect the privacy of users [133]. There are 28 current data protection PPs available on the CC portal, which cover cryptographic modules, encrypted storage device and cryptographic protocols. There is also a collaborative Protection Profile for full drive encryption. There are 66 Certified Products under the category of data protection. In addition, there are a number of research efforts on the data protection for CC development [72] [75] [91]. With the aid of functional requirements defined in the CC for data protection, Khan et al. [72] characterized user data protection of software components to boost the confidence and trust in component technologies. Furthermore, privacy and data protection issues of biometric applications are always a recurring question when applying existing data protection legal frameworks to respond to the new threats under the fundamental rights to respect for privacy and data protection. Kindt [75] systematically analyzed the privacy and data protection issues of biometric applications and summarized the key requirements according to the CC for Information Technology Security Evaluation. Furthermore, to develop and run the biometric systems in compliance with European data protection legislation, Meints et al. [91] investigated the most relevant data protection principles in the field of biometric systems.

- **Databases:** A database is the organized collection of structured data stored in the computer system [74]. Typically, a database is controlled by a database management system. A relational database is the most common type of database systems, including Structured Query Language (SQL) server, Oracle Database, MySQL, etc. In addition, there are other types of databases available in the market nowadays, including NoSQL databases [44], distributed databases [99], graph databases [6], cloud databases [45], centralized databases and commercial databases. Currently, there are 11 database management systems related PPs and one cPP available on the CC portal and 14 Certified Products, including the industry-leading advanced databases from IBM, Microsoft, Oracle, and HUAWEI.

- **Detection devices and systems:** Intrusion detection and prevention system protects users' ICT systems and applications by identifying suspicious activity and behavior. Detection devices and systems usually operate by monitoring and analyzing network traffic and providing proactive and preventive measures to ensure the security of the machines on which they are deployed [85]. There are 17 expired and archived PPs on intrusion detection systems scanners and analyzers, while there is no current PP

on the CC portal in this stage. Moreover, nine products that do not conform to any PPs under the category of detection devices and systems are certified through EAL-based evaluation.

- **ICs, smart cards and smart card-related devices and systems:** The category which sees most comprehensive application of the CC is Integrated Circuits (ICs), smart cards and smart card related devices and systems. ICs and smart cards are physical electronic authorization devices used to access a resource [113]. Usually, it is a card with an embedded integrated circuit, which may require physical contact or can be contactless. There are 84 current PPs covering JavaCard, electronic residence permits, electronic passports, Machine Readable Travel Documents (MRTDs), security module cards, and health cards. There is a cPP for the dedicated security component. There are 571 Certified Products under this category.

- **Key management systems:** Key management systems refers to the management of cryptographic keys in cryptosystems [54] [60] [135] . Key management systems and appliances are designed to centrally manage enterprise digital keys and certificates for enterprise applications, users and devices throughout their lifecycle. A key management system handles key generation, distribution, usage, automated rotation, renewal and revocation. Therefore, successful key management is critical to the security of a cryptosystem. Limited PPs and Certified Products are included in the CC portal. However, a secure, usable, unified and centralized suite of complementary requirements for key management systems is expected by vendors, purchasers and research community [121]. Based on our experience gained through the $DACCA$ project [123], we will review and summarize the lessons learned from the practical PP development on encryption key management components in Section 4.

- **Mobility:** The mobility category covers the evaluations of mobile device fundamentals and mobile device management. The mobile device provides essential services, such as cryptographic services, key storage services, and data-at-rest protection to support the operation of applications on the device securely [53]. Furthermore, a mobile device management is the administration of mobile devices, including smartphones, tablets, and laptops [59]. A total of 27 Certified Products are evaluated under the CC standard, including the mobile devices from Samsung, Google, Apple, Blackberry and other mobile devices representatives.

- **Multi-function devices:** A Multi-Function Device (MFD) refers to an equipment that can print, copy and scan. Threatened by vulnerabilities in relation to network connections, MFD devices may be laden with security vulnerabilities and may fall victim to security incidents like data exposure and eavesdropping [80]. There are 229 MFD certified devices listed on the CC portal and five PPs for hardcopy devices available as part of certification processes according to the CC.

- **Network and network-related devices and systems:** Network devices are physical devices that are needed for communication and interaction between hardware on the computer network [130]. Common network devices include hubs, switches, routers, gateways, bridges, modems, repeaters, and wireless access points. There are 232 Certified Products and 13 current PPs under the network and network-related devices category, there is one collaborative Protection Profile (cPP) for the network devices [29] that was developed by the networking international Technical Community (iTC) and was updated over time. Typically, a cPP is a PP that has been created through a collaborative process consisting of vendors, test laboratories, CCRA nations, and academia to define requirements and testing methodology through industry engagement.

- **Operating systems:** An operating system is the system software that manages computer hardware, software, and contributes common services for computer programs. This category includes a considerable number of PPs and Certified Products (e.g., MacOS Catalina 10.15, Windows 10 and Windows Server 2019 Version 1809, HongMeng V1.2, etc.) for operating systems in networked environments.

- **Products for digital signatures:** The digital signature is a mathematical algorithm for validating the authenticity and integrity of digital messages or documents [104]. Products for digital signatures

are one of the application categories of CC evaluation. There are 53 Certified Products available on the CC portal, such as DocuSign. Within this category, there are also 23 PPs for cryptographic modules and digital signature creation devices.

- **Trusted computing:** Trusted computing refers to technologies developed for resolving network security problems by enhancing hardware and modifying associated software components. The computer industry has accommodated the idea of trusted computing that is designed and promoted by Trusted Computing Group (TCG) in various ways. The TCG published the Trusted Platform Module (TPM) specification and a corresponding PP, which represents efforts to develop formal criteria for evaluating its security [4]. Although some people argue that trusted computing is unlikely to become a complete remedy for security problems [98], there has been a sharp rise in the number of PPs and Certified Products under the category of trusted computing in recent years. Löhr et al. [87] demonstrated how to advance PP development for trusted computing technology with exemplar projects.

- **Other devices and systems:** This category contains Certified Products and PPs for everything else which do not fit in the afore-mentioned categories, including web browsers, voting machines, smart TVs, etc.

2.2.2. Potential categories of emerging technologies and compliance with privacy legislations

The increasing adoption of emerging technologies motivates the study on potential categories of the CC. We list below the emerging technologies and compliance requirements with privacy legislations that may be included as new CC categories in the future.

- **Blockchain mechanisms and systems:** Blockchain offers innovative and integrated approaches to ensure information storage and transactions executed in an open environment are easily verifiable and auditable to all participants [77]. Blockchain is considered a ground-breaking technology for cryptography and cyber security, with application in many areas including cryptocurrency systems, smart contracts, and smart grids over IoT devices. [112]. However, the security and privacy concerns attributed to the blockchain technology should not be ignored when deploying blockchain in different applications. Furthermore, the maturity of the blockchain technology and relevant protocols are not sufficient to subside security concerns without subjecting blockchain-enabled IT products to standardized security evaluation and validation[138]. For example, Matsuo [90] pointed out that the application logic layer of the blockchain technology, that contains the scripting language for the financial transaction does not yet have a standard to provide security analysis.

- **Quantum computing:** The emerging technology of quantum computing encodes information in qubits as a non-classical approach, enabling computing to be conducted 2^n times faster than classical computing [55]. There are considerable speculations from industry and academia about the impact of quantum computing on cyber security [21]. In light of the potential power of quantum computers at non-trivial scale, it will be important to study and explore the incorporation of quantum-resistant algorithms or alternative approaches (such as quantum key distribution) into CC requirements around network security. These requirements will require modification to ensure Certified Products can continue to meet security guarantees around confidentiality and integrity of their data, particularly if transmitted over an untrusted network between trusted endpoints. In addition, the investigation into zero knowledge proofs' reliance on post-quantum hardness assumptions for security should be considered in CC development.

- **Privacy-preserving authentication:** In the last few years, many privacy-preserving authentication methods have been proposed to make authentication technologies reliable and secure [71] [134]. With the use of privacy-preserving authentication on the rise, its emergence as a new CC category is expected. For example, to ensure compliance with legislation (e.g., the European Union's General Data Protection Regulations), the feasibility of specifying the concept of privacy-by-design in the CC needs to be investigated, which can be achieved by incorporating privacy-preserving authentication into standards.

- **Artificial intelligence systems:** Artificial Intelligence (AI) systems demonstrate the capability to produce tertiary consciousness such as self-recognition, cognitive feedback, components of self-concept, and so forth [100]. However, in light of this capability as well as its misuse, the assurance of cyber security for AI systems is imperative. In January 2017, a group of artificial intelligence researchers developed 23 principles for AI called Asilomar AI principles [109], which underlines that AI systems should be safe and secure throughout the whole operational lifetime, and verifiable so where applicable and feasible. Since then, many other questions remain as to what is a safe and secure AI system and how to achieve it, especially verifying the security features in the context of the rapidly expanding and developing areas in financial trading, health care, translation, transportation etc. The increasing dependence on AI for critical functions and services create more incentives for attackers and lead to more severe damages [84]. In the past years, there has been an accelerated growth of policy proposals and government interest in the security of AI system. For instance, the European Commission is proposing for a regulation laying down harmonized rules on AI [28]. These security-focused policies for AI systems mainfest the importance of transparency, measurement and accountability for the AI system.

- **Internet of Things applications:** The IoT refers of the system of interrelated and internet-connected devices that are able to collect and transfer information over the wireless network without human to human or human to computer interaction [52]. With the emergence of IoT, numerous gadgets, services, and products containing innovative IoT technologies (such as smart TVs, voice controllers and mobile robots) provide consumers with convenience and improve the quality of their life [69]. IoT ecosystems are complex with significant security challenges, including insufficient data protection, weak password protection, insecure interfaces, and other risks. However, these risks must be reduced and mitigated for the entire lifecycle of IoT devices. Recently, there are a few studies on the approaches to CC certification for IoT devices [69] [73] [89] [122] with a number of PPs developed in this space. Building trust in IoT devices with powerful IoT security solutions that keep IoT systems safe and ensures the availability, integrity, and confidentiality of the IoT solution is a potential future direction for CC development.

3. Common Criteria adoptions

To pave the way for widespread adoption of the Common Criteria, we investigate possible adoption barriers to determine if organizations have concerns related to cyber security regulatory issues as well as determining organizations' attitudes towards cyber security standards. In this section, we present the current worldwide adoption of the CC and summarize the adoption barriers of the CC.

3.1. Trends in Common Criteria evaluations: some statistics

To investigate the current adoption, development trend and users' trust of the Common Criteria internationally and nationally, we studied the cases, including Certified Products [37] and Protection Profiles [40], listed on the CC portal [38]. In this subsection, we present the statistics of Common Criteria obtained after processing accessible information on the CC portal and the comparative analysis of Certified Products and Protection Profiles by category, scheme and assurance level.

Figure 3(a) shows the number of Certified Products and archived Certified Products approved through the CC evaluation and certification process. They are listed on the CC portal according to the categories of the TOEs. There are a total of 1619 Certified Products and 3226 archived Certified Products up to Dec 2021. The category of ICs, smart cards and smart card related devices and systems is the undisputed leader. Given the mutual recognition by all CCRA signatory countries and the comprehensive coverage of technologies and security functionalities, the number of signatory countries is progressively increasing [35]. Also, the number of Certified Products is rising annually. In the year of 2019 and 2020, the number of Certified Products was 275 and 367 respectively. Usually, the certificates will remain on Certified Products List with a five years validity[37]. The validity period may be determined by a scheme or a technical community that
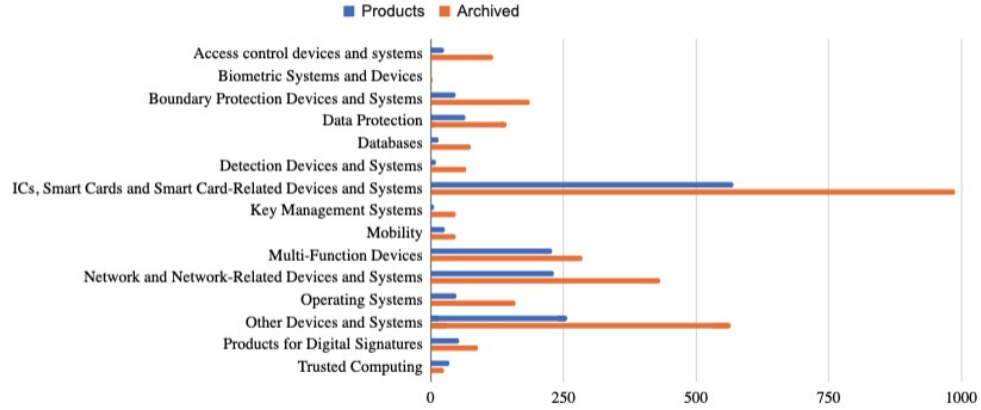
(a) The number of Certified Products and archived Certified Products by TOE category (a Certified Product may have multiple categories associated with it)
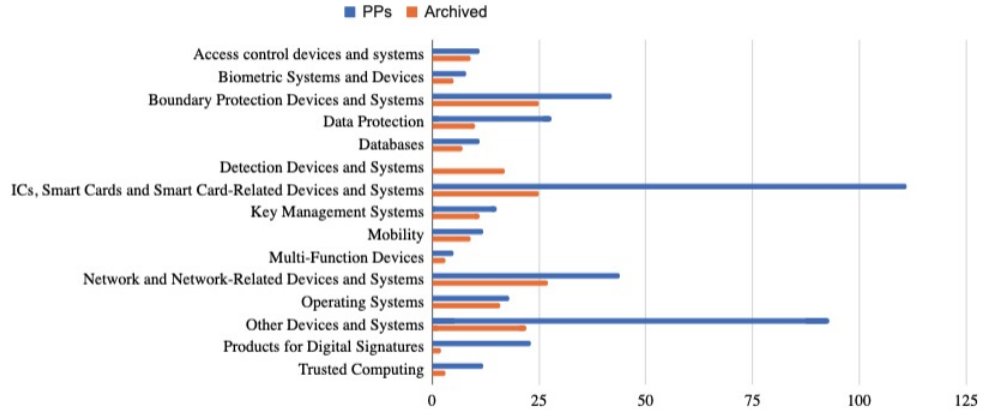
(b) The number of Protection Profiles and archived Protection Profiles by TOE category (a Protection Profile may have multiple categories associated with it)

Figure 3: The number of Certified Products and Protection Profiles under CC certification scheme

developed the PP. The validity period may impact a vendor's return on investment from a certification. The trend of PPs is similar to Certified Products when looking at the number of PPs and archived PPs, whose number increases year by year. Based on the number of PPs and archived PPs by TOE category as shown in Figure 3(b), the category with the most Certified Products and PPs listed is the ICs, smart cards and smart card-related devices and systems.

As mentioned above, the Evaluation Assurance Level is a number that ranges from EAL 1 to EAL 7, describing the depth and rigor of an evaluation. EAL 1 is the least rigorous level, and EAL 7 the most exacting. Each EAL corresponds to a Security Assurance Requirements package that covers the complete development process with the given level of strictness. The Certificate Authorizing Participants implement CCRA compliant CC certification requirements to produce certificates under certificate authorizing schemes. Based on the 17 Certificate Authorizing Schemes [36], shares of Certified Products under different schemes, are shown in Figure 4(b). As shown in Figure 4(a), investigating by assurance levels, most products are rated under EAL4+. The French, German, and Netherlands schemes have produced the most certificates listed on the CC portal. When observing the number of Certified Products in 2021, the US leads the number on 33, Germany on 31, France on 20 and Canada on 8. In particular, the US keeps the Certified Products listed for two years before being archived, while the other countries keep them for five years. Different from the most applied schemes in Certified Products, it is worth noting that the United States scheme takes the

(a) The proportion of Certified Products by EAL

(b) The proportion of Certified Products by CC Certification Scheme
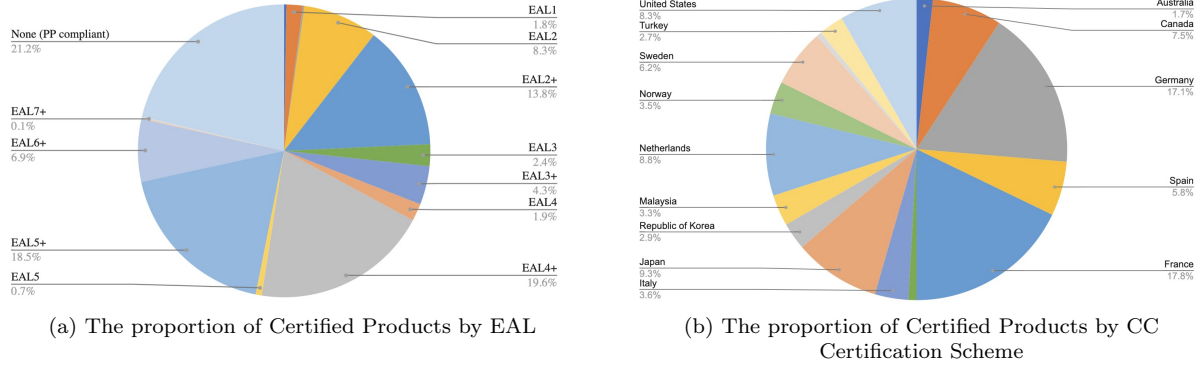
Figure 4: The proportion of Certified Products under CC evaluations

maximum amount of adoption in PPs. In addition, in the same way of CC Certified Products, the EAL4+ takes up the largest proportion (33.5%) by investigating the PPs by certification assurance level. From the perspective of adoption of PPs, it is worth noting that the United States scheme certified against PPs exclusively.

3.2. Common Criteria adoption barriers

Despite the importance and value of the CC, there are barriers in it adoption. Below, we highlight the barriers to the adoption of Common Criteria certification for ICT products.

- **Cost and complexity of evaluation:** The CC evaluation cost is commonly regarded as a barrier to the CC certification adoption [11][89], particularly for companies with a limited budget and for products with small market shares and low margin. In the competitive market of ICT products, products with a low-profit margin may not be able to justify and defray the cost of the CC certification. Based on the investigation on Certified Products [37], vendors of ICT products with high profit margin and capability for protecting sensitive government networks are relatively more inclined to adopt CC certifications. Extensive resources are required to complete the complex evaluation activities in the evaluation process by the laboratory. Based on the Australian scheme, the CC certification process generally consists of four phases, namely *pre-evaluation*, *conduct*, *conclude*, and *assurance continuity*. Generally, the pre-evaluation phase is essential to ensure success and avoid delays by conducting initial assessments and planning all building blocks of the CC evaluation process including development of the ST and the schedule of evaluation. Other tasks include writing of the functional and high/low level design specifications. Secondly, the conduct phase is to verify any claimed security functionality under the requirements of CC and other claimed cryptographic functionality under the specific security standard, such as FIPS 140-2 [50]. In the conclude phase, the evaluation and certification activities are finalised. Lastly, the assurance continuity phase establishes a way to minimize the number of evaluations and allows the determination to be made that the certification may be extended to the updated version of the TOE. The total cost of an evaluation varies depending on the security assurance level or PP conformance claims and the complexity of the TOE [115]. Four components, namely internal costs, external costs, lab fees, and certification fees make up the overall evaluation cost. The internal costs are incurred preparing deliverables and supporting the evaluators. The external costs consist of consulting fees. The lab fees are paid to the evaluation labs, and the certification fees are paid to the corresponding certification body if applicable. A recently estimated average cost for a CC certification lifecycle is US$250,000 [89] depending on the evaluation assurance level and re-use of past evaluation effort. The cost of an evaluation against a PP is generally lower. This is due to the reduced effort in developing the evaluation documentation. Because of the cost and complexity of evaluation, it is challenging to evaluate the products against the CC standard for companies with narrow profit margins and budgets.

- **Time of evaluation:** With rapid changes in technology development, the time-consuming process of CC evaluation and certification significantly slows down the commercialization of security products in markets. This is particularly undesirable for products with a short lifecycle. For example, the technology for producing a low-cost IoT device may have become obsolete when the CC certification process completes. The CC testing process needs to go through a sequence of stages, including ST evaluation, design evaluation, guidance evaluation, life-cycle evaluation, functional testing and penetration testing. Besides, the requirement on formal documentation and processes takes time [68] [95]. According to recent figures from the Australian Certification Authority, the average evaluation completion time is around six months. According to the Cyber Security Agency of Singapore, a typical evaluation takes about 3 to 6 months [114]. According to [127], a CC certification of an EAL 4 evaluation would take 6 to 9 months depending on the technology type. The completion of CC certification can take about 9 to 12 months [111], according to the Lightship Sec Lab. The Canadian Centre for CyberSecurity would allow the total of about 6 months from the Product in Evaluation (PiE) date [42]. Generally, the average time needed for the CC certification is 6 months to 1 year [89]. For products that require frequent replacements or updates or have a short time-to-market, the time for evaluation indeed hinders the adoption of CC evaluation.

- **Lack of government supports and incentives:** Government supports and incentives promote the adoption of CC evaluation and CC Certified Products to a certain degree. The consumers of CC Certified Products can be categorized based on market sectors: the public and private sectors. In terms of the public sector, government support can increase the adoption of CC certification by requiring the procurement of CC Certified Products. Furthermore, setting policy requirements for the procurement process used by governmental departments and agencies stimulates CC adoptions. For example, the US government issued a policy requiring CC certification for products intended for certain applications, which encourages vendors to participate in CC evaluations [115]. With respect to the private sector, government incentives can promote the adoption of CC Certified Products as well. For instance, the IT Investment Promotion Tax Incentive in Japan allows businesses to claim tax deductions for the use of CC Certified Products, which consequently increases the acquisition of the Certified Products [136]. The government's support and incentives would play an essential role in boosting the adoption of CC certification as the vendors can address legal risks and gain economic benefit from performing the CC evaluation.

- **Availability of approved Protection Profiles:** The CC certification process of ICT products may be hindered due to the lack of approved PPs. For example, the Australasian and Singaporean CC schemes encourage products to be certified against an approved PP [114][24]. Products to be certified without PP conformance (such as using ST only) may only be accepted on a case-by-case basis or when no suitable PP exists. Hence, the unavailability of approved PPs may discourage vendors from obtaining the CC certification. For mutual recognition under the CCRA, a CC certificate claiming compliance to EAL 3 or higher but not claiming compliance to a collaborative Protection Profile is generally treated as an equivalence to EAL 2 [114].

- **Implementation of *security-by-design* in products:** Implementing *security-by-design* in product engineering processes means that the product must be designed from the ground up to be secure. This may shorten the evaluation and certification process significantly [114] because the incremental certification of products for additional product features can be more accessible with the integration of certification evaluation activities in the security system engineering process [5][15]. However, it is challenging to integrate *security-by-design* in security product engineering processes [105]. Therefore, the lack of *security-by-design* in products may leave the products with many vulnerabilities [103], which makes it difficult for obtaining a security certification.

- **Complexity of the CC standard:** The structure and the readability of the CC standard is somewhat complex and not easily understandable. This has led to the need for many product vendors to engage evaluation supporting consultants at the pre-evaluation stage in order to prepare specific evaluation

14

material which increases the overall evaluation time and cost. Major review work is underway by international experts through the International Organization of Standardization (ISO). This should see an improvement of the CC for wider adoption. Further review work is likely needed to ensure usability and readability and to make the standard simpler to understand and use.

3.3. State-of-the-art of security standards

Besides the CC, there are other cyber security standards that aim to protect the users' cyber operational environment and organizations involved [106]. Started from the objective that mitigates and reduces security risks, a series of cyber security standards are promulgated, including policies, guidelines, best practices, and so forth, to contribute to establishing a trusted cyber security environment. This subsection surveys the current existing and state-of-the-art standards, including international standards, national standards, and industry-specific standards, which are widely considered to address the cyber security posed by threats. To further demonstrate the impacts of adopting the CC, Table 3 summarizes the state-of-the-art cyber security standards and compare the CC with these cyber security standards from the perspective of the scope, mutual recognition agreement, target candidates, publicly available, and cost and time for evaluation.

3.3.1. International standards

We first outline the international standards, focusing on the objective, context of use, and cost and time for obtaining the certificate.

- **ISO 27K:** ISO/IEC 27000-series, also known as Information Security Management System (ISMS) Family Standards or ISO 27K, consists of information security standards published by International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The representative ISO/IEC 27001 establishes requirements on how to manage information security [66]. The objective of ISO/IEC 27001 is to provide guidelines for organizations on how to manage the information and data. Therefore, the standard is not applicable to the IT industry only, also to other candidates, including organizations and government bodies that aim to protect their information. Through the requirements for establishing, implementing, maintaining and constantly improving the ISMS, the standard helps organizations make data assets more secure [66]. The recognized national accreditation body properly accredits the certification if the organizations meet the requirements and pass the audits, which usually costs from £2,850 to £14,250 and takes 2 to 15 days [56] based on the size of the organization. Furthermore, ISO/IEC 27002 provides best practices on information security management for those who are responsible for implementing and maintaining the ISMS. Besides, ISO 27K includes the standards from ISO/IEC 27000 to ISO/IEC 27050, ISO/IEC 27701 and ISO/IEC 27799 [63]. The ISO 27K standards are routinely reviewed and updated on a roughly five-year cycle. The standards related to digital forensics and cyber security are in preparation. Compared with CC, ISO 27K is related to the information security certification for companies, while the CC certifies products.

- **IEC 62443:** Some standards tend to specialize in a specific domain in cyber security. IEC 62443 targets Industrial Automation and Control Systems (IACS) by defining common standards in processes, techniques and security requirements [79]. There are four categories, respectively General, Policies and Procedures, System and Component, covering foundational information, asset owner, system design guidance and requirements, and specific product development and technical requirements for IACS [58].

- **ISO/SAE 21434**: New vehicle usage trends, including car-sharing platforms and mobility-as-a-service, are growing. However, the number of attack vectors in the connected cars and automotive industry is significant [93]. Under the circumstance, a new cyber security standard for the development lifecycle of road vehicles is under development by ISO and the Society of Automotive Engineers (SAE). ISO/SAE 21434 sets the guidelines for securing the high-level processes and cyber security standards in the connected cars and automotive industry [110]. Different phases, namely requirements

Table 3: Comparison of state-of-the-art cyber security standards regarding scope (I indicates international standard, N indicates national standard, and D indicates industry-specific stand), mutual recognition agreement (Y indicates that more than two countries agree on the standard), target candidates, publicly available (Y means that the security standard is publicly available, N indicates standard is not publicly available), cost and time for evaluation (NA means the cost and time spent on the standard are not available)

Standard	Scope	Mutual Recognition Agreement	Target Candidate	Publicly Available	Cost	Time
CC	I	Y	Product	Y	US$250,000	6 months to 1 year
ISO 27K	I	Y	Organization	Y	£2,850 to £14,250	2 to 15 days
IEC 62443	I	Y	Industrial Automation and Control Systems	Y	NA	NA
ISO/SAE 21434	I	Y	Automotive Industry	Y	NA	NA
ISO/IEC 20924 & ETSI EN 303645	I	Y	IoT	Y	NA	NA
Cyber Essentials	N	UK	Organisation	Y	£300	1 to 14 days
Essential 8	N	Australia	Organisation	Y	NA	NA
UK NCSC & CPA	N	UK	Smart Meters	Y	US$1,300 per day	6 to 18 months
CSPN	N	France	Product	Y	£25,000 to £35,000	35 days to 2 months
IT-Grundschutz	N	German	Organisation	Y	NA	NA
NIST	N	US	Organisation	Y	NA	NA
NERC CCS	N	North American	Electrical Power Industry	Y	NA	NA
FIPS 140	N	US	Cryptography	Y	US$50,000 per module	Up to 1 year
PCI DSS	D	Y	Payment Card	Y	US$15,000 to US$40,000	NA
UL 2900	D	Y	Medical Device	N	US$225 to US$750 on check standards, US$40,000 to US$150,000 on certification	NA

engineering, design, specification, implementation, test and operations are taken into consideration on security aspects.

- **ISO/IEC 20924 and ETSI EN 303645:** During the past decade, IoT that encompasses various protocols and technologies to interconnect physical devices to Internet infrastructure is one of the most relevant scenarios in cyber security [2]. ISO/IEC 20924 [67] provides the definition along with the terms and definitions forming the terminology foundation for IoT, which fills the gap between traditional security standards to the extension on the adoption of IoT systems in the early stages [57] [88]. Furthermore, the ETSI EN 303645 standard provides the baseline requirements for security in IoT devices [49], which was released in 2020. The standard compasses the technical controls and organizational policies for the developers and vendors of IoT devices [49]. For IoT devices involving multiple Personally Identifiable Information (PII), the standard facilitates their compliance to the General Data Protection Regulation (GDPR) [108].

3.3.2. National standards

Besides international security standards, national governments enact standards to set expectations and requirements for ICT products and organizations regarding cyber security. The national standards are described below with a focus on the application context, harmonization with international standards, and evaluation workflow.

- **Cyber Essentials:** Cyber Essentials is a national security standard developed by the UK government that specifies the assurance framework and a set of security controls to protect information from threats, concerning technical rules designed to protect devices, internet connection, data and services [22]. This standard is a government-backed certification scheme that helps to tighten overall cyber security within the organization, and it is also mandatory for businesses looking for specific government contracts [48]. The certification usually takes a day to a fortnight to complete the assessment and costs around £300. Cyber Essentials certification is valid for 12 months upon successful application.

- **ASD Essential 8:** The Essential Eight is a series of baseline mitigation strategies to combat cyber security incidents produced by the Australian Signals Directorate (ASD) [9]. These strategies aim to aid organizations in protecting against adversaries to compromise systems. The Essential Eight Maturity Model provides advice on how to implement the strategies as well as assists the organizations in self-testing the maturity of implementation. As one of the most effective mitigation strategies in ensuring the security of systems, application control is designed to protect against malware executing on the systems. The other strategies include assessing security vulnerabilities and applying patches, Microsoft Office Macro Security, restricting administrative privileges, implementing multi-factor authentication, and the other strategies to mitigate cyber security incidents.

- **UK NCSC and CPA:** National Cyber Security Centre [96] is the UK government organization that gives support and advice to the public and private sector to help them avoid security threats. The Commercial Product Assurance (CPA) [25] was set up to help organizations demonstrate the security functions of the products met defined NCSC standards. The Assured Service Providers is used to conduct testing and assessment by NCSC. The products are tested against the published CPA Security Characteristics [25]. The certification usually needs 6 to 18 months, and the cost of the certificate is US$1,300 per day of work [27]. However, since March 2019, the NCSC no longer accepts new product evaluation under the CPA scheme unless they are Smart Meters or smart metering products.

- **CSPN:** The Certification de Sécurité de Premier Niveau (CSPN) is a cyber security certification methodology proposed by the National Cybersecurity Agency of France (ANSSI) in 2008 [7]. The main objective of CSPN is to verify the product's compliance with its security specifications. Compared with CC, CSPN is a lightweight certification standard [89] that assesses the product in a shorter period, typically taking from 35 days to 2 months. Generally, the cost for evaluation and certification is around from €25,000 to €35,000 [27]. However, CSPN is only recoginzed in France as a national standard.

- **BSI IT baseline protection:** IT baseline protection (also known as IT-Grundschutz) from the German Federal Office for Information Security (BSI) is a methodology to identify and implement cyber security measures in an organization. The goal of BSI IT baseline protection is to achieve the adequate and appropriate level of security for IT systems [128]. To achieve the goal, BSI recommends "well-proven technical, organizational, personnel, and infrastructural safeguards" [18]. The organizations show the systematic approach to secure their IT systems by obtaining the ISO/IEC 27001 certificate based on IT-Grundschutz.

- **NIST:** The National Institute of Standards and Technology (NIST) of the US proposed cyber security framework on the basis of standards and guidelines to help organizations manage security risks [120]. Based on Executive Order 13636, the framework was defined to improve the cyber security of critical infrastructure in 2014 [119] and updated to address the emerging scenarios in cyber security in 2018 [120]. Furthermore, a series of special publications describe the security principles and provide advice on cyber security management, which is aligned to the framework.

- **NERC CCS:** Some national standards target a specific area in cyber security. North American Electric Reliability Corporation (NERC) Cyber Security Standards (CCS) was created in 2003 to be used to secure the electrical power industry [125]. As the enhancement of the requirements, the newest and most widely recognized NERC security standard is NERC 1300, which provides bulk electric system standard to network administration and supports the best-practice industry processes.

- **FIPS 140:** In the area of cryptography and database security, Federal Information Processing Standards (FIPS) are the US government security standards that specify the requirements for the cryptography modules [118]. FIPS 140-2 and FIPS 140-3 are current and active standards. In support of the cryptography block in CC functional security requirements, FIPS provides the specifications for cryptographic modules, and a set of standards that specify the cryptographic algorithm in use [17]. Four security levels from Level 1 to Level 4 are defined in FIPS 140-2. FIPS 140 validations can take up to one year and cost over $50,000 per module. The individual ratings and overall rating are listed on the vendor's validation certificate in the general flow of FIPS testing and validation [97].

3.3.3. Industry-specific standards
After recapping the international and national standards, we further replenish the state-of-the-art security standards by including the industry-specific standards.

- **PCI DSS:** The usage of payment cards, such as debit card, credit card, and prepaid card, is continuously increasing [86]. Consequently, the number of security incidents, like data breach, related to payment cards cause damages on businesses, customers' benefits and retailers' reputation [94]. The Payment Card Industry Data Security Standard (PCI DSS) is an industry-specific security standards administered by the PCI Security Standard Council, which sets the information security standards for organizations that handle payment cards from the major card schemes. The objective of the standard is to tighten payment card information and reduce cyber incidents on payment card, such as credit card fraud. An audit that accesses the organization's compliance with the PCI DSS costs around $15,000 to $40,000, depending on the business types, size, security environment, and the specific processing methods of the usage of payment card [10].

- **UL 2900:** UL 2900 is a set of standards published by Underwriters Laboratories (UL) that is a global security certification organization. And it includes the general cyber security requirements (UL 2900-1), specific requirements for medical products (UL 2900-2-1), industrial systems (UL 2900-2-2), and security and life safety signaling systems (UL 2900-2-3) [137]. The standard requires effective security countermeasures implemented to protect data as well as other data assets, such as command and control data. Besides, security vulnerabilities in the software should be eliminated, and the security of software should be verified through penetration testing [129]. The UL 2900 standards are not publicly available, leading to the harmonization and standardization aspects that should be addressed further
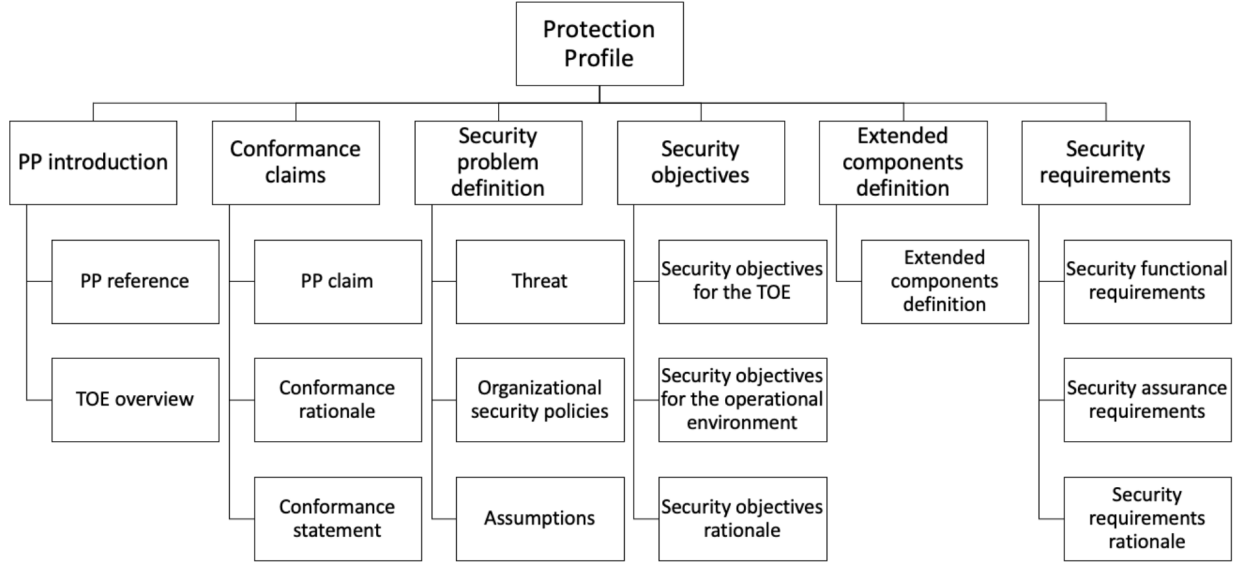
Figure 5: Main Structural Blocks of a Protection Profile

[89]. Typically, check on the criteria will spend between US$225 to US$750 based on the number and delivery format of the standards. And a fee ranging from US$40,000 to US$150,000 will be needed to certify the products [26].

4. Lessons learned, challenges and future directions on Protection Profile development

In this section, combined with the lessons learned from the recent project, *Development of the Australia Cyber Criteria Assessment (DACCA)*, we reflect on the challenges of developing PPs, present the lessons learned and propose potential ways to improve the CC standard.

4.1. Best practices

Through the *DACCA* project [123], we are developing a Protection Profile for the encryption key management components in collaboration with the Australian Certification Authority at the Australian Cyber Security Centre [2] and QuintessenceLabs [3].

In Figure 5, the structure of a generic PP is outlined, which consists of the main blocks, including PP introduction, conformance claims, security problem definition, security objectives, extended components definition, and security requirements. In terms of the development process of a PP, it is an iterative and incremental procedure where the specifications are broken down into multiple blocks. The development process is gradually and iteratively built up with the core blocks, and the supplementary features are added further. The following are the lessons we have learned.

- **Iterative and incremental approach:** We have taken an incremental approach in the project by iterating the following steps to mature the PP. This approach proved to be of particular effectiveness for an inter-sectoral project like *DACCA* with partners from the academia, industry, and certification authority. The first step, *Q&A*, begins with brainstorming with initial questions and answers. The initial questions identified to help explain the TOE and the objectives include what the common characteristics and functions for the encryption key managers are, what the required non-TOE

---

hardware/software/firmware for the TOE is, what the operational environment for the encryption key management products is, and so forth. The second step, *Draft*, aims to draft contents for each chapter and section following the PP specifications listed in Figure 5. The third step, *Refinement*, refines the contents based on literature review, cross-reference to related PPs, and feedback from industrial partners. The fourth step, *Polishing*, is to reduce impractical and repetitive items surrounding the risks demonstrated in Section 2.1.3, which makes sure the security countermeasures are correct and sufficient to respond to the considered risks. The fifth step *Evaluation* reviews and evaluates the deliverability of the PP to improve the consistency with the CC standard. The incremental process of PP developments iterates to gradually improve the quality of PP documents and the assurance of security.

- **PP-Module development:** The new evolution of CC supports the comparability among the results of independent cyber security evaluations through collaborative Protection Profile (cPP) [89]. A PP-module builds on a cPP, and conforming TOEs are obligated to implement the functionality required in the cPP along with the additional functionality defined in the PP-module. Hence, building upon the cPP rather than developing a standalone PP will not reinvent the wheel on certain functionality and ensure the specified functionality is sufficient to enhance cyber security for the technology and product. In the *DACCA* project, for the target TOE - key encryption management components, we utilize the collaborative Protection Profile for Network Devices (NDcPP) as the Base-PP and develop PP-Module intended for use with the NDcPP. This Base-PP is valid because a device that implements centralised enterprise Encryption Key Management is a specific type of network device. There is nothing about implementing Encryption Key Management that would prevent any of the security capabilities defined by the Base-PP from being satisfied. In the developed PP-Module, only the security functionalities of Encryption Key Management components in terms of the CC and assurance requirements for such products that are not included are needed to be added in the PP-Module, which avoids repetitive and redundant information, and also simplifies the development process.

- **Threats analysis:** A CC certification requires comprehensible product documentation, including a detailed threat analysis [14]. The following analytical approaches have been proved to be effective for such a purpose in our PP development. The anecdotal way is generally adopted by brainstorming a list of known threats and then culling, categorizing by assets, and assigning to operating environments. An alternative and more analytical way is to order, delete or retain the threats according to the priority, severity, and mitigation cost of the threats. Alternatively, work in [116] defined the data as assets and then generalized data assets (e.g., documents, configuration data) and asset state (e.g., in transit, at rest) to apply different threats to different states. Different threats may materialize in various operational environments or arise from vulnerabilities. Hence, defining the security threats based on the operational environments and supplementary threats derived from various vulnerabilities are another two effective approaches. The hybrid method that combines the above five approaches makes sure the identified threats in the PP are comprehensive, which paves the way for specifying the security requirements desired for the product under the CC standard.

- **Security functional requirements specification:** Specifying high-quality security requirements is an essential but complex task [92]. The starting point can be tailoring through existing SFRs listing in CC Part 2 [32] through *iteration, assignment, selection and refinement*. Generally, *iteration* enables a component to be used more than once with varying operations. *Assignment* provides the specification of parameters. *Selection* allows the specification of one or more items from a list. *Refinement* permits the addition of details. However, there are some security objectives for the TOE that cannot be transformed to SFRs listed in CC Part 2, for example, organizational policies or other third party requirements. The extended security functional requirements are set and included with definition and detailed requirements on the condition that the security objectives are hard to translate. Furthermore, in the PP development process, the SFRs are required to be specifically and precisely defined based on the corresponding functionalities of target TOE instead of generically described. For example, when defining the SFRs of key encryption management components in the *DACCA* project, cryptography's

concrete aspects, including the cryptographic features of encryption and decryption, hashing, keyed hash algorithm, and digital signatures, are included in the SFRs rather than the general description.

4.2. New challenges ahead

Informed by the best practices we have learned from the *DACCA* project and in the light of the security implications attributed to emerging technologies, we envisage that the following challenges will have to be addressed.

4.2.1. Transferability of Protection Profiles

With the target TOE, there are many different configurations, methods and parameters for key management products [43][54]. For example, a pure software key management product is a standalone TOE that generates, stores and manages key materials. Moreover, some key management products use specialised hardware for key material generation (through True Random Number Generators (TRNGs)), or for providing extra security properties via an internal Hardware Security Module (HSM). Besides, some key managers require the operating system for the supporting hardware platform or have the embedded operating system in the product. To fulfill encryption-related operations, such as using key material to sign by clients, the key management products require client-side software to be securely linked. The description of the TOE is the foundation of a PP and determines the number of PPs that will be developed [132]. To achieve harmonization, the TOE description facilitates the further comparison of the same types of products when conducting evaluation by comparing technical documents [41]. *Can one Protection Profile satisfy a class of products that is composed of many combinations of options* is a challenge to be addressed in future PP development.

4.2.2. Compactness and sufficiency of requirements

The CC has already defined 11 categories of security functional requirements concerning desirable security functionalities to provide a standard way of expressing the requirements for a TOE. However, the up-front analytical work is essential when specifying the complete, atomic, and testable requirements through the lifecycle for gathering, analyzing, and synthesizing security requirements [116]. In the lifecycle of PP development, the SFRs will be refined by filtering the irrelevant requirements and noisy features. Therefore, another main challenge is *the formulation of a compact but sufficient set of security functional requirements*. Additionally, the SFRs need to be polished through matching and augmenting by packages for each function and option of key management products, as mentioned in the first challenge.

4.2.3. Future-proofing of requirements

Due to the complexity and diversity of operational environments, the Common Criteria approach might lack linguistic expressiveness for the full range of security requirements. The CC is technology agnostic in terms of security functional and assurance requirements and this leads to the formulation of product-specific requirements. Working in collaboration with industry partners to identify relevant product and system specific requirements for inclusion in the PPs is important. Simultaneously, PP developers need to ensure that the requirements do not contradict the CC requirements. Additionally, adding threat awareness into the PPs by incorporating a better understanding of threats from vulnerability is desirable in the PP development [8][83]. Furthermore, the security implication of emerging technologies, such as quantum computing and zero-knowledge proofs, need to be considered in the future PP development [51]. In summary, extended requirements are expected to be incorporated based on analysis of features of products, security threats, and emerging technology. Extrapolation from existing guidance and Protection Profiles for complicated operational environments is the direction for extensions of CC requirements.

4.3. Future directions

Below, we summarize the key findings from our study of CC adoptions as well as the PP development through the *DACCA* project. Moreover, the recommendations and future directions for CC evaluation to establish the trusted security ecosystem are proposed.

- **Latest renovations of the CC:** There is the new generation of PP type where an EAL is not specified within the PP itself. That means assurance is gained through customized assurance activities developed as part of the PP for the given technology and is based on SARs of different assurance levels. Another renovation is the transformation of evaluations with exact compliance to technology-specific PP to provide achievable, repeatable, testable evaluation results. For example, the National Information Assurance Partnership (NIAP) [102] which oversees a national program to evaluate Commercial Off-The-Shelf (COTS) ICT products' conformance to the CC, no longer accepts EAL-based evaluations. Products being evaluated against a NIAP-approved PP must be in exact compliance with that PP. NIAP has worked closely with government agencies, including the National Institute of Standards and Technology (NIST), to ensure all references to Evaluation Assurance Levels and Robustness were removed from applicable documentation. Occasionally, EAL or Robustness is mentioned, usually in regards to product acquisition.

- **Accommodation of emerging technologies:** The CC covers a wide range of ICT security-related technologies and the evaluations in terms of security functionalities and security assurance. In Section 2.2.1, the categories of existing CC applications were reviewed. Traditional ICT technology and products, such as ICs, database and network devices, are sufficiently covered and evaluated under the CC standard in the past decades [62]. In light of emerging technologies as listed in Section 2.2.2, the evaluation of the newly emerging technologies, including blockchain, quantum computing, AI, and IoT, as well as the compliance requirements with privacy legislations for high assurance products, such as privacy-preserving authentication, need to be covered in the CC standard.

- **Elimination of CC adoption barriers:** Increased adoption of CC evaluation contributes to improving ICT ecosystem security for end-users. To lay the foundation for more extensive adoption of the CC evaluation, we analyzed the CC adoption barriers in Section 3.2. An effective way to bolster CC adoption is to eliminate the identified barriers. The possible solutions include cost, time and complexity reduction through the normalization of evaluation process, support and incentives from government agencies, increase of the availability and coverage of cPPs, and the integration of evaluation activities with product design and engineering procedures.

- **Standardization of evaluation activities:** Traditional PPs are implementation-independent documents [81], which define the security requirements for the ICT technology that the consumers require. Competent and independently licensed laboratories evaluate the products to decide whether the claimed security properties have been achieved[47]. For cPPs, unified processes and formalized steps for evaluation activities reduce the complexity of the evaluation. The standardization of evaluation and testing procedures improves the transparency of the certification process. Through standardization, the evaluation activities are better defined in PPs and corresponding supporting documents to provide guidance for evaluators.

- **Comparability and harmonization of evaluation:**

  Based on the fact that various cyber security standards internationally, nationally, and at the industry-specific level are adopted worldwide, it is hard to compare the level of security properties across diverse security standards. Even for the CC standard, it is difficult to reach the objective of comparison due to complex technical documents [89]. The standardization process of evaluation activities mentioned above can improve the comparability and harmonization of evaluation. In addition, rigorous security metrics that indicate the level of threats, risks and security provided by the products can be developed to address the issue of comparability.

- **Improvement of user confidence:** The adoption of security-sensitive ICT products and services heavily relies on the users' trust in the security functionality of the ICT products. Cyber security standards and certification is considered as a driving force for increasing the users' trust. The collaboration among vendors, technical specialists, customers and governments to raise the bar of security in ICT products is a never-ending endeavor. The sharing of information on the core blocks of CC evaluation and certification, such as threats, vulnerabilities and evaluation activities through education

22

and information provided on the CC portal [38] or other platforms will also contribute to this cause. Similarly, improvement to the usability and readability of the CC standards would also help with the users of the standard.

5. Conclusion

The last decade has witnessed a security paradigm shift from subjective risk management to more objective and measurable trust validation. One of the main driving forces of this shift is security evaluation and certification. The promotion of security standards, particularly the CC, also facilitates mutual recognition of secure ICT products, adds value to the products and services to give the industrial partners the competitive edge to operate in the global market. Certification provides consumers with a level of assurance in the security of ICT products and enables them to make better informed decisions when it comes to procurement. This paper provides the readers who are interested in trusted cyber security development from academia, government agencies, and industry with references and guidelines for the specification, development, evaluation, certification, procurement, and operation of ICT products with security functionality. This paper also provides a rigorous review of CC standards and certification. Through our own experience from the PP development of an inter-sectoral project, we have presented the best practices as well as the lessons learned. We identified the challenges on the adoption of the CC and offered suggestions on direction for future endeavors.

References

[1] A. Adler, P. Samouelian, M. Atighetchi, Y. Fu. Remote management of boundary protection devices with information restrictions. In: Proceedings of the AAAI Conference on Artificial Intelligence. volume 33 (2019) p. 9398–9403.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials (2015) 17(4):2347–2376.

[3] A. O. Alaswad, A. H. Montaser, F. E. Mohamad. Vulnerabilities of biometric authentication "threats and countermeasures". International Journal of Information & Computation Technology (2014) 4(10):947–58.

[4] T. C. P. Alliance. Trusted platform module protection profile (2002). www.commoncriteriaportal.org/public/files/ppfiles/PP_TCPATPMPP_V1.9.7.pdf.

[5] M. Andrea, M. Philippe, D. Sbastien, G. Jeremy. Towards incremental safety and security requirements co-certification. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE (2020) p. 79–84.

[6] R. Angles, C. Gutierrez. Survey of graph database models. ACM Computing Surveys (CSUR) (2008) 40(1):1–39.

[7] ANSSI. Certification de sécurité de premier niveau (cspn) (2008). https://www.ssi.gouv.fr/administration/produits-certifies/cspn/.

[8] S. Ardi, N. Shahmehri. Introducing vulnerability awareness to common criteria's security targets. In: 2009 Fourth International Conference on Software Engineering Advances. IEEE (2009) p. 419–424.

[9] ASD. Essential eight (2021). https://www.cyber.gov.au/acsc/view-all-content/essential-eight.

[10] G. Ataya. Pci dss audit and compliance. Information security technical report (2010) 15(4):138–144.

[11] G. Baldini, A. Skarmeta, E. Fourneret, R. Neisse, B. Legeard, F. Le Gall. Security certification and labelling in internet of things. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). IEEE (2016) p. 627–632.

[12] A. Barabanov, A. Markov. Modern trends in the regulatory framework of the information security compliance assessment in russia based on common criteria. In: Proceedings of the 8th International Conference on Security of Information and Networks (2015) p. 30–33.

[13] A. Barabanov, A. Markov, V. Tsirlov. Russian it security certification scheme: Steps toward common criteria approach. In: Proc. of 15th International Common Criteria Conference (ICCC-2014), New Delhi, India (2014) p. 1–11.

[14] K. Beckers, D. Hatebur, M. Heisel. A problem-based threat analysis in compliance with common criteria. In: 2013 International Conference on Availability, Reliability and Security. IEEE (2013) p. 111–120.

[15] K. Beznosov, P. Kruchten. Towards agile security assurance. In: Proceedings of the 2004 workshop on New security paradigms (2004) p. 47–54.

[16] D. M. Bowers. Access control and personal identification systems. Butterworth-Heinemann, (2013).

[17] K. H. Brown. Security requirements for cryptographic modules. Fed Inf Process Stand Publ (1994) :1–53.

[18] BSI. Bsi - it-grundschutz (2021). `https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html`.

[19] M. Bures, T. Cerny, B. S. Ahmed. Internet of things: Current challenges in the quality assurance and testing methods. In: International Conference on Information Science and Applications. Springer (2018) p. 625–634.

[20] L. A. Bygrave. Data protection law. Wolters Kluwer Law & Business, (2002).

[21] S. Cadzow, I. Sanchez, G. Baldini. An analysis on the development and application of cybersecurity standards. Joint Research Centre (JRC) (2018) .

[22] A. Calder. Cyber Essentials: A Pocket Guide. IT Governance Ltd, (2014).

[23] A. C. S. Centre. Acsc annual cyber threat report (2020). `https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf`.

[24] A. C. S. Centre. Australia information security evaluation program (2021). `https://www.cyber.gov.au/acsc/view-all-content/programs/australasian-information-security-evaluation-program`.

[25] CESG. The commercial product assurance (cpa) build standard (2021). `https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa`.

[26] I. Code DX. Cyber ul certification: A time-saver for application security testers? (2011). `https://techbeacon.com/app-dev-testing/cyber-ul-certification-time-saver-application-security-testers`.

[27] E. Commission. Tannex 8: Jrc analysis and recommendations for a european certification and labelling framework for cybersecurity in europe (2017). `https://ec.europa.eu/transparency/regdoc/rep/10102/2017/EN/SWD-2017-500-F1-EN-MAIN-PART-6.PDF`.

[28] E. Commission. Proposal for a regulation laying down harmonised rules on artificial intelligence (artificial intelligence act) (2021). `https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence?_hsenc=p2ANqtz-8i9qv6jXapHhtaLDsbZ54258VH5Q9jVJDOOvrJIOPF2l_2WbnMpOChp_OW_vSAvU2Z54qmbmnuYZlh7iDBWQXHH2aVyA&_hsmi=124043656&utm_campaign=The%20Batch&utm_content=124043656&utm_medium=email&utm_source=hs_email`.

[29] N. I. T. Community. Collaborative protection profile for network devices (2020). `https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.2E.pdf`.

[30] C. Criteria. Arrangement on the recognition of common criteria certificates in the field of information technology security (2014). `https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf`.

[31] C. Criteria. Common criteria for information technology security evaluation - part 1: Introduction and general model (2017). `https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5_marked_changes.pdf`.

[32] C. Criteria. Common criteria for information technology security evaluation - part 2: Security functional requirements (2017). `https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf`.

[33] C. Criteria. Common criteria for information technology security evaluation - part 3: Security assurance components (2017). `https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf`.

[34] C. Criteria. About the common criteria (2021). `https://www.commoncriteriaportal.org/ccra/`.

[35] C. Criteria. About the common criteria (2021). `https://www.commoncriteriaportal.org/ccra/`.

[36] C. Criteria. Certificate authorizing schemes (2021). `https://www.commoncriteriaportal.org/ccra/schemes/`.

[37] C. Criteria. Certified products (2021). `https://www.commoncriteriaportal.org/products/`.

[38] C. Criteria. The common criteria portal (2021). `https://www.commoncriteriaportal.org/`.

[39] C. Criteria. Licensed laboratories (2021). `https://www.commoncriteriaportal.org/labs/`.

[40] C. Criteria. Protection profiles (2021). `https://www.commoncriteriaportal.org/pps/`.

[41] J. Cugini. The common criteria: on the road to international harmonization. Computer standards & interfaces (1995) 17(4):315–320.

[42] C. C. for Cyber Security. Canadian common criteria program instructions (2021). `https://cyber.gc.ca/en/guidance/canadian-common-criteria-program-instructions`.

[43] W. Daniel, D. Chen, Q. Liu, F. Wang, Z. Wei. Emerging issues in cloud storage security: encryption, key management, data redundancy, trust mechanism. In: International Conference, MISNC. Springer (2014) p. 297–310.

[44] A. Davoudian, L. Chen, M. Liu. A survey on nosql stores. ACM Computing Surveys (CSUR) (2018) 51(2):1–43.

[45] G. C. Deka. A survey of cloud database systems. It Professional (2013) 16(2):50–57.

[46] J. P. Dias, F. Couto, A. C. Paiva, 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). IEEE (2018) p. 104–109.

[47] A. S. Directorate. Common criteria portal (2020). `https://www.cyber.gov.au/acsc/view-all-content/referral-organisations/common-criteria-portal`.

[48] C. Essentials. Cyber essentials scheme: Assurance framework. His Majesty's Government (2015) .

[49] ETSI. Etsi en 303 645 (2021). `https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf`.

[50] D. L. Evans, P. Bond, A. Bement. Fips pub 140-2: Security requirements for cryptographic modules. Federal Information Processing Standards Publication: Gaithersburg, MD, USA (2002) 12.

[51] A. Farkas, C. Walsh. A perspective of the common criteria in modern it business'. In: 3rd International Common Criteria Conference, May. Citeseer (2002) p. 1–8.

[52] Y. Fathy, P. Barnaghi, R. Tafazolli. Large-scale indexing, discovery, and ranking for the internet of things (iot). ACM Computing Surveys (CSUR) (2018) 51(2):1–53.

[53] C. Gao, A. Gutierrez, M. Rajan, R. G. Dreslinski, T. Mudge, C.-J. Wu. A study of mobile device utilization. In: 2015 ieee international symposium on performance analysis of systems and software (ispass). IEEE (2015) p. 225–234.

[54] A. Ghosal, M. Conti. Key management systems for smart grid advanced metering infrastructure: A survey. IEEE Communications Surveys & Tutorials (2019) 21(3):2831–2848.

[55] S. S. Gill, A. Kumar, H. Singh, M. Singh, K. Kaur, M. Usman, R. Buyya. Quantum computing: A taxonomy, systematic review and future directions. arXiv preprint arXiv:201015559 (2020) .

[56] I. Governance. Typical iso 27001 certification costs (2021). `https://www.itgovernance.co.uk/iso27001-certification-costs`.

[57] J. Granjal, E. Monteiro, J. S. Silva. Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials (2015) 17(3):1294–1312.

[58] J.-P. Hauet. Isa99/iec 62443: a solution to cyber-security issues? (2012).

[59] D. Hayes, F. Cappa, N. A. Le-Khac. An effective approach to mobile device management: Security and privacy issues associated with mobile applications. Digital Business (2020) 1(1):100001.

[60] A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, P. Spilling. A survey of key management in ad hoc networks. IEEE Communications Surveys & Tutorials (2006) 8(3):48–66.

[61] C. Hennebert. A first step towards a protection profile for the security evaluation of consensus mechanisms. In: 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS). IEEE (2020) p. 1–6.

[62] D. S. Herrmann. Using the Common Criteria for IT security evaluation. CRC Press, (2002).

[63] S. Higgins. Information security management: The iso 27000 (iso 27k) series. Department of Information Studies: Digital Curation Centre (2009) .

[64] C. Hill. Wearables–the future of biometric technology? Biometric Technology Today (2015) 2015(8):5–9.

[65] L. Hu, H. Li, Z. Wei, S. Dong, Z. Zhang. Summary of research on it network and industrial control network security assessment. In: 2019 IEEE 3rd information technology, networking, electronic and automation control conference (ITNEC). IEEE (2019) p. 1203–1210.

[66] E. Humphreys. Implementing the ISO/IEC 27001: 2013 ISMS Standard. Artech House, (2016).

[67] ISO. Information technology—internet of things (iot)—vocabulary (iso/iec 20924:2018) (2021). `http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/94/69470.html`.

[68] S. P. Kaluvuri, M. Bezzi, Y. Roudier. A quantitative analysis of common criteria certification practice. In: International Conference on Trust, Privacy and Security in Digital Business. Springer (2014) p. 132–143.

[69] S. Kang, S. Kim. How to obtain common criteria certification of smart tv for home iot security and reliability. Symmetry (2017) 9(10):233.

[70] M. Kara. Review on common criteria as a secure software development model. International Journal of Computer Science & Information Technology (2012) 4(2):83.

[71] P. Karger, S. McIntosh, E. Palmer, D. Toll, S. Weber. Lessons learned: Building the caernarvon high-assurance operating system. IEEE Security & Privacy (2010) 9(1):22–30.

[72] K. M. Khan, J. Han, Y. Zheng. Characterising user data protection of software components. In: Proceedings 2000 Australian Software Engineering Conference. IEEE (2000) p. 3–11.

[73] J.-H. Kim, H.-M. Jung, H.-J. Cho. Design plan of secure iot system based common criteria. Journal of the Korea Convergence Society (2017) 8(10):61–66.

[74] W. Kim. Relational database systemsr. ACM Computing Surveys (CSUR) (1979) 11(3):187–211.

[75] E. J. Kindt. Privacy and data protection issues of biometric applications. volume 1. Springer, (2016).

[76] R. Kissel. Glossary of key information security terms. Diane Publishing, (2011).

[77] J. Kolb, M. AbdelBaky, R. H. Katz, D. E. Culler. Core concepts, challenges, and future directions in blockchain: a centralized tutorial. ACM Computing Surveys (CSUR) (2020) 53(1):1–39.

[78] I. Kuzminykh, A. Carlsson. Analysis of assets for threat risk model in avatar-oriented iot architecture. In: Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Springer (2018) p. 52–63.

[79] B. Leander, A. Čaušević, H. Hansson. Applicability of the iec 62443 standard in industry 4.0/iiot. In: Proceedings of the 14th International Conference on Availability, Reliability and Security (2019) p. 1–8.

[80] D. Lee. A study on protection profile for multi-function devices. Journal of the Korea Institute of Information Security & Cryptology (2015) 25(5):1257–1268.

[81] K. Lee, Y. Lee, D. Won, S. Kim. Protection profile for secure e-voting systems. In: International Conference on Information Security Practice and Experience. Springer (2010) p. 386–397.

[82] R. Leszczyna. Cybersecurity and privacy in standards for smart grids–a comprehensive survey. Computer Standards & Interfaces (2018) 56:62–73.

[83] H. Li, X. Li, J. Hao, G. Xu, Z. Feng, X. Xie. Fesr: A framework for eliciting security requirements based on integration of common criteria and weakness detection formal model. In: 2017 IEEE International Conference on Software Quality, Reliability and Security (QRS). IEEE (2017) p. 352–363.

[84] J.-h. Li. Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering (2018) 19(12):1462–1474.

[85] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, K.-Y. Tung. Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications (2013) 36(1):16–24.

[86] J. Liu, Y. Xiao, H. Chen, S. Ozdemir, S. Dodle, V. Singh. A survey of payment card industry data security standard. IEEE Communications Surveys & Tutorials (2010) 12(3):287–303.

[87] H. Löhr, A.-R. Sadeghi, C. Stüble, M. Weber, M. Winandy. Modeling trusted computing support in a protection profile for high assurance security kernels. In: International Conference on Trusted Computing. Springer (2009) p. 45–62.

[88] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, W. Ni. Anatomy of threats to the internet of things. IEEE communications surveys & tutorials (2018) 21(2):1636–1675.

[89] S. N. Matheu, J. L. Hernández-Ramos, A. F. Skarmeta, G. Baldini. A survey of cybersecurity certification for the internet of things. ACM Computing Surveys (CSUR) (2020) 53(6):1–36.

[90] S. Matsuo. How formal analysis and verification add security to blockchain-based systems. In: 2017 Formal Methods in Computer Aided Design (FMCAD). IEEE (2017) p. 1–4.

[91] M. Meints, H. Biermann, M. Bromba, C. Busch, G. Hornung, G. Quiring-Kock. Biometric systems and data protection legislation in germany. In: 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IEEE (2008) p. 1088–1093.

[92] D. Mellado, E. Fernández-Medina, M. Piattini. A common criteria based security requirements engineering process for the development of secure information systems. Computer standards & interfaces (2007) 29(2):244–253.

[93] T. Micro. Iso/sae 21434: Setting the standard for connected cars' cybersecurity (2021). `https://documents.trendmicro.com/assets/white_papers/wp-setting-the-standard-for-connected-cars-cybersecurity.pdf`.

[94] E. A. Morse, V. Raval. Pci dss: Payment card industry data security standards in context. Computer Law & Security Review (2008) 24(6):540–554.

[95] S. J. Murdoch, M. Bond, R. Anderson. How certification systems fail: Lessons from the ware report. IEEE Security and Privacy (2012) 10(6):40.

[96] NCSC. The national cyber security centre (2021). `https://www.ncsc.gov.uk/`.

[97] C. No. Fips 140-2 validation certificate. Signature () 1:5.

[98] R. Oppliger, R. Rytz. Does trusted computing remedy computer security problems? IEEE Security & Privacy (2005) 3(2):16–19.

[99] M. T. Özsu, P. Valduriez. Distributed and parallel database systems. ACM Computing Surveys (CSUR) (1996) 28(1):125–128.

[100] J. F. Pagel. Dream science: Exploring the forms of consciousness. Academic Press, (2014).

[101] A. O. W. Paper. Computer security criteria: Security evaluations and assessment (2001). `https://www.oracle.com/technetwork/topics/security/seceval-wp-133226.pdf`.

[102] N. I. A. Partnership. The national information assurance partnership portal (2021). `https://www.niap-ccevs.org/`.

[103] M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker, H. Chen. Uninvited connections: a study of vulnerable devices on the internet of things (iot). In: 2014 IEEE joint intelligence and security informatics conference. IEEE (2014) p. 232–235.

[104] E. Paul. What is digital signature-how it works, benefits, objectives, concept. EMP Trust HR (2017) .

[105] S. Peisert, J. Margulies, D. M. Nicol, H. Khurana, C. Sawall. Designed-in security for cyber-physical systems. IEEE Security & Privacy (2014) 12(5):9–12.

[106] V. Y. Pillitteri, T. L. Brewer. Guidelines for smart grid cybersecurity. National Institute of Standards and Technology (2014) .

[107] G. J. Popek, C. S. Kline. Encryption and secure computer networks. ACM Computing Surveys (CSUR) (1979) 11(4):331–356.

[108] P. Regulation. General data protection regulation. Intouch (2018) .

[109] A. researchers, et al. Asilomar ai principles (2017). `https://futureoflife.org/ai-principles/`.

[110] C. Schmittner, G. Griessnig, Z. Ma. Status of the development of iso/sae 21434. In: European Conference on Software Process Improvement. Springer (2018) p. 504–513.

[111] L. Security. What is common criteria? (2021). `https://lightshipsec.com/common-criteria/`.

[112] P. Sharma, R. Jindal, M. D. Borah. Blockchain technology for cloud storage: A systematic literature review. ACM Computing Surveys (CSUR) (2020) 53(4):1–32.

[113] K. M. Shelfer, J. D. Procaccino. Smart card evolution. Communications of the ACM (2002) 45(7):83–88.

[114] C. S. A. of Singapore. Cybersecurity certification guide (2021). `https://www.csa.gov.sg/-/media/csa/documents/sccs/cybersecurity_certification_guide_v2.pdf`.

[115] R. E. Smith. Trends in security product evaluations. Information Systems Security (2007) 16(4):203–216.

[116] B. Smithson. Protection profile development for hardcopy devices: Lessons learned (2010).

[117] W. Stallings, L. Brown, M. D. Bauer, A. K. Bhattacharjee. Computer security: principles and practice. Pearson Education Upper Saddle River, NJ, USA, (2012).

[118] S. H. Standard. Fips pub 180-1. National Institute of Standards and Technology (1995) 17:15.

[119] N. I. of Standards, Technology. Framework for improving critical infrastructure cybersecurity, version 1.0 (2014). `https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf`.

[120] N. I. of Standards, Technology. Framework for improving critical infrastructure cybersecurity, version 1.1. technical report (2018). `https://doi.org/10.6028%2Fnist.cswp.04162018`.

[121] A. J. Stieber. Enterprise cryptographic key management realities and issues. IEEE (2010) .

[122] G. Suciu, C. Istrate, I. Petre, A. Scheianu. Lego methodology approach for common criteria certification of iot telemetry. In: World Conference on Information Systems and Technologies. Springer (2019) p. 165–174.

[123] N. Sun, B. D. Le, C.-T. Li, W. Armstrong, I. Md Zahidul, I. Md Rafiqul, L. Y. Zhang, H. Chan. Progress on and lessons from the pp development for encryption key management (part 1), technical report submitted to australian cyber security cooperative research centre (2021).

[124] N. Sun, J. Zhang, P. Rimba, S. Gao, L. Y. Zhang, Y. Xiang. Data-driven cybersecurity incident prediction: A survey. IEEE communications surveys & tutorials (2019) 21(2):1744–1772.

[125] N. . S. Technologies. Nerc cyber security standards, cip-002-1 through cip-009-1: Compliance reference (2006). `http://www.netsectech.com/wp-content/uploads/2013/05/WP_NERC_CSS_Compliance_Ref_NST.pdf`.

[126] N. Tekampe, A. Merle, J. Bringer. D6. 5: Towards the common criteria evaluations of biometric systems. Evaluation (2011) 1.

[127] J. Tierney, T. Boswell. Common criteria: Origins and overview. In: Smart Cards, Tokens, Security and Applications. Springer (2017) p. 193–216.

[128] B. Tsoumas, D. Gritzalis. Towards an ontology-based security management. In: 20th International Conference on Advanced Information Networking and Applications-Volume 1 (AINA'06). IEEE; volume 1 (2006) p. 985–992.

[129] UL. Ul standards (2021). https://standardscatalog.ul.com/Default.aspx.

[130] M. A. M. Vieira, C. N. Coelho, D. j. da Silva, J. M. da Mata. Survey on wireless sensor network devices. In: EFTA 2003. 2003 IEEE Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No. 03TH8696). IEEE; volume 1 (2003) p. 537–544.

[131] R. Von Solms, J. Van Niekerk. From information security to cyber security. computers & security (2013) 38:97–102.

[132] V. I. Vorobiev, L. N. Fedorchenko, V. P. Zabolotsky, A. V. Lyubimov. Ontology-based analysis of information security standards and capabilities for their harmonization. In: Proceedings of the 3rd international conference on Security of information and networks (2010) p. 137–141.

[133] S. Wachter. Data protection in the age of big data. Nature Electronics (2019) 2(1):6–7.

[134] D. Wang, H. Cheng, D. He, P. Wang. On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices. IEEE Systems Journal (2016) 12(1):916–925.

[135] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, M. Galloway. A survey of key management schemes in wireless sensor networks. Computer communications (2007) 30(11-12):2314–2341.

[136] H. Yajima, M. Murata, N. Kai, T. Yamasato. Consideration of present status and approach for the widespread of cc certification to a private field˜ cases in japan˜ ().

[137] S. Yuan, A. Fernando, D. C. Klonoff. Standards for medical device cybersecurity in 2018 (2018).

[138] R. Zhang, R. Xue, L. Liu. Security and privacy on blockchain. ACM Computing Surveys (CSUR) (2019) 52(3):1–34.