네트워크 보안 환경에서의 현장적용 중심 암호품질 만족도 평가 메트릭스 설계 프로세스

노시춘* · 김점구**

요 약

네트워크 보안 암호화 방식은 단대단 암호화 방식과 링크간 암호화 방식으로 구분된다. 네트워크 환경에서 보안 품질 요구사항 이란 시스템이 제공해야 할 보안품질 속성의 수준이다. 품질속성은 관찰할 수 있고 측정할 수 있어야 하기 때문에 품질 요구사항도 가능하면 정확한 수치로 제시되어야 한다. 품질 요구사항이 정의되어야 구체적 품질 관리 목표가 설정된다. 품질속성에서 기능적 요구사항은 암호화를 통해 얻을 수 있는 서비스 기능에 대한 요구조건이다. 비 기능적 요구사항은 암호화를 통해 얻을 수 있는 서비스의 품질 요구조건이다. 본 연구에서 제안하는 암호화 품질 평가체계는 기능적 요구사항과 비 기능적 요구사항 2개영역으로 도출한다. 평가지표의 동일 분류내 척도를 산출한 후 각 지표의 품질 측정값에 대한 연계지표를 작성한다. 품질평가 매트릭스는 품질측정 값에 대한 연계지표 분석용 2- factor 평가로서 기능적 요구사항과 비기능적 요구사항 두 가지 기준으로 평균치를 산출 한다. 산출결과는 추세를 분석하여 종합 평가가 가능하도록 한다. 이와같은 방식을 적용할 경우 네트워크 보안 암호화 품질평가의 기반을 구성할 수 있다.

A Study of Quality Metrics Process Design Methodology for Field Application Encryption under Network Security Environment

SiChoon Noh* · Jeom goo Kim**

Abstract

The network security encryption type is divided into two, one is point-to-point, second method is link type. The level of security quality attributes are a system security quality requirements in a networked environment. Quality attributes can be observed and should be able to be measured. If the quality requirements can be presented as exact figures, quality requirements are defined specifically setting quality objectives. Functional requirements in the quality attribute is a requirement for a service function which can be obtained through the encryption. Non-functional requirements are requirements of the service quality that can be obtained through the encryption. Encryption quality evaluation system proposed in this study is to derive functional requirements and non-functional requirements 2 groups. Of the calculating measure of the evaluation index in the same category, the associated indication of the quality measure of each surface should be created. The quality matrix uses 2-factor analysis of the evaluation for the associated surface quality measurements. The quality requirements are calculated based on two different functional requirements and non-functional requirements. The results are calculated by analyzing the trend of the average value assessment. When used this way, it is possible to configure the network security encryption based on quality management.

keywords : Quality Metrics ; Design Methodology; Field Application; Encryption; Network Security

접수일 2015년 9월 3일, 수정일(1차:2015년 9월 16일), 게재확정일 2015년 9월 22일

* 남서울대학교 컴퓨터학과
** 남서울대학교 컴퓨터학과

1. 서 론

암호화 기술은 정보보안 기반기술로서 신뢰성 높은 기술이다. 암호화는 프라이버시, 인증, 무결성 및 데이터에 대한 제한적 접근을 제공하는 강력한 수단이자 서비스이다. 암호화 기술이 실무현장에서 사용되는 분야는 전자 서명, 인증, 메일 암호, 전자상거래, 전자 화폐, 전자지불 시스템, 디지털 워터마킹, 핑거프린팅, 전자 선거, 전자 입찰, 경매, 전자 계약 등 다양하다. 네트워크 보안 환경에서 적용되는 암호화 프로토콜은 IPSEC, VPN, SSL, TLS, S-HTTP, WTLS, WALS 등 이다. 이와 같은 암호화 기술들은 보안을 적용해야 하는 실무 현장에서 응용되고 있지만 암호화를 업무에 적용시켜야 할 실무자 입장에서 보면 암호화가 필요한 요구사항 정의에서부터 시작하여 어떤 기능을 어떻게 설계하고 도입해야 할지 프로세스 자체에 대한 대안이 연구되어 있지 못하는 경우가 많다. 특히 암호화 요구사항에 대한 품질 평가 자체가 현실적으로 매우 어려운 과제로 대두되고 있다. 이 과제를 해결하기 위해서는 암호화 기술과 알고리즘에 대한 이해가 필요하며 특히 그 적용 방법을 현장실무에 적합하게 연구해야한다. 유감스럽게도 암호화 분야에 대한 많은 연구는 알고리즘에 관련된 소재가 대부분을 차지하며 현장에서의 적용프로세스에 대한 연구는 거의 이루어지지 않고 있다. 이와 같은 현장의 필요성을 절감하고 본 연구를 착수하게 되었다. 따라서 본 연구의 목적은 실무를 다루는 현장에서 암호적용 프로세스와 암호 품질 평가를 어떻게 해야하는지에 대한 대안을 제시하고자 한다. 이를 위해서는 암호화 요구사항 정의와 함께 암호화 성과를 측정할 수 있는 현장 적용 중심 암호품질 만족도 평가 방법론 개발이 필요하다. 이를 위해서 본 연구는 네트워크 보안 환경에서의 기능적 요구사항과 품질 요구사항 2개영역으로 분류하는 현장 적용 중심 암호품질 만족도 평가 메트릭스 설계 방안을 제시한다. 본 연구 기술순서는 서론, 품질 모델의 체계, 네트워크 보안 암호화품질 요구사항 정의, 암호화 품질 평가프로세스 설계, 결론의 순서이다.

2. 품질모델의 체계

2.1 품질속성

암호품질이 측정되어야 하는 암호시스템은 암호화 및 복호화 과정으로 구성된다. 암호시스템에서는 키나 알고 리즘이 핵심이며 하나의 비밀 키(private key, secret key)를 암호화와 복호화에 모두 사용하는 관용 암호계(conventional crypto system)와 비밀키와 공개키를 구분하는 공개키(public key system) 시스템으로 나뉜다. 어떤 품질을 이해하려면 품질속성을 찾아야 하는데 품질속성은 이해관계자들의 관심사와 요구사항을 반영하는 지표이다. 품질 요구사항이란 시스템이 제공해야 할 품질속성의 수준이다. 암호 품질 평가에서 품질속성은 관찰할 수 있고 측정할 수 있어야 하기 때문에 품질 요구 사항도 가능하면 정확한 수치로 제시되어야 한다. 품질요구 사항이 정의되어야 구체적 품질 관리 목표가 설정된다. 암호시스템에서 암호품질 속성은 양(quantity)이나 질(quality)로 관찰하여 수치로 측정 할 시스템 특성이다. 언어적 표현으로의 만족도 수준이 정성적이며 수치로 측정되는 만족도 수준이 정량적이다[1][2].

2.2 품질모델 구조

암호품질을 확보하려면 품질모델 구조가 필요하다. 품질 모델 구조는 품질의 구성체계이자 요구사항을 만족시 키는 틀로서 ISO/IEC9000에 의하면 Quality(품질), Quality Factor(항목), Quality Subfactor(내부항목), Metric(측정기준)으로 다음과 같이 계층화된다[1][4].

- ○ Quality(품질): 시스템이 충족해야 할 품질이다.
- ○ Quality Factor(항목) : 사용자나 관리자 중심으로 시스템이 외부에 보이는 품질, Characteristics, Factors 라고도 한다.
- ○ Quality Subfactor(내부항목) : 구현자,시스템 내부의 구현자가 다루는 품질,Quality Factor를 측정할 수 있는 속성.Sub-characteristics, Criteria라고도 한다.
- ○ Metric(측정기준) :평가자 중심, 품질측정 방법과 척도이다.

<표1> ISO/IEC9000 품질모델의 체계

제 목	의 미	이해 관계자
품질(quality) 정의	목표 시스템이 충족해야 할 네트워크보안 품질	전체관련자
품질항목 (quality factor)	사용자나 관리자 중심으로서 시스템이 외부에 보이는 품질	사용자나 관리자
세부항목 (quality Subfactor)	시스템 내부의 구현자 다루는 품질이며 세부항목을 측정할 수 있는 속성으로 바꾼 것.	구현자
측정기준 (metric)	평가자 중심의 품질을 측정하는 방법과 척도	평가자

3.네트워크보안 암호화품질 요구사항 정의

3.1 품질요구사항

네트워크보안에서 암호화품질 요구사항이 정의되어야 구체적 품질관리 목표가 설정된다. 본 연구에서 제안하는 암호화 품질체계는 ISO/IEC9000의 품질 구조를 참조하여 암호화 분야에서의 기능적 요구사항과 비 기능적 요구사항 2개영역으로 분류하여 다음과 같이 제안하고자 한다[3][4].

3.2 기능적 요구사항 5개영역 설계

네트워크 환경에서 암호화는 두 개의 호스트 간, 혹은 두 개의 응용 시스템 간에 적용될 수 있으며 암호품질은 이해당사자, 즉 관계자들이 원하는 수준으로 품질 속성을 달성해야 한다. 기능적 요구사항은 암호화를 통해 얻을 수 있는 서비스 기능에 대한 요구조건이다. 네트워크 환경에서의 암호화 시스템 기능 요구사항은 필수적으로 수행되어야 할 동작과 현상이며 본 연구에서는 다음과 같은 5개영역을 도출하였다.

● 데이터 발신처 인증

발신처 인증 메커니즘에는 패스워드와 같은 단순한 신분 확인 정보를 이용하는 것에서부터 암호 기술을 이용하는 것까지 다양한 방법이 있다. 비인가된, 무자격의 사용자의 정보자원에 대한 접근으로부터 접근을 차단하므로서 정보자원을 보호한다.

● 접근 통제

인증을 통해 신원확인이 된 경우에도 사용자의 권한에 따라 접근하는 방법이다. 사용자의 접근권한을 결정하거나 사용자의 고유성, 사용자에 관한 정보 또는 사용자의 자격 등을 이용한다. 사용자가 비인가된 자원에 대하여 접근을 시도하거나 인가된 자원일지라도 불법적인 방법으로 접근 하면 접근시도를 통제한다. 사용자의 신분이 확인된 이후에는 해당 사용자가 정보 자원에 대하여 어느 수준의 접근 자격을 갖고 있는지를 결정한다.

● 비밀 보장

네트워크를 통하여 전달되는 정보가 비인가된 사용자, 주체, 그리고 여러가지의 불법적인 행위 및 처리 등 으로 인하여 그 내용이 노출되는 것을 방지한다. 비밀 보장 범위는 접속 비밀 보장, 비접속 비밀 보장, 선택 영역 비밀 보장, 트래픽 흐름 비밀보장 등이다.

● 데이터 무결성

네트워크상에서 데이터의 정확성을 점검하는 메커니즘이다. 데이터의 내용이 인가되지 않은 방식에 의하여 변경 또는 삭제되는 것을 방지하는 서비스이며 송신자와 수신자가 각각 무결성을 결정한다. 복구 기능을 갖는 접속 무결성, 복구 기능이 없는 접속 무결성, 선택 영역 접속 무결성, 비접속 무결성, 선택 영역 비접속 무결성 등이 있다.

● 부인 방지

데이터의 발신지가 발신 사실을 부인하지 못하도록, 또는 수신자가 수신 사실을 부인하지 못하도록 방지하는 서비스이다. 부인 방지는 발신 부인 방지, 수신 부인 방지. 송,수신자들이 자신이 데이터를 송, 수신한 사실을 부인하는 경우 방지한다.

<표2> 네트워크보안 5개영역 기능 메트릭스

기능요구항목	품질설명	메트릭스(%)
데이터 발신처 인증	비인가, 무자격 사용자의 정보자원 접근차단	접근차단율
접근통제서비스	신원확인 경우에도 사용자 권한에 따라 정보접근	접근통제율
비밀보장	불법적 행위로 인해 정보 노출 방지	노출 방지율
데이터무결성	인가되지 않은 방식에 의하여 데이터 내용 변경, 삭제방지	변경, 삭제방지율
부인방지	발신지의 발신 사실 부인방지, 수신자 수신 사실 부인 방지	부인방지율

3.3 비 기능적 품질 요구사항 설계

비 기능적 요구사항은 기능적 요구사항과 달리 암호화를 통해 얻을 수 있는 서비스 기능의 품질에 대한 요구조건이다.

• 처리시간 부담

CPU 연산기의 기능은 모든 데이터 처리를 담당하며 제어 신호에 의하여 동작 결정한다. 연산 수행 결과는 상태 레지스터에 저장된다. CPU의 사용용량과 프로세서 기능에 직접적인 부담 요인으로 알고리즘을 수행하는데 걸리는 시간의 양을 의미한다. 알고리즘 수행시간의 양은 연산의 횟수를 통해서 알고리즘의 빠르기를 판단하므로 시간의 양이란 결국 연산 횟수를 의미한다. 다른 각도에서는 데이터의 수 n에 대한 연산의 횟수 함수를 T(n)으로 표기한다. 이때 암·복호 작동은 거의 CPU 사이클에 의존한다. 현재 CPU 클러스터링 구조는 수십 개의 4GHz를 초과하는 Clock을 가진 CPU 장착 서버들이 대종을 이루고 있다. 4GHz로 동작하는 30개의 CPU를 가진 서버의 경우 가용한 총 CPU 사이클은 초당 120GHz이 된다.

• DB 부하

데이터베이스 암호화는 한번 구축하고 나면 되돌리기 어렵기 때문에 처음 암호화 방법론 선택이 매우 중요하다. 암·복호화 작업으로 DB기능 자체는 부하가 없지만 DB내부에 설치되는 암호화 솔루션으로 암호화하지 않은 데이터까지 모두 제어· 기록하게 되면 DB부하를 수반한다. 또한 암호화된 데이터에 대해서는 색인검색이 불가능하다. Meta Table에서부터 Full Table Scan이 발생하며 이때 암·복호화 이전에 없던 새로운 부하를 발생시킨다. 접근제어 제품은 그 대상을 접근 제어 및 감사 대상을 DB전체로 하지만 일부 hole이 존재하며 DB암호화 제품은 암호화된 칼럼만을 대상으로 하지만 hole은 발생하지 않는다.

• 키관리 안전성

암호 알고리즘의 안전성은 데이터를 암호화한 후 암호화 키와 함께 전송하기 때문에 키관리가 매우 중요하다. 고도의 암호화 알고리즘을 사용해 암호화한 데이터라 해도 암호화 키가 함께 유출되면 쉽게 복호화할 수 있기 때문이다. 평문의 각 문자 정보가 암호문 전체에 분산되는 특성을 확산(diffusion)이라 하며, 암호 해독자는 해독을 위해 더 많은 양의 암호문을 필요하게 된다. 또한 암호 해독자는 평문의 어떤 문자가 암호문에서 어떤 문자로 바뀌는지 알 수 없어야 한다.

• 현장 테스트 용이성

암호화의 현장 적용을 위해서는 테스트가 사전에 수행되어야 한다. 이때 현장 테스트가 현장에서 운용환경에서 실시되는 것이 핵심이다. 현장 테스트는 데이터에 대한 암호화 프로세스와 품질의 체크가 관건이며 테스트가 필요하다. 개발용 서버를 사용하여 실제 환경에서 테스트가 중용하며 어떤 데이터들을 암호화 하였고 색인은 어떻게 되어 있는지 까지 세밀한 검토가 필요하다. 현장 적용방식은 다음의 세가지 방법론을 중심으로 구성된다.

- API 방식은 API를 AP서버에 설치하는 방법이다. API에 연동되는 애플리케이션을 수정되어야 한다. 암.복호 부하는 AP서버에 발생하며 색인 검색이 불가능하고 주로 비밀번호 암호화 용도로 사용한다.

- Appliance 방식은 AP서버와 DB서버 사이에 설치하는Appliance 방식이며 애플리케이션을 수정해야 한다. 암.복호 부하는 Appliance에서 발생한다. 색인 검색이 불가능하고 비밀번호 암호화 용도로 사용된다.

- Plug-In 방식은 암호화 모듈 삽입방식이며 DB 서버에 설치하며 애플리케이션의 수정은 불필요하다.

암.복호 부하는 DB서버에서 발생하고 색인검색이 가능하다.

- **암호강도(strength of cipher)**

암호강도는 암호화 알고리즘을 알고 있는 암호 공격자가 키 혹은 평문을 알아내고자 했을 때의 노력의 정도를 의미한다. 암호강도가 클수록 그 암호계는 안전한 암호계가 된다. 특별한 경우를 제외하고는 비밀키가 남에게 알려지지 않도록 잘 관리되어야 한다. 알고리즘이 공개된 상태에서 키마저 알려진다면 누구든지 쉽게 평문을 알아낼 수 있기 때문이다. 한편, 암호강도의 정도를 나타내기 않기 위해 사용되는 평가지표를 강도 지표라 한다. 대표적 강도지표로 정보이론적인 지표인 암호문으로부터 평문이나 키를 유추해 내기 어려운 정도인 불확정성(equivocation)과, 이와 관련되어 평문이나 키를 유추해 내기 위해 필요한 최소한의 암호문의 길이를 나타내는 판별거리(utility distance)가 있으며, 암호공격에 소요되는 계산횟수를 의미하는 워크 팩터(work factor)등도 자주 이용된다. 워크 팩터는 키를 알지 못하는 공격자가 모든 가능한 키를 만들어 암호 알고리즘을 수행시킬 때 평문을 찾아 낼 수 있는 평균적인 횟수를 뜻한다. 워크 팩터가 클수록 그 암호 알고리즘은 보다 강력하다.

<표3> 네트워크보안 5개영역 품질 메트릭스

품질항목	품질설명	메트릭스 (%)
처리시간 부담	CPU 사용용량과 프로세서의 직접 부하율	CPU 부하
DB 부하	Meta Table에서부터 Full Table Scan 발생 시 암·복호화 부하	DB 부하
키관리 안전성	암호화 데이터라 해도 암호화 키 유출 시 복호화 위험방지	키관리 안전도
현장테스트 용이성	암호화 적용 프로세스와 품질 체크 용이성	테스트 용이성
암호강도	암호 공격자가 키 혹은 평문을 알아 내고자 노력의 정도	암호강도

4. 암호화 품질 평가 프로세스 설계

4.1 품질 측정 시나리오

품질속성 시나리오를 활용해서 시스템이 달성해야 할 품질 목표를 결정한 품질 요구사항을 정의한다. 이 품질 요구사항을 달성할 수 있는 방안을 선택해야 한다. 이 방안은 미리 정해져 있을 수도 있고 상황에 맞춰 직접 개발할 필요도 있다. 어떤 경우에 어떤 품질속성 달성 방안이 필요하고 이 방안을 어떤 구성요소들이 만족하는지 정해놓은 품질속성 시나리오를 준비해야한다

- 영향 분석 : 암호화로 인한 기존 애플리케이션의 운영에 어떤 영향이 있을 것인지를 사전에 면밀히 분석한다. 방법으로는 모니터링하고 분석해 본 후 영향을 줄 수 있는 문제를 찾아낸다.
- 환경 체크 : 작업에 필요한 여분의 임시(temporary disk) 공간은 있는지, 기타 DB의 환경변수들은 적절한지, 필요한 패키지나 패치 레벨 등이 적절히 설치되어 있는지 등을 체크한다.
- 완료 후 테스트 : 작업이 완료되고 나면 필요에 따라 암호화한 데이터가 정확히 변환 되었는지 정합성 체크를 실시한다. 애플리케이션을 수행하여 문제가 있지는 않은지 성능저하는 어느 정도인지 확인한다.
- 대책 수립 : 문제 쿼리가 만일 배치작업의 쿼리이고 Tuning 차원의 수정이 가능한 상태라면 쿼리 문장의 Optimizing을 실시한다.

4.2 품질측정 메트릭스(metric) 설계

네트워크 환경에서 개발자와 사용자 모두가 성능측정 결과를 이용할 수 있도록 하는 객관화된 형태의 기준과 방법체계를 개발한다. 개발내용은 기능적 요구 사항과 비 기능적 요구사항을 2개영역으로 분류하여 도출한다. 품질 항목은 요구사항의 비 기능적 요구사항 중에서 평가 방법론을 토대로 5개항목을 도출한다. 이 두 기능을 종합적으로 상호 연계되는 성능측정방법론 개발이다. 본 연구의 제안 방법론을 사용하여 체계적인 측정환경을 설계할 경우 운용시스템 상에서 암호 알고리즘 QoS의 만족도 산출이 가능하다. 본 연구에서는 특정한 하나의 장비나 소프트웨어의 성능이 아닌 네트워크 환경 아키텍처 전반에서 얻을 수 있는 대표적인 성능지표를 도출한다.

4.3 품질평가 방안

네트워크 환경에서 품질평가는 구현하고자하는 기능을 통해 요구성능이 충족되도록 방법론 및 분석도구를 통하여 구체적인 내용으로 분석되고 구현 및 테스트 방안이 구체적으로 기술되어야 한다. 품질 모델은 품질 속성을 분류하고 정의하여 누구나 인정할 수 있는 품질모델 도입 시 품질 정식화(formalization)가 가능하다. 측정 체크 리스트는 품질 파라메터별 측정 기준을 점검방법에 따라 점검한다.

4.4 품질 측정값에 대한 연계지표 분석

네트워크 환경에서 평가지표의 동일 분류내 척도를 산출한 후 각 지표의 품질 측정값에 대한 연계지표 별로 작성한다. 파라메타는 기능적 요구사항 평가 항목과 비 기능적 요구사항 평가 항목으로 구분하여 구성한다. 본 연구에서 품질측정값에 대한 연계지표 영역별 품질평가 매트릭스 모델과 파라메타의 항목을 제시하고 상세 체크리스트 작성은 생략한다. 품질평가 매트릭스 방법론 에서는 2- factor 평가방법을 제시한다. 품질측정 값에 대한 연계지표 분석용 2-factor 평가는 기능적 요구 사항 평가와 비기능적 품질평가 사항 두가지 기준으로 평균치와 합계치를 산출하고 그 추이를 분석하여 종합 평가가 가능하도록 <표4>와 같이 예시만을 제시한다. 2-factor 추이 분석 매트릭스를 활용하며 평균값과 합계 값을 추이 분석할 수 있다. <표4> 품질만족도 매트릭스 설계는 품질만족도에 대한 평가결과 프레임이며 <표5>는 기능적 만족도와 비기능적 만족도의 2- factor 품질만족도 평가 매트릭스를 연계하여 예시한 것이다. 현장에서는 이 연구에서 제시된 매트릭스 예시를 활용하여 자체 운용 실정에 적합한 세부 모델을 개발하여 적용하여야 한다.

<표4> 네트워크보안 품질만족도 평가 매트릭스(예시)

품질항목	세부 항목수 (예시)	메트릭스	점수 (예시)	가중 점수 (예시)	최종 점수 (예시)
처리시간 부담	3	%	1-100	0.1-0.9	
DB부하	3	%	1-100	0.1-0.9	
키관리안전성	5	%	1-100	0.1-0.9	
현장테스트용이성	4	%	1-100	0.1-0.9	
암호강도	3	%	1-100	0.1-0.9	

<표5> 2- factor 품질만족도 평가 매트릭스(예시)

구분		품질요구사항				
		처리시간 부담	DB 부하	키관리 안전성	현장테스트 용이성	암호 강도
기능적 요구사항	데이터 발신처 인증	YYY	Y	Y	YY	Y
	접근 통제	Y	Y	YYY	Y	Y
	비밀 보장	YY	Y	Y	Y	YY
	데이터 무결성	Y	YY	Y	YY	Y
	부인 방지	YY	YY	Y	Y	YYY

* 보기(예시) : Y -> 만족도미흡, YY->만족도보통, YYY-> 만족도우수

5. 결 론

좋은 암호는 어떤 조건을 만족시켜야 하는가에 대한 의문은 오랫동안 제기되고 있다. 본 연구에서 제안하는 암호화 품질 평가체계 설계 방법은 기능적 요구사항과 비 기능적 요구사항인 품질을 만족시켜야 할 목표를 정립하여 관리하는 방법이다. 네트워크 보안 환경에서는 환경의 변화가 편리함과 생산성을 향상 시키지만 동시에 이해 관계자의 암호화 요구 사항을 만족시킬 수 있는 효과적인 암호화체계를 도입해야 한다. 이같은 필요를 충족시키기 위해 현재 다양한 방법으로 암호화 방법이 개발되고 있고 다양한 암호화 애플리케이션이 등장한다. 암호화 품질평가는 구현하고자하는 기능을 통해 요구 성능이 충족되도록 방법론 및 분석도구를 통하여 구체적인 내용으로 분석되고 구현 및 테스트 방안이 구체적으로 기술되어

야 한다. 암호화 품질 모델은 품질 속성을 분류하고 정의하여 누구나 인정할 수 있는 품질모델 도입 시 품질 정식화(forma lization)가 가능하다. 그러나 실무 현장에서는 이같은 암호화 애플리케이션들이 갖춰 야 할 기본적 조건을 만족하고 있는지 별도 관점에서 고찰하지 않으면 안된다. 암호화품질 측정은 암호화 품질목표와 비교하여 달성도를 분석하는 과정이 추가로 발굴되어야 하며. 암호화 품질 만족도 미진분야는 발췌하여 원인분석 및 개선작업에 활용하는 방법론이 개발되어야 한다.

참고문헌

[1] 김점구,노시춘, ISO/IEC9000모델을 참조한 웹 애플리케이션 보안품질 관리체계 설계, 한국융합보안학회논문지, 2012.6

[2] 노시춘, 나상엽, 품질 연계지표 평가방법을 사용한 암호화모듈 현장 적용체계 연구, 한국융합보안학회논문지, 2014.6

[3] 김점구,노시춘, 공격코드 사례분석을 기반으로 한 SQL Injection에 대한 단계적 대응모델 연구, 한국융합보안학회논문지, 2012.6

[4] 노시춘, 품질기반 웹 애플리케이션 개발을 위한소프트웨어아키텍쳐 설계절차 예제 정립, 한국융합보안학회논문지, 2012.9

[5] SiChoon Noh, "A Study of Security QoS(Quality of Service) Measurement Methodology for Network Security Efficiency", Journal of Korea Convergence Security Association, Vol. 10,No3, PP40-41, 2011.1

[6] Konschak CB, Jarrell LP, Consumer-Centric Healthcare : Opportunities and Challenges for Providers, pp.260, Health Administration Press, 2010.

[7] SANDEEP K. S. GUPTA Department of Computer Science and Engineering(Affiliated with BMI, BME, EE)School of Computing and Informatics Ira A. Fulton School of Engineering Arizona State University Tempe, Arizonasandeep.gupta@asu.edu,Safe and Dependable Bio-Sensor Networking for Pervasive Healthcare,2004

[8] McGraw-Hill, BOOK: Fundamentals of Mobile and Pervasive Computing, Publisher,Dec. 2004

[저 자 소 개]

노 시 춘(SiChoon Noh)

1987년 2월 :고려대학교경영정보학석사
2005년 2월: 경기대학교
정보보호기술 박사
1999년 9월: KT 시스템보안부장
2004년 3월: KT 충청전산국장
2005년3월~2015년2월 : 남서울대학교
컴퓨터학과 교수
2015년2월~현 재 : 남서울대학교
컴퓨터학과 외래교수
IT융합연구소 연구위원

email : nsc321@nsu.ac.kr

김 점 구(Jeom goo Kim)

1990년 2월 광운대학교
전자계산학과 이학사
1997년 8월 광운대학교
전자계산학과 석사
2000년 8월 한남대학교
컴퓨터공학 박사
1999년 3월~ 현재 남서울대학교
컴퓨터학과 교수
IT융합연구소장

email : jgoo@nsu.ac.kr