RFID를 이용한 디지털 문서 보안 아키텍처

최 재 현[†] · 이 우 진[††] · 정 기 원[†††]

요 약

디지털 문화의 보급과 확산에 따라 이제 모든 문서는 디지털 전자 문서로 작성되어 사용되고 있지만, 이러한 디지털 문서가 포함하고 있는 다양한 지적 재산과 기술, 핵심 리소스, 개인 정보 등은 광대한 네트워크의 발달과 해킹 기술의 발달 및 전파로 인해 내외부적으로 많은 위협에 노출되어 있다. 대부분의 가정 및 기업 내부의 PC는 운영체제 자체에서 사용자의 ID와 패스워드를 통해 내부 데이터에 대한 접근을 통제하거나 소프트웨어 및 플래시 메모리와 같은 보안 기술을 이용하여 디지털 문서에 대한 접근을 막고 있지만, 디지털 문서의 활용 및 사용 정책과 중요도 및 가치에 비해 상대적으로 그 기능은 부족한 점이 있다. 따라서, 본 논문은 상대적으로 저가인 RFID 태그와 암호화 기법을 이용하여 향상된 보안성을 보장하는 디지털 문서의 보안 아키텍처를 제시한다. 이는, PC에 저장된 디지털 문서를 암호화하고, 이 문서에 접근하기 위해 필요한 정보들을 RFID 태그에 저장함으로써, 태그를 가지지 않은 다른 내외부자로부터의 접근을 원천적으로 배제하며, 해당 디지털 문서를 직접 암호화함으로써 네트워크 상에서 해당 문서를 공유하거나 전송하는 경우에도, 디지털 문서에 대한 보안성이 유지되도록 한다.

키워드 : RFID, 디지털 문서, 보안, 아키텍처

An Architecture for Securing Digital Documents Using Radio Frequency Identification(RFID)

Jaehyun Choi[†] · Woojin Lee[††] · Kiwon Chong[†††]

ABSTRACT

Digital documents have become the mainstay of the paperless office. This is due to the increased usage of computer networks and the widespread digital culture. Along with the increased usage of digital documents comes the problem of securing them. The documents may have very important information such as confidential business policies and intellectual property statements. Generally, most of users protect them by using a password or secured flash memory or security software, but it has several weaknesses. Accordingly, we propose a new architecture for securing digital documents. The proposed architecture bases on RFID and several encrypting techniques. It makes up for the weakness of traditional securing architectures, and supports various policies for digital documents of users.

Key Words : Radio Frequency Identification(RFID), Digital Documents, Security, Architecture

1. 서 론

컴퓨터의 보급과 인터넷의 확산으로, 개인과 기업 사이에서는 대부분의 문서가 펜을 사용한 하드 카피 형식의 문서에서 벗어나 이제는 소프트 카피 형식의 문서인 디지털 문서로 작성되어 사용되고 있다. 하지만, 광대한 네트워크의 발달과 해킹 기술의 발달 및 전파로 인해 이러한 디지털 문서가 포함하고 있는 다양한 지적 재산과 기술, 핵심 리소스, 개인 정보 등은 내·외부적으로 많은 위협에 노출되어 있다. 실제, 한국 인터넷 침해 사고 대응 지원 센터의 통계자료에 따르면, 우리나라의 해킹 피해사례는 2001년 4,265건, 2002년 6,684건, 2003년 13,184건으로 해마다 빠르게 증가하고 있으며[1], [2], 미국의 경우에도, 2004년 CSI/FBI Computer Crime & Security Survey에 따르면 1999년부터 2004년에 사이의 모든 조사대상의 60% 이상이 현재 사용하고 있는 컴퓨터에 대해 인증되지 않은 사용자의 접근이 있었다고 응답하였다[3]. 이러한 통계 자료 및 조사 결과는, 사용자의 컴퓨터에 있는 디지털 문서가 더 이상 내·외부로부터의 침입에 대해 안전하지 못하다는 사실을 단적으로 보여주고 있다.

대부분의 가정 및 기업 내부의 PC는 운영체제 자체에서 사용자의 ID와 패스워드를 통해 내부 데이터에 대한 접근을 통제하여 디지털 문서의 접근을 막고 있지만, 피해 사례에 나타났듯이, 디지털 문서의 중요도 및 가치에 비해 상대적으로 보안 및 접근 통제 수준은 미약한 실정이다. 또한, 이를 보완

※ 본 연구는 숭실대학교 교내연구비 지원으로 이루어졌음.
† 준 회 원 : 숭실대학교 대학원 컴퓨터학과 석사과정
†† 준 회 원 : 숭실대학교 대학원 컴퓨터학과 박사과정
††† 종신회원 : 숭실대학교 컴퓨터학부 교수
논문접수 : 2005년 7월 26일, 심사완료 : 2005년 12월 2일

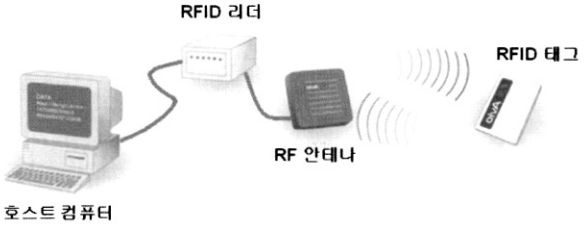
하기 위해 보안 기능을 갖춘 플래시 메모리를 사용하거나, 암호화 기능을 가진 소프트웨어를 사용한 보안 방법들이 사용되고 있지만, 플래시 메모리는 상대적으로 파손 위험이 크고, 디지털 문서에 대한 직접적인 암호화가 아닌 메모리 자체의 보안기능을 제공하기 때문에 공유네트워크 상에서는 보안성을 유지하기 힘든 단점이 있다. 또한 소프트웨어만을 사용하는 경우에는 사용자 패스워드만을 가지고 암호화를 수행하는 방법으로 보안성이 다소 부족한 측면이 있다.

따라서, 본 논문은 상대적으로 저가인 RFID 태그와 암호화 기법을 이용하여 개선된 디지털 문서의 보안 및 접근 제어 아키텍처를 제시한다. 이는, PC에 저장된 디지털 문서를 암호화하고, 이를 복원하기 위한 정보를 RFID 태그에 저장함으로써, 해당 사용자가 아닌 다른 내부자로부터의 접근을 원천적으로 배제하며, 해당 디지털 문서를 직접 암호화함으로써 해당 문서가 외부로 유출된다 하여도, 디지털 문서가 가지고 있는 정보의 판독이 불가능하도록 하는 이중 인증 방식을 가진다.

2. 관련 연구

2.1 RFID(Radio Frequency Identification)

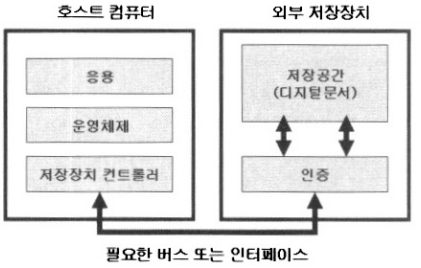
RFID는 사물에 태그를 부착하고, RFID 리더를 사용하여 태그로부터 라디오 전파를 이용하여 사물의 정보(Identification) 및 주변 환경정보를 인식하여 각 사물의 정보를 수집, 저장, 가공 및 추적함으로써 사물에 대한 원격처리 및 관리와 정보교환 등 다양한 서비스를 제공하는 기술이다[4], [5], [6]. 이러한 RFID 기술은 1970년대에 탄도미사일 추적을 위한 군사목적으로 미국에서 최초로 개발되었으며, Transponder라 불리는 RFID 태그와 안테나, 그리고 리더기로 구성된다. 반도체 칩이 들어 있는 태그에는 일련의 정보가 저장되며, 안테나는 이러한 정보를 무선으로 수 미터에서 수십 미터까지 전송하며, 리더기는 이 신호를 받아 해독하여 태그 내의 정보를 인식하게 된다[7], [8]. 이러한, RFID 기술은 반도체 기술의 지속적인 발전과 더불어 네트워크와의 결합을 통해 정보화의 범위를 사람이 아닌, 모든 사물에 이르기까지 확대시킬 수 있는 계기를 마련하였으며, 차세대 컴퓨팅 환경인 유비쿼터스 환경에서 핵심기술로 발전할 것으로 예상된다[9], [10]. (그림 1)은 RFID의 구성요소를 나타낸다.



(그림 1) RFID의 구성

2.2 외부저장 장치를 이용한 디지털 문서 보안 아키텍처

디지털 문서를 보호하는 방법으로 최근 널리 보급되고 있는 USB 메모리와 같은 별도의 외부 공간에 디지털 문서를 저장하는 방법이 있다. 이것은, 디지털 문서를 별도의 외부 공간에 저장하여 네트워크와 같은 디지털 문서로의 접근 경로를 차단함으로써 디지털 문서의 유출을 방지하고, 사용자 패스워드를 사용하여 인증되지 않은 사용자의 접근을 차단함으로써 디지털 문서를 보호한다. 이러한 방법의 대표적인 예로는, 최근에 USB 메모리가 많이 사용되고 있으며, (그림 2)는 그러한 외부저장장치를 이용한 디지털 문서 보안 아키텍처를 나타내고 있다. 이러한 방식에서는 특히 외부저장장치의 저장영역에 보안 영역을 설정하고, 보안 영역에 대해서는 프로그램을 통해 접근을 제어함으로써 디지털 문서를 보호한다. 이러한 외부저장장치를 이용한 디지털 문서 보안 방법 중 대표적인 것이 USB 메모리 장치[11]를 이용하는 방식이며, 이러한 USB 메모리 장치는 휴대하기 간편하고 사용하기 편리해 개인 디지털 문서를 보호하는 방법으로 많이 사용되고 있다. 하지만, 이러한 외부 저장장치를 이용하는 방식은 해당 문서를 접근하기 위해서 패스워드만을 사용하는 단순 인증 방식을 사용하는 방식으로, 프로그램을 사용한 반복적인 단순 대입을 통한 무력화가 비교적 쉽고, 부서지거나 회로고장을 일으키는 물리적 충격이나 불순물의 유입 등으로 인한 파손의 위험이 크다는 것이 단점으로 지적될 수 있다. 뿐만 아니라, 이러한 방식은 디지털 문서의 보호가 특정 영역에 국한되므로 해당 문서를 공유 네트워크상에서 공유하거나 전송하는 경우에 보안이 이루어지지 않아 조직 문서의 관리나 공유 문서의 관리에 활용되기 어려운 점이 있다.



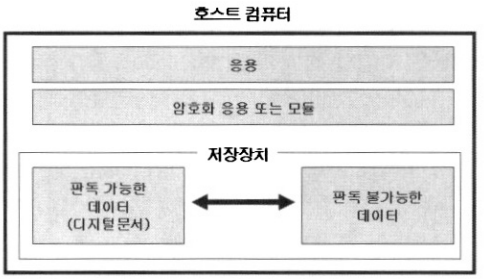
(그림 2) USB 메모리를 이용한 디지털 문서 보안 아키텍처

2.3 소프트웨어 기반의 디지털 문서 보안 아키텍처

디지털 문서에 대한 암호화는 문서를 작성하는 워드 프로세서 프로그램이나 다른 여타 압축프로그램과 같은 암호화 기능을 탑재한 소프트웨어에 의해 이루어 질 수 있다[12], [13]. 이 경우에는 내부적으로 암호 설정기능을 통해 문서를 암호화하고, 문서를 다시 사용하고자 할 때, 패스워드를 통해 문서를 복원하는 방식을 취하고 있다. (그림 3)은 이러한 아키텍처를 나타내고 있다.

하지만, 단순히 디지털 문서에 대한 접근을 제어하기 위해 사용자 패스워드 만을 사용하고, 원본 문서의 내용이 여전히 사용자 컴퓨터의 내부에 존재해 네트워크를 통해 내·외부로 유출될 위험이 높다는 점이 보안상 다소 부족한 점으로 지적할 수 있다. 특히, 이렇게 호스트 컴퓨터가 네트워크 상에 존재할 경우에는 디지털 문서에 대한 내·외부 접근이 용이해

져 디지털 문서에 대한 높은 안전성을 보장하기가 힘들다. 하지만, 암호화/복호화 용용의 구현 정도에 따라 다양한 디지털 문서 활용 방안을 지원할 수 있고, 사용 방식 또한 단순하다는 장점을 지닌다.



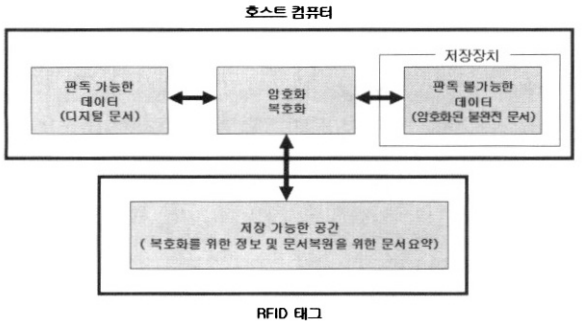
(그림 3) 소프트웨어 기반의 디지털 문서 보안 아키텍처

3. RFID를 이용한 디지털 문서 보안 아키텍처

3.1 RFID를 이용한 디지털 문서 보안 아키텍처

본 논문에서는 외부저장장치를 이용한 디지털 문서 보안 아키텍처와 소프트웨어를 이용한디지털 문서 보안 아키텍처를 결합함으로써 디지털 문서에 대한 안전성을 강화할 수 있는 RFID를 이용하는 디지털 문서 보안 아키텍처를 제시한다 RFID 태그는 외부저장장치로 이용되는 하드디스크나 메모리 스틱에 비해 소형화가 가능하고, 하드웨어에 대한 물리적인 충격에 강해 외부저장장치의 손실로 인한 정보의 손실을 최소화 할 수 있는 대안으로 활용이 가능하다. 또한, 데이터의 일부를 RFID 태그에 저장하는 것은 사용자 컴퓨터가 아닌 다른 외부에 저장함으로써 네트워크를 통한 데이터로의 불법적인 접근을 효율적으로 차단하여 보안성을 증대시킨다. 뿐만 아니라, 휴대성이 좋고, 사용하기 편리한 장점도 지닌다.

(그림 4)는 본 논문에서 제시하고 있는 디지털 문서 보안 아키텍처를 나타내고 있다.



(그림 4) RFID를 이용한 디지털 문서 보안 아키텍처

본 아키텍처상에서 디지털 문서는 원본 문서에서 추출해 낸 문서요약과 그로 인해 생성된 불완전 문서로 분리 된다. 문서요약은 원본 문서에서 일정량의 정보를 추출해 낸 것으로 RFID 태그에 저장된다. 이러한 문서요약의 추출은 외부저장장치를 활용하여 디지털 문서를 보호하기 위한 것으로, 일정 데이터를 네트워크와 독립된 공간에 저장함으로써 완전한 데이터의 노출을 방지하여 디지털 문서의 안전을 극대화한다. 즉, 데이터의 일부를 권한자가 휴대게 하여, 다른 비 권한자의 접근을 차단하고, 이를 통해 디지털 문서의 안전성을 증대시킨다. 그리고, 이러한 과정에서 생성된 불완전 문서는 사용자 패스워드를 바탕으로 암호화하여 보호한다.

이 과정에서, 호스트 컴퓨터 내에 저장되는 불완전 문서에 RFID 태그의 고유 번호와 같은 유효성 검증을 위한 정보들을 추가적으로 저장함으로써 복제나 분실에 대비할 수도 있다. 그러나, 궁극적으로 이러한 문제는 RFID에 대한 보안기술에서 고려될 사항이며, 본 논문에서는 RFID 기술의 하나의 활용방안으로써 RFID 기술을 디지털 문서의 보안에 적용하는 방식과 절차만을 다룬다. 즉, 디지털 문서 보안 아키텍처는 향후 RFID 보안기술의 발달과 RFID 태그 성능의 향상에 따라 더욱 강력함을 지니게 될 것이다.

3.2 문서 요약 추출

본 기법에서는 RFID 태그의 사용을 위해 문서 요약을 추출한다. 이것은 실제 원본 디지털 문서의 데이터 일부분을 추출하여 생성한 것으로 이 정보가 없는 한 원래의 문서는 복원될 수 없으며, 이러한 정보를 RFID 태그에 저장하는 것은 디지털 문서를 복원과정에서 RFID 태그가 반드시 제시되도록 하는 연결점을 제공한다.

문서 요약 정보는 디지털 문서를 구성하는 각 바이트의 특정 비트 값을 추출하여 생성되며, 추출한 후에는 원래의 비트 값을 변경하여, 원본 문서를 읽을 수 없도록 한다. 대상 비트 값은 추출 과정에서 임의로 선택되며, 이를 복원하기 위한 정보와 함께 RFID 태그 내에 저장된다. (그림 5)는 문서 요약을 추출하는 알고리즘이다.

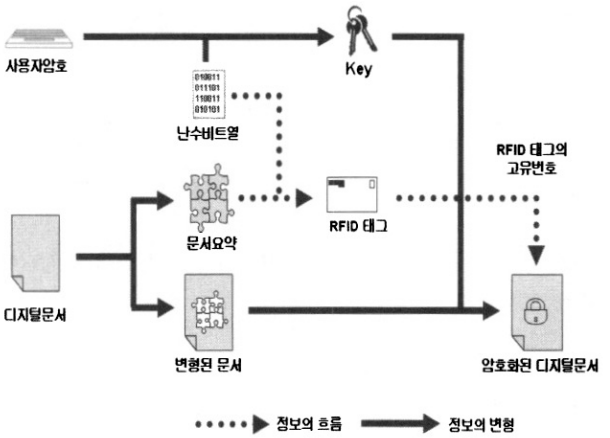
```
byte[] summraize(byte[] bytes, int n) {

        byte packedByte[];
        int index = 0;

        for each byte in bytes[]
          1. Get 1 bit from byte.
          2. Change the bit of the byte. ( 0 to 1, 1 to 0 )
          3. Save the bit to packedByte.
          4. if 8-bits are packed in packedByte[index], increse index.
        next

        return packedBytes;
}
```

(그림 5) 문서요약 추출 알고리즘

위 알고리즘에 따라 문서요약은 원본 문서 크기의 1/8정도로 추출된다. 이러한 크기는 실제 현재의 RFID 태그의 저장용량과 성능을 감안할 때, 합리적이지 않을 수 있지만, RFID 태그의 저장용량과 성능은 해마다 개선되고 있고, 앞서 언급한 바와 같이 본 논문에서는 이러한 태그 기술의 문제에 대해서는 논의하지 않도록 한다. 하지만, 알고리즘의 개선이나 추출된 문서요약을 압축하는 것과 같은 소프트웨어적인 방식으로써의 개선은 추후 연구를 통해 수행될 것이다.

3.3 디지털 문서의 암호화

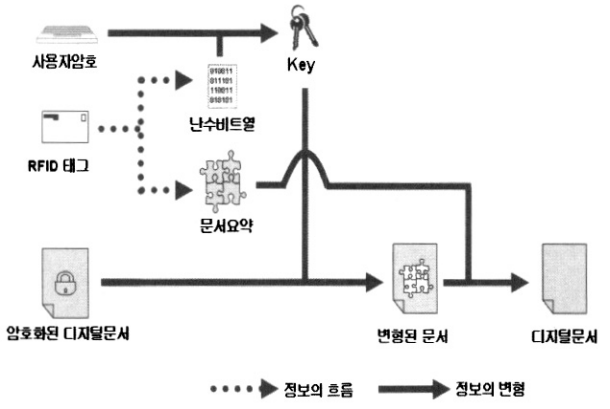
(그림 6)은 디지털 문서의 암호화 과정을 나타낸 것이다. 디지털 문서 암호화 과정에서는 우선 암호화 대상이 되는 문서가 입력이 되고, 그 후 가장 먼저 대상 문서의 문서 요약이 추출된다. 이 과정이 끝나면, 암호화를 위한 키를 생성하고, 키를 사용해 문서를 암호화한다. 그리고, 키를 생성하기 위한 난수비트열과 대상 문서의 문서 요약은 RFID 태그에 저장된다. 이렇게 복원정보를 사용자 컴퓨터 내부가 아닌 외부에 저장하는 것은 태그의 보유여부를 또 하나의 인증단계로 작용하게 하여, 보안성을 증대시킬 수 있다. 뿐만 아니라, 태그의 보유여부만 가지고도 조직이나 공유네트워크 상에서의 특정 문서에 대한 권한정책을 실현함으로써 보다 유연한 보안 정책을 지원할 수 있다.



(그림 6) 디지털 문서의 암호화 과정

3.4 디지털 문서의 복호화

암호화된 디지털 문서의 복호화 과정에서는 암호화된 문서를 선택한 후, 사용자 패스워드와 RFID 태그를 제시하면 태그의 유효성을 검사하고, 복원을 위한 키를 생성한다. 키가 생성되면 이를 사용하여 암호화된 문서를 해독하고, 마지막으로 문서 요약정보를 사용하여 원래의 문서를 복원한다. 이 과정은 (그림 7)에 나타나 있다.

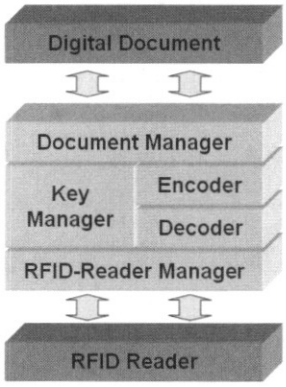


(그림 7) 암호화된 문서의 복호화 과정

4. RFID를 이용한 디지털 문서 보안 아키텍처 기반의 애플리케이션

4.1 애플리케이션 설계

앞서 제시한 아키텍처를 바탕으로 실제 동작 가능한 애플리케이션을 구현하였다. RFID를 이용한 디지털 문서 보안 애플리케이션은 디지털 문서의 암호화 및 복원과정 전반을 관리하는 Document Manager, 암호화 키를 생성 및 관리하는 Key Manager, 그리고 암호화와 복원을 담당하는 Encoder와 Decoder 및 RFID 리더를 관리하는 RFID-Reader Manager로 구성된다. (그림 8)은 RFID를 이용한 디지털 문서 보안 애플리케이션의 구조를 나타낸 것이다.



(그림 8) RFID를 이용한 디지털 문서 보안 애플리케이션의 구조

<표 1> 애플리케이션 구성 모듈

구성 요소	설 명
Document Manager	디지털 문서의 암호화와 복원과정을 관리한다. 문서의 암호화 과정에서는 문서에 대한 문서 요약을 추출하고, 문서의 복원 과정에서는 암호화된 문서와 문서 요약을 결합하여 원본 문서를 생성하는 일을 담당한다. 또한, RFID 태그의 고유번호를 암호화된 문서 내에 저장하여 태그의 유효성을 검증한다. 이 과정에서 좀더 신뢰성 있는 검증을 위해 MD5[14] 해싱 알고리즘을 사용하였다.
Key Manager	키 생성을 위한 난수 비트열을 생성하고, 사용자로부터 인증패스워드를 입력 받아 디지털 문서의 암호화 및 해독을 위한 키를 생성한다. 이 때, 난수 비트열은 암호화 과정에서만 생성되고, 복원과정에서는 인증패스워드와 RFID 태그내의 정보를 조합하여 키를 복원해 낸다
Encoder	Key Manager에 의해 생성된 키를 사용하여 사용자의 컴퓨터에 저장되어 있는 디지털 문서를 한다.
Decoder	Key Manager에 의해 복원된 키를 사용하여 사용자의 컴퓨터에 저장되어 있는 디지털 문서를 해독한다.
RFID-Reader Manager	RFID 태그정보를 읽고, 쓰기 위해 RFID 리더와 직접적으로 상호연동하며 관리한다.

Document Manager는 디지털 문서의 암호화 과정 및 복원 과정에 있어서 전반적인 관리 기능을 수행하며, 다른 클래스들은 각각의 기능을 수행하기 위한 메소드들로 구성되어 있다. 본 애플리케이션의 구현과정에서 RFID 태그의 유효성을 검증을 위해 RFID 태그의 고유번호를 암호화된 문서에 저장하여 검증하도록 하였으며 이 과정에서 MD5 해싱 알고

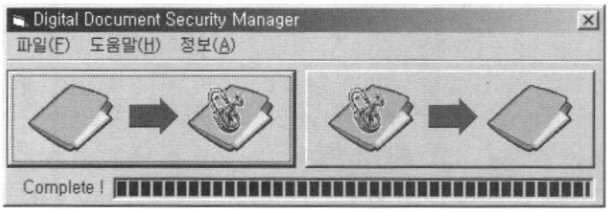
리즘이 사용되었다. 이러한 고려는 태그를 검증하기 위한 최소한의 절차로 보안성 향상을 위해 추가적인 방안이 도입될 수 있으며, 또한 해싱 알고리즘으로 사용된 MD5는 좀더 안전한 알고리즘으로 대체될 수 있다.

<표 1>은 애플리케이션을 구성하는 각 모듈의 기능을 정리해 놓은 것이다.

4.2 애플리케이션 구현

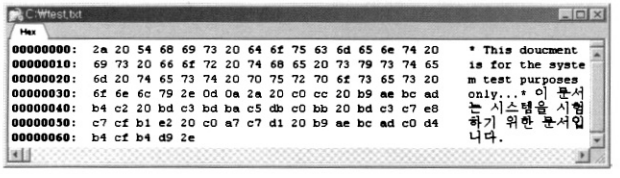
앞서 제시한 RFID기반 디지털 문서 보안 애플리케이션을 Microsoft Visual Basic 6.0을 사용하여 구현하였으며, Document Manager, Decoder, Encoder, Key Manager, RFID Reader-Manager의 5개의 클래스 모듈과 사용자 인터페이스로 구성하였다.

해당 애플리케이션은 문서 암호화 기능 및 복원 기능을 수행하며, 구현된 애플리케이션의 사용자 인터페이스는 (그림 9)에 나타나 있다.



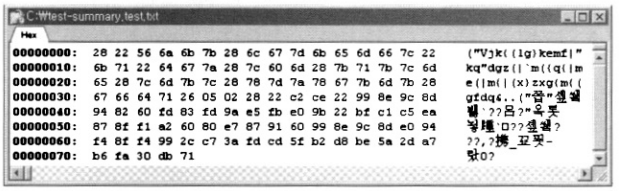
(그림 9) RFID 기반 디지털 문서 보안 애플리케이션의 사용자 인터페이스

구현된 애플리케이션으로 실제 디지털 문서의 암호화 및 복원과정을 수행하였다. 애플리케이션은 MS 워드 문서나 한글 문서 등 다양한 워드프로세스 문서나 액셀 파일 및 이미지 등 모든 디지털 문서에 대해 적용가능하나, 암호화 상태 및 복원 상태를 잘 살펴볼 수 있도록 (그림 10)에 나타난 일반 텍스트 문서를 대상으로 수행하였으며, 이 때 사용된 RFID 리더는 Inside Contactless 사의 M210-2G 모델이며[15], 사용된 RFID 태그 역시 Inside Contactless 사의 Pico Tag (2K bytes)이다[16].



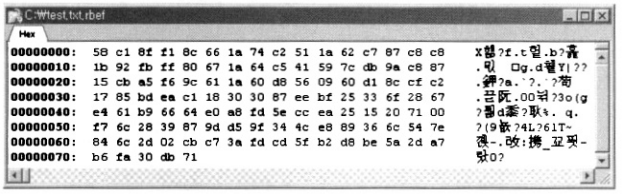
(그림 10) 애플리케이션 시험을 위한 문서

RFID기반 디지털 문서 보안 애플리케이션은 먼저 본래의 디지털 문서에서 문서요약을 추출하고 원본 문서를 변형시킨다. 이러한 과정에 의해, 사용자 패스워드만을 가지고는 원본 문서를 복원하는 것은 거의 불가능하게 된다. 즉, 사용자 패스워드만을 가지고 찾아낼 수 있는 문서는 오로지 문서요약 추출에 따라 변형된 문서이며, 이러한 변형된 문서는 올바르게 식별할 수 없는 상태로 존재하므로, 사용자 패스워드가 정확한 것인지조차 알 수 없기 때문이다. (그림 11)은 문서요약 추출에 따라 변형된 문서를 보여주고 있다. 본 구현에서는 이 과정에서 태그의 검증을 위해 태그의 고유번호가 삽입되므로, 원본 문서와의 길이가 차이가 나게 된다.



(그림 11) 문서요약 추출로 인해 변형된 디지털 문서

본 애플리케이션에서는 위와 같이 변형된 문서를 사용자 패스워드와 난수비트열로 결합한 키에 의해 단순 XOR 암호화 알고리즘을 사용해 암호화하였다. 여기서 제시된 구현은 단순히 디지털 문서 보안 아키텍처의 실제를 보여주기 위한 구현이며, 이 아키텍처를 적용함에 있어서 사용되는 암호화 알고리즘은 신뢰성이 높은 다른 알고리즘으로 대체될 수 있다. (그림 12)는 최종적으로 암호화된 디지털 문서를 보여주고 있으며, (그림 13)은 본 애플리케이션에서 사용한 암호화 알고리즘을 보여주고 있다.



(그림 12) 암호화된 디지털 문서

본 구현에서는 사용된 암호화 알고리즘은 사용자 패스워드를 2배 길이로 확장하기 위해서는 원래의 패스워드를 역순으로 바꾼 사용자 패스워드와 연결하는 방법을 사용하였으며, 이렇게 확장된 사용자 패스워드와 난수비트열을 XOR 연산하여 키를 생성하였다. 그리고 이렇게 생성된 키와 원래의 데이터를 XOR 연산함으로써 데이터를 암호화하였다. 앞서도 언급하였지만, 이러한 데이터 암호화 알고리즘은 보다 신뢰성 높은 암호화 알고리즘으로 대체함으로써, 보안성을 증대시킬 수 있으며, 본 구현에서는 단순한 암호화 기법들을 사용하였다.

```
void Encrypt(byte[] bytes, string pwd) {

    1. Extend the length of the pwd by two times of the length.
       ( ex. 11011100001110100101100 ->
         1101110000111010010111001100010110100011110000100 )

    2. Generate the random bit string with length of the pwd.
       ( ex. 01011011010100110100110110011001011001011010101 )

    3. Generate the key
       ( ex. 10000111011010010001000101011100110001100110101001 )

    4. Encrypt the bytes
       ( bytes XOR the key )

}
```

(그림 13) 본 구현에서 사용된 암호화 알고리즘

(그림 14)는 본 과정에서 태그 내에 저장된 정보를 보여주고 있다.

Block Description	Hexadecimal	ASCII
Serial Number	$E0$19$22$00$01$00FFFF	?" r ÿÿ
Configuration Block	FFFFFFFF$F9$1FFFAD	ÿÿÿ?ÿ?ÿÿ
Application Issuer Area	FFFFFFFFFFFFFFFF	ÿÿÿÿ 0
Block 3	$00$20$30$62$6A$25$70$66	bj %pf
Block 4	$2C$2A$22$64$72$70$62$70	,*"drpbp
Block 5	$78$7F$00$24$B4$48$B7$DB	x□ $´H·Þ
Block 6	BFBD$B1$B0$B4$BBBAD0	¿½±°´»°Ð
Block 7	$B2$B4$0E$77$D5$F1$67$5A	²´ wÕñgZ
Block 8	$74$80$C2$75DC5C$2E$76	t €Âu?. vS
Block 9	$53$00$00$00$00$00$00$00	

(그림 14) RFID 태그에 저장된 정보

RFID 태그 내의 정보는 TAG 고유 정보와 데이터 블록으로 나누어져 있으며, 디지털 문서의 복원 정보는 Block 3 에서부터 저장되어 있다. Block 3의 앞의 4바이트는 복원정보의 길이를 담고 있으며, 그 뒤로 문서 요약과 함께 난수 비트열이 저장되어 있다.

5. 평 가

5.1 기존 아키텍처들과의 비교평가

<표 2>는 각각의 보안 아키텍처들간의 비교 분석 표이다. 인터페이스의 범용성은 암호화 매체에 대한 하드웨어적인 인터페이스에 대한 범용성이며, 아직까지 개인용 PC에 대한 편리한 RFID 인식 카드가 제공되지 않고 있는 만큼, RFID를 기반으로 할 경우 인터페이스 범용성이 다소 떨어진다고 할 수 있다. 하지만, 이러한 것은 조직이나 기업 내부적으로 문서의 보호에 있어서는 오히려 이점이 될 수 있다. 공유네트워크상에서의 보안은 해당문서가 조직이나 기업 내에서 공유되어 있을 때, 문서의 보안성을 유지하는 것을 의미한다. 이것은, 조직내의 중요문서가 권한을 가진 관리자나 상급자와 같은 특정 그룹에 의해 공유되도록 제한될 때 필요로 하게 되는데, 외부 저장장치를 사용하는 경우 직접적으로 문서에 대한 보안기능을 수행하기 보다는 메모리 영역에 대한 보안기능을 수행하기 때문에, 해당 문서를 네트워크 상에서 공유하면 보안성을 보장하지 못하게 된다. RFID의 경우에는, 이 경우 복제 태그가 이용될 수 있도록 하는 보안 절차가 필요하며, 태그의 보안성을 높이기 위한 추가적인 조치가 필요하다.

디지털 문서의 보안에 있어서 암호화된 데이터의 기밀성도 고려되었다. 이것은, 암호화를 거친 디지털 문서일지라도, 외부적으로 완전하게 노출되어 있다면 공격자에 의해 해독을 위한 기반을 제공해 주는 계기가 될 수 있으므로 하나의 비교항목이 될 수 있다. 이러한 데이터의 기밀성을 보장하기 위해서는 다양한 접근 경로를 차단해야 하는데 그것은 네트워크가 아닌 오프라인 상에 데이터를 보관함으로써 가능하다.

5.2 아키텍처의 활용 방안

본 논문에서 제시하고 있는 디지털 문서 보안 아키텍처는 공유네트워크를 사용하는 조직에서 내부 문서를 관리하기 위한 방안으로 활용될 수 있다. 이 경우, 조직원들의 권한이나 직위에 따라 RFID 태그를 관리함으로써 특정 문서에 대해 권한을 가진 사람만이 접근 가능하도록 함으로써, 디지털 문서를 신뢰성 있고, 안전한 방식으로 교환 및 공유 가능하다. 이 경우에는 RFID 태그에 권한 정보를 담기 위한 별도의 메커니즘이 추가적으로 확장되어야 한다. 그리고 상황에 따라서는, 태그 내에 저장되는 정보 또한 제한적으로 조정될 수 있다. 이러한 모델에서, 향후 RFID 태그의 보안 기술의 발전에 따라, 디지털 문서의 접근을 위해 사용되는 패스워드는 RFID 태그로 완전히 대체될 수 있으며, 이 경우, 사용자가 별도의 패스워드를 입력해야 하는 번거로움 없이 디지털 문서를 접근할 수 있는 보안 시스템의 구축이 가능하다.

또한, 향후 RFID 태그의 초소형화 및 용량 문제가 해결된다면, 디지털 저작권 관리에도 활용이 가능하다. 디지털 제작

〈표 2〉 디지털 문서 보안 기술들과의 비교

비교기준 \ 아키텍처	외부저장장치를 이용한 보안 아키텍처	소프트웨어 기반의 보안 아키텍처	RFID를 이용한 보안 아키텍처	
인증방식	1단계 (사용자암호)	1단계 (사용자암호)	2단계 (태그+사용자암호)	• 이중 인증 방식을 통한 보안성의 증대
암호화 매체	SW + HW	SW	SW + HW	• 기존의 아키텍처들을 결합함으로써 양단간의 장점을 결합하고 단점을 보완
암호화된 데이터의 기밀성	높음	낮음	높음	• 암호화된 정보를 전부 외부에 노출시키지 않으므로 기밀성이 높음
암호화 매체의 안전성	낮음	높음	높음	• RFID의 경우 소형화가 가능하고 복잡한 내부회로를 가지지 않으므로 물리적으로 비교적 안전함
공유네트워크상에서의 보안	보장하지 않음	보장함	보장함	• 암호화된 데이터를 모두 네트워크를 통해 전송하지 않으므로 네트워크상에서도 안전성을 보장 • 아키텍처의 활용성이 높음
인터페이스의 범용성	높음	높음	낮음	• 인터페이스의 보급도가 낮아 별도의 장비가 필요 • 조직에서는 오히려 인터페이스의 기밀성으로 인한 보안성 및 안전성 증대를 가져올 수 있음

물 제작회사에서 제작되는 디지털 저작물은 이를 담고 있는 저장매체에 부착된 초소형 RFID 태그에 의해 유효성이 결정되도록 하여, 유통될 수 있다. 이 경우, 디지털 저작물은 RFID 태그의 정보가 없는 한 접근이 불가능하며, 이러한 태그가 없이 불법으로 추출되어 공유되거나 전송되는 디지털 저작물은 유효성이 없어 사용될 수 없으므로, 디지털 저작물의 저작권을 보호할 수 있다. 이 경우에도 역시, RFID 태그 내에 저장되는 정보는 제한적으로 조정될 수 있으며, 필요시 아키텍처에서 디지털 저작물을 위한 별도의 응용 애플리케이션 모듈이 추가될 수 있다.

6. 결론 및 향후 과제

본 논문에서는, RFID 기술의 응용 방안으로써 기존의 디지털 문서 보안 방법의 단점을 보완하기 위한 RFID 태그를 이용한 디지털 문서 보안 아키텍처를 제안하고 이를 바탕으로 한 애플리케이션을 구현하여 시험하였다. 여기서 제시된 아키텍처는, 소형화가 가능하고 외부의 물리적 충격에 따른 하드웨어 파손으로 인한 정보 손실 가능성이 적은 RFID 태그를 디지털 문서의 암호화 및 복원을 위한 정보의 저장소로 사용함으로써 하드웨어적인 안정성을 보장하고, 동시에 소프트웨어만을 통하여 암호화하지 않음으로써 암호화 이후의 해독이나 공격에 대해서도 보다 향상된 안전성을 보장한다. 즉, 이것은 기존 아키텍처들의 장점을 결합하고 단점을 보완하는 것으로, 디지털 문서의 보안을 위한 하나의 대안이 될 수 있으며, RFID 기술의 발전과 더불어 다양하게 활용 가능하다.

앞으로 향후 연구에서는, 본 아키텍처에서의 보안성 증대 및 제약사항의 극복을 위해 대용량의 문서 암호화를 위한 RFID 태그의 문서 요약 추출 알고리즘 개선에 대한 연구와 RFID 리더와 태그간의 유효성 검증을 위한 현실적인 대안에 대하여 연구를 진행할 것이다.

참 고 문 헌

[1] 한국 인터넷 침해 사고 대응 지원 센터, "2003년 12월 해킹바이러스 통계 및 분석월보," http://www.krcert.or.kr, 2003.

[2] 한국 인터넷 침해 사고 대응 지원 센터, "2002년 12월 해킹 통계 보고서," http://www.krcert.or.kr, 2002.

[3] CSI (Computer Security Institute), "2004 CSI/FBI Computer Crime and Security Survey," http://www.GoCSI.com, 2004.

[4] Steven Shepard, "RFID(McGraw-Hill Networking Professional)," McGraw-Hill, 2004.

[5] 표철식, 채종석, "RFID 기술 및 표준화 동향," TTA Journal, 2004.

[6] 권수갑, "RFID 개념과 동향," 한국전자부품연구원, 2004.

[7] 김광조, "RFID/USN 정보보호 기술," TTA Journal, 2004.

[8] Weis, S.A, "RFID Privacy Workshop," Security & Privacy Magazine, IEEE, Volume 2, Issue 2, Mar-Apr 2004 Page(s): 48-50, 2004.

[9] Want, R., "Enabling ubiquitous sensing with RFID," Computer Volume 37, Issue 4, April, 2004, Page(s): 84-86, 2004.

[10] Sangani, K., "RFID sees all," IEE Review, Volume 50, Issue 4, April, 2004, Page(s): 22-24, 2004.

[11] IDC, "IDC, Worldwide Flash Memory Card and USB Flash Drive Forecast and Analysis, 2003~2007"

[12] Microsoft Office Online, "Protect a document from unauthorized changes," http://office.microsoft.com/en-us/assistance/HP010446741033.aspx

[13] www.winzip.com, "Secure your documents with 128- or 256-bit AES encryption," http://www.winzip.com/powertips.htm #encrypt

[14] R. Rivest, "The Message-Digest Algorithm," IETF RFC 1321, http://www.ietf.org/rfc/rfc1321.txt?number=1321, 1992.

[15] Inside Technology, "M210-2G Proximity Coupler," http://www.insidecontactless.com/pdf/M210_2G.PDF

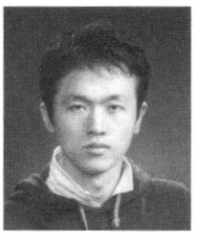
[16] Inside Technology, "PicoTagTM: ISO 15693 Memory Chips," http://www.insidecontactless.com/pdf/PicoTag.pdf

[17] Ollivier, M.M., "RFID-a new solution technology for security problems," Security and Detection, European Convention on,16-18 May, 1995, Page(s): 234-238, 1995

[18] Len Bass, Paul Clements, Rick Kazman, Software Architecture in Practice, Addison Wesley, 2003.

[19] Lilianan Dobrica, Eila Niemela, "A Survey on Software Architecture Analysis Methods," IEEE Transactions on Software Engineering, Vol.28, No.7, pp.638-653, July, 2002.

[20] R.Kazman, M.Klein, M.Barbacci, H.Lipson, T.Longstaff, and S. J. Carriere, "The Architecture Tradeoff Analysis Method," Proc. Fourth Int'l Conf. Eng. Of Complex Computer Systems (ICECCS '98), pp.68-78, Aug., 1998.



최 재 현

e-mail : uniker80@empal.com

2004년 숭실대학교 컴퓨터학부(공학사)

2004년~현재 숭실대학교 대학원 컴퓨터학과 석사과정

관심분야 : 임베디드 시스템, RFID/USN, 유비쿼터스 컴퓨팅, 소프트웨어 테스팅, Persistent Software Attributes

이 우 진

e-mail : bluewj@empal.com

2000년 숭실대학교 컴퓨터학부(공학사)

2002년 숭실대학교 대학원 컴퓨터학과(공학석사)

2002년~현재 숭실대학교 대학원 컴퓨터학과 박사과정

관심분야 : 웹 어플리케이션, 웹서비스, 유비쿼터스 컴퓨팅, 모바일 컴퓨팅, 홈네트워크, 임베디드 시스템

정 기 원

e-mail : chong@ssu.ac.kr

1967년 서울대학교 전기공학과(공학사)

1981년 미국 알라바마주립대(헌츠빌) 전산학과 석사

1983년 미국 텍사스주립대(알링턴) 전산학과 박사

1971년~1975년 한국과학기술연구소 연구원

1975년~1990년 국방과학연구소 책임연구원

2002년~2003년 한국전자거래학회 회장

1990년~현재 숭실대학교 컴퓨터학부 교수

2001년~현재 IT감리포럼 회장

관심분야 : 소프트웨어공학, 소프트웨어프로세스, 정보시스템감리, 전자거래(CALS/EC), 유비쿼터스 컴퓨팅