논문 14-39C-04-02
The Journal of Korea Information and Communications Society '14-04 Vol.39C No.04
http://dx.doi.org/10.7840/kics.2014.39C.4.326

# 온라인 서비스를 위한 보안성 평가 지표 모델

추 연 수◆, 박 재 표°, 전 문 석*

# Security Assessment Metrics Model for Online Services

Yeun-Su Choo◆, Jae-Pyo Park°, Moon-Seog Jun*

요 약

인터넷을 이용한 서비스는 보안 문제를 가지고 있다. 이에 따른 적절한 보안 대책을 위해서 보안 등급을 설정하는 것은 반드시 필요하다. 지금까지는 CIA(Confidentiality, Integrity, Availability) 보안 등급을 이용하여 보안 등급을 설정하였다. 하지만 CIA 보안 등급은 중간 강도의 보안 설정에 대한 보안 대책이 모호하다는 문제점이 있으며, 서비스에 따라 별도의 사용자 인증을 하지 않으면 보안 등급의 중복 현상이 나타난다. 또한 CIA 보안 등급 중 실제 서비스에 사용할 수 없는 등급들이 존재한다. 따라서 본 논문에서는 모호한 대책을 야기시키는 중간 강도의 보안 강도를 삭제하고 인증을 보안 등급 설정의 요소로 추가하여 CIAA 보안 등급 모델을 제안한다. CIAA 보안 등급 모델이 CIA 보안 등급보다 더 구체적인 보안 대책 설정이 가능하다. 제안하는 보안 등급 모델은 거의 모든 온라인 서비스에 적용가능하며 추후에 새롭게 제공되는 온라인서비스에도 적용 가능한 보안 등급 모델이다.

**Key Words :** Information Security, Security Levels, CIAA(Confidentiality, Integrity, Availability, Authentication)

ABSTRACT

Internet Services have security issues. To prepare proper security measures for these security issues, security level setting is positively necessary. Until now, we use a security level with CIA (Confidentiality, Integrity, and Availability) Security Levels. However, CIA Security Levels has problems with ambiguous measures for the middle level of security setting. Moreover, security level overlap occurs, in some cases, when user authentications are not done. Additionally, there exist some levels among CIA Security Levels which cannot be applied to Internet services. In this paper, new security level model, CIAA Security Levels with deletion of ambiguous middle level of security setting and addition of authentication to one of security level setting factors, is proposed. The CIAA Security Levels model can be applied to more concrete security measures than CIA Security Levels. The proposed Security Levels model is applicable to almost any on-line services and it can be applied to new online services.

## Ⅰ. 서 론

인터넷의 보급이 보편화되면서 인터넷을 이용한 많은 서비스들이 발생하고 있다. 또한 스마트 폰의 보급으로 모바일 네트워크가 빠른 속도로 발전하면서 휴대폰을 이용한 모바일 서비스가 각광 받고 있다. 이렇게 온라인을 통해 제공되는 서비스가 다양해짐에 따라 개인 정보와 기업 및 국가에서 조심스럽게 다루어야하는 '기밀 정보 유출'이라는 문제도 함께 대두되고

◆ First Author : Department of computer Graduate School Soongsil University, lets-priase@hanmail.net, 학생회원
° Corresponding Author : Graduate School of Information Sciences Soongsil University, pjerry@ssu.ac.kr, 정회원
* Department of computer Graduate School Soongsil University, mjun@ssu.ac.kr, 종신회원
논문번호 : KICS2013-12-550, Received December 26, 2013; Revised March 7, 2014; Accepted April 11, 2014

있다. 이러한 문제를 해결하기 위한 다양한 연구[1-8]가 진행되었고 여러 가지 보안 요소들을 통해 보안 등급[9,10]을 설정하고 보안 등급에 따른 보안 대책을 수립하여 개인정보 및 기업, 국가의 기밀 정보들을 보호하려는 노력이 이루어지고 있다. 보안 등급을 설정하는 보안 요소는 일반적으로 CIA(Confidentiality, Integrity, Availability)보안 요소[10]를 사용한다. 제공되는 서비스는 CIA 보안 요소를 보장하기 위해 보안 등급을 설정하고 보안 장비 등의 솔루션을 사용하고 있다. 하지만, CIA 보안 요소를 고려하여 보안 등급을 설정할 때 다양하게 제공되는 서비스들의 기능을 모두 적용할 수 없게 되며, 다른 케이스의 보안 등급이 설정되어야 함에도 동일한 보안 등급이 설정(보안 등급 중복)되어 악의적인 목적을 가진 공격자에게 취약점을 노출하게 된다. 또한 서비스를 이용하는 사용자들의 보안 레벨을 고려하지 못하는 경우가 발생한다. 같은 기능의 서비스라도 서비스를 이용하는 사용자의 보안 레벨에 따라 제공되는 데이터가 달라져야 하는데 CIA 보안 요소를 이용한 보안 등급 설정은 같은 등급을 설정할 가능성이 많다. 따라서 본 논문에서는 CIA 보안 요소를 이용한 등급 설정에서의 문제점을 수정하고, 사용자 인증 요소를 추가하여 새로운 CIAA(Confidentiality, Integrity, Availability, Authentication) 보안 등급 모델을 제안한다. 제안하는 CIAA 보안 레벨 모델은 CIA 보안 요소 기준을 이용했을 때 중복되게 설정되었던 서비스 기능을 좀 더 세분화할 수 있도록 인증요소(Authentication)를 추가하였으며, CIA에서 적용될 수 없었던 보안 레벨, 기밀성은 높지만(High) 무결성은 낮은(Low) 레벨과 같은 보안 레벨들을 제거하여 더 간단하지만 강력한 보안 레벨을 제안한다. 본 논문의 2장은 보안 등급에 대한 관련연구와 CIA 보안 레벨에 대한 문제점을 제시하며, 3장은 제안하는 CIAA 보안 레벨을 기술하며, 4장은 비교분석, 5장은 결론으로 구성되어 있다.

## Ⅱ. 관련연구

온라인 서비스의 보안은 크게 2가지로 구분될 수 있다. 안전하지 않은 네트워크에 대한 대책과 온라인 서비스를 이용하는 사용자의 신원 확인과 이 과정에서 사용되는 개인정보를 보호하기 위한 대책이 그것이다. 안전하지 않은 네트워크에 대한 대책은 기밀성, 무결성, 가용성을 보장하기 위한 대책들이며, 개인정보보호를 위한 대책은 X.1254와 같은 세계 표준과 국내에서는 금융감독원에서 제공하는 보안 등급 등이 있다.

### 2.1 X.1254

다양한 온라인 서비스 제공으로 인해 본인 확인을 위한 사용자 인증의 문제가 대두되고 있다. 개체인증 보증을 관리하기 위한 프레임 워크를 제공하기 위해 ITU-T에서는 X.1254로 명명하여 국제 표준화를 진행중이며, ISO/IEC 29115에서 표준으로 비준 받았다. 개체 인증 프레임워크는 개체가 인증되는 과정을 3단계로 정의하고 있으며, 신뢰 수준에 따라 총 4단계의 보증 레벨을 제시하고 있다. 보증 레벨에 따라 어떤 용도로 사용 가능한지 기술하고 있다. 또한 보증 레벨을 부여하기 위해 신원확인 방법을 기술하여 해당하는 보증 레벨의 신원확인이 이루어질 수 있도록 하였다. 이렇게 획득한 신원 인증 수단의 인증서는 보안 등급에 따라 인증 방식을 달리하고 있으며, 표 1은 인증서의 보증 레벨과 인증 방식, 저장 방식, 대표적 사용 웹 사이트를 소개하고 있다.[9]

표 1. 보안 레벨별 인증 방식
Table 1. Authentication Method of Security Levels

| Level | Authentication method | Representative element of authentication | Authentication storage | Representative sites |
|---|---|---|---|---|
| 1 | Protection of authentication information by using hardware Token | Same as level 3 | TRM H/W | Banking sites |
| 2 | Level 3 requirements + Multiple authentication methods +Confidential information sharing through secured tunnel | · ID/PW + OTP + SSL/TLS<br>· ID/PW + OTP + Certificate + SSL/TLS | Computer or special H/W (USB) | Patent sites |
| 3 | Single sign-on mechanism + Proof of protecting | ID/PW + SSL/TLS | Protection provisions of saved | Insurance sites which allow the changes of received |

| | | | | |
|---|---|---|---|---|
| | authentication information + Usage of safe authentication protocol + Protection provisions of wiretapping and online attacks | | authentication information | address |
| 4 | Not required | ID/PW or MAC address | | Merchandise sites with new product information |

### 2.2 CIA 보안 등급 개요

온라인에서 제공되는 많은 서비스들은 보안 요소를 고려하여 반드시 보안 대책을 강구하여야 한다. 이 때 고려되는 일반적인 보안 요소는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)이다.[10] 3가지 보안 고려 요소를 이용하여 만든 보안 등급을 CIA 보안 등급이라 한다. 하지만 CIA 보안 등급은 실제 서비스에 적용할 수 없는 등급을 가지고 있고, 보안 등급의 중복이라는 단점을 내재하고 있다. 본 절에서는 CIA 보안 요소를 이용한 보안 등급의 단점에 대해 기술한다.

#### 2.2.1 실제 서비스에 사용할 수 없는 경우

모든 서비스는 CIA 보안 등급을 이용하여 서비스의 보안 등급을 결정한다. 표 2는 CIA 보안 등급을 나타낸 것이며, 이 등급들 중에서 실제 서비스에 사용될 수 없는 등급들의 예를 보여주고 있다. 보안 요소들 중 기밀성과 무결성은 상호 의존성이 깊은 보안 요소이다. 따라서 한 요소가 특정 등급으로 설정될 때 다른 한 요소는 설정할 수 없는 등급이 발생하게 된다. 9등급의 경우, 기밀성은 'H', 무결성과 가용성은 'L'로 설정되어 있지만, 실제 서비스에서 적용할 수 없는 보안 등급이다. 기밀성이 높은 데이터는 반드시 무결성도 유지되어야 한다. 그렇지 않으면 데이터로서 사용가치가 없다. 이와 같이 사용할 수 없는 등급이 CIA 보안 등급에 상당히 많이 존재한다.

#### 2.2.2 보안 등급의 중복

CIA 보안 등급은 다른 보안 등급으로 설정되어야 하는 서비스들을 같은 보안 등급으로 설정해 버리는

표 2. CIA 보안 등급
Table 2. CIA Security Levels

| Grade | Confidentiality | | | Integrity | | | Availability | | | Remark |
|---|---|---|---|---|---|---|---|---|---|---|
| | H | M | L | H | M | L | H | M | L | |
| 1 | * | | | * | | | * | | | |
| 2 | * | | | * | | | | * | | |
| 3 | * | | | * | | | | | * | |
| 4 | * | | | | * | | * | | | Service-available models do not exist (With high confidentiality being guaranteed, integrity needs to be guaranteed) |
| 5 | * | | | | * | | | * | | |
| 6 | * | | | | * | | | | * | |
| 7 | * | | | | | * | * | | | |
| 8 | * | | | | | * | | * | | |
| 9 | * | | | | | * | | | * | |
| 10 | | * | | * | | | * | | | |
| | | | | | . . . | | | | | |
| 18 | | * | | | | * | | | * | |
| 19 | | | * | * | | | * | | | Service-available models do not exist (With high confidentiality being guaranteed, integrity needs to be guaranteed) |
| 20 | | | * | * | | | | * | | |
| 21 | | | * | * | | | | | * | |
| 22 | | | * | | * | | * | | | |
| 23 | | | * | | * | | | * | | |
| 24 | | | * | | * | | | | * | |
| | | | | | . . . | | | | | |
| 27 | | | * | | | * | | | * | |

'보안 등급의 중복'이 발생한다. 사용자의 정보 취급 레벨에 따라 다른 보안 설정이 필요함에도 같은 보안 등급이 설정되는 경우가 발생한다. 예를 들면, 인터넷 뱅킹의 조회 서비스와 이체 서비스는 다른 서비스이며, 다른 등급의 보안 설정이 필요하다. 실제로 계좌 조회 서비스는 공인인증서를 이용하여 서비스를 제공하지만, 이체 서비스는 공인인증서와 함께 보안 토큰 또는 보안 카드, OTP(One Time Password)를 이용하여 서비스하고 있다. 하지만, CIA 보안 등급을 이용하면 표 3과 같이 같은 수준의 보안 등급이 설정된다. 만약 신규 서비스를 제공할 때 이와 같이 보안 등급을 설정하게 된다면 추후에 사용자 인증에 대한 보안 프로세스를 다시 고려해야만 한다.

또한 보안 요소 기밀성은 서비스를 제공받지 않는 사람에게 데이터를 노출시키지 않아야 하기도 하지만 서비스를 제공받는 사람들에게도 사용자의 레벨에 따라서 선별 제공되어야 한다. 따라서 본인 확인 여부가 반드시 동반되어야만 한다. 하지만 CIA 보안 등급은 이러한 고려사항들을 충분히 만족시킬 수 없다. 이러

표 3. CIA 보안 등급의 중복 설정의 예
Table 3. Example of overlap setting of CIA Security Levels

| Level | Confidentiality | | Integrity | | Availability | | Example of Service | Remark |
|---|---|---|---|---|---|---|---|---|
| | H | L | H | L | H | L | | |
| 1 | * | | * | | * | | Inquiry Service | Overlap |
| 1 | * | | * | | * | | Transfer Service | |

한 단점들을 보완하여 3장에서는 CIAA 보안 등급 모델을 제시한다.

## Ⅲ. CIAA 보안요소를 작용한 보안 모델

### 3.1 제안하는 보안 모델을 위한 고려 요소

2장에서 나타난 CIA 보안 등급의 문제점을 해결하기 위해 기존의 CIA 보안 등급에 인증(Authentication)을 추가한 CIAA 보안 등급 모델을 제안한다.

#### 3.1.1 기밀성(Confidentiality)

기밀성은 서비스가 제공될 때 서비스를 위한 정보가 임의로 공개되지 않아야 함을 의미하며, 서비스에서 사용되는 정보의 중요도에 따라 매우 민감한 정보와 그렇지 않은 정보로 분류하였다.

표 4. 기밀성의 정의
Table 4. Definition of confidentiality

| Security Factor | Degree of Level | Consideration |
|---|---|---|
| Confidentiality | H | Unable to release randomly because of high sensitive information |
| | L | Irrelevant with information being randomly released |

#### 3.1.2 무결성 (Confidentiality)

무결성은 서비스를 제공하기 시작할 때의 정보가 서비스를 받을 때 변조 및 삭제되지 않고 서비스 받을 수 있어야 함을 의미하며, 서비스를 위해 사용되는 정보가 변조 및 삭제되었을 때 심각한 문제가 발생하는 민감한 정보와 그렇지 않은 정보로 분류하였다.

표 5. 무결성의 정의
Table 5. Definition of integrity

| Security Factor | Degree of Level | Consideration |
|---|---|---|
| Integrity | H | Not falsify randomly due to high sensitive information |
| | L | Information which has no problem being falsified |

#### 3.1.3 가용성 (Availability)

가용성은 제공되는 서비스가 사용자가 원할 때 서비스되어야 함을 의미하며, 사용자가 원할 때 서비스가 반드시 가능해야하는 민감한 정보와 서비스되지 않아도 큰 문제가 되지 않는 정보로 분류하였다.

표 6. 가용성의 정의
Table 6. Definition of availability

| Security Factor | Degree of Level | Consideration |
|---|---|---|
| Availability | H | Always be available due to high sensitive information. |
| | L | Information which has no problem being not in service |

#### 3.1.4 인증 (Authentication)

인증은 제공되는 서비스가 민감한 정보를 가지고 있어 허가된 사용자들에게만 제공되거나 사용자를 그룹화하여 그룹별 맞춤 서비스가 가능하도록 하기 위한 보안 고려사항이다.

표 7. 인증 요소의 정의
Table 7. Definition of Authentication

| Security Factor | Degree of Level | Consideration |
|---|---|---|
| Authentication | H | High level of service users' standard to verify are required |
| | M | Low level of service users' standard to verify are required |
| | L | No need to verify users |

보안 레벨에 대한 분류는 높은 수준의 사용자 확인이 필요한 경우, 낮은 수준의 사용자 확인이 필요한 경우, 별도의 사용자 확인이 필요하지 않은 경우, 3단계로 분류하였다. 제시한 보안 요소 중 앞의 3가지는 신규 서비스 및 보안성 검토를 위해 많이 사용되는 보안 요소들이며, 마지막 요소인 "인증"은 논문에서 제시한 CIAA 보안 등급 모델에서 추가된 요소이다. 하

지만 생소한 요소는 아니며, 대체로 기밀성과 혼용해서 사용하는 경우가 많다. 하지만 본 논문에서는 분리하여 별도의 보안 점검 요소로 제시한다. 본 논문에서의 기밀성은 서비스의 내용이 네트워크를 통해 외부에 유출되지 않는 것을 의미한다. 서비스의 내용에 따라서 기밀성을 적용하는 것은 암호화 여부를 결정하게 되며, 인증은 서비스를 허가 받은 사람에게 제공하느냐를 고려하게 된다. CIAA 보안 등급 모델은 CIA 보안 등급에서 사용한 'M'등급을 인증 요소에만 적용하여, 보안 모델을 단순화하였다.

### 3.2 제안하는 CIAA 보안 등급 모델

위에서 제시한 보안 요소들을 이용하여 신규 서비스 및 기존 서비스의 보안성 검토 시 서비스별 보안 등급을 분류하면 표 8과 같다. 보안등급은 서비스에 대하여 각 보안 요소별 경우의 수를 나열한 것이다. 약 700여개의 웹사이트와 모바일 웹, 모바일 앱 등을 CIA 등급으로 분류하는 과정에서 CIA 보안 등급이 부여되지 않는 등급이 있다는 것을 발견하였다. CIA 보안 등급 중 실제 서비스에 적용될 수 없는 등급은 제외하여, 제안하는 CIAA 모델은 A등급부터 J등급까지 10등급으로 구성되며 모든 서비스는 이 10등급 중 하나가 적용될 수 있다. 신규 서비스를 개발하거나 보안성 검토를 의뢰하였을 경우 서비스의 유형과 사용되는 데이터의 중요도 및 사용자 등급에 따라 서비스 및 시스템의 보안 담당자는 등급별 보안 대책을 적용할 수 있다. 등급별 보안 대책은 서비스 제공자마다 다르게 적용할 수 있으며, 선택사항이므로 구체적인 대책은 제시하지 않는다.

각 보안등급의 특성과 적용될 수 있는 서비스 영역에 대한 자세한 설명은 다음과 같다.

* A 등급 : 모든 보안 요소가 높게 설정된 경우로서, 가족 관계 증명서와 같은 각종 증명서와 같은 개인정보를 포함한 행정 문서들을 열람, 발급하는 서비스, 금융기관의 서비스들이 이 등급에 속함
* B 등급 : A등급과 인증 요소만 'M'으로 설정된 등급으로 본인 계좌 조회 등과 같은 서비스가 이 등급에 속함
* C 등급 : A등급과 가용성만 다른 보안 요소를 가지고 있는 등급으로 온라인 증명서 발급 서비스가 이에 속함
* D 등급 : C등급과 인증만 다른 보안 요소를 가지고 있는 등급으로 개인 상담 서비스가 이에 속함
* E 등급 : 기밀성과 인증이 'L'로 설정되고 다른 요소는 'H'로 설정된 등급으로 온라인 행정 서비스의 사용법 등이 이에 속함
* F 등급 : E등급과 가용성만 다른 보안 요소를 가지고 있는 등급으로 민감한 정보가 아닌 정보조회 서비스가 이에 속함
* G 등급 : E등급과 무결성만 다른 보안 요소를 가지고 있는 등급으로 각종 행사 소개 서비스가 이에 속함
* H 등급 : 모든 요소가 'L'등급으로 누구든 사용 가능한 자유게시판 등이 이에 속함
* I 등급 : 기밀성은 'L', 무결성, 가용성은 'H'이며 인증은 'M'인 등급으로 주민신고, 온라인 민원 서비스 등이 이에 속함
* J 등급 : I등급과 가용성만 다른 보안 요소를 가지고 있는 등급으로 의견 제안 및 일반적인 메일링 서비스가 이에 속함.

표 8. 제안하는 CIAA 보안등급
table 8. Suggested CIAA Security Levels

| Level | Confidentiality | | Integrity | | Availability | | Authentication | | |
|---|---|---|---|---|---|---|---|---|---|
| | H | L | H | L | H | L | H | M | L |
| A | * | | * | | * | | * | | |
| B | * | | * | | * | | | * | |
| C | * | | * | | | * | * | | |
| D | * | | * | | | * | | * | |
| E | | * | * | | * | | | | * |
| F | | * | * | | | * | | | * |
| G | | * | | * | * | | | | * |
| H | | * | | * | | * | | | * |
| I | | * | * | | * | | | * | |
| J | | * | * | | | * | | * | |

## Ⅳ. 사례 적용 및 검증

3장에서 제시한 보안 모델은 현재 제공되는 모든 서비스 및 신규로 제공하고자 하는 서비스에 적용 가능하다. 제안한 CIAA 모델과 CIA 보안 등급을 증권 HTS(Home Trading System) Software와 온라인 자격 시험 서비스에 적용하여 보안 등급을 결정하는 절차에 대해서 비교한다.

### 4.1 증권 HTS S/W에 적용한 보안 등급 분석 비교

증권 HTS는 주식을 집에서 사고 팔 수 있는 PC 버전의 소프트웨어로 금융계좌와 직접 연결되므로 민감한 정보가 사용되는 온라인 서비스이다. HTS 소프트웨어는 강력한 보안이 필수적이며, 인증서를 보유한 본인 외에는 접근을 철저히 제한해야 한다. HTS는 다

양한 기능을 제공하지만 본 논문에서는 단순 시세 조회, 자신의 보유한 종목 조회, 주식 거래로 3가지로 보안 등급 설정 범위를 제한한다. 먼저 CIA 보안 등급을 적용하여 보안 등급을 설정하면 표 9와 같다. 보유 종목 조회와 주식 거래 서비스는 기밀성, 무결성, 가용성이 모두 높은 1등급으로 설정된다.

표 9. CIA 보안 등급을 이용한 HTS 보안 등급 설정
Table 9. HTS security level setting by using CIA Security Levels

| Level | Confidentiality | | | Integrity | | | Availability | | | Example of Service | Remark |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | H | M | L | H | M | L | H | M | L | | |
| 10 | | * | | * | | | * | | | Simple Stock quotations Inquiry | |
| 1 | * | | | * | | | * | | | Possessed Items Inquiry | Overlap |
| 1 | * | | | * | | | * | | | Stock Trading | |

하지만 보유 종목 조회 서비스와 주식 거래 서비스는 반드시 보안 등급의 차이가 필요하다. 금융 서비스는 반드시 최고 등급의 보안 설정이 필요하지만, 보유 종목에 대한 단순 조회 서비스는 중간 수준의 인증이면 충분하다.

표 10. CIAA 보안 등급을 이용한 HTS 보안 등급 설정
Table 10. HTS security level setting by using CIAA Security Levels

| Level | Confidentiality | | Integrity | | Availability | | Authentication | | | Example of Service |
|---|---|---|---|---|---|---|---|---|---|---|
| | H | L | H | L | H | L | H | M | L | |
| E | | * | * | | * | | | | * | Simple Stock quotations Inquiry |
| B | * | | * | | * | | | * | | Possessed Items Inquiry |
| A | * | | * | | * | | * | | | Stock Trading |

HTS 소프트웨어를 제안하는 CIAA 보안 요소 모델에 적용하면 표 10과 같다. 제안하는 CIAA 보안 모델을 HTS 소프트웨어에 적용하면 HTS가 제공하는 3가지 서비스는 모두 무결성과 가용성은 제공되어야 한다. 단순 시세 조회 서비스일 경우 HTS 소프트웨어를 이용하는 모든 사람들에게 제공될 수 있는 정보이므로 기밀성과 인증은 고려하지 않아도 된다. 하지만 보유 종목에 대한 조회 서비스의 경우 기밀성은 보장되어야 하며, 본인을 위한 인증은 중간 정도의 인증 수준을 제공하면 된다. 종목 거래를 위한 서비스의 경우 기밀성, 무결성, 가용성이 반드시 보장 되어야 하며, 본인만 금융 거래를 할 수 있도록 해야하기 때문에 강력한 인증 수준이 필요하다. 따라서 단순 시세 조회 서비스는 E등급, 보유 종목 조회 서비스는 B등급, 종목 거래 서비스는 A등급의 보안 등급으로 보안 등급이 결정된다.

위와 같이 HTS 소프트웨어를 단순화하여 3가지 서비스만을 적용하였지만, HTS에서 제공되는 모든 서비스를 CIA 보안 등급을 적용한다면 반드시 추후에 추가적으로 인증에 대한 보안 요소를 서비스별, 사용자별로 고려하여 보안 등급 설정을 재설정하여야 한다. 하지만 CIAA 보안 요소 모델을 적용하면 추가적인 작업을 줄일 수 있다.

### 4.2 온라인 자격시험 서비스(신규 서비스)에 적용한 보안 등급 분석 비교

온라인 자격시험 서비스는 오프라인에서 실시하던 자격시험을 온라인 형태로 변형한 것으로 수험자에 대 한 정확한 신분 확인과 시험 정보에 대한 데이터가 노출되지 말아야하는 서비스이다. 온라인 자격시험 서비스 역시 여러 가지 기능이 다양하게 있지만 범위를 크게 수험자 합격 정보 조회, 온라인 시험 2가지로 정하고 CIA 보안 등급과 CIAA 보안 등급을 적용하여 비교한다.

온라인 자격시험 서비스의 2가지 기능을 CIA 보안 등급에 적용하면 표 11과 같이 설정될 수 있다. 합격 정보 조회는 수험자 본인에게만 서비스될 수 있으면 된다. 따라서 중간 단계의 기밀성이 적용되었으며, 합

표 11. CIA 보안 등급을 이용한 온라인 자격시험 서비스 보안 등급 설정
Table 11. Online Eligibility Tests security level setting by using CIA security levels

| Level | Confidentiality | | | Integrity | | | Availability | | | Example of Service | Remark |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | H | M | L | H | M | L | H | M | L | | |
| 10 | | * | | * | | | * | | | Passing Information inquiry | Needs to set levels of authentication |
| 1 | * | | | * | | | * | | | Online Eligibility Test | |

격 정보는 변조되면 않되는 정보이며, 수험자라면 합격자 발표 후 언제든 확인할 수 있어야 한다. 온라인 시험은 문제 유출을 대비하기 위하여 강력한 기밀성이 보장되어야 하며, 답안을 제출할 때 답안 정보가 변조되면 않되며, 시험을 시작한 이후에는 가용성을 반드시 보장해주어야 한다. 온라인 자격시험 서비스는 사용되는 데이터들이 외부로 유출되는 것을 막는 기밀성의 확보 이외에 수험자의 인증이 반드시 필요하다. 하지만 CIA 보안 등급은 보안 등급 설정 후 사용자 인증을 다시 고려해야한다.

반면 CIAA 보안 등급을 적용하면 사용자 인증에 대한 추가적인 고려없이 보안 등급을 설정할 수 있다.

표 12. CIAA 보안 등급을 이용한 온라인 자격시험 서비스 보안 등급 설정
Table 12. Online Eligibility Tests security level setting by using CIAA security levels

| Level | Confidentiality | | Integrity | | Availability | | Authentication | | | Example of Service |
|---|---|---|---|---|---|---|---|---|---|---|
| | H | L | H | L | H | L | H | M | L | |
| E | * | | * | | * | | | * | | Passing Information inquiry |
| A | * | | * | | * | | * | | | Online Eligibility Test |

## V. 결 론

온라인 서비스의 보안등급을 설정하기 위해서 사용했던 CIA 보안 등급 모델은 각 요소별 모호한 중간 강도(Middle)이 존재하였으며, 실제 서비스에 적요할 수 없는 보안 등급이 존재하였으며, CIA 보안 모델을 이용한 보안 설정을 완료한 이후에 같은 등급의 보안 모델에 대해서 고려되지 않았던 인증을 추가로 고려해야하는 번거로움이 있었다. 따라서 CIAA 보안 등급 모델은 기존의 CIA 보안 등급에서 사용하지 않았던 "인증" 요소를 추가하였으며, CIA의 모호한 중간 강도("Middle")를 삭제하였다. 이에 따라 CIAA 보안 등급 모델은 좀 더 세분화하여 보안 등급을 구분할 수 있으며, 서비스되지 않는 보안 등급 유형에 대해서 고려하지 않아도 된다. 또한 서비스 구현 시 인증 요소를 따로 고려해야하는 번거로움과 사용자 레벨을 분류하는 추가적인 프로세스를 줄일 수 있다. 그러나 보안 등급을 분류할 수 있지만 보안 등급에 맞는 보안 대책을 제시하지 못하는 한계점이 있다. 추가적인 연구로 제안하는 CIAA 보안 등급과 매칭되는 SSL과 TLS, VPN 등의 보안 프로토콜과의 연계성을 고려하여 각 등급에 맞는 포괄적인 보안 권고사항을 개발할 필요성이 있다.

## References


[1] J. Bang, R. Ha, P. Kang, and H. Kim, "Security verification framework for e-GOV mobile app," *The Korea Inst. Commun. Inf. Sci.*, vol. 37c, no. 2, pp. 119-130, Feb. 2012.

[2] J. Bang and R. Ha, "Research on major weakness rules for secure software development," *The Korea Inst. Commun. Inf. Sci.*, vol. 38c, no. 10, pp. 831-840, Oct. 2013.

[3] J. Bang and R. Ha, "Validation test codes development of static analysis tool for secure software," *The Korea Inst. Commun. Inf. Sci.*, vol. 38c, no. 5, pp. 420-427, May 2013.

[4] L. M. Yeal, "A study of information security pre-evaluation model in ubiquitous information technology of u-logistics service environment," Department of Information Sevurity Gradute School, University of Soongsil, 2011.

[5] J.-S. Sung, "A study of contents secure in smart phone," *J. Security Eng.*, vol. 8, no. 6, pp. 665-672, Dec. 2011.

[6] L. G. Seok, L. J. Myung, and B. J. Ho, "Correlation analysis between strength of function and evaluation assurance level of common criteria," *Korea Inf. Commun. Soc. Summer Conf.,* pp. 1627-1628, Jeju island, Korea, Jun. 2009.

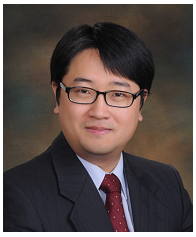
[7] J. Ahn, J. Bang, and E. Lee, "Quantitative scoring criteria on the importance of software weaknesses," *J. Korea Inst. Inf. Security Cryptology*, vol. 22, no. 6, pp. 1407-1417, Dec. 2012.

[8] "Study of malware detection based mobile OS," *Korea Inf. Security Agency*, 2010

[9] ISO/IEC JTC 1/SC 27, *Information technology - Security techniques - Entity authentication assurance framework*, 2011

[10] "The preliminary diagnosis practice guidebook for information security," *Korea Inf. Security Agency*, 2010

**추 연 수** (Yeun-su Choo)



2003년 8월 : 호서대학교 컴퓨터공학과 졸업
2005년 8월 : 숭실대학교 컴퓨터학과 석사
2005년 9월~현재 : 숭실대학교 컴퓨터학과 박사과정
<관심분야> 컴퓨터통신, 정보보안, 사용자인증, 암호학

**박 재 표** (Jae-Pyo Park)

1998년 8월 : 숭실대학교 컴퓨터학과 석사
2004년 8월 : 숭실대학교 컴퓨터학과 박사
2004년 9월~2009년 8월 : 숭실대학교 정보미디어기술연구소 전임 연구원
2010년 3월~현재 : 숭실대학교 정보과학대학원 교수
<관심분야> 컴퓨터통신, 정보보안, 포렌식, 암호학

**전 문 석** (Moon-Seog Jun)

1981년 2월 : 숭실대학교 전자계산학과
1986년 2월 : University of Maryland Computer Science 석사
1989년 2월 : University of Maryland Computer Science 박사
1989년 3월~7월 : Morgan State University 조교수
1989년 9월~1991년 2월 : New Mexico State University Physical Science Lab 책임연구원
1991년 3월~현재 : 숭실대학교 컴퓨터학과 정교수
<관심분야> 정보보호, 전자여권, 전자상거래