스마트폰 환경에서의 DLP 방식 개인정보 보호의 문제점

최종욱*, 박주미**, 이용진*
e-mail : juchoi@markany.com*, pjmhappy@naver.com**, yjlee@markany.com*
마크애니*, 상명대학교 컴퓨터과학과**

Privacy Protection using DLP in the Smart Environment

Jong Uk Choi*, Ju Mi Park**, Yong Jin Lee*
*Markany
**Dept. of Computer Science, Sangmyoung University

요 약

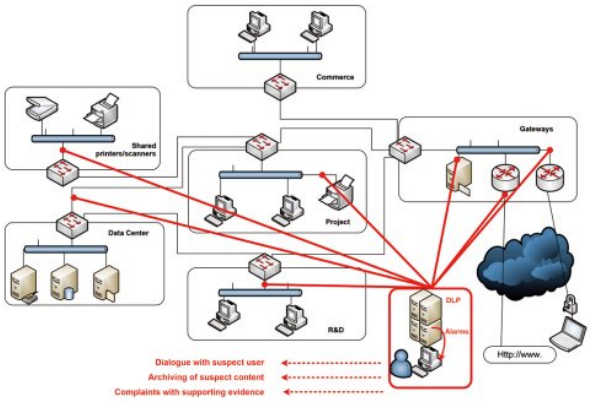
DLP 방식의 개인정보 보호 시스템에서는 문서나 메일의 내용을 검색하여 개인정보 관련한 데이터를 검색으로 찾아내는 내용검색을 사용하고 있다. 이러한 내용 검색을 위해서는 네트워크 송수신 기기에서, 혹은 사용자의 컴퓨터에서 모든 문서를 평문으로 유지해야 한다는 점을 강조하고 있다.
그러나 이러한 평문 유지 방식은 현재 빠르게 보편화되고 있는 스마트폰 환경에서는 카메라에 의한 촬영을 막기 어렵다는 점에서, 최근 활발해지고 있는 APT 공격에 대응하기 어렵다는 점에서 문제점으로 지적되고 있다. 더구나 고객 정보를 수집 보관하고 있는 기관의 '직원' 사생활 데이터를 검색할 수 있다는 점에서 문제가 제기되고 있다.
본고에서는 '개인정보 보호법'의 실시로 설치되고 있는 DLP 시스템의 문제점을 짚어보고, 가능한 대응책을 제시한다.

1. 개인 정보 보호의 기술적 과제

올 해 2 월 23 일, 미국 백악관은 투명성, 소비자 의사 존중, 보안, 소비자 접근성, 정확성, 제한된 수집, 책임 등을 골자로 하는 소비자 사생활 권리장전(consumer privacy Bill of Right)을 발표하였다[25][26]. 이는 온라인 광고업계가 웹브라우저 상에 추적금지 버튼을 누르면 네티즌의 개인정보를 수집할 수 없게 하는 계획을 자발적으로 추진한다고 밝혔다. 온라인 광고업계 단체인 디지털광고 연합(DAA)은 구글, 야후, MS, AOL 등과 함께 추적 금지 버튼 도입을 약속했다. EU 에서는 유사한 조치를 이미 올해 1 월에 내놓은 바 있다.
올해 시행되는 '개인정보 보호법'의 발효로 IT 업계에서는 여러 가지 기술들이 제안되고 있는데 이중에서 DLP 방식은 기존 정보 유출 방지 기술을 '개인정보 보호'에 적용한 것으로, 몇 가지 문제점이 있어 논의가 필요하다. 본고에서는 기존 DLP 기술의 문제점을 지적하고자 한다.

2. DLP 방식의 개인정보 유출 방지

DLP(Data Loss Prevention)방식은 사용자 컴퓨터나 네트워크를 통해 전달되는 데이터를 체크하여 사전에 입력한 패턴과 일치하거나 유사한 경우 감지(detection)하여 조치를 취하는 기술이다[3]. Symantec 이 사용하는 DLP 방식은 텍스트로 이루어진 문자열이나 문자집합에서 보안 정책을 위반하는 데이터를 찾아내고 이에 따라 규정을 집행하는 구조이다[24]. DLP 기술의 적용대상은 사용자 컴퓨터에 저장되었거나 송수신된 문서, 메일과 모든 탐색 가능한 데이터로 확대되고 있다. 즉, 이메일과 같은 동적 데이터(data in motion)로부터 중요한 데이터를 추출할 수 있다는 Zamer[1990]의 DLP 기본 아이디어에서 정적으로 보관된 데이터로, 사용중인 응용프로그램에 의해 활성화된 모든 파일과 데이터로, 그리고 네트워크로 연결된 모든 기기와 시스템으로 그 검색 대상이 확대되고 있다. 개인이 보관하는 파일이나 데이터 중에서 민감하거나 중요한 정보의 패턴을 인식하고 이를 바탕으로 파일을 삭제하던지, 송수신을 막는 방식은 [Zoppas, Hermann, O'Raghallaigh, Bothwell, and Fontana 2011]에 의해 제안되었다.



(그림 1) DLP Architecture (source: http: news.bull.com/bulldirect/2010/10/07)

이처럼 DLP 방식은 데이터 내용 검색에 바탕을 두고 있기 때문에 기본적으로 데이터가 평문(plaintext)로 존재해야 한다는 점을 가정하고 있다.
이는 사용자의 데이터를 네트워크 상에서 검색하든, 컴퓨터에서 검색하든, 혹은 데이터 사용을 검색하든, 데이터가 평문이어야 한다는 것인데, 데이터의 내용을 검색하기 위한 조건으로 스마트폰이 활성화되고 있는 IT 환경에서는 몇 가지 문제를 갖고 있다.

3. DLP 방식의 문제점

DLP 기술이 갖고 있는 기본적인 가정, 사용자 컴퓨터에 있는 문서는 평문이어야 한다는 점에서 문제가 제기되고 있다.
첫째, DLP 기술은 평문을 통한 내용검색 기술에 의존하고 있어 외부 해킹에 취약하다. 보안 업계에서 심각히 우려하고 있는 APT(Advanced Persistent Threat) 공격에 대해 내용 검색을 위해 평문을 보관하거나 송수신하는 기존의 DLP 기술이 대응하기 어렵다는 점이 지적되고 있다. APT 는 SK 커뮤니케이션즈나 넥슨 사례에서 보듯 초기 기획부터 대상을 명확히 설정, 집중적으로 공격하고, 조직 구성원인 개인을 공격한다. 일반적으로 조직 내 개인 PC 는 상대적으로 관리가 취약하여 APT 에서는 이러한 PC 를 공격 침입 경로로 이용해 효과적이고 은밀하게 조직 내부에 침투한다[4][5]. DLP 기술은 송수신시 의심되는 유출을 차단하여 개인정보를 보호할 수 있다고 주장하지만, 최근 APT 가 암호화하거나 위장하여 문서를 탈취하는 경우가 늘고 있어 현재의 DLP 기술로는 적절한 대응이 어렵다.
둘째, 스마트폰에 의한 정보 유출을 막을 수 없다는 점이다. 스마트폰에는 카메라(camera), 녹음 (recorder), 저장(SD) 기능이 있고, 특히 고해상도 촬영 기능을 갖춘 스마트폰이 일반화되면서 카메라에 의한 정보 유출이 우려되고 있다. 예를 들어 의료업계, 은행, 통신업계의 고객서비스 부서가 아닌 부서 직원이 중요 고객 정보 화면을 촬영하는 경우, 현재의 DLP 방식으로는 막을 수가 없다. 더구나 기업내부에서 사용되던 전자결제용 그룹웨어와 메일 시스템이 스마트폰에서 작동되면서 정보 유출 가능성은 더욱 높아지고 있다. 회사 밖에서의 문서 송수신이나 촬영에 적극적으로 대응할 수 없다는 점에서 DLP 기술이 앞으로 전개될 스마트워크 시대의 개인정보 보호 기능 수행이 어려울 것으로 보인다.
셋째, 개인정보 보호(privacy protection)라는 관점에서 은행, 통신사, 호텔, 백화점의 경우 '고객정보' 보호뿐 아니라, 거기서 일하는 '직원의 정보'도 중요하다는 점이다. 미국이나 유럽에서 DLP 시스템에 대한 회의적인 의견이 피력되는 이유는 직원들의 사생활 침해 때문이다. DLP 는 기업 비밀 유출방지를 위한 내용검색 기술이다. 몇 가지 중요한 키워드만 입력하면 관련 문서 검색으로 통계적 자료를 추출하고 송수신 과정을 제어하도록 설계되어 있다. 그런데 논란이 되는 것은 검색시 고객정보 외에도 회사 정책에 위배되는 사생활 정보가 포함될 수 있다는 점이다. 즉 사업체에서 정책적으로 금지하고 있는 키워드, 예를 들어, 性에 관련된 내용이나 직장 이전에 관련된 내용이 검색될 경우, 직원들의 개인 정보가 보호되기 힘들다는 점이다. 즉, 개인정보 보호가 '고객 정보' 뿐만 아니라 그 기관에서 일하고 있는 '직원의 정보'로 확대할 경우 DLP 기술은 대단히 위험하다는 주장이 제기되고 있다[1][6][11].
이처럼 기존 DLP 기술로는 기관 '내부 직원'의 개인정보 보호와 외부 해킹에 의한 '정보 탈취'를 막을 수 없고, 스마트폰의 기능 향상(카메라, 저장장치)에 효과적으로 대처할 수 없다는 문제점이 있다.

참고문헌:

[1] 김진형, 김현종, "정보유출 방지와 프라이버시 침해에 대한 고찰", 정보보호학회지, 21(5), pp.45-49., 2011.8.
[2] 오현식, "Market Inspection: 정보 유출 방지", 데이터 넷, pdf.datanet.co.kr/211/211150pdf., 2011
[3] 이민형, "DLP 솔루션을 도입해야 하는 이유는…"ddaily, ddaily.co.kr, 2012.2.3.
[4] 장윤정, "APT 공격, 99.999% 당한다: 다계층 보안 및 전 직원 보안교육 등 전방위 대비 필요", 보안 닷컴, http://www.boan.com/news/articleView.html?idxno=5596, 2011.11.
[5] Zamora E.M., *Computer Method for Automatic Extraction of Commonly Specified Information from Business Correspondence*, US Patent 4,965,763, registered by IBM, Oct.1990.
[6] Zoppas M., Hermann J., O'Raghallaigh C., Bothwell E., and Fontana A., *Method and Apparatus for Detecting Policy Violations in a Data Repository Having an Arbitrary Data Schema*, US Patent No 7,996,373, Aug.2011.
[7] 김명환, MK 뉴스, "미국, 온라인 개인정보 유출차단 나선다 ", 매경뉴스, http://news.mk.co.kr/v3/, 2012.2.24
[8] 김희연, "세계는 지금 '개인정보보호 열풍', ZD Net, hee@zdnet.co.kr, 2012.1.27