PC의 개인정보보호 취약점 분석과 정량화된 보안진단 연구

서미숙* · 박대우*

*호서대학교 벤처전문대학원

A Study on Quantitative Security Assessment after Privacy Vulnerability Analysis of PC

Mi-Sook Seo* · Dea-Woo Park*

*Hoseo Graduate School of Venture

E-mail : msseo@smsinfo.co.kr · prof_pdw@naver.com

요 약

개인정보보호법이 2012년 3월 30일 시행을 하였다. 일반적으로 개인정보를 관리하는 DB서버는 보안을 강화하기 위한 보안시스템을 갖추고 있으나, PC에서는 개인정보보호를 위한 취약점 분석과 보안성 자가진단에 대한 연구가 필요하다. 본 논문에서는 PC에서 개인정보보호 관련 정보를 검색하고, 암호화하여 보안성을 강화하고 삭제대상 파일은 복구 불가능하게 삭제한다. PC에서 검색된 취약성 분석은 사용자계정점검, 공유폴더점검, 서비스 방화벽 점검, 화면보호기, 자동패치업데이트를 점검한다. 점검 후에 취약점에 관한 정량화 분석과 표현을 통해, 보안성 강화를 위한 점검리스트을 작성해서 보여주고, PC보안 관리를 반자동화하여 서버에서 관리하여 작동시킨다. 본 논문을 통해 PC개인정보보호와 PC보안강화로 국민의 경제적 피해와 고충을 줄이는데 기여할 것이다.

ABSTRACT

Privacy Protection Act of 30 March 2012 was performed. In general, personal information management to enhance security in the DB server has a security system but, PC for the protection of the privacy and security vulnerability analysis is needed to research on self-diagnosis. In this paper, from a PC to search information relating to privacy and enhance security by encrypting and for delete file delete recovery impossible. In pc found vulnerability analysis is Check user accounts, Checking shared folders ,Services firewall check, Screen savers, Automatic patch update Is checked. After the analysis and quantification of the vulnerability checks through the expression, enhanced security by creating a checklist for the show, PC security management, server management by semi-hwahayeo activates. In this paper the PC privacy and PC security enhancements a economic damage and of the and Will contribute to reduce complaints.

키워드

PC vulnerabilities, vulnerability analysis, information security, security checks, privacy

Ⅰ. 서 론

최근 해킹 및 개인정보 유출로 인한 개인 컴퓨터를 보호하기 위한 다양한 보호조치들을 하고 있다. 특히 PC보안(내부정보 유출방지)은 최근 서버 이외에 PC의 해킹사고가 증가하고 있고 PC보안사고 대부분이 내부자에 의한 자료 유출 및 위·변조 등의 피해사고로 그 필요성이 커지고 있다.

하지만 PC보안을 위해 설정해야 하는 항목들이 사용자들이 이해하기 어려운 면이 많으며 인식 또한 부족하다. Windows 운영체제를 사용하는 개인용 컴퓨터는 다양한 취약성에 노출되면서 이를 이용한 공격 패턴 또한 다양하다. 개인정보가 포함된 파일의 경우도 활용(각종 명부 등) 후 저장된 위치를 기억하지 못하여 그대로 방치 되거나, 자료공유시스템 등 웹사이트를 통해 열람(접근)된 개인정보파일이 개인 PC내 임시 파일로

PC의 하드디스크에 저장된 상태로 방치가 되기도 한다[1].

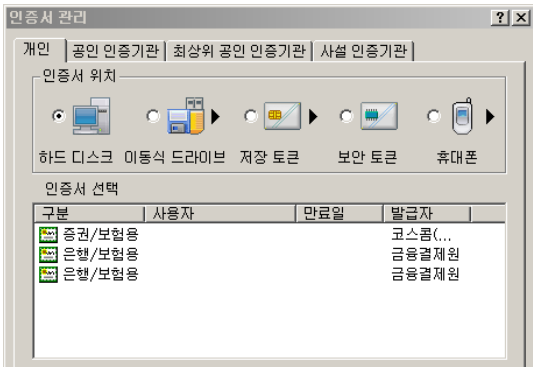

그림 1. PC의 저장된 개인정보파일

이에 본 논문은 Windows 시스템의 각종 취약점을 점검하여 반자동 조치와 함께 개인정보가 포함된 파일들을 검색하여 암호화 및 완전삭제 할 뿐 아니라 점검된 자료를 점수화하여 보완 및 관리 할 수 있도록 하며, 점검된 자료를 관리자 서버로 전송하여 전체 및 부서나 기관별로 통계화 할 수 있도록 하는 기술과 방안에 대한 연구가 필요하다.

Ⅱ. 관련연구

2.1 개인정보보호법 제정과 시행

개인정보보호법은 2011년 3월 29일 제정을 하여 2012년 3월 30일부터 시행이 되었다. 이 법은 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정함을 목적으로 한다.

개인정보보호법에 따르면 개인정보처리자는 개인정보의 안전환 관리를 위한 기술적·관리적·물리적 보호조치 등을 철저하게 수행해야 한다. 개인정보보호법의 내용의 일부 중 개인정보처리자가 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다. 개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 하여야 한다.

1) 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제

2) 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 파쇄 또는 소각

2.2 개인정보의 기술적·관리적 보호조치에 관한 사항

제21조(고유식별정보의 안전성 확보 조치) 법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조를 준용한다. 이 경우 "법 제29조"는 "법 제24조제3항"으로, "개인정보"는 "고유식별정보"로 본다.

제30조(개인정보의 안전성 확보 조치)

① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

1) 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행

2) 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

3) 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치

4) 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치

5) 개인정보에 대한 보안프로그램의 설치 및 갱신

6) 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

② 행정안전부장관은 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 행정안전부장관이 정하여 고시한다. 가 포함되어 있다[2].

2.3 PC 보안

일반적으로 기업 및 개인이 소유하고 있는 컴퓨터 단말기(서버) 자체 또는 컴퓨터 단말기(서버)내의 기본적인 자원(운영체제)을 보호하기 위한 총체적인 보안 기술을 말한다. PC보안 적용법위는 컴퓨터 단말기에 대한 하드웨어 보안 및 소프트웨어 보안을 모두 포함한다[3].

2.4 취약성 분석

PC의 취약점을 사용자계정 점검, 네트워크 및 공유폴더 점검, 서비스 및 방화벽 점검, 화면보호기 점검, 자동업데이트의 5가지 형태로 분석을 한다[4].

Ⅲ. PC개인정보의 검색, 암호화, 삭제

3.1 PC개인정보의 검색

PC에 개인정보가 포함된 파일들을 열지 않고도 주민등록번호, 외국인등록번호, 면허 번호, 전화번호, 여권번호, 사업자등록번호, 계좌번호, 이메일, 신용카드, 주소, 새주소 등 중요정보가 포함된 패턴으로 검색 하여야 하며, TXT, PDF, TIF, RTF, PST, EML, MS Office 문서, 한글문서, 아웃룩 문서 등 다양한 종류의 전자문서를 검색할 수 있어

야 한다. 또한 압축파일 (zip, gzip, alzip, bzip, 7Z, BZ2, rar, tar), 다단계 압축파일에서 검색, 파일 내의 OLE 객체에 포함된 개인정보, 위·변조된 확장자 및 숨김 속성 파일/폴더에 대한 검색이 지원되어야 한다.

3.2 PC개인정보의 암호화

PC에 저장된 개인정보 파일들을 검색하여 국가보안기술연구소(NSRI)주도로 개발한 국가 암호화 알고리즘으로 암호화 한다.

ARIA의 주요 특성은 다음과 같다.

* 블록 크기 : 128비트(바이트 기준 16바이트)
* 키 크기 : 128/192/256비트(AES와 동일 규격)
* 전체 구조 : Involutional Substitution-Permutation Network
* 라운드 수 : 12/14/16(키 크기에 따라 결정)

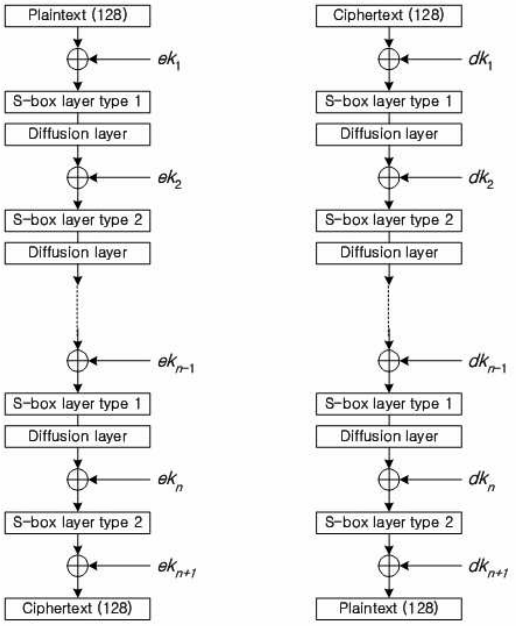

그림 2. SP-Network를 이용한 암호화 라운드

3.3 PC개인정보의 완전삭제

윈도우 파일시스템에서 파일은 크게 파일 데이터와 메타데이터로 나뉘어져 저장되고 관리된다.

파일데이터는 파일의 실제 데이터를 의미하며 메타데이터는 파일 이름, 파일 크기, 실행 권한, 파일데이터가 저장된 클러스터 등의 부가적인 정보를 의미한다.

사용자가 파일을 삭제하거나 포맷을 하면 메타데이터의 일부는 삭제가 되지만 파일데이터는 전혀 손상되지 않는다.

파일을 삭제할 경우, 파일데이터와 일부 메타데이터(파일명, 파일크기)가 초기화되어 복구가 불가능해지도록 완전삭제를 한다.

아래와 같이 파일이 저장되어있는 상황을 예로 들어 삭제방법을 살펴보자.(size 뒤에 있는 05는 파일이 저장된 클러스터의 주소이다.)

FAT1	FAT2	Directory		clusters	
11100100	11100100	filename, size, 05	···	filedata	···

그림 2. 파일 삭제 방법

ㄱ. 파일데이터가 저장된 클러스터에 데이터를 설정된 횟수와 방법에 따라 덮어쓴다.(1회시 랜덤 - 0x00 - 0xFF 값으로 3회 덮어쓰며 빠른 쓰기 동작 시 1회시 랜덤 값으로 1회 덮어쓴다.)

FAT1	FAT2	Directory		clusters	
11100100	11100100	filename, size, 05	···	**쓰레기값**	···

그림 3. 파일명 초기화

ㄴ. 파일명을 초기화한다.

FAT1	FAT2	Directory		clusters	
11100100	11100100	_____, size, 05	···	쓰레기값	···

그림 4. 파일명 초기화

ㄷ. 파일크기를 초기화한다.

FAT1	FAT2	Directory		clusters	
11100100	11100100	_____, 0byte,05	···	쓰레기값	···

그림 5. 파일크기 초기화

ㄹ. 파일을 삭제한다.

FAT1	FAT2	Directory		clusters	
11100000	11100000	_____, 0byte, 05	···	쓰레기값	···

그림 6. 파일 삭제

Ⅳ. PC의 취약점 분석 및 정량화

PC의 windows의 운영체제의 전반적인 취약점을 다음과 같은 항목들을 분석하고 점검하여 정량화 하여 관리 할 수 있도록 개발한다.

4.1 사용자 계정점검 및 정량화

* Guest 계정관리 불필요한 Guest 계정의 사용을 제한하고 있는지, 불특정 다수의 접근이 필요할 경우 Guest가 아닌 일반 사용자 계정을 생성해 사용하는지 점검한다.
* SAM 파일 접근 통계

계정에 대한 패스워드가 암호화된 형태로 보관되는 SAM파일에 대한 시스템운용자만이 접근 가

능한지를 점검한다.

* 패스워드 최소 길이 정책 점검 설정

사용자의 최소 암호 길이 설정이 적용 되어 있는지 점검한다.

* 패스워드 최대 사용기간 정책 점검 설정

사용자의 암호 사용기간이 설정 되어 있는지 점검한다.

* 사용자 최근암호 기억(최근 패스워드 기억정책 점검)

패스워드 변경 직후 이전 패스워드를 재사용하는 것을 방지하기 위하여 패스워드 최근암호기억 설정이 되어 있는지 점검한다.

* 패스워드 만료 설정 점검

현재 로그온 사용자의 "패스워드 사용 기간 제한 없음"이 설정 되어 있는 지 점검한다.

* TrivialPassword (로그온 패스워드 점검)

패스워드가 없거나, 사용자 ID와 동일 또는 유추가 용이한 쉬운 패스워드를 사용하고 있는지 점검하여 정량화 하여 관리한다.

4.2 공유폴더 점검 및 정량화

* 관리용 공유 폴더 설정 점검

관리용 공유 폴더가 설정되어 있는지 점검

* 사용자 공유 폴더 설정 점검한다.

사용자가 생성한 공유 폴더가 설정되어 있는지 점검 하여 정량화 하여 관리한다.

4.3 서비스방화벽에서 점검 및 정량화

* Alert 서비스 점검

Alert 서비스는 연결된 다른 컴퓨터에 관리 경고 메시지를 보내는 서비스를 점검한다.

* Telnet 보안 설정(서비스 사용안함)

Telnet 서비스에 대해 NTLM 인증을 사용하는지, ID/PASSWORD를 직접 입력하여 인증을 수행하고 있는지 등의 보안설정을 점검

* Computer Browser 서비스 점검한다.

네트워크에 있는 모든 컴퓨터의 목록을 갱신하고 관리하며 이 목록을 브라우저로 저장된 컴퓨터에 제공하는 서비스를 점검한다.

* Fast User Switching · Compatibility 서비스 점검한다.

여러 사람이 공동으로 사용하는 PC에서 PC를 이용하던 이용자가 로그오프하지 않은 채 다른 사용자가 로그온하여 PC를 사용할 수 있게 하는 서비스를 점검한다.

* Messenger 서비스 점검

네트워크상에서 메시지를 전달하는 기능을 하는 서비스를 점검한다.

* Netmeeting Remote Desktop Sharing 서비스 점검

자신의 컴퓨터에 원격으로 접근할 수 있도록 허용하고 다른 컴퓨터와 바탕 화면 원격 공유를 사용할 수 있게 하는 서비스 점검한다.

* 방화벽 설정 점검

자신의 컴퓨터에 외부접근을 통제하는 방화벽이 설정되어 있는지 점검한다.

4.4 화면보호기

* 자동 로그온 점검

현재 로그온 한 사용자가 패스워드의 입력 없이 자동으로 로그온 하도록 설정되어 있는 지 점검한다.

* 화면 보호기 활성화 설정 점검

화면보호기가 동작하도록 설정되어 있는지 점검

* 화면 보호기 자동실행 설정 점검한다.

화면보호기의 대기시간이 5분 이내인지 점검

* 화면 보호기 화면잠금 설정 점검

화면보호기가 패스워드로 보호되는지 점검한다.

4.5 보안패치 자동업데이트

* 백신 프로그램의 설치 여부 점검한다.

* 백신 프로그램이 실행되고 있는지 여부 점검한다.

* 백신 프로그램의 엔진이 항상 최신버전을 유지할 수 있도록 주기적으로 업데이트 하고 있는지 확인 점검한다.

* 운영체제의 자동업데이트 설정 여부를 점검한다.

Ⅴ. PC개인정보 취약점 보안관리

5.1 취약점 보안관리 내용

취약점 진단, 개인정보 진단 결과를 진단점수/항목별 전체점수로 사용자에게 보여주며 취약점이 있는 경우 자동수정 버튼의 클릭으로 수정하며, 개인정보 검색결과를 암호화 버튼으로 암호화하여 관리를 한다.

5.2 취약점 보안 자동화 작동

위의 취약점들을 모두 진단하여 자동으로 작동을 하며 아울러 검색된 개인정보 파일을 자동암호화를 하여 안전하게 관리하도록 한다.

Ⅵ. 결론

기업의 중요정보 유출 및 개인정보 유출 사고가 증가하고 개인정보보호법 시행 등 정보보안의 중요성은 계속 증가하고 있다. 이러한 유출사고는 PC보안의 설정 및 PC의 보안패치, 개인정보 관리를 통하여 PC의 보안 강화와 정보유출을 최소화 할 수 있다.

본 논문에서는 PC의 취약점을 자동으로 분석하고 점검하여 사용자가 요구하는 보안 수준을 유지하고 반자동 수정을 하여 조취를 취할 수 있도록 하며 개인정보를 검색하여 검색된 개인정보

파일을 안전하게 암호화 또는 불필요하거나 사용 기간이 지난 개인정보파일을 복구 할 수 없도록 영구삭제를 하여 PC를 다양한 위험으로부터 보호하여 취약점을 제거하며 파일을 관리 할 수 있도록 연구 개발하였다.

향후 연구로는 PC보안이나 취약점 제거에 대한 스크롤머신과 셋팅 자동업데이트에 대한 연구가 필요하다.

참고문헌

[1] 행정안전부, "개인정보의 안전성 확보조치 기준 및 해설서", 2011년 9월.

[2] 개인정보의 기술적·관리적 보호조치, http://www.law.go.kr/법령/개인정보보호법(10465), 2011년 3월.

[3] 박병연, 양종원, 서창호, "Windows 기반의 PC 보안 정책 관리 및 취약성 점검을 위한 시스템 설계 및 구현," 한국정보보호학회, 정보보호학회논문지, 제18권 제1호, pp. 23-30, 2008년 2월.

[4] 남원희, 박대우, "입법기관의 보안강화를 위한 Cloud 네트워크 분석 및 보안 시스템 연구," 한국해양정보통신학회논문지, 제15권 제6호, pp.1320-1326, 2011년 6월.