디지털 복합기의 잔여정보 완전삭제 기능 시험/평가방법론 개발

김찬일*, 이광우***, 조영준***, 김동근**, 심원태*, 김승주***
*한국정보보호진흥원 평가기획팀, **삼성전자 프린터사업부 S/W개발 1그룹
***성균관대학교 전자전기컴퓨터공학과
*e-mail : chankim, wtsim@kisa.or.kr, **e-mail : dongk70.kim@samsung.com
***e-mail : kwlee, yjcho, skim@security.re.kr

Development Testing/Evaluating Method about Residual Data Protection Technology based on the MFP

Chan-Il Kim*, Kwang-Woo Lee***, Young-Jun Cho***, Dong-Keun Kim***, Wan-Tae Sim*
Seung-Joo Kim***
*Policy Support Team Korea Information Security Agency
**SW R&D Group1 Digital Printing Division, SAMSUNG ELECTRONICS CO., LTD.
***Dept of Electrical and Computer Engineering, Sungkyunkwan University

요 약

현재 기업 및 공공기관에서는 산업기술 유출 방지를 위해 잔여데이터 완전삭제 등 보안기능이 구현된 디지털 복합기를 사용하고 있다. 이에 따라 국제적으로 특히 일본 평가기관들 중심으로 공통평가기준으로 평가·인증 많이 받고 있다. 그러나 국내에서는 MFP에 대한 인식과 평가 노하우(know-how)의 부족하여 평가·인증 방법에 미비한 상태이다, 본 논문에서는 MFP의 핵심 중요 기술인 잔여정보 완전삭제 기능을 공통평가기준으로 평가할 수 있는 국내 시험/평가 방법론을 제시하고자 한다.

1. 서론

현재 대다수의 기업 및 공공기관에서는 업무의 효율성 증대와 경비 절감을 위해 프린터에 복사기, 스캐너, 팩스 등의 기능을 통합한 디지털 복합기(이하 MFP, Multi-Function Peripheral로 한다)를 사용하고 있다. 최근에는 산업기술 유출 방지를 위해서 MFP에 중요 데이터 유출 방지를 위한 식별 및 인증, 잔여데이터 완전삭제, 파일접근제어, 암호통신 등 보안기능을 구현하고 있다.

이에 따라 MFP의 보안기능 평가·인증이 국제적으로 통용되는 공통평가기준(CC, Common Criteria)으로 일본 평가기관들을 중심으로 활발히 진행되고 있다. 국내에서는 MFP 내의 하드디스크 데이터의 완전삭제 기능에 대한 보안 적합성 검증을 의무화하고 있지만 개발자 및 평가자 측면에서 MFP에 대한 인식과 평가 노하우가 부족하여 평가·인증 방법에 미비한 상태이다. 본 논문에서는 MFP의 핵심 중요 기술인 잔여정보 완전삭제 기능을 공통평가기준으로 평가할 수 있는 국내 시험/평가방법론을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 MFP의 보안기능과 3장에서는 공통평가기준으로 평가받은 현황을 소개하고 4장에서는 잔여정보 보호기술을 소개한다. 그리고 5장과 6장에서는 완전 삭제 기능 시험/평가 방법론을 제시하고 7장에서 제시된 방법론으로 시험/평가한 결과를 요약정리하고 마지막으로 결론을 맺는다.

2. MFP의 보안기능

국내·외의 MFP에 포함되어 있는 일반적인 기능으로는 인쇄, 복사, 스캔, 팩스 기능 등이 있고 보안기능이 탑재된 MFP에서의 일반적인 보안기능은 식별 및 인증, 저장장치 완전삭제, 그리고 데이터 암호화 등이 있고 <표 1>에서 국내외 MFP 개발업체별 보안기능 구현 여부를 조사하였다.

<표 1> MFP 개발업체별 보안기능

MFP 개발업체	식별 및 인증	암호화	완전 삭제	기타 보안기능
삼성전자	O	O	O	- 감사기록
신도리코	O	O	X	- SSL - 부정출력 방지
후지제록스	O	O	O	- 감사기록
HP	O	O	O	
Kyocera	O	O	O	

MFP에서는 이러한 식별 및 인증 기능은 대부분 우리가 알고 있는 패스워드 기반이며 범주는 크게 두 가지로 구분된다. 첫째는 사용자가 네트워크 자원에 접근하기 위하여 정당한 사용자임을 밝히기 위해 필요한 식별 및 인증이며, 다른 한 가지는 MFP 내의 하드디스크에 저장된 데이터에 접근하기 위한 식별 및 인증이다.

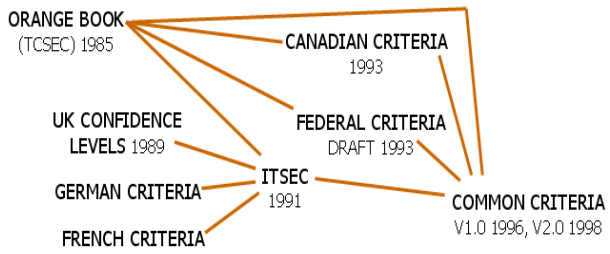
최근 출시되는 기업용 MFP에서는 기본적으로 완전삭제 기능을 제공하고 MFP에서 사용된 데이터는 대부분 하드디스크에 저장된다. 데이터 삭제 시 데이터 영역을 완전 포맷하지 않으므로 단순한 삭제만으로는 데이터가 완전히 삭제되지 않고 복원 유틸리티 등을 사용하면 복구가 가능하다. 완전삭제 기술 중 하나로 미 국방성 표준인 DoD 5220.22-M[1]의 매체의 모든 접근 가능한 위치를 단일 문자, 그것의 보수, 그리고 임의의 문자로 세 번을 덮어쓴 후 검증하는 절차가 있다.

MFP 내의 저장매체에는 중요 데이터가 보관될 수 있는데, 이러한 중요 데이터는 공격자에게 노출될 수 있다. 따라서 저장장치 내에 저장되는 데이터는 비밀성을 위해 암호화를 필요로 한다. 보안기능 암호는 저장장치에 기록되는 데이터의 암호화 알고리즘으로 암호화 된 후 저장장치에 기록되며, 저장장치에 기록된 데이터는 암호화 알고리즘으로 복호화 하여 사용될 수 있다.

디지털 워터마킹(Digital Watermarking) 기술은 데이터의 복제 및 위조 방지를 위해 사용되는 보안기능이다. 워터마킹은 저작권 보호, 위·변조 판별, 불법복제 추적, 사용자 제어, 내용 보호, 내용 라벨링 등의 기능을 제공한다.

3. MFP 보안기능 평가·인증 현황

최근의 MFP는 보안기능이 탑재된 IT제품으로 분류되어, 보안기능을 ISO 표준(ISO/IEC 15408:1999)인 공통평가기준으로 보안성 평가를 받는다. 공통평가기준은 IT 보안성 평가를 위한 기준 개발이 각 국가와 국가들의 연합으로 이루어져 오다가 1993년 6월 국제 표준화 기구인 ISO에서 일반 사용자를 위한 '공통평가기준 프로젝트'라고 명명된 프로젝트가 시작되었고 1996년 1월 CC v1.0이 완료되고 현재 CC v3.1r2까지 발표 되었고 CC v4가 현재 개발 중에 있다. 다음 그림은 CC로 통합되어 가는 과정을 보여주는 그림이다.



(그림 1) 공통평가기준 통합 과정

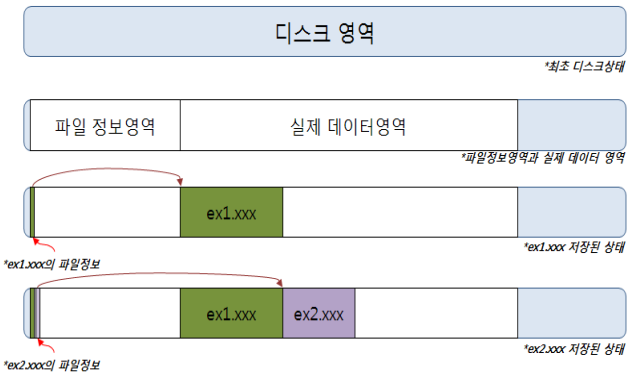
MFP 국내외 평가 현황은 MFP의 보안기능과 관련하여 평가를 수행한 평가기관과 평가 의뢰 업체를 중심으로 평가 현황을 조사한 결과, <표 2>에서 MFP 보안기능 관련 평가는 일본과 미국에서 주로 진행되고 있음을 알 수 있다. 특히 일본의 ITSC(48%), MIZUHO(29%), ECSEC(6%)와 미국의 COACT(4%), CSC(13%)는 MFP 보안기능과 관련된 평가에 있어 독보적인 점유율을 차지하고 있다.

<표 2> MFP 국가별 평가현황

국가	평가기관	건수
미국	COACT	4건
	CSC	7건
일본	ECSEC	15건
	ITSC	56건
	MIZUHO	34건

4. 잔여정보 보호기술

MFP에서 저장장치는 하드디스크와 플래시 메모리로 구분 할 수 있으며 하드디스크에 파일이 저장될 때는 크게 두 부분으로 나누어져 기록된다. 하드디스크는 파일위치정보와 파일이름이 저장되는 파일 정보영역과 실제 데이터가 저장되는 실제 데이터 영역으로 구성된다.



(그림 2) 디스크에서의 파일저장 구조

흔히 파일을 삭제라는 것은 실제 데이터 영역의 파일위치를 가지고 있는 파일 정보영역의 내용만 삭제한 것이다. 따라서 데이터 영역에 새로운 데이터가 덮어 쓰이지 않았다면 완전 삭제되지 않고 데이터가 하드디스크에 남아 있는 것이다. 그리고 삭제 시 파일의 링크 정보와 함께 실제 데이터 영역에 '난수' 또는 '0'으로 일정횟수 이상 중복해서 덮어씀으로써 데이터 복구가 불가능하도록 하는 기술이 잔여정보 보호기술이고 완전삭제 기능이다. <표 3>에서 저장매체별 완전삭제 알고리즘을 요약 정리하여 하였다.

1) US Department of Defense et al., "National Industrial Security Program Operating Manual(NISPOM)," DoD 5220.22-M, 1995

<표 3> 잔여정보 완전삭제 기능

구분	완전삭제 알고리즘	내용
하드 디스크	Super Fast Zero Write	3 섹터까지 0x00으로 덮어씀
	Zero Write	0x00으로 덮어씀
	Random Write	임의의 문자로 덮어씀
	Random & Zero Write	임의의 문자 & 0x00으로 덮어씀
	P-5239-26MFM	0xffffffff, 0xbfffffff로 & 임의 값으로 덮어씀
	Bit Toggle	0x00, 0xff, 0x00, 0xff를 각 1회씩 덮어씀
	Random Random Zero	임의의 문자로 2회 & 0x00으로 덮어씀
	DoD 5220.22-M	임의의 문자로 5회 & 그 보수로 7회 덮어씀
	North Atlantic Treaty Organization standard	0x00, 0xff로 6회 & 임의의 문자로 1회 덮어씀
	Peter Gutmann	임의의 문자로 35회 덮어씀
	Bruce Schneier's	0x00, 0x11로 2회 & 임의의 문자로 5회 덮어씀
	NSA erasure	0x00, 0x11로 7회 덮어씀
플래시 메모리	DoD 5220.22-M Supplement 1	모든 영역에 특정 문자 기록 후 문자의 보수 & 임의의 문자를 다시 덮어씀
	NSA/CSS Storage Device Declassification Manual	임의의 패턴으로 Flash memory 전체를 덮어쓴 후, 검사 수행
	NIS(정보시스템 저장매체 불용처리지침)	완전파괴(소각, 파쇄, 용해) 또는 완전포맷(저장매체 전체는 난수, 0, 1로 저장하는 방식)을 수행

5. 완전삭제 기능 시험·평가 항목

본 논문에서는 공통평가기준 기반으로 잔여정보 완전삭제 기능을 시험·평가해야 할 시험·평가 항목을 도출하고 국내 시험·평가 방법론을 제시한다. 공통평가기준의 시험(ATE)/취약성(AVA) 클래스에서 시험·평가 항목은 2종류로 구분 될 수 있다. 첫 번째는 개발자 시험 검증하는 항목으로 개발자 시험의 완전성 측면과 개발자에 의한 시험 수행하고 그 시험이 문서화 되는 방법을 평가하는 측면이다. 그리고 나머지는 평가자 시험 검증하는 항목으로 평가자가 개발자 시험의 일부 또는 전체를 재연하거나 독립적으로 시험을 수행하는 측면이다.

<표 4> 시험/취약성 클래스 평가 항목

구분	패밀리	평가 항목
개발자 시험	COV	- 개발자 시험과 제품의 보안기능 시험 범위간의 일치성 검증
	DPT	- 개발자 시험과 제품의 설계 및 보안 구조 시험 범위간의 일치성 검증
	FUN	- 개발자가 시험을 올바르게 수행하고 문서화하였는지 검증
평가자 시험	IND	- 평가자가 매개변수 변경 및 개발자 전략의 보안 등 추가적인 시험 수행
	VAN	- 기능 무력화 및 우회 시험

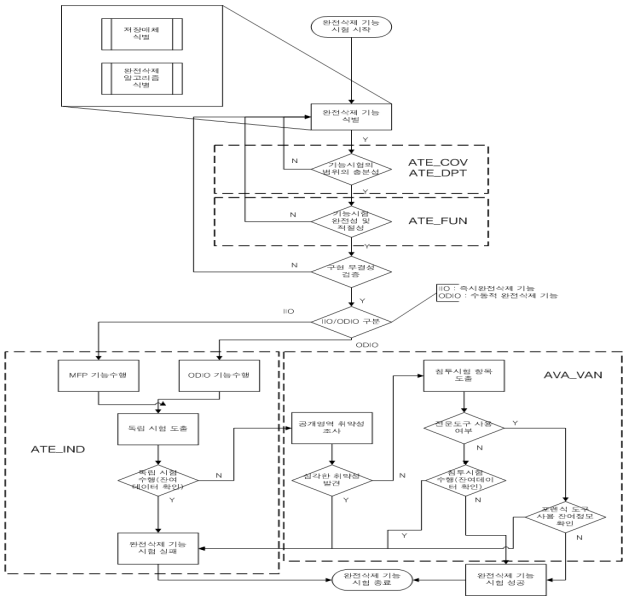
잔여정보 완전삭제 기능은 저장장치가 외부로 유출시 해당 데이터의 복구를 막기 위한 기술로 잔여정보 완전삭제 기능과 관련하여 어떤 저장매체를 사용하고 있는지, 어떤 완전삭제 알고리즘을 사용하고 있는지 식별해야한다. 따라서 공통평가기준을 기반으로 완전삭제 기능은 다음과 같은 항목을 시험 또는 평가해야 한다고 본 논문에서 제시한다.

<표 5> 완전삭제 기능 시험·평가 항목

구분	시험 항목	설명
COV DPT	완전삭제 기능 식별	저장매체별 및 알고리즘별 기능 시험 식별
	기능시험 범위 충분성 분석	기능별 및 설계상별로 기능 동작여부가 모든 시험에 포함되었는지 시험범위의 충분성 및 일치성 분석
DPT	기능시험 완전성 및 적절성 분석	시험절차가 재연이 가능 수준으로 완성도가 있는가, 시험이 올바르게 시험을 수행했는지 문서화로 조사
IND	완전삭제 메커니즘 구현 무결성 검증	완전삭제 메커니즘이 정해진 대로 구현되어 있는지 확인
	독립 시험	평가자가 중요성 등 여러 요소들을 판단하여 독립적인 시험
VAN	공개 영역의 취약성 분석	공개 영역에서 알려진 취약성 항목을 분석
IND VAN	완전삭제 기능 침투 시험	평가자가 노하우 및 전문도구를 이용하여 기능 무력화 우회할 수 있는지 시험

6. 완전삭제 기능의 국내 시험·평가 방법론 개발

5장에서 제시한 완전삭제 기능 시험·평가 항목은 아래 그림과 같은 시험/평가 절차를 가지고 <표 6>에서와 같이 완전삭제 기능의 국내 시험·평가 방법론을 제시한다.



(그림 3) 완전삭제 기능 시험 흐름도

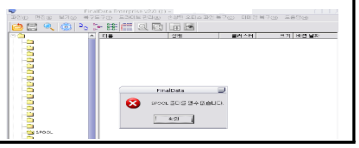
<표 6> 완전삭제 기능 시험·평가 평가방법론

완전삭제 기능 식별
MFP의 사용하는 저장매체에 따라 완전삭제를 구현하는 방법이 다를 수 있으므로 저장매체별(하드디스크, 플래시메모리) 및 완전삭제 알고리즘별 어느 것을 사용하고 있는지 식별해야 한다.
기능시험 범위 충분성 분석
시험 문서 내의 시험항목과 기능명세 및 설계문서의 인터페이스간의 일치성 및 누락 여부를 확인하고 시험이 보안기능 내의 모든 인터페이스가 시험되었음을 개발자 시험에서 입증되어짐을 확인하다.
기능 시험 완전성 및 적절성 분석
시험문서에 시험에 대한 종속관계, 시험목적, 시험조건, 시험방법, 예상 시험결과, 실제 시험결과 등 시험절차가 재연이 가능한 수준으로 완성도가 있는지 조사해야 하고 시험목적과 시험방법, 실험결과가 올바르게 수행하고 적절한지를 조사해야 한다.
완전삭제 메커니즘 구현무결성 검증
완전삭제 알고리즘을 자체 구현하였다면 알고리즘 검증을 통하여 구현상의 문제점이 없는지 확인하는 단계가 필요하고 기존 알고리즘을 이용하여 구현하였다면 구현무결성 시험을 통하여 올바르게 구현하였는지 여부만 확인해야 한다.
독립 시험
평가자는 시험의 엄격성, 신뢰성, 중요성, 복잡도, 시험의 내포성, 인터페이스 유형, 혁신성 등 여러 요소를 고려하여 시험항목을 도출
공개 영역의 취약성 분석
공개 영역에서 기술되어 있는 취약성 분석 사이트를 통하여 알려진 취약성이 조사해야 한다. 공개된 영역 취약성 분석 사이트 ① National Vulnerability Database(NIST) ② SecurityFocus→bugTraq ③ Secunia ④ CVE(Common Vulnerability and Exposures) ⑤ Black hat
완전삭제 기능 침투 시험
평가자의 축적된 노하우 및 포렌식[2] 툴 등 전문도구를 이용하여 기능을 무력화 및 우회하여 데이터 복구 여부 확인해야 한다. 포렌식 복구 도구 ① Logicube (www.logicube.com) 디스크 복제 장치로 디스크를 비트단위로 복제하는데 사용 ② FinalData (www.finaldata.com) 삭제된 파일 복구 및 삭제된 데이터베이스를 복구 ③ WinHex(www.winhex.com) 검색도구로 하드디스크 또는 파일을 헥사코드 형태로 확인 ④ EnCase (www.encase.com) Search 자동화, 이미지 파일 미리보기, 암호 해독, 데이터 캡쳐 분석, 원격 데이터 복구 등에 사용된다.

7. 시험·평가 방법론으로 시험결과

본 논문에서 제시된 시험·평가 방법론으로 시험·평가 한 결과를 요약하여 다음과 같이 정리하였다.

<표 7> 시험·평가 결과요약

구분	시험 항목	결과
COV DPT	완전삭제 기능 식별	저장매체 : 하드디스크
	기능시험 범위 충분성 분석	즉시/수동적 2종류의 완전삭제 기능을 식별하고 시험이 충분함을 확인함
DPT	기능시험 완전성 및 적절성 분석	개발자 시험의 재연 문서 평가임으로 본 논문에서 기술을 제외함
IND	완전삭제 구현 무결성 검증	무결성 구현 무결성 시험 수행함 메커니즘 비공개 원칙으로 제외
	독립 시험	2종류 각 2변수 변경으로 시험·평가 수행 결과 정상동작 확인함
VAN	공개 영역의 취약성 분석	취약성 분석 결과 비공개 원칙으로 제외
IND VAN	완전삭제 기능 침투 시험	FinalData 포렌식 툴로 복구 파일이 없음을 확인함 

8. 결론

본 논문에서 제시된 국내 시험·평가 방법론은 공통평가기준에 기반으로 하였기 때문에 보안기능 동작여부를 시험하는 것은 물론이고 시험의 충분성 및 수행절차의 완전성 등 시험범위에 대한 부분과 평가자 직접 수행하는 기능의 독립 시험 및 취약성 분석도 국내 시험·평가 방법론 개발 범위에 포함하였다.

MFP의 다양한 기능 중 일부인 완전삭제 기능에 대하여 적용할 시험·평가 방법론만을 제시하였음으로 향후 MFP 보안성 평가를 위해서는 본 논문에서 제시한 것 외에 다른 기능에 대한 시험·평가 방법론 개발도 필요하다.

참고문헌

[1] 한국정보보호진흥원, “프린터 보안기능 기반기술 시험방법 연구”, 2008.

[2] 한국정보보호진흥원, "중고 PC 데이터 복구 방지 방법 안내", 2005.

[3] Electronic Commerce Security Technology Laboratory Inc Evaluation Center, “www.ecsec.jp/english_index.html”

[4] Information Technology Security Center Evaluation Department, “www.itsc.or.jp/en”

[5] KISA, “정보보호시스템 신분확인기능 및 무결성기능 평가방법 연구”, 최종 연구보고서, 1999.12

[6] 한국정보보호진흥원, “정보보호 시스템 보안정책 모델 평가 방법론 연구”, 최종 연구보고서, 2004.11.

2) 포렌식(forensics): 전자 증거물 등을 사법기관에 제출하기 위해 데이터를 수집, 분석, 보고서를 작성하는 일련의 작업