보안공학연구논문지 *Journal of Security Engineering*
Vol.10, No.6 (2013), pp.669-680
http://dx.doi.org/10.14257/jse.2013.12.05

클라우드 컴퓨팅에서의 문서관리 서비스 보안 취약점 분석

조성목1)

An Analysis of Security Vulnerability on Document Management Service by Cloud Computing

Sung-Mok Cho[1)]

요 약

클라우드 컴퓨팅은 휴대전화, 태블릿 컴퓨터, 랩탑 컴퓨터, 개인용 PC 등 개인이 가지고 있는 정보통신기기에서는 주로 입·출력 작업만 이루어지고, 정보의 분석, 처리, 저장, 관리 등의 작업은 인터넷을 통하여 접근할 수 있는 클라우드라는 공간에서 이루어지는 컴퓨팅 시스템을 말한다. 이러한 컴퓨팅 환경은 다양한 개인정보통신 기기를 단말기로 사용할 수 있고, 복잡한 클라우드 컴퓨팅 인프라를 이해하지 못해도 일치된 사용자 환경을 제공해 줌으로써 사용자가 편리하게 사용할 수 있으며, 사용자의 정보를 신뢰성이 높은 서버에 저장하고 관리함으로써 안전하게 데이터를 보관할 수 있는 등 많은 장점을 제공하고 있다. 그러나 서버가 공격당하거나 보안상의 문제점으로 인해 개인정보가 유출된다면 데이타를 되살리지 못하게 되거나 사용자의 데이터가 유출 또는 손상될 수 있는 위험성이 있다.

이에 본 논문에서는 국내에서 서비스 중인 J사의 S제품, M사의 D제품, D사의 D제품, H사의 P제품 및 E사의 M 제품 등의 서비스에 대한 취약점을 분석하였다. 그 결과 J사의 S제품과 M사의 D제품 서비스에서는 쿠키에 의한 개인정보 노출 등 로그인 취약점이 나타났으며, J사의 S제품, M사의 D제품, D사의 D제품, H사의 P제품 및 E사의 M 제품 서비스에서는 모두 파일이름과 파일내용이 평문으로 나타나는 등 업로드 취약점이 나타났음을 확인할 수 있었다.

핵심어 : 클라우드 컴퓨팅, 개인정보, 로그인 취약점, 업로드 취약점

Abstract

Cloud computing is the computing system that only the input/output jobs are performed in personal information communication devices such as a mobile telephone, tablet computer, laptop computer, and personal computer, while information analysis, processing, storage, and management procedures are serviced in the space labeled as a cloud that can be accessed over the internet. In this circumstances, users can utilize their various personal information communication devices as a terminal for cloud computing and conveniently use it by being provided a coherent user environment even though they do not make sense of its complex infrastructure in the cloud computing that supports them. In addition, cloud computing services provide them with many merits which they make their data keeping securely according to being stored and managed their information on the highly reliable servers. But if servers are attacked or personal information is leaked due to the troubles in relation with security, it happens that some dangerousness beyond data

접수일(2013년10월31일), 심사의뢰일(2013년11월01일), 심사완료일(1차:2013년11월14일, 2차:2013년11월29일)
게재일(2013년12월31일)

[1]608-711 부산광역시 남구 신선로 428번지, 동명대학교 정보보호학과 교수.
email: smcho@tu.ac.kr

ISSN: 1738-7531 JSE

recovering or the risk of the leak and the damage of their information.

In this paper, we analyze the vulnerabilities on the S service of J company, the D service of M company, the D service of D company, the P service of H company, the M service of E company within the country. The results reveal the login vulnerability of the personal information exposure by a cookie on the D service of M company as well as the S service of J company, and the upload vulnerability which upload filename and file contents come into sight as a plain text on the S service of J company, the D service of M company, the D service of D company, the P service of H company, the M service of E company.

Keywords : Cloud Computing, Personal Information, Login Vulnerability, Upload Vulnerability

1. 서론

오늘날 인터넷을 통해 유통되는 데이터양의 증가 속도가 기하급수적으로 늘어나고 있으며, 이와 더불어 ICT를 기반으로 한 기술들이 복합적으로 융합하면서 고도로 집약된 기술 서비스의 형태들이 출현되고 있다. 이중, 서비스 인프라에 대한 사용자의 이해를 전제로 하지 않으며, 사용자가 보다 손쉽게 사용할 수 있도록 각종 개인정보통신 기기의 사용자 환경을 제공할 뿐만 아니라 서비스 활용을 위한 초기 투자비용과 유지보수 비용 등 별도의 경제적인 비용이 소요되지 않는 클라우드 컴퓨팅 기술이 집중적인 주목을 받고 있다.[1-3]

많은 기업체와 포털 사이트 및 통신 사업체에서는 이미 시공간에 구애받지 않는 이동성과 편이성, 비용절감 등의 다양한 장점으로 인해 클라우드 컴퓨팅 기술을 도입하거나 구축하고 있으며, 클라우드 컴퓨팅 기술과 관련된 시장도 급속도로 성장하고 있는 추세이다. 그러나 클라우드 컴퓨팅은 서버와 스토리지 등 물리적으로 산재해 있는 별도의 자원을 가상화 기술을 사용하여 사용자의 자료를 보관하고 처리하고 관리하므로 사용자가 직접 자료를 관리하는 것보다 보안 측면에서 상대적으로 유리하다고 할 수 있으나, 보안 취약점이 노출되어 공격을 받았을 경우에는 대규모 피해의 가능성이 있고, 개인적으로는 자신의 개인정보와 자료에 대한 직접적 통제가 불가능하게 된다.

따라서 인터넷 기반의 서비스를 제공하고 있는 클라우드 컴퓨팅은 개인정보와 자료유출 또는 손실 등 보안 측면에서의 위험성이 상존하고 있으므로 자료를 저장할 때 기밀성 유지를 위하여 사용자 인증, 컨텐츠 보안, 적절한 보안 정책수립 등의 방법을 통하여 보안 위협요소를 해결하여야 한다.[4]

최근 ,문서관리 솔루션을 판매하는 각 업체에서는 자사의 제품에 대하여 자신들이 개발한 솔루션의 성능을 위주로 프로모션하고 있지만 문서관리에 대한 체계적인 보안 관리 기법의 제시는 미비한 실정이다. 클라우드 컴퓨팅 환경에서의 문서관리 보안 위협요소에 대한 선제적 대응만이 보다 안전하고 편리하게 문서를 분석하고 처리하고 저장하고 관리하는 필수 선결과제가 되므로 클라우드 환경에서의 보안과 개인정보보호 기술이 서비스의 성패를 가르는 매우 중요한 요인으로 간주되고 있다.[5-6]

따라서 본 논문에서는 국내에서 상용화된 제품으로 서비스 중인 J사의 S제품, M사의 D제품, D사의 D제품, H사의 P제품 및 E사의 M 제품 등을 통한 서비스에 대한 보안 취약점을 살펴보고 그

보안위협 요소를 분석하였다.

2. 보안 취약점 분석을 위한 환경 구성

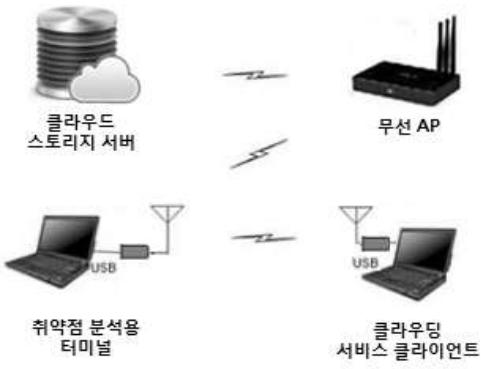
일반적으로 보안 취약점이라 함은 불법적인 사용자의 시스템 접근 위협, 정상적인 서비스를 방해하는 위협, 관리중인 중요한 정보의 유출, 삭제, 변조 등 데이터의 손실 등을 일컫는다. 본 논문에서는 이러한 취약점 분석을 위하여 다음과 같은 방법으로 시스템과 네트워크를 구성하였다.

2.1 시스템 구성

취약점 분석을 위한 터미널과 클라우딩 서비스를 사용하는 터미널에는 각각 USB 무선 랜카드 ipTIME 11n USB(V 3.2.1.0)를 장착하였고, 취약점 분석용 터미널에는 분석용 도구 Wireshark을 설치하였으며, 클라우딩 서비스 클라이언트에는 분석 대상 프로그램을 모두 설치하였다.[7] 또한, 네트워크 분석을 위한 목적으로 유무선 인터넷 사용이 가능하도록 무선 AP(Wireless Access Point)를 준비하였고, USB 무선랜 카드의 AP기능 설정을 위하여 [그림 1]과 같이 ipTIME 11n USB 프로그램을 실행하여 soft AP모드로 변경하고, WAN 랜카드에서 Atheros AR9485WB-EG Wireless Network로 설정하였다.

[그림 1] USB 무선 랜카드의 AP설정
[Fig. 1] AP setup of USB wireless LAN card

이와 같이 구성된 시스템은 [그림 2]와 같은 네트워크 구성도에 따라 동작하게 되는데, 클라우딩 서비스를 이용하는 클라이언트가 취약점 분석용 터미널을 거쳐 사용자 ID와 패스워드 정보를 USB 무선 랜카드를 통해 취약점 분석용 터미널을 거쳐 무선AP를 경유하여 클라우드 스토리지 영역에 보내지면 클라우드 스토리지에서는 사용자 ID와 패스워드에 대한 스토리지 영역정보를 요청 받았던 경로로 되돌려 주게 된다. 이러한 절차에 따라 사용자 세션이 생성되면 클라우딩 서비스 클라이언트 터미널은 동일한 네트워크 경로를 통해 데이타를 업로드하고 다운로드하게 된다.



[그림 2] 취약점 분석을 위한 네트워크 구성도
[Fig. 2] A Network Configuration for Vulnerability Analysis

3. 보안 취약점 분석을 위한 실증적 실험 결과

보안 취약점 분석은 국내에서 서비스되고 있는 5개의 문서관리 서비스를 대상으로 OWASP(Open Web Application Security Project) Top10 2013의 취약점 분류에 따라 인증 및 세션 관리와 관련된 애플리케이션의 결함으로 인한 패스워드 취약점, 사용자 세션 가로채기 및 사용자 도용과 관련된 취약점, 그리고 업로드 및 다운로드 취약점 등 개인정보를 적절하게 보호하지 못함으로써 발생하는 패스워드 관련 취약점, 응용프로그램 취약점, 패킷 취약점 등을 중점적으로 분석하여 로그인시 사용자 ID와 비밀번호 취약점 및 데이터 업로드 시 파일이름과 내용에 관한 암호화 여부를 조사하였다.[8]

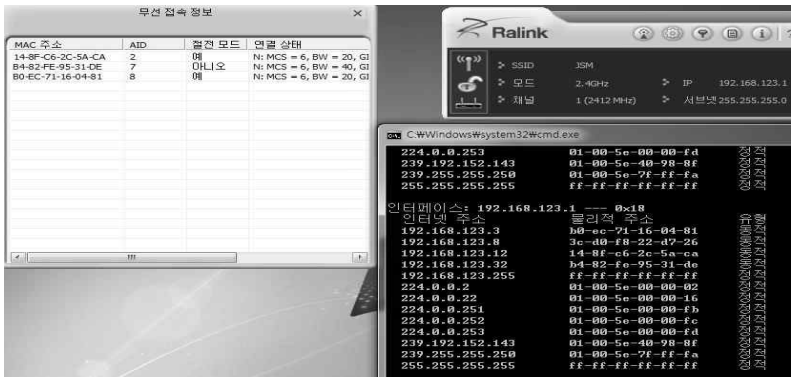
3.1 무선 랜 AP 접속 시 취약점

Wi-Fi를 사용하는 스마트폰의 활용 빈도가 증가함에 따라 무선 랜 보안설정에 대한 인식도 높아지고 있지만, 방송통신위원회와 한국인터넷진흥원(KISA)이 '2012년 무선 랜 보안 실태조사'를 통해 발표한 자료를 살펴보면 전체 무선 AP 중 약 20%인 1만5천136대에서 보안설정 기능을 전혀 제공하고 있지 않다고 밝혔다.[9] 악의적인 의도를 가진 해커들이 이미 카페나 기타 무선공유기가 설치된 공공장소에서 에빌 트윈(Evil Twin)과 같이 무선 랜 접속주소를 위장하고 있으며, 이를 통해 인터넷에 접속한 사용자들의 비밀번호, 신용카드 정보 등의 데이터를 흔적을 남기지 않고 훔쳐가는 수법이 널리 사용되고 있다. 즉, 합법적인 WiFi 접근 노드 부근에서 합법 노드가 사용하는 노드 이름과 주파수를 사용하여 무선 신호를 보내면 최종 사용자는 에빌 트윈이 마치 강한 신호를 발사하는 하나의 핫스폿으로 알고 접속하게 되고, 에빌 트윈이 최종 사용자의 인터넷 접근 노드가 되어 에빌 트윈을 운용하는 공격자들이 패스워드나 신용 카드 정보와 같은 중요한 데이터를 가로챌

수 있게 된다. 따라서, 공용 무선인터넷 사용자의 입장에서 악의적인 공격으로부터 적절한 방어를 위해서는 아무리 익숙한 무선 네트워크 이름이라고 하더라도 안전하지 아니므로 한번 접속했던 무선 랜에 자동접속하지 않도록 설정을 변경해야 하고, 방송통신위원회가 발표한 KT의 'QOOKnSHOW', 'ollehWIFI', SK텔레콤의 'SKT-Tspot', LG유플러스의 'U+ Wi-Fi100', 기타 커피숍, 호텔 등에서 제공하는 무선 랜 주소 외에는 접속하지 말도록 권고하고 있다.[10]

3.2 보안 취약점 분석을 위한 시나리오

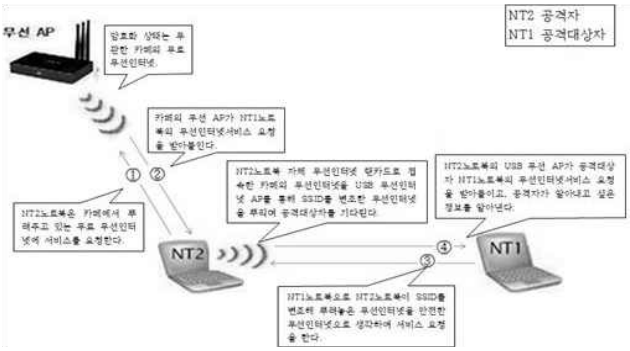
요즈음 대중교통, 카페, 패스트 푸드점, 교육기관 등에서 무선 AP를 많이 사용하고 있다. 대중교통 이용 시에는 별 다른 암호화가 되어 있지 않아 인증 없이 무선LAN을 사용할 수 있으며, 카페나 패스트 푸드점에는 해당 매장에서 판매하는 제품을 구입할 경우 무선AP 인증 패스워드를 제공해주고 있다. 따라서 도청과 정보 수집을 목적으로 별도의 툴을 사용하지 않더라도 [그림 3]과 같은 정보들을 획득할 수 있다. [그림 3]의 무선 접속 정보 창에서는 설치된 AP에 접속된 사용자들의 MAC주소, AID, 연결 상태 등을 확인 할 수 있으며, arp -a 명령어를 통하여 MAC 주소와 IP 주소를 확인할 수 있게 되므로 2차적인 공격으로부터 안전하지 못하다는 것을 알 수 있다.



[그림 3] USB 무선 랜카드에 접속된 기기들의 MAC 주소와 IP 주소

[Fig. 3] The MAC and IP Addresses of Devices connected to USB Wireless LAN Card

따라서 [그림 4]에서와 같이 악의적인 목적을 가진 해커가 어느 카페에서 노트북2를 가지고 카페의 무료 무선인터넷(암호화 유무 상관없음)에 연결한 다음 노트북2의 USB무선 인터넷 AP를 통해 카페내의 안전한 무료 무선 인터넷인양 SSID를 비슷하게 Angel ln-us로 지정하여 뿌려주고 공격할 대상을 기다리면 이를 눈치 채지 못한 사용자는 카페로 들어와 어떤 무선인터넷이 안전한지 확인하지 않고 중요문서를 해커가 뿌려놓은 Angel ln-us를 노트북1에 연결하여 문서관리 프로그램으로 송신하게 되고, 해커는 노트북1로 작업하는 사용자가 어떤 프로그램으로 어떤 문서를 어떤 곳으로 보내어 주는지 파악할 수 있게 된다.



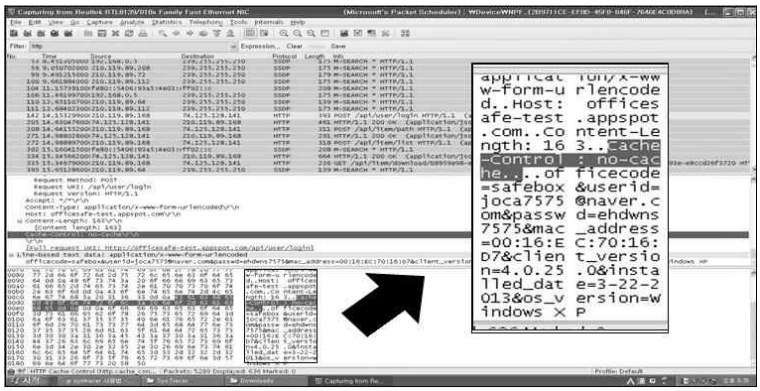
[그림 4] 설정가상 시나리오 순서도

[Fig. 4] AP setup of USB wireless LAN card

본 논문에서는 이와 같은 메카니즘을 이용하여 분석 대상 문서관리 서비스에 대한 취약점을 분석하는 절차를 구성하였다.

3.3 서비스의 취약점 분석

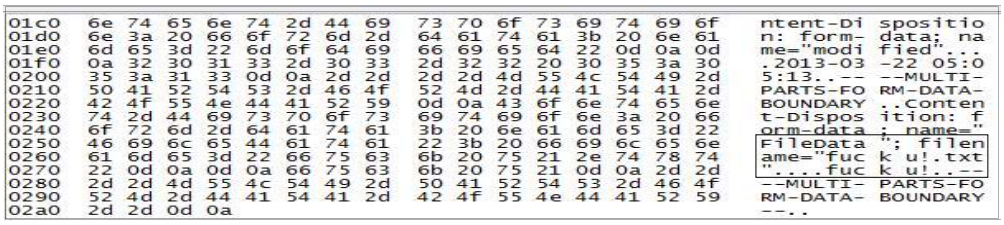
본 논문에서는 Wire Shark를 이용하여 사용자 로그인 시 쿠키에 의한 개인정보 노출에 관한 취약점을 분석하였다. 스토리지 서버에서 각종 상태 정보를 사용하기 위해서는 사용자 단말기에 쿠키를 저장하게 된다. 그런데 [그림 5]를 살펴보면 J사 S서비스의 프로그램에 의해 생성되는 쿠키 정보에는 가입자 계정 패스워드가 평문으로 저장됨을 확인할 수 있었다.



[그림 5] J사 S서비스의 로그인 취약점

[Fig. 5] Login Vulnerability on S Service of J Company

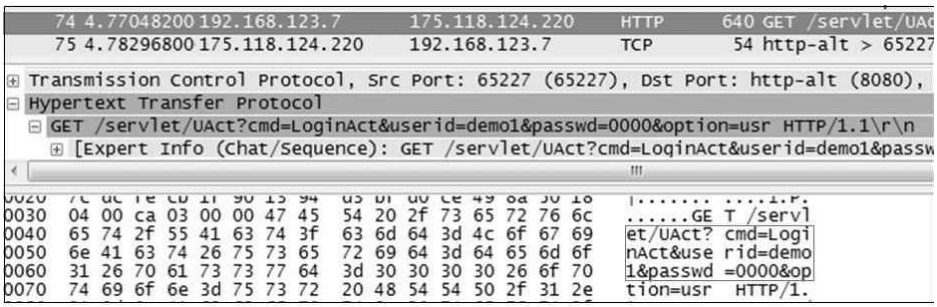
뿐만 아니라 J사 S서비스는 파일 업로드와 다운로드 시 파일이름과 형식 그리고 파일내용이 모두 평문으로 나타나고 있음을 [그림 6]에서와 같이 확인할 수 있었다.



[그림 6] J사 S서비스의 파일 업로드 및 다운로드 취약점

[Fig. 6] Upload and Download Vulnerability on S Service of J Company

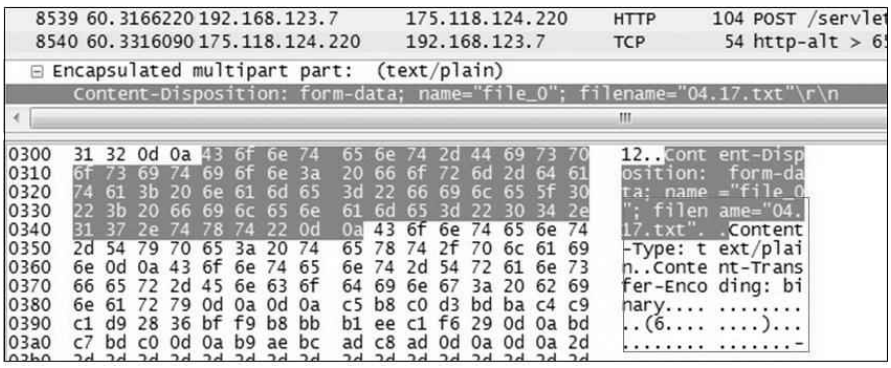
M사 D서비스 또한 [그림 7]에서 보는 바와 같이 프로그램에 의해 생성되는 쿠키 정보에는 가입자 계정 패스워드가 평문으로 저장됨을 확인할 수 있었다.



[그림 7 M사 D서비스의 로그인 취약점

[Fig. 7] Login Vulnerability on D Service of M Company

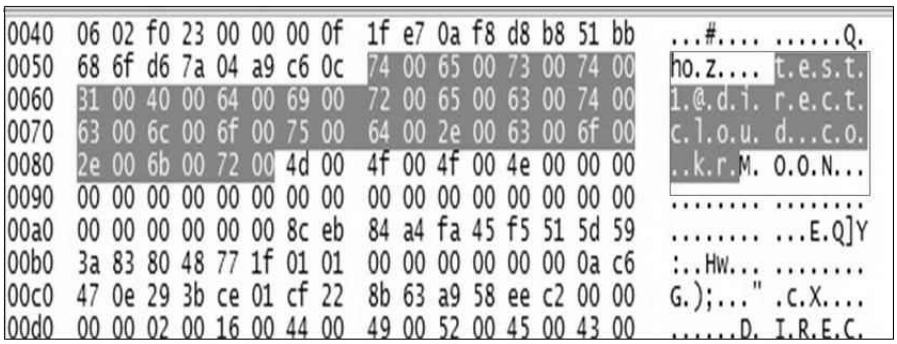
또한, J사 S서비스와 마찬가지로 M사 D서비스에서도 파일 업로드와 다운로드 시 파일이름과 형식 그리고 파일내용이 모두 평문으로 나타나고 있음을 [그림 8]에서와 같이 확인할 수 있었다.



[그림 8] M사 D서비스의 파일 업로드 및 다운로드 취약점

[Fig. 8] Upload and Download Vulnerability on D Service of M Company

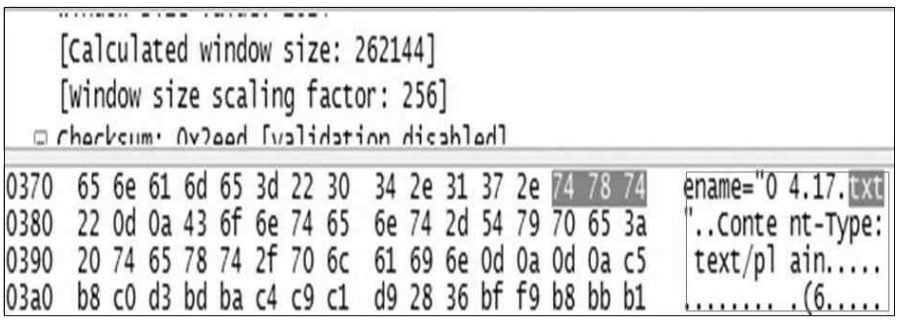
그러나 D사 D서비스는 J사 S서비스나 M사 D서비스와 달리 프로그램에 의해 생성되는 쿠키 정보에 가입자 계정은 평문으로 저장되지만, 패스워드는 암호화되어 비문으로 저장되고 있음을 [그림 9]에서와 같이 확인할 수 있었다.



[그림 9] D사 D서비스의 로그인 취약점

[Fig. 9] Login Vulnerability on D Service of D Company

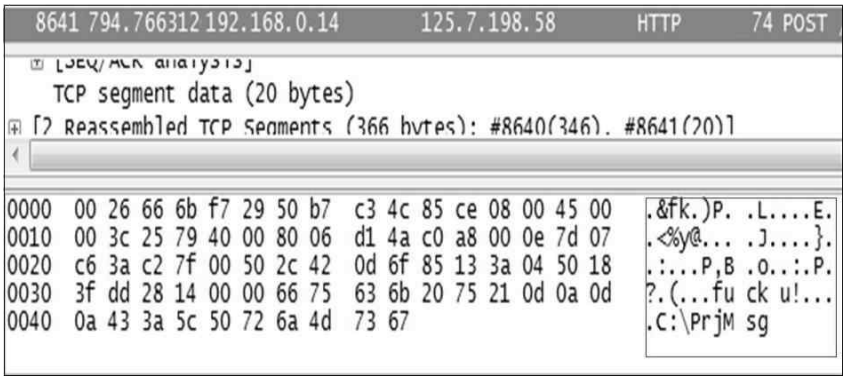
그렇지만 D사 D서비스는 J사 S서비스나 M사 D서비스와 마찬가지로 파일 업로드와 다운로드 시 파일이름과 형식 그리고 파일내용이 모두 평문으로 나타나고 있음을 [그림 10]에서와 같이 확인할 수 있었다.



[그림 10] D사 D서비스의 파일 업로드 및 다운로드 취약점

[Fig. 10] Upload and Download Vulnerability on D Service of D Company

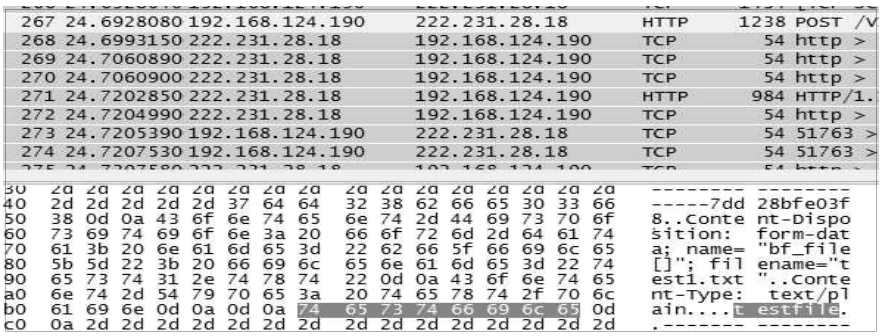
H사 P서비스는 J사 S서비스, M사 D서비스, D사 D서비스와는 달리 프로그램에 의해 생성되는 쿠키 정보에서 사용자 계정과 패스워드를 검색할 수 없었지만, 파일 업로드와 다운로드 시 파일내용이 여전히 평문으로 나타남을 [그림 11]에서와 같이 확인할 수 있었다.



[그림 11] H사 P서비스의 파일 업로드 및 다운로드 취약점

[Fig. 11] Upload and Download Vulnerability on P Service of H Company

E사 M서비스 역시 H사 P서비스와 같이 프로그램에 의해 생성되는 쿠키 정보에서 사용자 계정과 패스워드를 검색할 수 없었지만, 파일 업로드와 다운로드 시 파일 내용이 여전히 평문으로 나타남을 [그림 12]에서와 같이 확인할 수 있었다.



[그림 12] E사 M서비스의 파일 업로드 및 다운로드 취약점

[Fig. 12] Upload and Download Vulnerability on M Service of E Company

이상에서 살펴본 본 바와 같이 국내에서 서비스 중인 J사의 S제품, M사의 D제품, D사의 D제품, H사의 P제품 및 E사의 M 제품 등을 통한 서비스의 취약점을 분석한 결과를 요약하면 [표 1]과 같다. J사의 S제품과 M사의 D제품을 사용하는 경우에는 쿠키에 의한 개인정보 노출 등 로그인 취약점이 확인되었고. J사의 S제품, M사의 D제품, D사의 D제품, H사의 P제품 및 E사의 M 제품 등을 통한 서비스에서 모두 파일이름과 파일내용이 평문으로 나타나는 등 업로드 취약점이 나타났음을 확인할 수 있었다.

[표 1] 서비스별 취약점 분석 현황
[Table 1] Status of vulnerability analysis according to service

서비스명	로그인 취약점	업로드/다운로드 취약점	비고
J사의 S서비스	○	○	로그인시 사용자 ID, 패스워드 및 파일 업로드 다운로드 시 파일명, 파일내용이 평문으로 나타남
M사의 D서비스	○	○	로그인 사용자 ID, 패스워드 및 파일 업로드 다운로드 시 파일명, 파일내용이 평문으로 나타남
D사의 D서비스	×	○	로그인 사용자 ID는 평문으로 저장되지만, 패스워드는 암호화되어 비문으로 저장되며, 파일 업로드와 다운로드 시 파일이름과 형식 및 파일내용이 모두 평문으로 나타남
H사의 P서비스	×	○	사용자 ID와 패스워드는 검색할 수 없었지만, 파일 업로드와 다운로드 시 파일 내용은 평문으로 나타남
E사의 M서비스	×	○	사용자 ID와 패스워드는 검색할 수 없었지만, 파일 업로드와 다운로드 시 파일 내용은 평문으로 나타남

4. 결론

최근 인터넷에 산재한 IT 자원들을 가상화 기술로 통합하여 인터넷만 가능하면 모바일 휴대전화, PC, 스마트 TV 등을 통해 사용자가 원하면 언제 어디서나 손쉽게 접속하여 원하는 작업을 수행할 수 있도록 해주는 클라우드 컴퓨팅이라는 혁신적인 기술이 각광을 받고 있다. 특히, 클라우드 컴퓨팅 기술 중 스토리지 서비스가 인터넷 오픈 마켓의 선두주자인 아마존을 비롯한 기업체와 구글 등의 포털 사이트를 통해 서버와 스토리지를 자체적으로 보유하기 힘든 개인이나 중소기업을 대상으로 제공함으로써 전 세계적으로 큰 반향을 불러일으켰다. 이러한 서비스는 개인이나 중소기업이 문서를 비롯하여 각종 자료를 관리하기 위해 갖추어야 하는 시스템을 구매하고 유지·보수하고 관리하는데 소요되는 비용과 시간 그리고 인력을 획기적으로 줄일 수 있다. 뿐만 아니라 자료를 개인적으로 보관할 경우 저장매체의 오류 등에 기인한 자료의 유실이나 손실에 대비해 자료를 안전하게 보관할 수 있는 등 많은 장점을 가지고 있다. 그러나 시스템이 외부의 공격으로 인하여 개인정보나 자료유출 등 대규모 피해가 우려되는 단점도 있으므로 자료의 기밀성과 무결성 유지를 위하여 자료를 암호화하고 사용자 인증, 컨텐츠 보안, 적절한 보안 정책수립 등의 방법을 통하여 보안 위협요소를 해결해야 한다.

이에 본 논문에서는 국내에서 상용화하여 서비스 중인 J사의 S제품, M사의 D제품, D사의 D제품, H사의 P제품 및 E사의 M 제품 등을 통한 서비스가 적절하게 운영되고 있는지를 살펴보기 위하여 각각의 서비스에 대한 보안 취약점을 살펴보고 그 보안위협 요소를 분석하였다. 그 결과 J사의 S제품과 M사의 D제품 서비스에서는 쿠키에 의한 개인정보 노출 등 로그인 취약점이 나타났으며, J사의 S제품, M사의 D제품, D사의 D제품, H사의 P제품 및 E사의 M 제품 서비스에서는 모두 파일이름과 파일내용이 평문으로 나타나는 등 업로드 취약점이 나타났음을 확인할 수 있었다. 이러한 결과는 문서관리 솔루션을 판매하는 각 업체의 서비스의 사업성 성패를 뛰어 넘어 외부의 불

법적인 공격과 침입을 통해 소중한 개인정보와 자료의 유출 및 손실 등이 동반된다는 측면에서 매우 위험한 상태에 노출되어 있음을 확인시켜 주었다.

따라서 보다 안전하고 신뢰성이 높은 클라우드 컴퓨팅 문서관리 서비스를 제공하기 위해서는 한국인터넷진흥원(KISA) 등의 정부기관과 함께 솔루션을 개발하는 업체들이 문서관리 보안위협 요소들에 대한 보안 요구사항들을 파악하고, 문서관리 보안 솔루션 개발을 위한 표준화된 지침서를 개발하여 솔루션 개발과정에 적용해야 할 것으로 판단된다.

한편, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 46조(집적된 정보통신시설의 보호)와 47조의 4(이용자의 정보보호) 및 48조의 1(정당한 접근권한)에 의한 제한 사항으로 인하여 각 솔루션 서비스의 취약점 분석 동의와 진행에 애로사항이 있었다. 향후 클라우드 컴퓨팅 서비스가 더욱 활성화되고 문서관리를 위한 스트리지 서비스가 더욱 확대될 것이 자명하므로 이에 대한 솔루션 개발 업체의 이해가 선결된다면 OWASP Top10을 기준으로 한 보다 심화된 취약점 분석을 실시할 예정이다.

Reference

[1] S. D. Lee, Cloud Service. OSIA Standards & Technology Review. (2013), Vol.26 No.1, pp52-65

[2] Y. Cui, M. Kim, H. Lee and O. Choi. Home Appliance Control and Management System Based on Cloud Computing Technology. Proceeding of the Korean Institute of Information Scientists and Engineers, (2013), Vol.2013, No.6, pp1325-1327

[3] http://ko.wikipedia.org/wiki/, Sep. 15 (2013)

[4] S. N. Park, A Study on the Security Strategy of Cloud Computing Services. (2013), A Master Dissertation. Paichi University.

[5] D. H. Park and T. Baek, The Study on the Issue of Cloud Computing Security and the Plans for the Personal Information Protection. Journal of KIISC REVIEW. (2011), Vol.21, No.5, pp.37-44.

[6] S. Y. Na and S. D. Lee, Study on Document Security Mechanism for Digital Document Repository. Journal of the Korean Institute of Communications Sciences. (2010), Vol.35, No.12, pp.263-267.

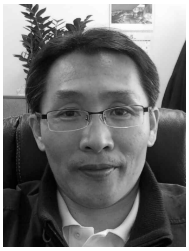
[7] http://www.wireshark.org/, Nov. 10 (2013)

[8] http://www.owasp.org/, Nov. 15 (2013)

[9] http://www.kcc.go.kr/download.do?fileSeq=36875, Nov. 18 (2013)

[10] http://terms.nate.com/dicsearch/view.html?i=3024114, Nov. 18 (2013)

Authors



조성목 (Sung-Mok Cho)

1988년 2월 경북대학교 전자공학과 졸업
1990년 2월 경북대학교 대학원 전자과 석사
1995년 2월 경북대학교 대학원 전자과 박사
2006년 3월 ~ 현재 동명대학교 정보보호학과 교수
관심분야 : 보안통제 시스템, 시스템·네트워크 보안, 개인정보보호관리체계