韓國컴퓨터情報學會 論文誌
第16卷 第8號, 2011. 8.

2011-16-8-3-6

워드프로세서의 전자서명 기능에 대한 취약성 분석

이 창 빈*, 박 선 우*, 이 광 우*, 김 지 연*, 남 정 현**, 이 영 숙***, 원 동 호*

Vulnerability Analysis on Digital Signature Function of Word Processors

Changbin Lee*, Sunwoo Park*, Kwangwoo Lee*, Jeeyeon Kim*, Junghyun Nam**,
Youngsook Lee***, Dongho Won*

요 약

최근 널리 사용되고 있는 전자문서는 문서가 변경되어도 이를 확인하기 어렵다는 특성을 가지고 있어 위·변조 및 이에 따른 피해가 우려되고 있다. 이에 따라 다양한 워드프로세서들은 전자문서의 신뢰성을 보장하기 위해 전자서명 생성 및 검증 기능을 제공하고 있다. 하지만 이러한 프로그램들이 전자서명 생성 및 검증을 정상적으로 수행하는지에 대한 연구가 미비하여 이를 완전하게 신뢰하기 어렵다는 문제점이 있다. 이에 본 논문에서는 현재 가장 보편적으로 사용되고 있는 워드프로세서인 Microsoft사의 Word와 한글과컴퓨터사의 흔글의 전자서명 기능에 대한 안전성 분석과 개선방안을 제안한다.

▸ Keyword : 전자문서, 전자서명, 인증서, 취약성 분석

Abstract

Recently, electronic documents are deployed in many areas. However, trust concerns arise owing to the fact that detecting whether an electronic document is modified or not is not an easy process. To facilitate this process, many word processors provide digital signature capabilities on themselves. However, there were not much research on the security of digital signature function of various programs including Microsoft Word and Hancom Hangul. Therefore, in this paper, we analyze the security of Microsoft Word and Hancom Hangul, and propose improvements for their digital signature schemes.

▸ Keyword : Electronic document, Digital signature, Certificate, Vulnerability Analysis

• 제1저자 : 이창빈 • 교신저자 : 원동호
• 투고일 : 2011. 07. 19, 심사일 : 2011. 08. 01, 게재확정일 : 2011. 08. 05
* 성균관대학교 정보통신공학부(School of Information and Communication Engineering, Sungkyunkwan University)
** 건국대학교 컴퓨터공학과(Department of Computer Engineering, Konkuk University)
*** 호원대학교 사이버수사 경찰학부(Department of Cyber Investigation Police, Howon University)
※ “본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 육성•지원사업”의 연구결과로 수행되었음” (NIPA-2011-C1090-1001-0004)

I. 서 론

정부가 추진하고 있는 저탄소 녹색성장 사업에 따라 정부 업무의 전산화가 빠른 속도로 진행되고 있다[1]. 주민등록, 병역, 특허, 조달, 세금 등의 행정이 전산화 되었을 뿐만 아니라, 전자민원G4C, 행정정보 공개, 행정정보 공유 등의 행정 관련 서비스도 전산화되었다. 정부 업무뿐만 아니라 세무, 공증, 금융, 의료 등 다양한 분야에서도 전산화가 진행되고 있으며 업무의 전산화에 따라 종이문서의 전자문서화도 함께 진행되고 있다[2][3]. 하지만 문서가 변경되거나 수정되어도 이를 확인하기 어렵다는 전자문서의 특성 때문에 전자문서의 위·변조 및 이에 따른 피해가 매년 끊임없이 발생하고 있으며 이는 사회적으로 심각한 문제가 되고 있다. 따라서 전자문서의 신뢰성을 확보하는 것은 전자문서 이용 활성화에 중요한 역할을 하고 있으며, 전자문서의 위·변조를 확인할 수 있는 전자서명 기술에 대한 수요도 증가하고 있다. 이러한 수요에 맞춰 몇몇 워드프로세서들은 전자문서의 신뢰성을 확보하기 위해 전자서명 기능을 제공하고 있다[4][5]. 하지만 이러한 워드프로세서들이 전자서명 생성 및 검증을 정상적으로 수행하는지에 대한 연구가 미비하기 때문에 이를 완전하게 신뢰하기에는 어려움이 있다. 이에 본 논문에서는 대표적인 워드프로세서인 MS Word와 훈글의 전자서명 이용 기술에 대해 분석해 보고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 MS Word의 전자서명 기능을 분석하고 이의 취약점을 살펴보며, 3장에서는 한글과컴퓨터사의 워드프로세서인 훈글의 전자서명 기능을 분석하고 이들의 취약점을 살펴본다. 4장에서는 두 프로그램의 분석 결과에 대한 정리 및 개선방안을 제안하며, 5장에서 결론을 맺는다.

II. Microsoft Word 전자서명 기능 분석

1. MS Word 개요

MS Word는 마이크로소프트(Microsoft)사에서 개발한 워드 프로세서이다. 현재 가장 널리 사용되는 워드프로세서 중 하나로, 여러 문서를 작성하는데 필요한 다양한 기능들을 포함하고 있다. MS Word는 1983년 MS-DOS용인 Word 1이라는 버전으로 처음 개발되어, 1985년에는 매킨토시용으로, 1989년에는 MS 윈도우용으로 각각 개발되었다. MS Word는 최초 버전 1에서 출발하여 현재 버전 14까지 발전하여 왔으며, 각 버전 중 MS 윈도우용의 버전별 전자서명 기능을 살펴보면 표 1과 같다[6].

표 1. MS Word 버전 단계별 자체 전자서명 기능
Table 1. Versions and Digital Signature Features of MS Word

발표년도	명칭	버전	전자서명 생성가능 여부	비고
1989	Word 1.0	1.0	-	-
1990	Word 1.1	1.1	-	-
1990	Word 1.1a	1.1a	-	-
1991	Word 2.0	2.0	-	-
1993	Word 6.0	6.0	-	-
1995	Word 95	7.0	-	-
1997	Word 97	8.0	-	-
1998	Word 98	8.5	-	-
1999	Word 2000	9	-	-
2001	Word 2002	10	-	-
2003	Word 2003	11	전자서명 생성가능	전자서명 자체 생성 기능 추가
2006	Word 2007	12	전자서명 생성가능	문서에 전자서명 표시 기능
2010	Word 2010	14	전자서명 생성가능	-

2. MS Word 전자서명 생성 기능

MS Word에서 사용하는 전자서명 생성 방식은 문서에 표시되는 서명란을 추가하여 하나 이상의 전자서명을 캡쳐하는 방식과 문서에 보이지 않는 전자서명을 추가하는 방식으로 나뉜다. 두 가지 방법 모두 인증서(디지털 ID)를 필요로 하며, 인증서는 그림 1과 같이 MS 제휴사로부터 발급받거나, 발급자와 주체가 동일한 인증서를 직접 생성할 수 있다. MS 제휴 프로그램으로는 Avoco secure2trust와 IntelliSafe 등이 있다.

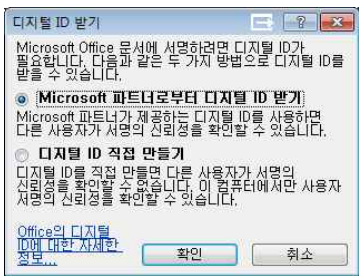

그림 1. MS Word의 디지털 ID
Fig. 1. Digital ID of MS Word

MS Word에서 직접 생성한 인증서의 유효기간은 발급일로부터 1년이며, 해당 인증서의 용도는 다음과 같다.

- 원격 컴퓨터에 사용자의 신분을 증명

- 전자 메일을 보호
- 디스크의 데이터를 암호화
- 모든 발급 정책

본 논문의 분석에서는 MS Word 버전 12(Word 2007)와 UltraEdit-32 버전 17.10.0.1009를 이용하였다.

2.1 전자서명 생성

2.1.1 문서에 표시되는 전자서명 생성

MS Word 2007에는 문서에 서명란을 삽입하는 기능이 추가되었다. 서명란은 인쇄 문서에 표시되는 일반적인 서명란과 모양은 동일하지만 작동 방식에서 차이가 있으며, 문서에 서명란을 삽입할 때 서명자에 대한 정보 및 서명자를 위한 지침을 지정할 수 있다. 문서의 전자 사본을 서명자에게 보내면 받는 사람에게 서명란이 표시되고 서명을 요청하는 알림이 나타난다. 서명자는 서명란을 클릭하여 문서에 전자서명을 할 수 있다. 서명자는 서명을 직접 입력하거나, 서명의 이미지를 선택하거나, Tablet PC의 잉크 기능을 사용하여 서명할 수 있다. 서명자가 문서에 눈으로 확인할 수 있는 형태의 전자서명을 추가하면 전자서명이 동시에 추가되어 서명자의 신원을 보증하게 된다. 전자서명된 문서는 내용을 수정할 수 없도록 읽기 전용으로 변경되며, 수정을 시도할 경우, 화면 하단에 “선택 영역이 잠겨 있기 때문에 수정할 수 없습니다.” 라는 메시지를 띄운다.

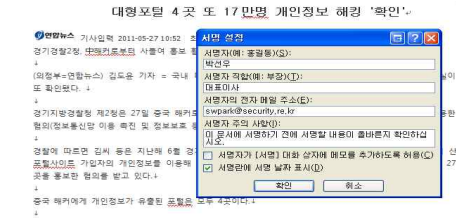

그림 2. MS Word의 서명란 설정
Fig. 2. Signature Configuration of MS Word

그림 3. MS Word의 문서에 표시되는 전자서명 생성
Fig. 3. A Visible Digital Signature of MS Word

위의 그림 2에서는 서명란을 설정하는 화면을 보여주며, 그림 3에서는 실제 전자서명을 생성하는 화면을 나타내고 있다. 그림 3과 같이 전자서명을 할 때 서명을 표시할 이미지를 함께 선택할 수 있다.

2.1.2 문서에 표시되지 않는 전자서명 생성

문서에 표시되지 않는 전자서명은 문서에 표시되는 서명란을 추가할 필요는 없지만 문서의 진위여부, 무결성 및 출처에 대한 보증이 필요한 경우 문서에 보이지 않는 전자서명을 추가할 수 있다. 문서에 표시되는 전자서명과는 달리 문서의 본문에는 표시되지 않지만 서명 보기 메뉴를 선택하거나 화면 아래쪽 상태 표시줄에 있는 리본 아이콘을 클릭하여 전자서명의 존재 여부와 해당 전자서명의 정보를 확인할 수 있다. 아래 그림 4는 문서에 표시되지 않는 전자서명을 생성하는 화면을 보여준다.

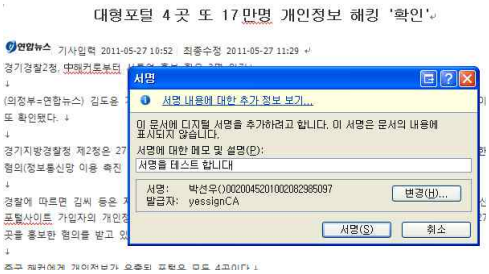

그림 4. MS Word의 문서에 표시되지 않는 전자서명 생성
Fig. 4. An Invisible Digital Signature of MS Word

2.2 전자서명 정보 확인

MS Word로 생성한 전자서명은 문서에 표시되는 전자서명과 문서에 표시되지 않는 전자서명 모두 그림 5와 같이 특정한 포맷을 가진다. 하지만 MS Word의 경우 전자서명과 관련된 표준이 존재하지 않아 포맷을 해석하는데 어려움이 따른다.

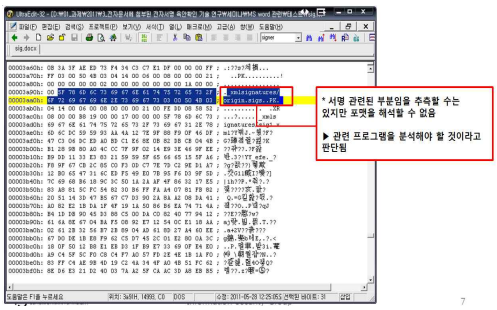

그림 5. MS Word의 전자서명 정보 확인 결과
Fig. 5. Signature Information of MS Word

3. MS Word 전자서명 검증 기능

MS Word에서 사용하는 전자서명 검증 방식은 생성 방식과 마찬가지로 문서에 표시되는 전자서명에 대한 검증과 문서에 보이지 않는 전자서명에 대한 검증으로 나뉜다.

3.1 전자서명 검증

3.1.1 문서에 표시되는 전자서명에 대한 검증

MS Word에서 문서에 표시되는 전자서명이 포함된 경우 그림 6과 같이 추가된 서명 이미지와 전자서명이 되었음을 알리는 리본을 보여준다.

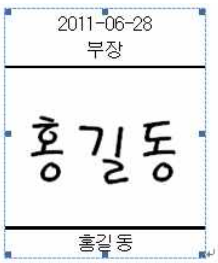

그림 6. MS Word의 문서에 표시되는 전자서명
Fig. 6. A Ribbon showing existence of Digital Signature

리본을 클릭하면 해당 문서에 존재하는 전자서명의 리스트를 보여주며, 검증하고자 하는 전자서명을 클릭하면 그림 7과 같이 전자서명에 대한 정보와 전자서명의 유효성 여부를 알려준다.

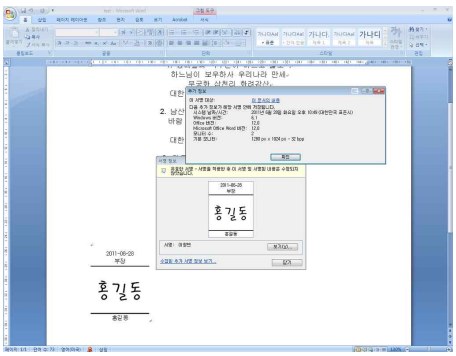

그림 7. MS Word의 전자서명 정보 및 전자서명 유효성 표시 1
Fig. 7. Validation Information of Digital Signature of MS Word 1

3.1.2 문서에 표시되지 않는 전자서명에 대한 검증

MS Word에서 문서에 표시되는 않는 전자서명이 포함된 경우에는 전자서명이 되었음을 알리는 리본만을 보여주며, 리본을 클릭하면 그림 8과 같이 전자서명에 대한 정보와 전자서명의 유효성 여부를 알려준다.

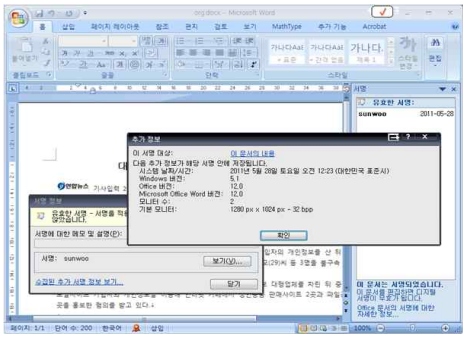

그림 8. MS Word의 전자서명 정보 및 전자서명 유효성 표시 2
Fig. 8. Validation Information of Digital Signature of MS Word 2

3.2 인증서 검증

전자서명의 유효성을 검증하기 위해서는 전자서명 검증과 더불어 인증서 검증이 함께 수행되어야 한다. 따라서 MS Word에서 인증서 검증을 정상적으로 수행하는지 확인해 보도록 한다[11][12].

3.2.1 인증서 경로 구축 및 최상위 인증서의 신뢰 목록 등록

인증서 검증을 수행하기 위해서는 우선 전자서명 검증에 사용되는 인증서의 경로를 구축해야 한다. MS Word의 경우 그림 9와 같이 인증경로를 정상적으로 구축하고 있으며, 운영체제에 등록된 신뢰된 루트 인증기관 정보를 통해 최상위인증기관의 인증서를 신뢰한다[11].

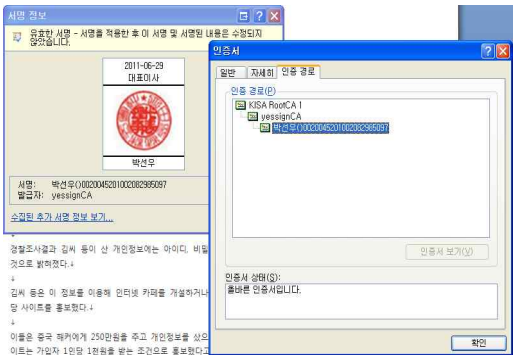

그림 9. MS Word의 인증서 경로 구축
Fig. 9. Certification Path Validation of MS Word

3.2.2 인증서 기본 검증

MS Word에서 인증서 기본 검증인 서명검증, 인증서 상태 검증, 유효기간 검증을 정상적으로 수행하는지 확인해보도록 한다.

(1) 인증서 서명 검증

MS Word에서 인증서 서명 검증을 정상적으로 수행하는지 확인하기 위하여 사용자 인증서에서 signatureValue 필드의 값을 1바이트 변경하여 전자서명을 시도해본 결과 그림 10과 같이 유효하지 않은 서명이라는 메시지를 확인할 수 있었다. 즉 MS Word에서는 인증서 서명 검증을 정상적으로 수행함을 알 수 있다.

그림 10. MS Word의 손상된 인증서로 서명한 경우 검증 결과
Fig. 10. Verification Result of Signature Signed with Damaged Certificate in MS Word

(2) 인증서 상태 검증

MS Word에서는 전자서명에 사용된 인증서가 폐지된 경우 그림 11과 같이 유효하지 않은 서명이라는 메시지를 출력해준다. 즉 MS Word에서는 인증서 상태 검증을 정상적으로 수행함을 알 수 있다.

그림 11. MS Word의 폐지된 인증서로 전자서명한 경우 검증 결과
Fig. 11. Verification Result of Signature Signed with Revocated Certificate in MS Word

(3) 인증서 유효기간 검증

MS Word에서는 전자서명에 사용되는 인증서의 유효기간이 지난 경우 전자서명에 사용할 인증서 목록에 해당 인증서를 보여주지 않음으로써 유효기간이 만료된 인증서의 사용을 방지한다. 하지만 유효기간 검사에 사용되는 현재 시간으로 사용자의 컴퓨터 시간정보를 사용하기 때문에 악의적인 사용자가 컴퓨터 시간을 조작하여 유효기간이 지난 인증서로 전자서명을 생성할 수 있다는 취약점이 있다.

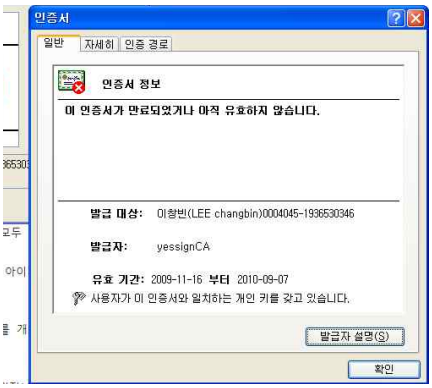

그림 12. MS Word의 전자서명에 사용된 유효기간이 지난 인증서
Fig. 12. An Expired Certificate

MS Word는 전자서명을 검증하는 시점에 인증서의 유효기간이 지난 경우 그림 12와 같이 전자서명에 사용된 인증서가 유효하지 않음을 표시해 사용해 사용자가 이를 확인할 수 있도록 한다.

III. 한글과컴퓨터 혼글 전자서명 기능 분석

1. 혼글 개요

혼글은 한글과컴퓨터사에서 개발된 한글 워드프로세서이다. 혼글은 국내에 가장 널리 보급된 한글 워드프로세서으로, 문서작성에 필요한 다양한 기능들을 포함하고 있다. 혼글은 1989년 혼글 1.0으로 시작하여 현재 혼글2010까지 개발되었으며, 각 버전의 기능을 살펴보면 표 2와 같다[7].

표 2. 흔글 버전 단계별 전자서명 기능
Table 2. Versions and Features of Hancom Hangul

발표 년도	명칭	전자서명 생성가능 여부	비고
1989	흔글1.0	-	-
1992	흔글2.5	-	-
1996	흔글96	-	-
1997	매킨토시용 흔글96	-	-
1999	흔글97 강화판	-	-
2000	흔글 워디안	-	-
2001	흔글2002	-	-
2003	흔글2004	-	XML 지원, 문서 암호 설정 기능
2004	흔글2005	-	-
2006	흔글2006	-	-
2007	흔글2007	전자서명 생성 가능	공인인증서로 전자서명 및 문서 암호화
2009	흔글2010	전자서명 생성 가능	개인정보보호 기능

2. 흔글 전자서명 생성 기능

2.1 전자서명 생성

흔글2007 및 흔글2010은 그림 13과 같이 공인인증서를 사용한 전자서명 생성 기능을 지원하며 전자서명을 문서에 표시하는 기능은 지원하지 않는다.

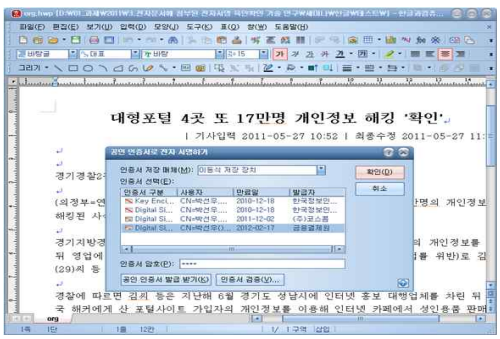

그림 13. 공인인증서를 사용한 흔글의 전자서명 생성
Fig. 13. Hangul's Digital Signing with Accredited Certificate

하지만 전자서명이 포함된 문서를 불러올 때 흔글2007은 '전자서명이 포함된 문서입니다.'라는 메시지를 띄움으로써 수신자에게 전자서명이 포함된 전자문서임을 알려주고, 흔글2010은 전자서명 유효성 검증 결과 메시지를 띄움으로써 전자서명이 포함되었다는 사실과 함께 전자서명의 유효성 검증 결과를 보여준다.

2.2 전자서명 정보 확인

흔글의 전자서명 정보를 확인하기 위해 UltraEdit로 파일을 열어보면 그림 14와 같이 XML Signature 포맷을 사용하는 것을 확인할 수 있었다.

그림 14에서 블록이 씌워진 부분을 통해, 전자서명 데이터가 XML Signature 포맷으로 저장되어 있다는 것을 확인하였다. XML 포맷은 가독성이 좋아 분석이 용이하며 분석 결과, 전자서명 알고리즘으로 RSA-SHA-1을, 해쉬 알고리즘으로는 SHA-1을 사용하였음을 알 수 있었다. 또한, Digest Value 즉, 메시지의 해쉬 값과 전자서명 값을 확인할 수 있었다. 전자서명 값은 base 64 인코딩된 값으로, 디코딩을 해보면 순수하게 128bit의 전자서명 값이 들어가는 것을 확인할 수 있었다.

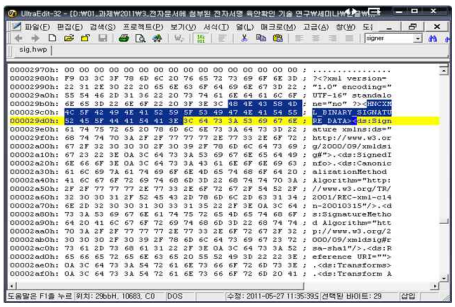

그림 14. 흔글의 전자서명 정보 확인 결과 1
Fig. 14. Digital Signature Information of Hangul

3. 흔글 전자서명 검증 기능

3.1 전자서명 검증

흔글2010에서는 전자서명된 문서를 열면 전자서명에 대한 검증이 자동으로 수행된다.

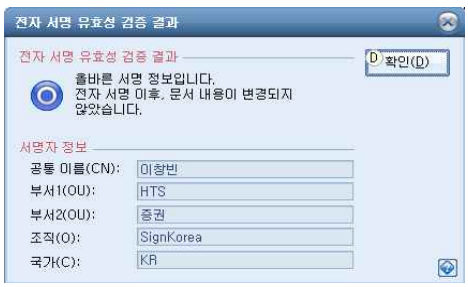

그림 15. 흔글의 전자서명 검증 성공
Fig. 15. A Successful Validation of Digital Signature

또한, 파일메뉴의 전자서명 탭에서 유효성 검증 버튼을 클릭하여 문서가 열린 후에도 언제든지 전자서명 검증이 가능하다. 위의 그림 15에서 볼 수 있듯이, 사용자는 해당 문서의 전자서명이 유효한지 여부와 서명자의 인증서에 대한 기본 정보를 확인할 수 있다. 만약 문서 내용이 변경되어 서명 데이터와 일치하지 않을 경우, 그림 16과 같이 유효성 검증에 실패하였다는 메시지를 출력한다.

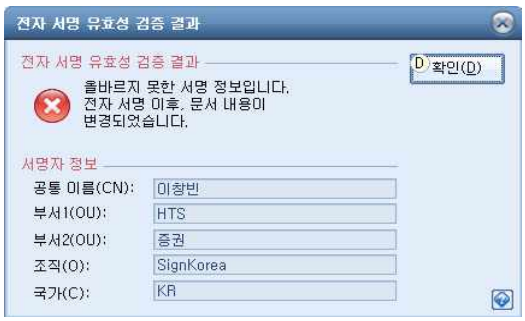

그림 16. 훈글의 전자서명 검증 실패
Fig. 16. A Failed Validation of Digital Signature

3.2 인증서 검증

2장에서 언급한 것과 같이 전자서명의 유효성을 검증하기 위해서는 전자서명 검증 이외에 인증서 검증이 함께 수행되어야 한다. 따라서 훈글에서 인증서 검증을 정상적으로 수행하는지 확인해 보도록 한다. 분석은 훈글2007과 훈글2010을 대상으로 수행되었으며, 수행결과가 동일하였기 때문에 인증서 검증 분석 결과는 훈글2007을 기준으로 기술되었다.

3.2.1 인증서 경로 구축 및 최상위 인증서의 신뢰 목록 등록

인증서 검증을 수행하기 위해서는 우선 전자서명 검증에 사용되는 인증서의 경로를 구축해야 한다. 훈글의 경우 사용되는 인증서를 공인인증서로 제한한다. 훈글은 전자서명에 사용된 인증서의 정보를 따로 보여주지 않아 인증서 경로를 정상적으로 구축했는지 여부를 확인하기는 어렵다.

3.2.2 인증서 경로 구축 및 최상위 인증서의 신뢰 목록 등록

훈글에서 인증서 기본 검증인 서명검증, 인증서 상태 검증, 유효기간 검증을 정상적으로 수행하는지 확인해보도록 한다.

(1) 인증서 서명 검증

훈글에서 인증서 기본 검증을 정상적으로 수행하는지 확인하기 위하여 사용자 인증서에서 signatureValue 필드의 값을 1바이트 변경하여 전자서명을 시도해 본 결과 그림 17과 같이 전자서명 유효성 검증 실패 메시지를 확인할 수 있었다. 즉 훈글에서는 인증서 서명 검증을 정상적으로 수행함을 알 수 있다. 하지만 전자서명의 유효성 검증 실패 사유를 명확하게 명시해 주지 않아 이를 확인할 수 없다는 문제점을 가지고 있었다.

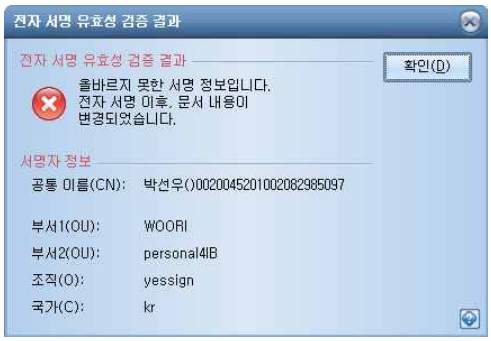

그림 17. 훈글에서 손상된 인증서로 서명한 경우 검증 결과
Fig. 17. Hangul's Verification Result of Signature Signed with Damaged Certificate

(2) 인증서 상태 검증

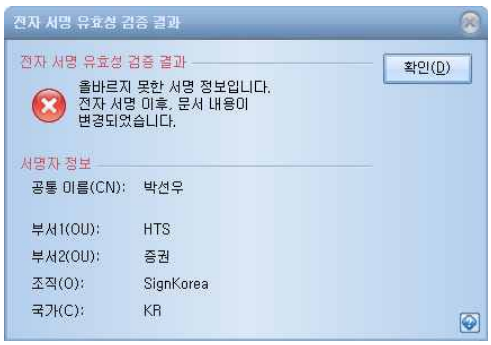

그림 18. 훈글의 폐지된 인증서로 서명한 경우 검증 결과
Fig. 18. Hangul's Verification Result of Signature Signed with Revocated Certificate

훈글에서는 전자서명에 사용된 인증서가 폐지된 경우 그림 18과 같이 전자서명 유효성 검증 실패 메시지를 출력해주며, 훈글에서 인증서 상태 검증을 정상적으로 수행함을 알 수 있다. 하지만 전자서명의 유효성 검증 실패 사유를 명확하게 명시해 주지 않아 사용자가 이를 확인할 수 없다는 문제점이 있다.

(3) 인증서 유효기간 검증

훈글에서는 서명에 사용되는 인증서의 유효기간이 지난 경우 그림 19와 같이 인증서를 사용할 수 없음을 표시함과 동시에 인증서 비밀번호 입력창을 비활성화 함으로써 인증서의 사용을 방지한다.

그림 19. 혼글의 유효기간 만료된 인증서 사용 방지 기능
Fig. 19. Protection from Signing with Expired Certificate in Hangul

하지만 유효기간 검사에 사용되는 현재 시간으로 사용자의 컴퓨터 시간정보를 사용하기 때문에 악의적인 사용자가 컴퓨터 시간을 조작하여 유효기간이 지난 인증서로 전자서명을 생성할 수 있다는 취약점이 발생한다. 그림 20은 PC의 시간을 조작한 경우 유효기간이 만료된 인증서의 비밀번호 입력창이 활성화 되는 화면을 보여준다.

그림 20. PC의 시간 조작을 통한 혼글의 유효기간 만료 인증서 사용 방지 기능 무력화
Fig. 20. Detour of the Protection from Signing with Expired Certificate in Hangul

혼글에서는 전자서명을 검증하는 시점에 인증서의 유효기간이 지난 경우에도 전자서명 유효성 검증 성공 메시지를 보여주는 것을 확인하였다. 즉 혼글에서는 인증서 유효기간 검증을 정상적으로 수행하지 않음을 알 수 있다.

IV. 분석 결과 및 개선방안

1. 분석 결과

MS Word의 전자서명 기능을 서명에 대한 검증과 인증서에 대한 검증으로 나누어 분석한 결과, 서명에 대한 검증은 잘 이루어지고 있었다. 인증서에 대한 검증은 인증서 경로 구축이 원활하게 이루어지는지에 대한 검증과 인증서 기본검증으로 나누어 진행되었다. 인증서 경로 구축은 운영체제에 등록된 신뢰된 루트 인증기관 정보를 통해 최상위인증기관의 인증서를 신뢰하는 형태로써 문제없이 이루어지고 있었다. 인증서 기본검증은 인증서의 서명 검증과 상태 검증, 그리고 유효기간의 검증으로 나뉘는데 이 중, 서명과 상태에 대한 검증은 정상적으로 수행되었다. 하지만 인증서의 유효기간 검증이 PC의 시간 정보를 사용하여 수행되기 때문에 PC의 시간을 조작할 경우, 유효기간이 지난 인증서에 대한 검증이 정상적으로 수행되는 문제가 있었다.

혼글의 경우 국산 소프트웨어의 성격상, 전자서명 시 공인인증서만 사용할 수 있도록 되어있었다. 하지만 전자서명에 사용된 인증서 정보를 따로 보여주지 않아 인증서 경로 구축 정보를 확인하기 어렵다. 인증서 기본검증 중 전자서명 검증과 상태 검증은 MS Word와 마찬가지로 잘 이루어지고 있었으나, 검증 실패 사유를 명확히 표시하지 않아 파악이 어렵다는 단점이 있었다. 또한 전자서명 생성 시에는 인증서 유효기간에 대한 검증을 수행하지만 MS Word와 동일하게 PC 시간정보를 이용하여 검증을 수행하는 문제가 있었으며, 전자서명 검증 시에는 전자서명에 사용된 인증서의 유효기간 검증 자체를 수행하지 않는 문제점이 있었다. 아래 표 3은 MS Word와 혼글의 분석 결과를 정리한 것이다.

표 3. 분석 결과
Table 3. Analysis Results

분석 내용			분석 결과	
			MS Word	한컴 혼글
전자서명 검증			○	○
인증서 검증	인증서 경로구축		○	○
	기본 검증	서명검증	○	○
		상태검증	○	○
		유효기간 검증	△	X

2. 취약점 분석 및 개선방안

MS Word에서는 전자서명 생성 및 검증 시 인증서의 유효기간 검증에 사용되는 시간정보로 PC의 컴퓨터 시간정보를 이용한다는 문제점이 존재하며 혼글에서는 MS Word와 동일한 문제점뿐만 아니라 전자서명 검증 시 유효기간검증을 수행하지 않는다는 문제점도 존재한다. 각 문제점에 따른 취약점 및 개선방안은 다음과 같다.

(1) 전자서명 생성 시 인증서 유효기간 검증

전자서명 생성 시 인증서 유효기간 검증에 사용되는 시간정보로 PC의 시간 정보를 이용하기 때문에 악의적인 사용자가 PC의 시간을 조작한 뒤 유효기간이 만료된 인증서로 전자

서명을 수행할 수 있다. 이러한 경우 전자서명에 사용된 인증서를 신뢰할 수 없기 때문에 전자서명 검증 시 전자서명을 신뢰할 수 없게 되고 악의적인 사용자의 서명에 대한 부인방지가 가능해진다. 이러한 취약점을 개선하기 위해서는 인증서 유효기간 검증에 사용되는 시간정보를 신뢰할 수 있는 시점확인 서버에서 제공받아야 한다[13][14].

(2) 전자서명 검증 시 인증서 유효기간 검증

인증서의 유효기간은 인증서에 사용된 암호 알고리즘의 안전성을 보증할 수 있는 기간을 의미한다. 따라서 유효기간이 지난 인증서의 경우 안전성을 보증할 수 없으며, 인증서의 전자서명키가 공격자에게 노출될 위험이 존재한다. 즉, 악의적인 공격자에게 유효기간을 초과하는 충분한 시간이 주어진다면 인증서에 대응하는 전자서명키를 찾아 전자서명을 생성할 수 있다. 따라서 전자서명 검증 시 인증서의 유효기간 검증은 필수적으로 이루어져야 한다[9].

한글의 경우 전자서명 검증 시 인증서 유효기간에 대한 검증을 수행하지 않아 인증서의 안전성을 신뢰할 수 없으며 따라서 전자서명의 안전성 또한 신뢰하기 어렵다. 이러한 취약점을 개선하기 위해서는 전자서명 검증 프로세스에서 인증서 유효기간 검증 기능을 추가해야 한다[10].

MS Word의 경우 전자서명 검증 시 인증서 유효기간에 대한 검증을 수행하고 있지만 인증서 유효기간 검증에 사용되는 시간정보로 PC의 시간 정보를 이용하고 있다. 이는 악의적인 사용자가 검증자 PC의 시간을 조작할 경우, 유효기간이 만료된 인증서로도 검증절차를 통과할 수 있도록 한다. 이러한 취약점을 개선하기 위해서는 인증서 유효기간 검증에 사용되는 시간정보를 신뢰할 수 있는 시점확인 서버에서 제공받아야 한다[8].

V. 결론 및 향후연구

전자서명 기술은 전자문서의 신뢰성을 확인하는 데에 매우 중요한 역할을 한다. 이에 여러 워드프로세서에서는 전자서명 기능을 기본으로 제공하고 있다. 하지만 기존에 이러한 전자서명 기능에 대한 연구가 충분히 이루어지지 않아 MS Word와 한글과컴퓨터 흔글 프로그램의 전자서명 기능에 대한 안전성 분석을 진행하였다. 분석 결과, 두 프로그램 모두 전자서명 자체에 대한 검증은 잘 수행하고 있었으나, 전자서명에 필요한 인증서에 대한 검증에는 문제점이 있었다.

향후, 진행한 분석 결과를 토대로 신뢰성 있는 전자문서 유통을 위한 보안 요구사항을 도출할 것이다. 이러한 연구를 통해 문서 저장의 안전성 및 신뢰성 증대를 도모하여 나아가 전자문서 이용을 촉진시키고 저탄소 녹색성장 사업에 기여하고자 한다.

참고문헌

[1] C. Jung, "e-Government", Seoul Economics and Mana gement, pp. 44-45, 2009.

[2] K. Oh, "e-Government and u-paradigm ", MnB, pp. 80-85, 2010.

[3] Presidential Committee on Government Innovation & Decen tralization, "e-Government of Participation Government", 2005.

[4] Timestamp Solution, http://www.timestamping.co.kr

[5] etnews, "What solutions exist for 'Paperless Office'", March 2011.

[6] Microsoft Office Products - Office.com, http://office. micro soft.com/ko-kr/products

[7] Hancom, http://www.hancom.co.kr

[8] KISA, "Digital Signature Certificate Profile", Sept. 2009.

[9] KISA, "Accredited Certificate Cryptosystem Sophist ication Plan", Sept. 2009.

[10] Y. Lee, J. Ahn, S. Kim, and D. Won, "A PKI System for Detecting the Exposure of a User's Secret Key", Proc. of EuroPKI 2006, Springer-Verlag, LNCS 4043, pp.248-250, June 2006.

[11] R. Housley, W. Polk, W. Ford, and D. Solo, "Intern et x.509 public key infrastructure certificate and CRL profile," IETF RFC 3280, April 2002.

[12] M. Myers, R. Ankney, A. Malpani, S. Galperin and C. Adams, "X.509 Internet PKI Online Certificate Status Protocol," IETF RFC 2560, June 1999.

[13] S. Pyo, "A Design of XML Structure for Digital Sign ature", Journal of The Korea Society of Computer and Information, Vol. 7, No. 4, pp. 66-74, Dec. 2002.

[14] K.S. Sung, J.J. Kim, and H.S. Oh, "System Design for the Safe store and Issue Service Assurance of the E-Document", Journal of The Korea Society of Computer and Information, Vol. 13, No. 6, pp. 173-180, Nov. 2008.

저 자 소 개

이 창 빈

2010 : 학점은행제 전자계산학 이학사.
현 재 : 성균관대학교 전자전기컴퓨터 공학과 석사과정.
관심분야 : 정보보호, 암호이론, 정보보호 제품 보안성 평가, PKI
Email : cblee@security.re.kr

박 선 우

2006 : 서울여자대학교 정보보호공학과 공학사.
현 재 : 성균관대학교 전자전기컴퓨터 공학과 석사과정.
관심분야 : 정보보호, 암호이론, PKI, 금융보안
Email : swpark@security.re.kr

이 광 우

2005~2007 : 성균관대학교 컴퓨터공학과 공학사, 석사.
2009 : 성균관대학교 전자전기컴퓨터공학과 박사수료.
관심분야 : 암호이론, 정보보호제품 보안성 평가, 전자투표, 디지털 복합기 보안
Email : kwlee@security.re.kr

김 지 연

1995 : 성균관대학교 정보공학과 공학사.
1997 : 성균관대학교 정보공학과 공학석사.
2006 : 성균관대학교 전기전자및컴퓨터공학과 공학박사.
현 재 : ISMS, PIMS, G-ISMS 심사원
관심분야 : 암호프로토콜, 암호이론, 정보보호관리체계 인증
Email : jeeyeonkim@paran.com

남 정 현

1997 : 성균관대학교 정보공학과 공학사.
2002 : University of Louisiana, Lafayette Computer Science M.S.
2006 : 성균관대학교 컴퓨터공학과 공학박사
현 재 : 건국대학교컴퓨터공학과 부교수
관심분야 : 컴퓨터보안, 암호학
Email : jhnam@kku.ac.kr

이 영 숙

1987 : 성균관대학교 정보공학과 공학사.
2005 : 성균관대학교 정보보호학과 공학석사.
2008 : 성균관대학교 컴퓨터공학과 공학박사.
현 재 : 호원대학교사이버수사경찰학부 조교수, 기획조정처 경영평가 실장
관심분야 : 암호프로토콜, 네트워크 보안, 스마트폰 보안, 디지털포렌식
Email : ysooklee@howon.ac.kr

원 동 호

1976~1988 성균관대학교전자공학과 공학사, 석사, 박사.
1985~1986 일본 동경공업대객원연구원.
1988~2003 성균관대학교 학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
2002~2003 한국정보보호학회장
현 재 성균관대학교 보통신공학부 교수, BK21 사업단장, 한국정보보호학회 명예회장.
관심분야 : 암호이론, 정보이론, 정보보호
Email : dhwon@security.re.kr