CRYPTOGRAPHIC MODULES VALIDATION PROCESS ACCORDING TO THE FIPS 140 AND ISO/IEC 15408

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

CANSU YENER

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
CRYPTOGRAPHY

SEPTEMBER 2020

Approval of the thesis:

CRYPTOGRAPHIC MODULES VALIDATION PROCESS ACCORDING TO THE FIPS 140 AND ISO/IEC 15408

submitted by **CANSU YENER** in partial fulfillment of the requirements for the degree of **Master of Science in Cryptography Department, Middle East Technical University** by,

Prof. Dr. Ömür UĞUR _____
Director, Graduate School of **Applied Mathematics**

Prof. Dr. Ferruh ÖZBUDAK _____
Head of Department, **Cryptography**

Assoc. Prof. Dr. Ali DOĞANAKSOY _____
Supervisor, **Mathematics, METU**

Assoc. Prof. Dr. Oğuz YAYLA _____
Co-supervisor, **Cryptography, METU**

Examining Committee Members:

Assoc. Prof. Dr. Murat CENK
Cryptography, METU _____

Assoc. Prof. Dr. Ali DOĞANAKSOY
Mathematics, METU _____

Assoc. Prof. Dr. Oğuz YAYLA
Cryptography, METU _____

Assoc. Prof. Dr. Fatih SULAK
Mathematics Department, Atılım University _____

Assist. Prof. Dr. Nurdan SARAN
Computer Engineering Dept., Çankaya University _____

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: CANSU YENER

Signature :

ABSTRACT

CRYPTOGRAPHIC MODULES VALIDATION PROCESS ACCORDING TO THE FIPS 140 AND ISO/IEC 15408

YENER, Cansu
M.S., Department of Cryptography
Supervisor : Assoc. Prof. Dr. Ali DOĞANAKSOY
Co-Supervisor : Assoc. Prof. Dr. Oğuz YAYLA

September 2020, 46 pages

With the advancement of technology, questions have arisen regarding the reliability of information technology products. Some standards have emerged to ensure the reliability of these products and to validate this reliability internationally. One of the standards issued to meet this need is ISO/IEC 15408 Common Criteria Standard. Thanks to this standard, the relevant institutions authorized to evaluate information technology products are evaluated and the reliability of this product is provided by the certificates issued by the competent authorities. In addition to this standard, the FIPS 140 standard has been created, which specifies the requirements of cryptographic modules specifically and is used for the approval and verification of these modules. This standard is used to determine the reliability of cryptographic modules. In this thesis, we first define these standards and how the evaluation process in accordance with them takes place in the world and how they should be implemented in Turkey. Then, we discuss the vulnerabilities of the AES-GCM algorithm in order to prevent the vulnerabilities of the cryptographic algorithms used in the cryptographic algorithm verification process, which is a part of the cryptographic module verification process, and talk about alternative AES modes. Finally, we complete the thesis by talking about test vectors that help us detect these vulnerabilities.

Keywords: CMVP, AMVP, Common Criteria, AES-GCM, Vulnerabilities

ÖZ

FIPS 140 VE ISO / IEC 15408'E GÖRE ŞİFRELEME MODÜLLERİ DOĞRULAMA SÜRECİ

YENER, Cansu
Yüksek Lisans, Kriptografi Bölümü
Tez Yöneticisi : Doç. Dr. Ali DOĞANAKSOY
Ortak Tez Yöneticisi : Doç. Dr. Oğuz YAYLA

Eylül 2020, 46 sayfa

Teknolojinin ilerlemesiyle birlikte bilgi teknolojileri ürünlerinin güvenilirliği ile ilgili sorular ortaya çıkmıştır. Bu ürünlerin güvenilirliğini sağlamak ve bu güvenilirliği uluslararası bir şekilde geçerli kılmak için bazı standardlar ortaya çıkmıştır. Bu ihtiyacı karşılamak için çıkarılan standardlardan bir tanesi ISO/IEC 15408 Ortak Kriterler Standardıdır. Bu standard sayesinde değerlendirme yetkisi olan ilgili kuruluşlar, bilgi teknoloji ürünlerini değerlendirmekte ve bu ürünün güvenilirliği yetkili otoritelerce verilen sertifikalarca sağlanmaktadır. Bu standardın yanı sıra ayrıca spesifik olarak kriptografik modüllerin gereksinimlerini belirten ve bu modüllerin onayı ve doğrulanması için kullanılan FIPS 140 standardı oluşturulmuştur. Kriptografik modüllerin güvenilirliğini belirlemek için ise bu standard kullanılmaktadır. Bu tezde öncelikle bu standardları ve bunlara uygun değerlendirme sürecininin dünya üzerinde nasıl gerçekleştiğini tanımlıyor ve ülkemizde nasıl uygulanması gerektiğinden bahsediyoruz. Ardından, kriptografik modül doğrulama sürecinin bir parçası olan kriptografik algoritma doğrulama sürecinin bu süreçte kullanılan kriptografik algoritmaların zafiyetlerinden etkilenmemesi için kullanılabilecek tüm algoritmalara örnek olması açısından AES-GCM algoritmasının zafiyetlerini ele alıyor ve buna alternatif AES modlarından bahsediyoruz. Son olarak bu zafiyetleri tespit etmemize yarayan test vektörlerinden bahsederek tezi tamamlıyoruz.

Anahtar Kelimeler: CMVP, AMVP, Ortak Kriterler, AES-GCM, Zafiyetler

Dedicated to my family...

ACKNOWLEDGMENTS

I would first like to thank my supervisor Assoc. Prof. Dr. Ali Doğanaksoy and my co-supervisor Assoc. Prof. Dr. Oğuz Yayla for their encouragements, patience, invaluable advices, and immense guidance throughout.

I would also like to thank my colleagues who were involved in the validation survey for this research project.

Finally, I must express my very profound gratitude to my parents for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

IT	Information Technology
TCSEC	Trusted Computer Security Evaluation Criteria
ITSEC	Information Technology Security Evaluation Criteria
NIAP	National Information Assurance Partnership
NVLAP	National Voluntary Laboratory Accreditation Program
CC	Common Criteria
SFR	Security Functional Requirement
SAR	Security Assurance Requirement
PP	Protection Profile
ST	Security Target
CEM	Common Evaluation Methodology
TOE	Target of Evaluation
EAL	Evaluation Assurance Level
CCRA	Common Criteria Recognition Arrangement
CMMI	Capability Maturity Model Integration
SPICE	Software Process Improvement and Capability Determination
FIPS	Federal Information Processing Standards
IG	Implementation Guidance
CSP	Critical Security Parameter
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
CMVP	Cryptographic Module Validation Program
CAVP	Cryptographic Algorithm Validation Program
AMVP	Automated Cryptographic Module Validation Protocol
ACVP	Automated Cryptographic Validation Protocol
CAVS	Cryptographic Algorithm Validation System
IUT	Implementation Under Test
DTR	Derived Test Requirements

AES	Advanced Encryption Standard
GCM	Galois/Counter Mode
NIST	National Institute of Standards and Technology
CSE	The Communications Security Establishment
CCCS	The Canadian Centre for CyberSecurity
MAC	Message Authentication Code
XOR	Exclusive or
IV	Initial Value
SIV	Synthetic Initialization Vector
AEAD	Authenticated Encryption with Additional Authenticated Data
GF	Galois Field
CTR	Counter Mode
CCM	Counter with CBC-MAC Mode
XEX	Xor–encrypt–xor
XTS	XEX-based tweaked-codebook mode with ciphertext stealing
CMS	Cryptographic Message Syntax

CHAPTER 1

INTRODUCTION

1.1 Motivation and Problem Definition

In Turkey, the process of evaluating information technology (IT) products according to the Common Criteria (CC) ISO/IEC 15408 Standard, which arises from the need to have an international certificate for reliability of IT products, and the testing process of cryptographic modules according to FIPS 140-2, which was created from ISO/IEC 19790-24759 Standards, and the FIPS 140-3 standards that will come into force in the future, are different from other countries. We carried out this thesis study in order to give the details of these processes.

1.2 Contributions and Novelties

Our contributions are as follows:

- Specification of an IT product evaluation and testing process according to the Common Criteria (ISO / IEC 15408) Standard in Turkey
- Specification of the security requirements required for testing cryptographic modules and how the process should be for this testing in Turkey
- Compilation of vulnerabilities that may arise in AES-GCM mode in Cryptographic Algorithm Validation Program (CAVP) and ACVP (Automated Cryptographic Validation Protocol)

- Specification of alternative algorithms that can be used to avoid these vulnerabilities
- Specification of test vectors to verify the presence of weaknesses causing vulnerabilities

1.3 The Outline of the Thesis

First, we recognize the Common Criteria (ISO/IEC 15408) Standard, Structure and Evaluation Methodology for Common Criteria in Chapter 2. In the next chapter, we introduce the FIPS 140-2 and FIPS 140-3 standards and security requirements for these standards. In Chapter 4, we mention Cryptographic Module Validation Program (CMVP) and Cryptographic Algorithm Validation Program (CAVP) and processes of these programs. After, we mention new automated version of these programs; Automated Cryptographic Module Validation Protocol (AMVP) and Automated Cryptographic Validation Protocol (ACVP) and processes of these protocols in Chapter 5. Then, we examine AES-GCM mode for CAVP and ACVP, and introduce the alternatives to AES-GCM because of the vulnerabilities of AES-GCM in Chapter 6. In last chapter, we write the test vectors for vulnerabilities in AES-GCM which we defined in Chapter 6.

CHAPTER 2

COMMON CRITERIA

In Turkey, the process of evaluating IT products according to the Common Criteria (CC) ISO/IEC 15408 Standard, which arises from the need to have an international certificate for reliability of IT products is different from other countries. Since cryptographic modules are included in IT products, we have reviewed this standard. In this section, we talk about what is the CC standard and how the evaluation is made worldwide according to the standard. Then we explain the process in Turkey and talk about how it should be.

2.1 History of Common Criteria

Research among information technology (IT) users shows that the users do not trust the security level guaranteed by the seller for the product they purchased, and they do not want to perform the security tests of the products themselves. As a solution, they want a third party to analyze IT products and determine the level of security guarantee through testing. Since cryptographic devices are included in IT products, this need has arisen for the cryptographic devices as well.

This need has led to the establishment of laboratories that test in accordance with the safety criteria accepted by countries. Initially, each country carried out its testing processes using the security criteria accepted by that country. In this process, based on the Trusted Computer Security Evaluation Criteria (TCSEC) standard prepared by the Ministry of Defense in the USA, European countries started to use Information Technology Security Evaluation Criteria (ITSEC) standard, based on TCSEC. These

two standards were sufficient for IT products to be used in the national networks of countries, but a common criteria was needed as the trade in IT products began to increase between countries. Because, for a manufacturer that sells its products in different countries, obtaining both ITSEC certification and TCSEC certification has become a long and costly process. TCSEC and ITSEC standards developed for military projects could not meet the needs of the private sector. For these reasons, countries have started working to develop a common standard.

As a result of the studies of USA, Canada, England, Germany, France, Australia and New Zealand countries, the Common Criteria standard, which was published in 1996, was developed. Following the changes made in May 1998, 2.0 version of the standard was published and in June of the same year, it adopted ISO Common Criteria as the international standard with the number ISO 15408. This version has been used for a long time in the international safety assessment of IT products. In order to meet the increasing needs, the 3.0 version of the standard with radical changes and 3.1 version of the standard was published in 2009 with revisions made upon the requests from the developers. An international committee is constantly working to update the standard in line with the developing technology, security and assurance perception, and today the work for the 4.0 version is about to be completed.

Common Criteria is a current standard that is still being developed. The number of countries that recognize this standard is increasing day by day and is rapidly progressing to become an internationally valid standard in IT security.

2.1.1 Common Criteria Standard

Common Criteria has two main uses. The first is that it provides "comparability" between assessments made at national and international borders. The results of the evaluation of functions according to Common Criteria can be easily comparable. The reason for this is that the features that the product meets during the evaluations are demonstrated by the wide-ranging, internally consistent security functional requirements (SFRs) defined in Common Criteria standard. These requirements are included in the second part of Common Criteria standard. Another benefit of Common Criteria is that it provides the guarantee that the product meets user's security requirements.

This assurance is provided by examining which of the security assurance requirements (SARs) that are consistent and dependent in the third part of Common Criteria standard are met by the product and which are not. Common Criteria has 4 main users in theory: consumers, product developers, evaluators and sponsors. But since product developers generally do the sponsorship, we can talk about three types of users.

Consumers use Common Criteria Standard as a guide to request products that provide the security features they want. They can also take advantage of the certified product library and check for products that meet their wishes. Product developers can use Common Criteria as a guide to provide the necessary safety features throughout the process from the design of the product to its release. Evaluators use IT products as the primary source when evaluating them according to the Common Criteria standard.

The Common Criteria standard consists of three parts. The first part, Introduction and General Model, is a guide that defines the general concepts of Common Criteria, what are the safety goals and requirements. In addition, the content of Security Target (ST) and Protection Profile (PP) is also included in this section. The second part is a reference book listing SFRs, that is, security functional requirements. The third section lists the security assurance requirements. In addition, this section shows assurance levels and assurance families that these levels should contain.

PPs and STs are the basic elements of Common Criteria evaluations. PPs are written by customers and requirements are specified for an IT product needed. STs, on the other hand, are documents prepared by the company that developed the product, before the product entered the Common Criteria assessment, and which security features and the level of safety of the product were specified.

In these documents, threats, policies and acceptance of the product are issued first and security objectives are determined to meet the threats and policies after the environment is defined. The functional requirements required to achieve these security objectives are prepared using the second part of Common Criteria. Then, the functional requirements are documented which functions of the product fulfill and how. Threats to these security functions ISO / IEC 15408 | INFORMATION TECHNOLOGIES MANAGEMENT: MODELS AND STANDARDS are checked to see if they meet and it can be concluded that the product provides the security it claims. The evaluator

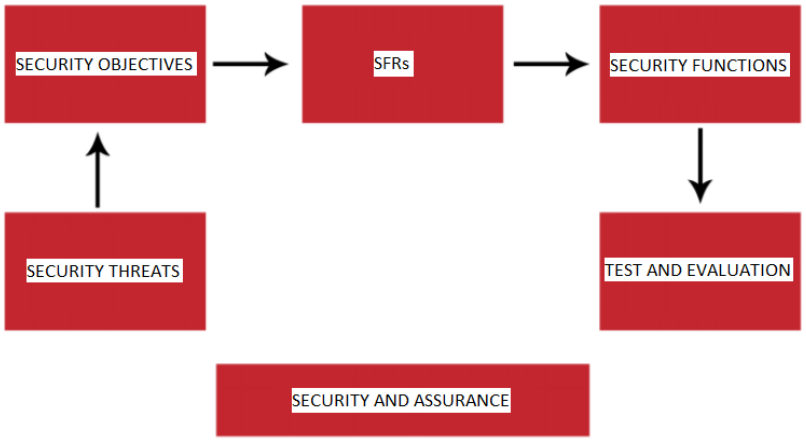

Figure 2.1: Common Criteria Security Structure

checks the accuracy of all these mappings when examining an ST or PP. In addition, while evaluating a particular product together with its ST, it is checked whether all its functions are working and whether all threats are met. As a result, if the product has passed the assessor tests, it is decided that it provides the security it claims. The next step is to examine the compliance with the assurance level claimed by the product.

2.1.2 Evaluation Methodology

In order to evaluate in accordance with the Common Criteria standard, the countries that prepared the standard also prepared an evaluation methodology. This guide, called CEM (Common Evaluation Methodology), explains step by step how to perform PP, ST of TOE (target of evaluation) evaluations. The laboratory performing the assessment has to act in accordance with this methodology. Otherwise, the evaluations made do not have their international validity.

After the ST of the product is evaluated and approved, the TOE is started to be evaluated. There are seven different levels of assessment by standard. EAL1 and EAL2 are low assurance levels. EAL3 and EAL4 are levels given to products that provide a medium assurance. EAL5 and EAL6 are highly guaranteed levels. EAL7 provides a complete level of assurance. When writing the ST, the manufacturer specifies the level of assurance it claims and the assurance requirements provided by the product. The evaluator should check; whether the assurance requirements provided by the product are sufficient for the claimed level of assurance, and whether these requirements

are correct. The evaluator requests some documents from the manufacturer during the evaluation of the TOE. These are called evaluation evidences. The manufacturer must provide these documents to the evaluator.

The product, which is evaluated in accordance with the methodology, is sent to the certification institution, which will issue the international Common Criteria certificate to the product together with the evaluation technical report.

2.1.3 CCRA and Common Criteria Structure

Countries forming the standard have signed a mutual recognition contract called Common Criteria Recognition Arrangement (CCRA). The purpose of this agreement is to ensure that the evaluation made in any of these countries is recognized by other countries. It is possible to sign the contract in two ways. The first is to sign the contract as a certificate customer. The country that signs CCRA as a certificate customer does not have the authority to produce internationally recognized certificates. The country can only become a customer of the certificates of other countries with this authority. Another signing option is to sign as a certificate producer. In this case, the country is able to make Common Criteria evaluations and ISO / IEC 15408 certificates are recognized by member countries. In order to sign the CCRA contract as a certificate manufacturer, it is imperative to demonstrate a structure of Common Criteria established and operating in the country.

The cornerstone of the Common Criteria structure is the certification body. This institution grants the evaluation licenses to the independent laboratories that will conduct the evaluations and performs the inspection duty during all evaluations. It also examines the evaluation technical report as a result of the evaluation and issues Common Criteria certificates to successful products. The certification body works under a government agency with the assurance of the country. The country is responsible for all certificates produced by the institution. Certification institution starts to establish Common Criteria structure in the country. It identifies all procedures required for Common Criteria evaluations, including licensing procedures, and operates transparently. Another important part of the structure is the independent test laboratories. They work under the supervision of the certification institution and have to obey

all the rules of the structure they work in. In general, when the Common Criteria structure is mentioned, the certification institution, independent laboratories and the relations between these institutions can be understood.

Turkey signed CCRA agreement in 2003 as a Certificate Customer and update the status of the country as of November 2010 Certification Producer. Since this date, the Common Criteria Certificates of all products certified under the National Common Criteria Structure, in which the Turkish Standards Institute operates as the Certification Authority, are valid internationally.

2.1.4 Evaluation Process in Turkey

Turkish Standards Institution Common Criteria Certification Scheme sponsored by Ministry of Science, Industry and Technology is the participant of the CCRA. Turkish Standards Institution - Common Criteria Certification System (OKBS in Turkish), the compliance of the Common Criteria standard and the requirements of the Common Evaluation Methodology regarding the claimed evaluation assurance level of an IT product by a Common Criteria Evaluation Laboratory (OKDL in Turkish) performs certification within the framework of the CCRA and related procedures. It is the type of certification realized as a result of its evaluation and determination of its suitability [7].

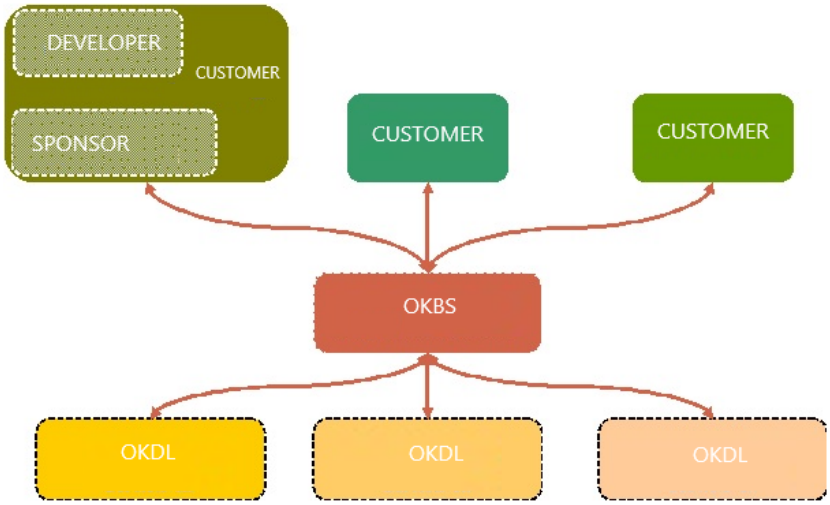

Figure 2.2: Common Criteria Certification System in Turkey [7]

- Common Criteria Certification System (OKBS) Customer can be the developer / manufacturer of the product to be directly certified, or a sponsor that finances the certification, or both.

- OKBS makes the testing and evaluation activities in accordance with the Common Criteria and Evaluation Methodology of the products to be certified by the Common Criteria Evaluation Laboratories (OKDL).

- Within this system, OKBS is obliged to ensure the technical competence of OKDLs and their consistency with each other. OKBS ensures this through laboratory examinations and meetings it conducts periodically.

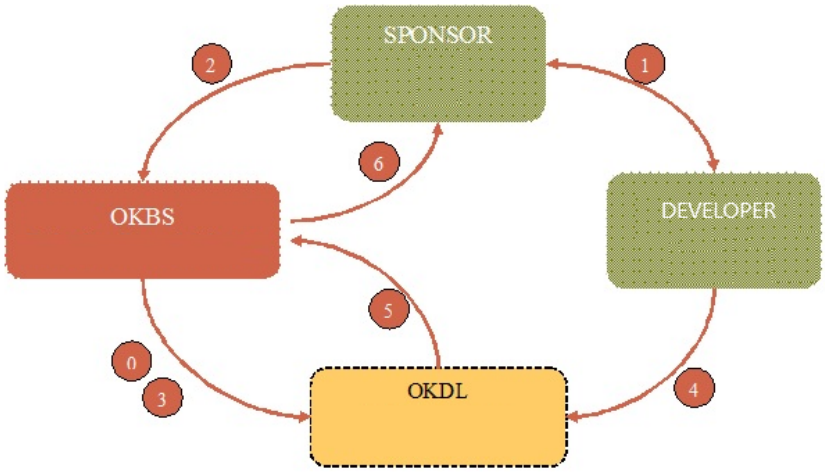

Figure 2.3: Common Criteria Certification Process in Turkey [7]

0. Licensing

1. Contract

2. Certification Application

3. Evaluation Request

4. Product and Documentation

5. Evaluation Reports

6. Certification Report, Common Criteria Certificate

2.1.5 Product Assessment Suitable for Common Criteria

The Common Criteria standard proposes a methodology that must be followed from the design stage to develop the product, taking into account the safety requirements. In product evaluation, these stages are verified by the response analysis and the integrity tests, customers are provided with the security and guarantee they need regarding the product.

After the assurance requirements are determined for the product to be tested, as suggested by the standard, the design phase should be started by creating a functional specification that includes internal and external interactions for each safety requirement. Then, in this functional specification, high-level designs of security functions defined by formal or non-formal methods should be prepared according to the assurance level. Following this design, the lower level design documentation should be created, in which the design of each security function will be shown in detail, and source code and/or hardware drawings should be created in accordance with this lower level design. Finally, the product should be developed by applying these drawings. While the product evaluation is carried out in accordance with the Common Criteria, the laboratory requests evaluation evidence from the product developer that they have designed and implemented in accordance with these steps. Especially at EAL4 and higher assurance levels, products should be developed in accordance with all of these steps. However, compliance with these steps is somewhat less sought at EAL3 and below.

Figure 2.4 shows the steps required for product development in accordance with Common Criteria and development evidence, which is one of the evaluation evidence of these products.

2.1.6 Related Standards and Models

Unlike other quality, process and standards, Common Criteria certification is an international standard developed by operating a certain level of quality process for the certification of IT products in terms of security. The requirements of Common Criteria for product safety are in line with the subject of verification of network components

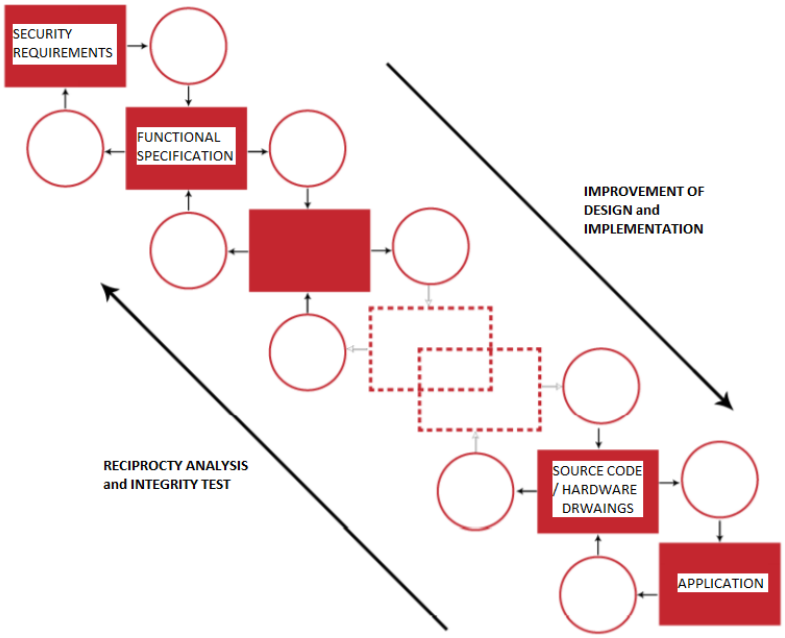

Figure 2.4: Product development stages in accordance with Common Criteria

in ISO/IEC 27001 standard. It is recommended to use verification methods similar to Common Criteria during the installation and integration of products to the infrastructure in companies where information security management system is established and operated.

For example; IT product outputs, where models for the maturation of product development processes such as CMMI, SPICE are applied, are highly effective in faster completion of the Common Criteria certification process.

Common Criteria include verifying that the purchased IT solution has developed security functions with sufficient resistance to threats found in the operational environment, and a vulnerability analysis performed by a third-party independent laboratory. In this context, the assurance that the documented products' weaknesses or risks that may arise in the system have been evaluated and met by the product developer are guaranteed by the Common Criteria certification. In this regard, it is important to choose a certified product especially in critical infrastructures in terms of full operation of other relevant standards and models.

CHAPTER 3

FIPS 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

Another standard required for determining and evaluating the requirements of cryptographic modules is the FIPS standard. In this section, we show how the requirements and security levels of cryptographic modules are determined worldwide and how they can be developed accordingly in Turkey.

3.1 Introduction

FIPS 140-2 Standard specifies and contains security requirements for the secure design and implementation of a cryptographic module. In the standard, 11 requirement areas and four security levels for each requirement area are specified. Although the aim of the standard is to provide security with these requirements, we can never say that a cryptographic module compliant with the standard is completely secure.

The requirements protection of critical data, protection of unauthorized processing and use, prevention of disclosure of critical data, prevention of unauthorized alteration, addition and deletion of critical data, keeping indicators related to the working status of the module, ensuring proper functioning of the module and detecting errors in the operation of the module in this standard for the cryptographic module are prepared according to security requirements [9].

3.2 Security Levels Requirements

Each security level contains the requirements of the previous security level. The higher the security level, the higher the requirements. Besides this, specially security level 2 and higher meets the functional requirements specified in Common Criteria Protection Profiles (PPs) listed in FIPS 140-2 Annex B: Approved Protection Profiles for FIPS PUB 140-2, Security Requirements for Cryptographic Modules. Requirements for security levels are stated below [9]:

- The software and firmware components of the cryptographic module can be run on a general purpose computing system using an unassessed operating system. (Security Level 1)
- The software and firmware components of the cryptographic module can be executed on a general purpose computing system using an operating system. (Security Levels 2,3,4)
- A reliable operating system rated as equivalent can be used. (Security Levels 2,3,4)
- The Common Criteria evaluation assurance level corresponds to EAL2 or higher. (Security Level 2)
- The Common Criteria evaluation assurance level corresponds to EAL3 or higher. (Security Level 3)
- The Common Criteria evaluation assurance level corresponds to EAL4 or higher. (Security Level 4)
- The cryptographic module must have at least one approved algorithm or approved security function. (Security Levels 1,2,3,4)
- The cryptographic module must have role based authentication. (Security Levels 2,3,4)
- The cryptographic module must have an identity based authentication mechanism. (Security Levels 3,4)

- Input or output of plaintext critical security parameters (CSPs) must be performed using ports physically separated from other ports or using interfaces that are logically separated from other interfaces using a reliable path. (Security Levels 3,4)

- The cryptographic module meets the FTP_TRP.1 security functional requirement (SFR) in the Common Criteria PART2 V3.1R5 document. (Security Levels 3,4) The cryptographic module meets the ADV_SPM.1 Formal Target of Evaluation (TOE) security policy model assurance component in the Common Criteria PART3 V3.1R5 document. (Security Levels 3,4)

- The cryptographic module must contain special environmental protection features designed to detect fluctuations and reset CSPs, or must pass rigorous environmental failure tests to provide reasonable assurance that it will not be affected by fluctuations outside the normal operating range in some way. (Security Level 4)

3.3 Security Requirements

Most of the security requirements of this standard include specific documentation requirements outlined in Annex A: Approved Security Functions for FIPS PUB 140-2 and Annex C: Approved Random Number Generators for FIPS PUB 140-2. Security requirements that the cryptographic module must meet are Cryptographic Module Specification; Cryptographic Module Ports and Interfaces; Roles, Services and Authentication; Finite State Model; Physical Security; Operational Environment; Cryptographic Key Management; Electromagnetic Interference / Electromagnetic Compatibility (EMI / EMC); Self Tests; Design Assurance; and Mitigation of Other Attacks.

All security requirements for how a cryptographic module should be and its documentation are contained in FIPS PUB 140-2. The standard has 4 additional documents. Annex A contains the Approved security functions, Annex B contains the list of Approved protection profiles, Annex C contains the list of Approved random number generators and Annex D contains the list of approved key establishment techniques.

The required methods for accredited laboratories to test whether cryptographic modules comply with the requirements of this standard are included in the Derived Test Requirements for FIPS PUB 140-2 document. Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program document provides guidance for the Derived Test Requirements for FIPS PUB 140-2 document [1].

3.4 FIPS 140-3 Security Requirements for Cryptographic Modules

The currently validated version is FIPS 140-2, but the FIPS 140-3 standard will replace the FIPS 140-2 standard. The final version of the FIPS 140-3 standard has been published. The FIPS 140-3 test will take effect on September 22, 2020, and the FIPS 140-2 test period will end on September 22, 2021. The FIPS 140-3 standard complies with ISO / IEC 19790: 2012 (E) and includes changes to the CMVP permitted Annexes. Tests for FIPS 140-3 requirements will be conducted in accordance with ISO / IEC 24759: 2017 (E).

There are differences in this standard in the security requirements required for the cryptographic module. Security requirements that the cryptographic module must meet are Cryptographic Module Specification; Cryptographic Module Interfaces; Roles, Services, and Authentication; Software/Firmware Security; Operating Environment; Physical Security; Non-invasive Security; Sensitive Security Parameter Management; Self-tests; Life-cycle Assurance; and Mitigation of Other Attacks in FIPS 140-3 [19].

CHAPTER 4

CRYPTOGRAPHIC MODULE VALIDATION PROGRAM (CMVP) AND CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM (CAVP)

The validation of cryptographic modules whose requirements and security levels are determined according to the FIPS is made according to CMVP. In this section, we talk about how the CMVP process works worldwide and how it should be in Turkey.

4.1 Introduction

CMVP was established in 1995 by NIST and The Canadian Centre for CyberSecurity (CCCS). The purpose of CMVP is to validate cryptographic modules according to FIPS 140. Cryptographic module owners use National Voluntary Laboratory Accreditation Program (NVLAP) approved Cryptographic and Security Testing (CST) laboratories to test their modules. CMVP provides testing of cryptographic modules for FIPS compliance by CST laboratories and shares test results with the government to prove the reliability of this cryptographic module. Until 2003, CMVP included CAVP. However, due to the increase in cryptographic algorithms, CAVP has been a separate program since 2003 [3].

4.2 CMVP

CMVP ensures the availability and assurance of cryptographic modules. It is ensured by the compliance of the cryptographic module to FIPS 140.

4.2.1 Roles of CMVP

- **VENDOR** designs and manufactures the cryptographic module. When this cryptographic module is ready to be tested, the vendor sends the module to the CST laboratory.
- **CST Laboratory** tests the cryptographic module against Derived Test Requirements (DTR) and Implementation Guidance (IG) for FIPS 140 and the CMVP according to the requirements specified in FIPS 140. Generates a test report for CMVP Validation Authorities if there is finding in the test. If there is no finding, the CST laboratory submits a report to the Validation Authorities.
- **CMVP Validation Authorities** are NIST for the USA and CCCS for Canada. They verify the test results for the cryptographic module. A verification certificate is issued for the module and the online verification list is updated.
- **USER** verifies that a module they are considering purchasing is verified by checking the version of the module at NIST's website.

4.2.2 Process

1. Cryptographic Module Vendor requests validation of implementation from Accredited Cryptographic and Security Testing Laboratory.
2. Cryptographic Module Vendor submits the module for testing under a contractual agreement.
3. Accredited Cryptographic and Security Testing Laboratory performs conformance test by Derived Test Requirements (DTR) for FIPS 140-2.
4. Accredited Cryptographic and Security Testing Laboratory prepares Cryptographic Module Test Report.

5. Accredited Cryptographic and Security Testing Laboratory submits report to CMVP.

6. NIST initiates cost recovery process.

7. The coordination process between CMVP and Accredited Cryptographic and Security Testing Laboratory continues until the CMVP receives the answers to all of its questions.

8. Cryptographic Module is validated by CMVP and information of cryptographic module sent to the verified modules list at NIST's website.

4.3 CAVP

CMVP validates cryptographic modules against FIPS 140-2. CAVP verifies whether cryptographic algorithm implementations are FIPS and NIST approved cryptographic algorithms. It makes the verification test takes place in the verification system, which includes the algorithm components, their features and the tests in which their functionality is tested in order to verify whether these cryptographic algorithms are approved algorithms or not. CAVP is also jointly managed by NIST and CSEC. Vendors use CST laboratories to test their cryptographic modules and validate cryptographic algorithm implementations [2].

4.3.1 Roles of CAVP

- **VENDOR** The vendor implements encryption algorithms. When the implementation is ready to be tested, the vendor sends it to the CST Laboratory for validation (the implementation can be tested in-house by the vendor or in the laboratory by the laboratory).

- **CST Laboratory** tests cryptographic algorithm implementations using the CAVS tool. If the person conducting the test is the vendor, the CST Laboratory sends the test input vectors to the vendor. The vendor sends the responses to the CST Laboratory. The CST Laboratory that performs the test runs the algorithm

tests that give the test results using the implementation and input test vectors. It also uses the CAVS tool to test the accuracy of the results.

- **CAVP Validation Authorities** are NIST for the US Government and CSE for the Government of Canada. CAVP Validation Authorities use validation systems to verify cryptographic algorithms. Validation systems include validation tests to test the cryptographic algorithm. CAVP Validation Authorities design and implement the CAVS test tool, generate validation system certification. The validation system documentation is published on the CAVP website for use by end users.
- **USER** verifies the cryptographic algorithms in the cryptographic module to be purchased from the http://csrc.nist.gov/groups/STM/cavp/validation.html.

4.3.2 Process

1. Vendor with Cryptographic Algorithm implementation requests validation of implementation from Accredited CST Laboratory.
2. Accredited CST Laboratory requests algorithm spesific information from Vendor.
3. Tester develops test suite (The cryptographic algorithm implementation can be tested by the vendor on-site or in the CST lab).
4. Accredited CST Laboratory generates input test vectors by Cryptographic Algorithm Validation System (CAVS) tool.
5. Accredited CST Laboratory sends test vectors to tester.
6. Tester inputs test vectors in implementation.
7. Tester sends test results to the Accredited CST Laboratory.
8. Accredited CST Laboratory verifies test results by using CAVS tool.
9. Accredited CST Laboratory sends validation submission (includes official verification request from the laboratory, verification test results for each algorithm tested, files generated from the CAVS tool) to the CAVP (NIST and CSESC).

10. CAVP (NIST and CSESC) rewievs submission and determines validation.

11. CAVP (NIST and CSESC) creates entries for validated algorithms implementations in website (http://csrc.nist.gov/groups/STM/cavp/validation.html).

CHAPTER 5

AUTOMATED CRYPTOGRAPHIC MODULE VALIDATION PROTOCOL (AMVP) AND AUTOMATED CRYPTOGRAPHIC VALIDATION PROTOCOL (ACVP)

In the previous section, we mentioned that the validation of cryptographic modules whose requirements and security levels are determined is made according to CMVP. In the days to come, CMVP will be replaced by its automated version, AMVP. In this section, we talk about how the AMVP process will be and how it should be in Turkey.

5.1 Introduction

CAVP testing was required for cryptographic modules that have passed conformity testing and validation performed according to the FIPS 140-2 specification and for Common Criteria evaluations performed according to the NIAP Common Criteria Evaluation and Validation Scheme. ACVP is the new protocol used for FIPS conformant testing and Common Criteria validation. It automates the testing of cryptographic algorithms.

Cryptographic algorithms were verified with the CAVS tool. The CAVS is a tool provided by CAVP to accredited laboratories to test cryptographic algorithms and send their results to CAVP.

5.2 AMVP

The current NIST validation process does not allow for rapid updates and patches while maintaining a verified status. It is designed to speed up test data production, reporting of results and verification of cryptographic algorithms in line with this need. It takes advantage of machine learning and artificial intelligence to enable automation. It includes the stages of an IUT, from the testing phase to the creation of evaluation evidence and their validation. For CMVP verification, cryptographic algorithm verification with CAVP is required, and for AMVP, cryptographic algorithms should be verified with ACVP first [6, 10].

5.3 ACVP

ACVP is a network protocol that enables the server to generate NIST's test vectors, validates responses, and issues a FIPS 140-2 compliance and NIAP's Common Criteria evaluation certificate if validation is successful. ACVP has three main parts: server, client and proxy [10].

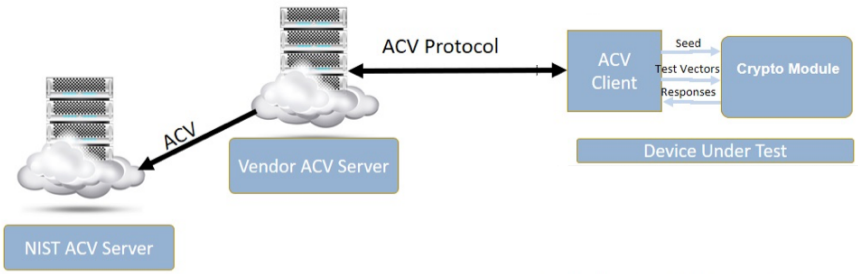

Figure 5.1: Automated Cryptographic Validation System [4]

5.3.1 ACVP Server

The server part is worked by NIST or any FIPS laboratory. ACVP is a cloud based test system so there is an interface between the server and the client created using ACVP. The server's tasks are generating test vectors, sending these test vectors to the

client, taking test results and posting certificate to the client [4, 5].

5.3.2 ACVP Client

The client's tasks are to connect to the cryptographic module to be tested, send requests for test vectors, send responses to test results, and send algorithm verification requests. For this, it communicates with the server. In addition to these tasks, it creates JSON for communication with the server, parses it, uses HTTPS GET, POST, PUT, DELETE messages for secure information transmission, and performs two-factor authentication [4, 5].

5.3.3 ACVP Proxy

A proxy can be used to manage the information transferred from the tested system to the server and communicate with this system when the system is offline. However, proxy is generally not preferred and client is used instead. It enables the test vectors to be retrieved from the server, the test results sent to the server, decisions regarding these results are made and certificate procured from the server. Proxy and parser work together to complete the test phases [4, 5].

5.3.4 ACVP JSON Parser

The obtained test vectors are stored in Testvector-request.json files and transferred to the system containing the cryptographic module. The JSON file is added to the encryption module to generate this file containing the test vectors. Parser's task is to parse JSON files, call the encrypting application, and generate test response JSON data. Besides, it determines what will be transferred to the JSON stream [4, 5].

5.3.5 Process

An example process for algorithm validation is as follows:

1. Client requests vectors from Lab Server.
2. The Lab Server requests the vectors from NIST Server.
3. The NIST Server sends the vectors to the Lab Server.
4. The Lab Server sends the vectors to the Client.
5. The Client sends the vectors to Cryptographic Module.
6. The Cryptographic Module sends the responses to the Client.
7. The Cryptographic Module sends the responses to the Lab Server.
8. The Lab Server sends responses to the NIST Server.
9. Finally, the NIST Server posts the certificate to the Lab Server.

CHAPTER 6

VULNERABILITIES IN AES-GCM

In this chapter, since the weaknesses in the algorithms affect the validation processes negatively, we exemplified the vulnerabilities of a cryptographic algorithm (AES-GCM) in order to prevent the vulnerabilities of the cryptographic algorithms used in the cryptographic algorithm validation program, which is a part of the cryptographic module validation program. In addition, we consider other commonly used AES encryption mode of operations. During the validation program of the cryptographic module, the situations that may cause vulnerability to the AES-GCM algorithm in the cryptographic algorithm validation phase are reusing the initial vector, becoming authentication tag short, using initial vector length different from default value and using weak keys. We also examined AES-GCM-SIV, AES-CCM and XTS-AES modes of encryption. A flow chart of AES-GCM mode of authenticated encryption for two blocks is given in Figure 6.1.

6.1 Reusing the IV

The first situation that may cause vulnerability to the AES-GCM algorithm is reusing the initial vector. In this part, we will look the results of using the initial vector more than once. It may decrease the security of the AES-GCM and it makes invalid the confidentiality of the messages encrypted with same initial vector.

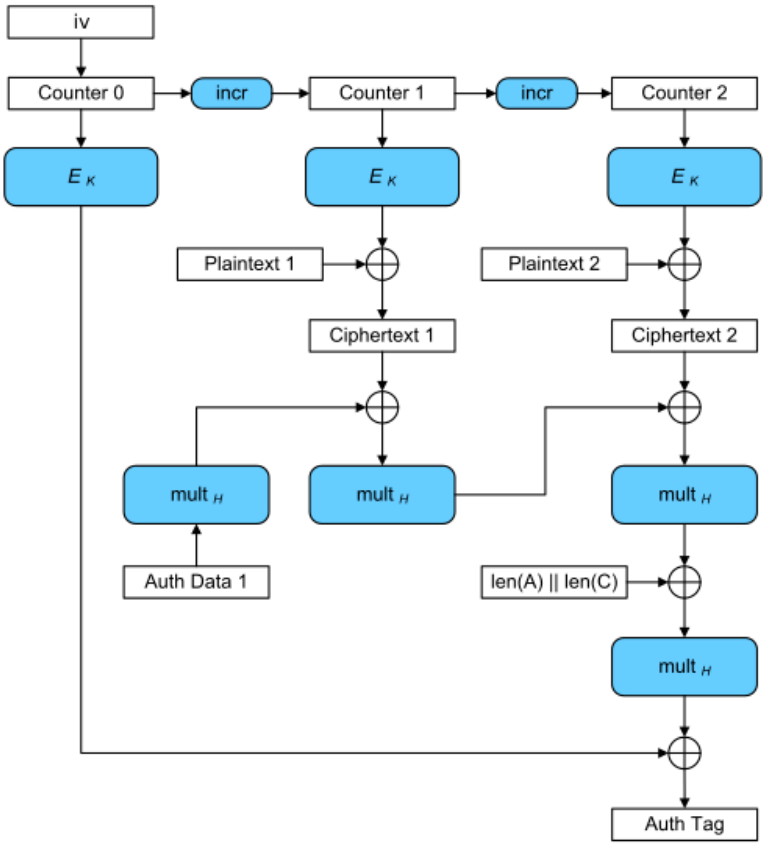

Figure 6.1: AES-GCM [11]

6.1.1 Forbidden Attack

Forbidden attack works with both NIST and original version of the GCM. It is assumed that the attacker/adversary/enemy only knows initial vector, associated data, ciphertext and MAC tag and initial value is repeated. It follows that, there are two different messages encrypted with the same initial vector and we get two different authentication tag. When we XOR these authentication tags; first we apply $GCTR_k$ function to the J_1 and J_2 counters but since initial values are same, our counter values are same, say $J_1 = J_2 = J$. Therefore output of $GCTR_k(J, S_1) \oplus GCTR_k(J, S_2)$ will be $S_1 \oplus S_2$. S_1 and S_2 are the value of a polynomial at H and also polynomial's coefficients can be derived from the ciphertext. The attacker can learn H root of the polynomial from $S_1 \oplus S_2$. When the polynomial degree is high, attacker may try to find two more different messages with same initial values or more and and get another polynomial(s) with root H. Then s/he can get the key H value. Therefore, the initial value should not be used more than once for different messages [13, 18].

6.2 Using Short Authentication Tag

The second situation that may cause vulnerability to the AES-GCM algorithm is using short authentication tag. In this part, we will look the results of using short authentication tag. It may lead to authentication weaknesses in AES-GCM. It increases the likelihood of a successful forgery attack and exposes the authentication key if the attacker can achieve the successful forgery attack.

6.2.1 Recovering H

Message size in AES-GCM is limited to the $2^9(2^{30}-1)$ bit and the use of byte lengths is preferred since the odd bit length provides a disadvantage over the application. Moreover, using large precomputed tables can be a problem in performance. So, small tables should be used to increase the performance of implementation. There are also some restrictions about authentication tag. First of all, a single authentication tag length must be used for the same key. Secondly, authentication tag length must be at least 128 bit for security reasons. We have some properties to recover the H in AES-GCM [18]:

1. $\overline{X}$= $(X_0...X_{127})^T$ where $X_0...X_{127}$ are individual bits of X polynomial's 128 coefficients.
2. $\overline{C \cdot X}$=$M_C\overline{X}$ means for each ciphertext C, there is M_C 128×128 matrix over GF(2) for all X polynomials.
3. $\overline{X^2}$=$M_S\overline{X}$ for all X polynomials where M_S is a fixed matrix.

The purpose of this attack is to change the ciphertext in the AES-GCM algorithm without the receiver noticing. First, we seperate the ciphertext C into sequences $C_1, C_2, ..., C_n$ to perform the attack where C_1 encodes the ciphertext length,
$C_2, C_3, ..., C_n$ are ciphertext blocks and n is the total number of blocks. Then authentication function T is equal to by the definition:

$$T := K_0 + \sum_{i=1}^{n} C_i H^i \text{ in GF}(2^{128})$$

where K_0 is the key stream block [11]. C_i's are the original ciphertext blocks and let C_i''s be the modified ciphertext blocks. We want $\sum_{i=1}^{n} C_i H^i = \sum_{i=1}^{n} C_i' H^i$ equality to ensure that the receiver does not understand that the ciphertext has been changed and to carry out the attack. This equality implies that $\sum_{i=1}^{n} (C_i - C_i') H^i = 0$. So, we are looking for the coefficients of $C_i - C_i'$ such that the leading bits of the $\sum_{i=1}^{n} (C_i - C_i') H^i$ are zero but we are just looking for the i's in form of $i = 2^j$ for some j to only have non zero coefficients. Therefore, we are searching for the leading bits of of the $\sum_{2^j} (C_{2^j} - C_{2^j}') H^{2^j}$. Using the properties we described above, we get $\sum_{2^j} M_{(C_{2^j} - C_{2^j}')} (M_S)^{2^j} \overline{H}$ where $(M_S)^{2^j}$ is a fixed known matrix for each value of 2^j and coefficients of each $M_{(C_{2^j} - C_{2^j}')}$ are linear combinations of the bits of the corresponding $(C_{2^j} - C_{2^j}')$. Then, we force bits of this polynomial to zero. We have $128 \cdot n$ free variables and we can force n-1 (except all zero solution) bits of the result of the equations from the equations used to force the bits of the polynomial to zero if we have n different $(C_{2^j} - C_{2^j}')$ coefficients to choose.

Assume that $m < 128$ bit authentication tag is used and there is a known message of 2^k blocks for some k. With k times 128 free variables we can find non zero solutions that zero out $m/2$ rows of the $\sum_{2^j} M_{(C_{2^j} - C_{2^j}')} (M_S)^{2^j}$ matrix. It means that the first $m/2$ bits of the authentication tag will not change if we apply the differences $(C_{2^j} - C_{2^j}')$ to the ciphertext. After $m/2$ forgery attempts we can expect a successful forgery.

6.3 Using Non-default Initial Value Length

The third situation that may cause vulnerability to the AES-GCM algorithm is using non-default initial value length. In this part, we will look the results of using initial vectors which have lengths different from 96 bits. Attacks described here work with only GCM's NIST version. It is assumed that the attacker/adversary/enemy can choose the plaintext and the initial value which belongs to this plaintext but s/he can not use the same initial value more than once [8].

6.3.1 Getting Collision and Forbidden Attack

This attack is based on the bad feature of the $GHASH_{core}$ function. We have

$$GHASH_{core_H}(\{\}, \widehat{IV}) = GHASH_{core_H}(\{\}, \widehat{IV||0})$$

property [11]. Normally, initial vector is right padded to the next block with zeroes. Therefore, both $\widehat{IV}$ and $\widehat{IV||0}$ is equal to the initial value's right padded form. As a result, the attacker/adversary/enemy can get an internal collision on the initial counter values by using these different initial values. In general, after processing about 2^{64} data blocks, a collision can be expected on the counter values. The next process is the same as Forbidden Attack in Section 6.1.1.

On the other hand, if we use an initial value with 0^l form in GCM's NIST version, then we start with J_0 with all zero block and H will be the zero. It follows that $T = E_k(J_0 \oplus S)$. We know that $J_0 = 0$ and $T = E_k(J_0 \oplus S)$ equation gives us S and $T = S \oplus T$ are the values of a known polynomials at H. Therefore, we can learn the H value by forcing a collision between H and some internal value. As a result, the default value of the IV length, 96 bits, should be used.

6.4 Using Weak Keys

In AES-GCM ciphertext C split into 128 bit blocks as $C = C_1||C_2||...||C_n$ and the authentication key $H = E_K(0)$. The authentication tag $T = Y_n \oplus E_K(IV||0^{31}1)$ where Y is evaluated by using Horner's rule in GF(2^{128}) as $Y_n = \sum_{i=1}^{n} C_i \otimes H^{n-i+1}$. In n rounds of AES-GCM, Horner's iteration:

$Y_1 = C_1 \times H$

$Y_2 = (Y_1 + C_2) \times H = C_1 \times H^3 + C_2 \times H^2 + C_3 \times H$

$\vdots$

$Y_m = (Y_{m-1} + C_m) \times H = C_1 \times H^m + C_2 \times H^{m-1} + ... + C_m \times H$ for some m

What if, say, $H = H^n$? Then we may just swap C_1 and C_n and the Y_n value will remain unchanged:

$Y_m = C_m \times H^m + C_2 \times H^{m-1} + ... + C_1 \times H$. Then, a cycle will lead to a cycling attack.

6.4.1 Cycling Attack

AES-GCM is vulnerable to cycling attacks. Bad values of the internal H key, which can be precalculated for certain AES key values, can negatively affect its security [21]. Powers of H will repeat in cycles which are determined by m =ord(H) according to the elementary group theory.

In order to perform the cycling attack, first we swap C_1 and C_m blocks or bits. We start with $H^1 = AES_k(0)$ for some k and generate $H^2 = H \times H$ from it. It follows like that and $H^k = H^1$ for some k and we get a collision. Hence, $H^{15} = H^0$ and it is the unique identity element with cycle length 1. The attacker does not know the H but s/he can easily attempt a blind forgery by swapping two or more message blocks. Juhani and Saarinen [21] shows the probability of this forgery in a theorem:

Theorem: Let n be a number satisfying gcd(2^{128} 1, n) = n. Blindly swapping blocks C_i and C_j, where $i \equiv j$ (mod n) will result in a successful forgery with probability of at least (n+1)/(2^{128}) if H is random.

6.5 Other Modes of AES Encryption

6.5.1 AES-GCM-SIV

AES-GCM, a type of Authenticated Encryption with Additional Authenticated Data (AEAD), is widely used with its improved performance with AES and polynomial multiplication directives. However, if two different messages are encrypted with the same initial value, it will fail in terms of privacy and integrity. Misuse-resistant Authenticated Encryption with Additional Authenticated Datas are not affected by this problem. AES-GCM-SIV is an ideal choice when unique initialization values cannot be guaranteed. Encrypting two messages with the same initial value only indicates whether these messages are equal. As a result, AES-GCM-SIV algorithm can be used as an alternative to AES-GCM, as it removes the reusing the IV vulnerability we identified for the AES-GCM algorithm [17, 14].

6.5.1.1 Algorithm

The key point of the algorithm is the use of a synthetic initialization vector (SIV) calculated using the Galois field multiplication using POLYVAL.

The algorithm uses a $K1$ hash key and a $K2$ encryption key. It applies hash function POLYVAL to the message to be encrypted and additional authentication data with $K1$. Only difference between POLYVAL and GHASH is that POLYVAL is defined over the reverse polynomial used in GHASH over GF(2^{128}). It XORes hash value and initial value and then produces an authentication tag by AES encrypting under $K2$. Finally, the message is encrypted with AES in CTR mode using $K2$ with an initial counter generated from the authentication tag [20, 17].

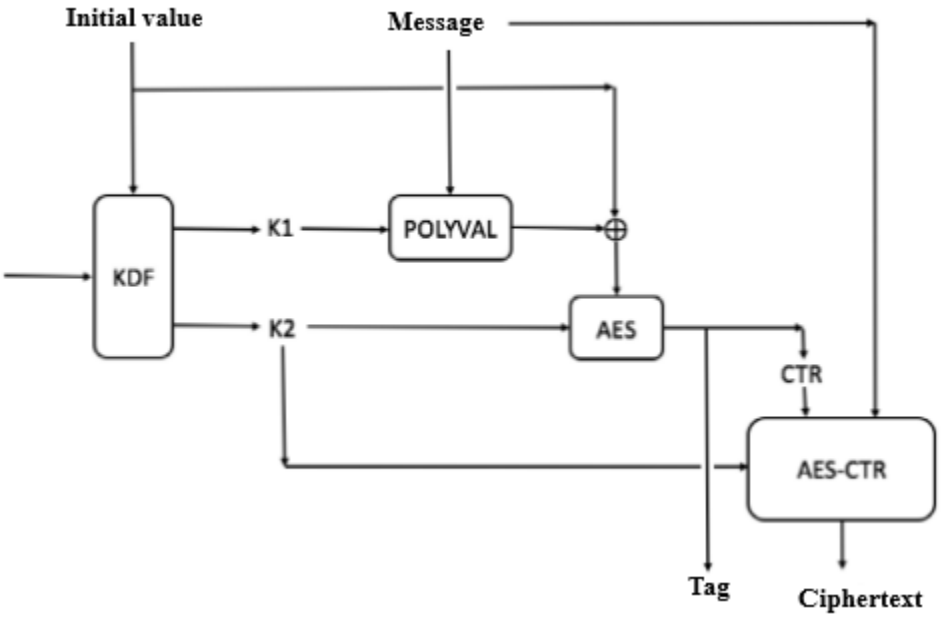

Figure 6.2: Diagram of AES-GCM-SIV [20]

Initial counter is pseudorandom for each distinct initial value/message pair. Therefore, the effective initial value which is used to mask encryption is different for distinct messages, even if the actual initial value is repetitive [16, 15].

6.5.2 AES-CCM

AES-CCM can be used as an alternative to AES-GCM. They have same four inputs: AES key, initial value, plaintext and additional authenticated data (optional) and they have same two outputs: ciphertext and authentication tag. Likewise, in both AES-GCM and AES-CCM, the party performing the authenticated encryption process generates the initial value.

6.5.2.1 Security Vulnerabilities

The initial value must be unique. Using the same initial value for two different messages encrypted with the same key creates a security vulnerability. Besides this, both AES-CCM and AES-GCM use the AES block cipher in counter mode for encryption. Unfortunately as in AES-GCM, if counter block values are used for more than one encryption operation with the same key, the same key stream is used to encrypt both plaintexts, privacy and integrity cannot be protected.

6.5.2.2 Increase the Security

To ensure the security, implementations should use an automated management system. They can be used safely with CMS authenticated enveloped data content type. It supports four key management techniques called key transport, key agreement, symmetric key encryption and passwords. These techniques ensure the requirements of automated key management system provided that a new content authenticated encryption key is produced for the conservation of every content.

6.5.3 XTS-AES

XTS stands for the XEX Tweakable Block Cipher with Ciphertext Stealing and the tweak is a 16-byte value. XTS-AES-128 encryption requires 256 bit key and XTS-AES-256 encryption requires 512 bit key.

The purpose of the XTS-AES mode is just cryptographic protection of data on storage

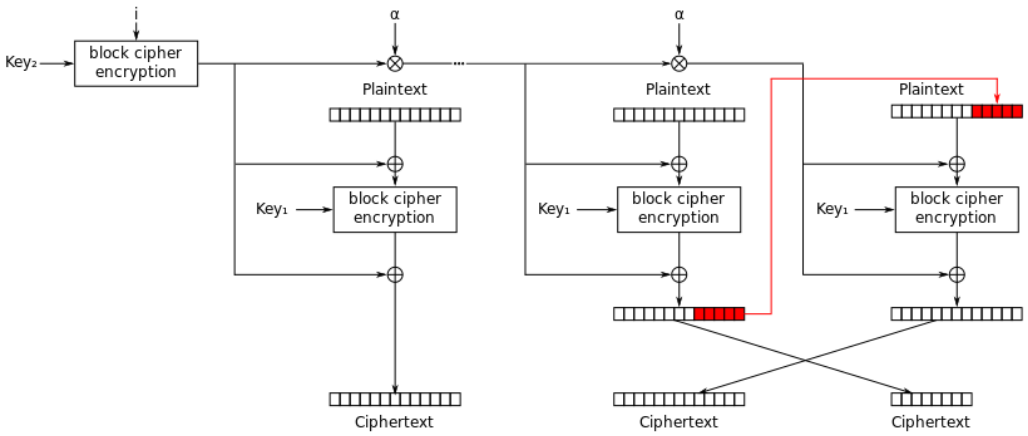

Figure 6.3: XTS-AES encryption [13]

devices using fixed length data units. Other approved cryptographic algorithms can also be used for this purpose. For this purpose, XTS-AES can be used as an alternative to AES-GCM. In the absence of authentication or access control situations, the XTS-AES algorithm provides greater protection against unauthorized manipulation of encrypted data than other approved privacy-only modes. Besides this, it is efficient in parallel encryptions in both hardware and software and random accessing to encrypted data blocks [12].

6.5.3.1 Security Vulnerabilities

- Any key-tweak pair should be unique because same pair will always give same ciphertext/plaintext when encrypted/decrypted.
- Encrypting multiple blocks with the same key reveals security vulnerabilities.
- Since the P1619 Task Group designed XTS-AES to provide encryption without data expansion, XTS-AES does not provide authentication and this causes the randomizing a sector attack.
- XTS-AES enforces the use of 128 or 256 bit key length and the data length can not exceed 2^{20} AES blocks.

CHAPTER 7

TEST VECTORS FOR VULNERABILITIES AND ATTACKS

This section describes the test vectors required to test whether a cryptographic module implementing AES-GCM contains the vulnerabilities described in Chapter 6. These vulnerabilities are reusing the initial vector, using short authentication tag, using non-default initial value length and using weak keys.

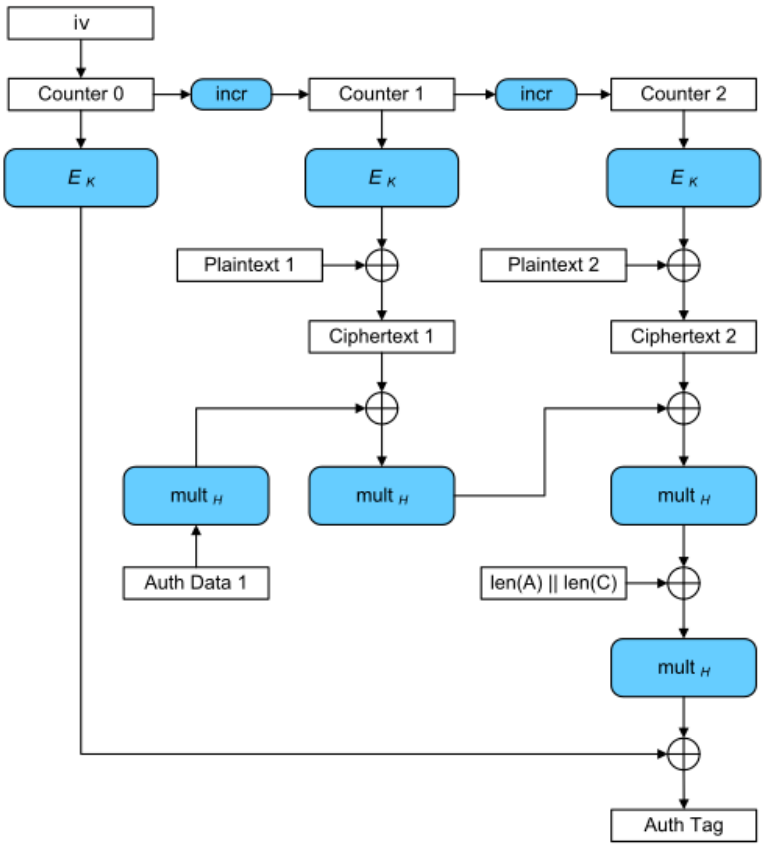

Figure 7.1: AES-GCM [11]

Reusing the IV In the case that the initialization value is used again for different messages M_1, M_2 in AES-GCM mode;

- J values will be calculated the same.
- In the original AES-GCM definition, $GHASH_{core_H}(\{\},\widehat{IV})$, while in the NIST definition, $GHASH_H(\{\},\widehat{IV})$.
- According to the AES-GCM definition used, J values are the same for different messages M_1, M_2 in both cases.
- We know that $T = GCTR_k(J, S)$. In this case, different S values and the same J values will give us different authentication tags T_1 and T_2.
- To test the same IV use case, different authentication tag values should be XORed, if the result is the same as the XOR values of the S values giving these authentication tags, it should be verified that the same IV value is used.

With an easier method, we can understand whether the IV is reused or not. Since $C = GCTR_K(inc_{32}\ (J_0), P)$, result of the $P \oplus C$ value gives the same values for different (P, C) pairs if IV is reused where P is the plaintext and C is the ciphertext. Therefore, we can verify whether the IV value is used twice or not just by looking at the value of $P \oplus C$.

Using short authentication tag In the case that the short authentication tag is used;

- The length of the authentication tag used should be measured.
- It should be noted that vulnerability may occur if verified to be less than 128 bits.

Using non-default initial value length In the case that the non-default initial value length is used;

- The length of the initial value used should be measured.
- It should be noted that vulnerability may occur if verified to be different from the default length 96 bits.

Using weak keys Weak H values are easy to find, but it is difficult to figure out how to identify the weak AES keys K that produce these weak H roots. Since authentication key H is generated as $H = AES_k(0)$ and GF(2^{128}) has a large number of lower order roots of unity, there are many weak AES-GCM keys. Juhani and Saarinen [21] found 32 128 bit weak AES keys K in their study. These keys should not be used to test weak key usage. Some of those are

$$
\begin{aligned}
n &\approx 2^{126.4} \quad K = \texttt{00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02} \\
n &\approx 2^{125.6} \quad K = \texttt{00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03} \\
&\ldots \\
n &\approx 2^{96.52} \quad K = \texttt{00 00 00 00 00 00 00 00 00 00 00 00 24 3E 8B 40} \\
n &\approx 2^{96.00} \quad K = \texttt{00 00 00 00 00 00 00 00 00 00 00 00 37 48 CF CE} \\
n &\approx 2^{93.93} \quad K = \texttt{00 00 00 00 00 00 00 00 00 00 00 00 42 87 3C C8} \\
n &\approx 2^{93.41} \quad K = \texttt{00 00 00 00 00 00 00 00 00 00 00 00 EC 69 7A A8}
\end{aligned}
$$

where n = ord($AES_K(0)$)

CHAPTER 8

CONCLUSION

The necessity of testing the functional features claimed by the product developers for the security products they produce in the IT sector in accordance with a certain standard by an organization independent of the customer or manufacturer, to document their conformity and to keep the continuity of the situation under control. In addition, it is necessary to ensure comparability between national and international assessments, and to guarantee to the customer that the requirements needed in the product are met with the safety functions claimed by the manufacturer. Due to these needs, some standards have emerged in order to evaluate and test IT products. Since cryptographic modules are classified as information technology products, the evaluations and tests to be made about them are according to these standards. Common Criteria (ISO/IEC 15408) Standard, one of these standards, has been developed to determine the security levels of information technology products and/or systems and to be tested in independent laboratories, based on TCSEC and ITSEC standards and is the basis of the International Standards Organization (ISO). It is the security standard adopted as the International Information Technologies Security Evaluation Standard in 1999. Cryptographic modules should be evaluated and tested according to this standard according to security and EAL levels. As a result of this evaluation, it is certified to be valid internationally. With this certificate, the customer or the user can verify the reliability of the functional properties of the product, make comparisons with other certified products, and guarantee that the requirements required in the product are met with the safety functions claimed by the manufacturer.

Another standard that determines the security requirements for these cryptographic

modules in information technology systems that ensure the security of critical data is the ISO/IEC 19790 standard. ISO/IEC 19790 standard includes cryptographic structures, physical structures, operating environment, documentation etc. in cryptographic modules. It contains requests on various subjects. To test the compliance of cryptographic modules with the ISO/IEC 19790 standard, the ISO/IEC 24759 standard has been prepared as a test methodology. This standard has been developed in order to prevent the ISO/IEC 19790 conformity tests from showing subjectivity from the laboratory performing the test to the laboratory. The ISO/IEC 24759 standard contains security requirements quoted from the ISO/IEC 19790 standard. There are no fundamental differences between the Federal Information Processing Standards (FIPS) 140 requirements and ISO/IEC 19790 requirements in terms of purpose and content. Participating countries for FIPS 140 are USA, Britain, Canada and Germany, and the algorithms evaluated under FIPS 140 criteria are limited to algorithms approved by NIST. Therefore, the ISO/IEC JTC1/SC27 working group has reconsidered the FIPS 140-2 criteria and published the ISO/IEC 19790 standard, which is the equivalent of these criteria. This standard also evaluates algorithms that FIPS140-2 has excluded from evaluation.

In 2014, NIST released a substantially different draft of FIPS 140-3, this version effectively directing the use of an International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standard, 19790:2012, as the replacement for FIPS 140-2. Initial publication was on March 22, 2019 and it supersedes FIPS 140-2. Validation and testing of cryptographic modules should also be performed according to this standard. It is included in the list of approved modules as a result of this validation. The customer or user can check here whether the cryptographic modules are validated or not, and still compare them between other modules.

As a result, ISO/IEC 15408 Common Criteria Standard and FIPS 140-3 standards should be taken into account when determining the requirements of cryptographic modules, validating, evaluating and testing the cryptographic modules, and the required process should be applied by accredited laboratories as specified in the thesis. These standards are described in detail and how the evaluation process in accordance with them takes place in the world and how they should be implemented are described in Turkey in the thesis. Moreover, vulnerabilities of the AES-GCM algorithm

are discussed as an example to prevent the vulnerabilities of the cryptographic algorithms used in the cryptographic algorithm verification process, which is a part of the cryptographic module verification process, and alternative AES modes are mentioned. Finally, test vectors that help us detect these vulnerabilities are explained in the thesis.

REFERENCES

[1] Implementation guidance for fips pub 140-2 and the cryptographic module validation program, 2006.

[2] Cryptographic algorithm validation program management manual, National Institute of Standards and Technology and Communications Security Establishment Canada, 2009.

[3] Cmvp – cryptographic module validation program, Encyclopedia of Cryptography and Security, 2011.

[4] *Automated Cryptographic Validation Testing: CSRC*, 2016 (last accessed September 2020), `https://csrc.nist.gov/Projects/Automated-Cryptographic-Validation-Testing`.

[5] *Automated Cryptographic Validation Protocol (ACVP) support from atsec*, 2018, November 26 (last accessed September 2020), `https://atsec-information-security.blogspot.com/2018/11/automated-cryptographic-validation.html`.

[6] *ALGORITHM TESTING AUTOMATION: THE CHANGE FROM CAVS TO ACVTS*, 2019, October 25 (last accessed September 2020), `https://www.corsec.com/algorithm-automation/`.

[7] *Common Criteria - What is common criteria*, (last accessed September 2020), `https://en.tse.org.tr/IcerikDetay?ID=770`.

[8] M. A. Abdelraheem, M. A. Abdelraheem, A. Bogdanov, and E. Tischhauser, Twisted polynomials and forgery attacks on gcm, Advances in Cryptology – EUROCRYPT 2015 Lecture Notes in Computer Science, pp. 762–786, 2015.

[9] R. Adams and D. Adams, *FIPS: Important update on algorithm testing*, 2019, November 7 (last accessed September 2020), `https://www.intertek.com/blog/2019-11-07-connected-world`.

[10] C. Conlon, *What Is ACVP?*, 2020, April 24 (last accessed September 2020), `https://www.wolfssl.com/what-is-acvp/`.

[11] M. Dworkin, Recommendation for block cipher modes of operation: Galois/-counter mode (gcm) and gmac, NIST Special Publication 800-38D, 2007.

[12] M. Dworkin, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*, 2010, January 18 (last accessed September 2020), https://csrc.nist.gov/publications/detail/sp/800-38e/final.

[13] N. Ferguson, *Authentication weaknesses in GCM*, May 2005, http://csrc.nist.gov/CryptoToolKit/modes/comments.

[14] S. Gueron, *AES-GCM-SIV*, 2018, January 27 (last accessed September 2020), https://github.com/Shay-Gueron/AES-GCM-SIV.

[15] S. Gueron, A. Langley, and Y. Lindell, Aes-gcm-siv: Nonce misuse-resistant authenticated encryption, Internet Research Task Force (IRTF) Request for Comments: 8452, 2019.

[16] S. Gueron, A. Langley, and Y. Lindell, *Webpage for the AES-GCM-SIV Mode of Operation*, (last accessed September 2020), https://cyber.biu.ac.il/aes-gcm-siv.

[17] A. Ierymenko, *Research Notes: AES-GMAC-CTR (SIV)*, 2019, September 04 (last accessed September 2020), https://www.zerotier.com/2019/09/04/aes-gmac-ctr-siv.

[18] A. Joux, Authentication failures in nist version of gcm, 2018.

[19] S. Kim, Fips 140-3 derived test requirements (dtr), 2020.

[20] S. Koteshwara, A. Das, and K. Parhi, Performance comparison of aes-gcm-siv and aes-gcm algorithms for authenticated encryption on fpga platforms, 2017 51st Asilomar Conference on Signals, Systems, and Computers, 2017.

[21] Markku-Juhani and O. Saarinen, Cycling attacks on gcm, ghash and other polynomial macs and hashess, Fast Software Encryption Lecture Notes in Computer Science, pp. 216–225, 2012.