Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.1, Feb. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.1.165

무인 복합 출력기 솔루션의 취약성 분석*

지 우 중,† 김 형 식‡
성균관대학교

A Security Vulnerability Analysis for Printer Kiosks*

Woojoong Ji,† Hyoungshick Kim‡
Department of Computer Science and Engineering, Sungkyunkwan University, Republic of Korea

요 약

무인 복합 출력기는 길거리, 지하철, 학교, 도서관 등 공공장소에서 사용할 수 있기 때문에, 현재 많은 곳에서 사용되고 있다. 사용자들이 때로는 무인 복합기를 통하여 민감한 정보가 포함된 문서를 출력할 수 있기 때문에 무인 복합 출력기에서는 해당 문서를 안전하게 저장 및 관리되어야 한다. 본 논문에서는 무인 복합 출력기에 대한 다양한 보안 위협 가능성을 분석하고, 실현 가능한 다양한 공격 시나리오를 제시하였다. 제시한 공격의 실현 가능성을 검증하기 위하여, 실제 사용 중인 상용 무인 복합 출력기의 네트워크 트래픽을 분석한 결과, 다른 사용자의 스캔 파일을 탈취할 수 있으며, 무인 복합 출력기의 홈페이지에서는 다른 사용자의 문서를 탈취 할 수 있었다. 이를 이용하여 해당 사용자의 민감한 개인 정보 또한 획득할 수 있음을 확인하였다.

ABSTRACT

They are frequently used today in public places such as street, subway, school or library. Since users can sometimes print documents that contain confidential data using Printer Kiosks, the devices should store and manage the documents securely. In this paper, we identify potential security threats in Printer Kiosks and suggest practical attack scenarios that can take place. To show the feasibility of suggested attack, we analyzed network traffic that were generated by the real Printer Kiosk device. As a result of our analysis, we have found that attackers can access other users' scanned files and access other users' documents from Printer Kiosk's home page. We confirmed that using our attack, we could retrieve other users' personal data.

Keywords: Printer kiosk, HTTP, URL meta data, URL guessing attack

I. 서 론

최근 고가의 프린터 장비와 이를 유지하기 위해 드는 유지 관리 비용 등 여러 가지 비용적인 측면에서 프린터 장비를 사지 않고 일정한 금액을 지불하고 무인 복합 출력기를 많이 사용하고 있는 추세이다. 무인 복합 출력기는 각종 저장매체나 이메일로 받은 각종 문서나 사진 등을 길거리, 지하철, 학교, 도서관 등에서 바로 인쇄 할 수 있고 문서작업은 물론, 인터넷 사용, 필요한 문서나 사진을 스캔하여 전송하는

Received(10. 01 2018), Modified(12. 20. 2018), Accepted(12. 21. 2018)
* 본 논문은 2018년도 하계학술대회에 발표한 우수논문을 개선 및 확장한 것임
* 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2018-2015-0-00403)
† 주저자, woojoong@skku.edu
‡ 교신저자, hyoung@skku.edu(Corresponding author)

기능 등 여러 가지 작업을 복합적으로 사용 할 수 있는 기기이다. 이렇게 무인 복합 출력기가 사람들에게 많은 인기가 있는 이유는 언제 어디서나 원하는 문서 작업을 할 수 있고 또 무인 복합 출력기를 이용하고자 하는 사용자들의 동선을 미리 파악하여 해당 장소에 설치하여 별도의 시설을 찾아다닐 필요 없이 평소 동선상이나 사람들이 많이 다니는 접근성이 좋은 장소에서 간편하게 이용 할 수 있도록 설치하여 사용자들의 접근성을 높여 많은 사용자들이 쉽고 빠르게 무인 복합 출력기를 사용할 수 있도록 하여 많은 사람이 사용하고 있는 추세이다.

그러나 많은 기업에서 이러한 무인 복합 출력기를 개발할 때 외적인 부분과 사용자 인터페이스 등 보안적인 관점이 아닌 다른 외적인 부분에 대해 더 많은 노력과 시간을 투자하는 경향이 있어 사용자의 개인정보나 사용자들이 무인 복합 출력기를 사용함으로써 생기는 보안적인 문제점이 발생 할 수 있다. 예를 들어 사용자들은 무인 복합기를 통하여 민감한 정보가 포함된 문서를 출력할 때이다. 이러한 경우 무인 복합 출력기에서 안전하게 문서가 저장 및 관리되어야 한다. 하지만 무인 복합 출력기 특성상 일반 사용자와 악의적인 사용자를 구분 할 수가 없다. 이렇듯 무인 복합 출력기가 가지는 특수성 때문에 제조사 및 개발자들은 보안에 더욱더 신경을 많이 써야한다. 예를 들어 악의적인 목적이 있는 사용자가 무인 복합 출력기에 일반적인 사용자로 위장하여 악의적인 행동을 수행하기 위해 악성프로그램을 설치하여 악의적인 행동을 하게 된다면 무인 복합 출력기를 사용하는 일반 사용자의 정보는 악의적인 사용자에게 전송되어 많은 문제점이 생길 수 있다.

본 논문에서는 무인 복합 출력기에 대한 공격자 모델, 다양한 보안 위협 가능성을 분석하고 실현 가능한 다양한 공격 시나리오를 제시하였다. 이러한 보안적인 문제점을 분석하기 위해 실제 사용 중인 상용 무인 복합 출력기의 네트워크 트래픽을 분석한 결과, 다른 사용자의 스캔 파일을 탈취할 수 있었으며 사용자의 개인 문서함에 존재하는 파일 역시 탈취 할 수 있었다. 이를 통하여 사용자의 민감한 개인 정보 또한 획득할 수 있음을 확인하였다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구를 설명하고, 3장에서는 무인 복합 출력기에 대한 공격자 모델에 대해 설명하고 4장에서는 무인 복합 출력기에 대한 공격 방법에 대해 설명한다. 5장에서는 4장에서 설명한 공격 방법을 적용하여 실제 사용자의 개인정보 유출 사례를 소개한다. 6장에서는 취약점 개선방안, 마지막으로 7장에서는 결론을 제시한다.

II. 관련 연구

2.1 무인 복합 출력기 보안

무인 복합 출력기는 길거리, 지하철, 학교, 도서관 등 공공장소에서 일반적인 사용자뿐만 아니라 악의적인 사용자도 일반 사용자의 신분으로 위장하여 사용할 수 있기 때문에 더욱 더 보안에 신경을 써야한다. 이와 같은 문제점으로 과거 연구에서는 공공장소에 설치된 무인 복합 출력기에 대한 위협들을 소개 하였다[1]. 무인 복합 출력기의 특징에 대해 설명하자면 무인 복합 출력기를 이용하는 사용자들은 대부분 무인 복합 출력기의 관리자나 직원의 개입 없이 사용할 수 있으며 개발된 목적 이외의 서비스들에 대해서는 제한적인 서비스를 제공한다[1]. 예를 들어 사용자가 개발된 목적 이외의 행동을 하거나 무인 복합 출력기에 설치된 소프트웨어를 조작할 시 사용자의 부적절한 행동에 대해서 무인 복합 출력기에서는 이러한 부적절한 행동을 탐지하여 사전에 차단하거나 개발된 목적에 맞는 서비스들만 동작할 수 있게 동작한다. 하지만 무인 복합 출력기의 특징 중 가장 큰 문제점은 관리자나 직원의 개입 없이 누구나 무인 복합 출력기에 접근 할 수 있는 특징이다. 예를 들어 사용자의 신원에 따라 권한을 할당 할 수 있는 기업 네트워크와는 달리, 무인 복합 출력기는 일반적인 사용자뿐만 아니라 악의적인 사용자를 포함한 모든 사용자가 동일한 권한을 갖는다. 따라서 무인 복합 출력기에서는 일반적인 사용자와 악의적인 사용자를 구별하기는 쉽지가 않다[1]. 이러한 무인 복합 출력기의 특징 때문에 실제 해킹 사건[2]으로 인해 피해를 본 사례가 존재하며 이러한 해킹 사건을 사전에 예방하기 위해서는 잠재적인 보안 위협을 도출하고 무인 복합 출력기를 개발하기 전 도출된 위협들에 대하여 사전에 예방하여야 한다.

과거 연구에서는 공공장소에 설치된 무인 복합 출력기에 존재하는 보안 위협들에 대하여 하드웨어에 대한 위협, 사용자에 대한 위협, 무인 복합 출력기를 구성하고 있는 제조사에 대한 위협 총 3가지로 분류하였다[1]. 각각의 위협에 대해서 정리하면 다음과 같다.

하드웨어에 대한 위협은 무인 복합 출력기의 물리

적인 접근 통제 장치에 대한 보안 위협이다. 예예를 들어 물리적인 장치로 잠긴 무인 복합 출력기에 대해서 강제로 자물쇠를 열어 기존의 하드웨어를 도난당하거나 악의적인 사용자가 악성 행위를 수행할 수 있도록 강제적으로 키보드, 마우스 같은 부속품을 교체하여 악성 키보드[3]로 인한 사용자가 입력한 민감한 정보에 대해서 악성 행위를 수행할 수 있다.

사용자에 대한 위협은 악의적인 사용자에 의해 생기는 보안 위협이다. 악의적인 사용자들의 최종 목표는 무인 복합 출력기에서 입력한 일반 사용자들의 민감한 정보들이다. 이러한 민감한 정보를 탈취하기 위해 무인 복합 출력기에 악성 소프트웨어를 설치하여 악의적인 사용자에게 실시간으로 탈취한 데이터를 전송한다.

제조사에 대한 위협은 무인 복합 출력기를 제조할 때 다른 회사에서 생산되어 무인 복합 출력기를 구성하는 제품 중 보안 안정성에 대한 검증과 취약점이 존재하는 제품에 대한 위협이다. 무인 복합 출력기는 대부분 네트워크에 연결되어있다. 하지만 안전하지 않은 무인 복합 출력기는 악의적인 사용자의 공격 목표가 될 수가 있는데 예를 들어 사용자의 오랜 비행이나 편의성을 위해 비행기 의자 뒤편에 무인 키오스크가 탑재하고 있다. 하지만 무인 키오스크를 구성하고 있는 네트워크 제품 중 보안에 취약하여 허가된 사람만이 제어 할 수 있는 비행기 제어 네트워크와 일반 사용자의 네트워크를 따로 분리하지 않을 수 있기 때문에 악의적인 사용자에 의해 비행기 제어는 물론 큰 인명 피해도 발생 할 수도 있다[4].

2.2 웹 어플리케이션 보안

웹 어플리케이션이란 웹 브라우저에서 이용할 수 있는 응용 소프트웨어를 말한다. 웹 어플리케이션의 취약점이 다른 레벨의 취약점 보다 상대적으로 많이 나타남을 알 수 있다[5]. 본 논문에서도 악의적인 사용자가 웹 어플리케이션 공격하기 위해서 공격대상 탐색, 정보수집, 시험, 공격계획 수립, 공격의 5가지의 단계로 진행 하였으며 특히 정보 수집 및 시험 단계에서 암호화가 전혀 되어 있지 않은 URL 메타데이터에 대한 공격을 진행하였다. URL 메타데이터에 대해서 암호화가 이루어져있지 않으면 해당 웹 어플리케이션이 어떻게 동작하는지 알 수 있으며 부적절한 접근을 통해 URL 메타데이터를 분석하고 공격을 할 수 있는 중요한 정보가 될 수 있다. 이러한 공격을 방지하기 위해서는 URL 메타데이터에 대한 값뿐만 아니라 누구나 식별할 수 있는 URL 메타데이터에 대한 정보를 모두 암호화하여 악의적인 사용자로부터 웹 어플리케이션을 안전하게 보호해야 한다.

또한 URL 메타데이터에 대한 암호화뿐만 아니라 웹 어플리케이션 보안을 높이기 위해 Bau, J. et al.[6]에서는 웹 어플리케이션에서 존재하는 보안 취약점에 대해 자동화 된 도구를 이용하여 기존의 웹 어플리케이션에서 발생했던 주요 취약점을 탐지하였다. 그 중 가장 많이 발견되었던 웹 어플리케이션 취약점은 Cross-Site Scripting, SQL injection, Cross-Channel Scripting, 민감한 정보 노출이 가장 많이 발견되었다.

III. 공격자 모델

이번 장에서는 실제 사용 중인 상용 무인 복합 출력기 시스템을 위협하는 공격자의 모델을 정의하고 무인 복합 출력기 시스템을 위협하는 공격자의 능력과 범위에 대해 내부 공격자와 외부 공격자에 대해 설명한다.

3.1 내부 공격자

공격자 모델에서 내부 공격자의 범위는 무인 복합 출력기 시스템에 접근이 가능한 모든 공격자를 의미한다. 예를 들어 무인 복합 출력기의 관리자나 이를 이용하는 익명의 모든 사람들이 포함 된다. 무인 복합 출력기의 성격상 일반 사용자와 악의적인 사용자를 구분 할 수 없기 때문에 무인 복합 출력기에 아무런 제한 없이 직접적인 접근이 가능하다. 이 말은 공격자는 조금 더 악의적인 행동을 적극적으로 수행 할 수 있다는 의미 이다. 예를 들어, 개인 정보 유출이라는 악의적인 행동을 수행하기 위해 바이러스 설치, 키로거 등 직접적으로 악성 프로그램을 설치 할 수 있다.

3.2 외부 공격자

외부 공격자는 직접적으로 무인 복합 출력기에 직접적으로 접근이 불가능하지만 외부에서 악의적인 목적을 가지고 해당 시스템에 접근하는 공격자를 의미한다. 본 논문에서 정의하는 외부 공격자는 내부 공격으로 얻은 정보를 활용하여 해당 시스템을 공격하

여 개인정보를 유출 하는 방식으로 악의적인 행동을 수행 한다.

외부 공격자는 무인 복합 출력기에 대해서 일반 사용자로 위장하여 내부 공격을 통하여 얻은 정보를 분석 하여 외부에서 무인 복합 출력기의 시스템과 서버에 존재하는 취약점을 이용하여 무인 복합 출력기의 회원인 사용자와 비회원의 스캔 파일과 각 사용자의 문서함에 존재하는 파일을 탈취 하는 실제 공격 사례를 제시한다. 위의 내용을 정리하면 다음과 같다.

1) 무인 복합 출력기에 접근 할 수 있는 모든 사람이 잠재적인 공격자가 될 수 있다.
2) 공격자는 무인 복합 출력기의 다양한 서비스 중 스캔 파일 서비스에 대해 다른 사용자의 스캔 파일에 대해 탈취 할 수 있다.
3) 공격자는 무인 복합 출력기뿐만 아니라 홈페이지에 존재하는 각 사용자의 문서함에 존재하는 파일 또한 탈취 할 수 있다.

IV. 메타 데이터를 이용한 공격

본 논문에서는 상용 무인 복합 출력기 A사에 대해 내부 공격을 통해 얻은 정보를 분석한 결과 URL 메타 데이터의 정보를 이용해 취약하게 관리되고 있다는 사실을 발견하였다.

이번 장에서는 메타 데이터에 대해 설명하고 메타 데이터를 활용하여 공격 할 수 있는 재전송 공격, 추측 공격 마지막으로 실제 사용 중인 상용 무인 복합 출력기에 대한 공격 시나리오에 대해 설명하겠다.

4.1 메타 데이터

메타 데이터란 일반적으로 데이터에 대한 데이터라는 추상적 개념으로 정의가 된다. 하지만 메타 데이터가 구체적인 의미를 갖기 위해서는 다시 정의를 내릴 필요가 있다. 이에 따라 ISO 15489에서는 메타 데이터를 기록의 맥락과 내용, 구조와 기록관리 전 과정을 기술한 데이터라고 정의하고 있다. 즉, 기록에 대하여 맥락, 내용, 구조, 관리내력 이라는 4가지 영역을 기술하는 데이터라고 이해할 수 있다.

메타 데이터의 유형 중 HTTP URL 메타 데이터가 있다. 이 URL 메타 데이터는 URL에 특정 데이터를 저장하는데 사용이 된다. 예를 들어 URL 메타 데이터에 대한 입력은 RFC 표준에 의하면 http://host:port/path?query의 구성으로 이루어져 있다[7]. 위의 구성으로 되어 있을 시 악의적인 사용자는 해당 URL이 어떤 데이터를 저장하고 어떤 행위를 하는지에 추측할 수 있다.

본 논문에서는 이러한 URL 메타 데이터의 정보를 이용해 취약하게 관리되고 있는 상용 무인 복합 출력기 A사에 대해 분석하였다.

4.2 재전송 공격

재전송 공격[8][9]이란, 사용자의 인증을 쿠키[10]에만 의존할 경우 공격자는 단순한 네트워크 도청을 통해 해당 쿠키 정보를 쉽게 탈취해 사용자의 인증을 도용할 수 있다. 예를 들어, 탈취한 쿠키 정보를 그대로 해당 사이트에게 다시 보내게 되면 해당 사이트는 쿠키만 가지고 사용자를 인증하기 때문에 그대로 탈취 당한 사용자의 계정으로 로그인이 되거나 해당 쿠키 정보가 적용된 타 사이트까지 이동이 가능하기 때문에 사용자의 민감한 데이터까지 탈취가 가능하다. 이렇게 탈취당한 쿠키를 이용해서 인증이 되는 이유는 요즘 웹 서비스들은 그룹 단위로 통합하는 곳이 늘어감에 따라 사용자의 쿠키 값으로 사용자를 인증하기 때문이다.

이렇듯 사용자의 로그인에 의해 생성되는 쿠키 정보가 매번 생성되는 정보가 아니거나 만료 시간이 존재하지 않는 경우나 고정된 쿠키 정보를 사용하게 된다면 악의적인 사용자에 의해 탈취당한 사용자 인증 쿠키 정보는 항상 해당 사용자의 권한을 가지고 있는 것이라고 할 수 있다.

본 논문에서도 쿠키 정보를 이용하여 무인 복합 출력기의 홈페이지에서 제공하는 각 사용자의 문서함에 존재하는 파일을 탈취하는 사례를 소개한다.

4.3 URL 추측 공격

본 논문에서는 해당 사용자를 나타내는 URL 메타 데이터의 정보가 취약하게 관리 되고 있어 추측 공격으로 다른 사용자의 개인정보까지 탈취가 가능한 것을 실제 사례를 통해 소개한다.

URL 추측 공격(Guessing Attacks)[11]이란, 공격자가 접근하고자 하는 URL에 대해 URL 메타 데이터를 많은 시도를 통해 추측하는 공격이다. 일반적으로는 URL 메타 데이터는 임의의 문자열로 구성되어 이러한 추측 공격에 대해 안전하다. 하지만 A사의 스캔 파일에 대한 URL 메타 데이터 같은 경우에

는 7자리의 연속적인 정수와 사용자의 유형으로 되어 있어 공격자는 쉽게 추측 할 수 있다.

다시 말해 URL 메타 데이터에서 사용자의 고유한 정보를 나타낸 정보를 이용하여 재전송 공격을 수행하거나 사용자를 나타내는 공간이 7자리로 제한적이기 때문에 악의적인 공격자는 제한된 공간만큼만 추측 공격을 수행하게 된다면 다른 사용자의 데이터까지 얼마든지 접근이 가능하다는 것을 확인하였다.

4.4 공격 시나리오

이번 절에서는 본 논문에서 제시하는 공격 시나리오에 대해 자세히 설명한다. 첫 번째 공격 시나리오는 사용자의 스캔 파일을 탈취하는 공격, 두 번째는 해당 홈페이지에 존재하는 각각의 사용자의 문서함에 존재하는 파일을 탈취하는 공격에 대해 설명하고자 한다.

4.4.1 스캔 파일 탈취 공격

먼저 해당 공격이 이루어지려면 무인 복합 출력기만의 특수성을 이용한다. Fig. 1에서는 일반 사용자와 악의적인 사용자가 함께 존재한다. 무인 복합 출력기에서는 이를 회원가입을 통해 구분하려고 하지만 A사의 경우 비회원도 이용이 가능하기 때문에 악의적인 사용자는 자신의 신분을 노출하지 않고도 악의적인 행동을 수행 할 수 있다.

Fig. 1에 대해서 설명하자면 ①에서 일반 사용자는 회원가입을 통해 회원으로 해당 솔루션을 이용하거나 비회원으로 선택하여 일정한 금액을 지불하고 해당 서비스를 이용하기 시작한다. 그런 다음 사용자는 자신이 원하는 문서작업, 인터넷 서핑, 스캔, 인쇄 등 여러 기능 중 사진을 스캔하는 작업을 한다고 가정하자. 사용자가 스캔한 스캔파일은 ②처럼 해당 솔루션 서버에게 보내게 된다. 그런 다음 해당 파일 서버는 ③처럼 각각의 사용자에게 받은 스캔파일을 랜덤한 7개의 정수로 구분하여 저장한다. 그런 다음 마지막으로 ④처럼 각 사용자가 회원가입 또는 비회원으로 사용했을 시 입력했던 이메일로 파일을 전송한다. 하지만 해당 시스템은 사용자가 스캔한 파일을 사용자가 회원가입을 할 때 입력했던 이메일로 해당 URL 정보를 평문의 값으로 넘겨주게 된다. 그 후 사용자는 평문으로 된 HTTP URL 메타 데이터를 통해 파일 서버에 스캔 파일을 다운로드 받는다.

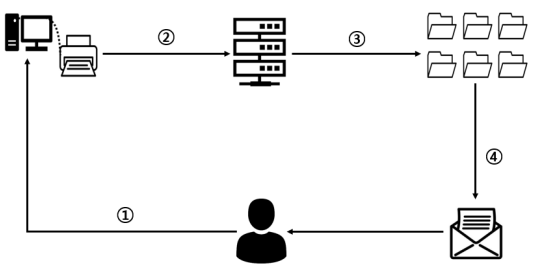

Fig. 1. General printer kiosk service structure

본 논문에서는 ④번 과정에서 스캔한 파일을 다운로드 받을 시 평문의 URL 메타 데이터를 조작하여 회원과 비회원의 스캔 파일을 탈취 하였다. Fig. 2는 해당 사용자의 이메일로 전송된 평문의 URL로 해당 파일을 다운로드 받을 때 WireShark[12]로 패킷을 캡쳐한 패킷 내용이다.

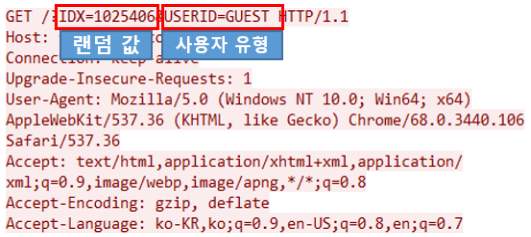

Fig. 2. Example of scan file request message for guest user.

위의 Fig. 2를 보면 해당 HTTP URL 메타 데이터에 대해 암호화가 전혀 적용되어 있지 않다. 이는 악의적인 사용자가 이를 분석하는 능력이 있다고 가정한다면 http://해당 솔루션 파일 서버의 host 주소/?IDX=특정한 랜덤 값&USERID=해당 유저의 타입 이라는 것을 쉽게 알 수가 있다. 위의 패킷 정보를 얻기 위해서 공격자는 일반 사용자로 위장하여 일반 사용자와 똑같이 해당 무인 복합 출력기를 이용하여 획득한다.

4.4.2 개인 문서함 탈취 공격

해당 A사의 홈페이지에서는 USB와 이메일을 사용하지 않더라도 사용자가 무인 복합 출력기를 이용하기 전에 해당 파일을 서버로 업로드 하여 자기 자신만이 접근 할 수 있는 Fig. 3처럼 내문서함이라는 기능을 도입하여 사용자가 편리하게 인쇄, 프린터, 스

Fig. 3. A list of documents box of malicious users in company A.

캔 등의 기능을 사용할 수 있도록 하여 사용자의 편의성을 높여 많은 사람들이 사용하고 있는 서비스 중 하나이다. 이 서비스는 비회원은 사용 할 수 없으며 해당 서비스를 이용하기 위해서는 해당 A사의 홈페이지에서 회원 가입을 통해 회원으로 가입을 해야 사용할 수 있는 서비스이다.

Fig. 4는 사용자의 문서함에 존재 하는 파일을 다운로드 받을 때의 패킷을 캡쳐 한 내용이다. A사의 파일 서버 같은 경우는 각각의 사용자가 자신의 문서함에 파일을 업로드하게 되면 bSeq와 intSeq에 랜덤한 값을 부여 받게 된다. 하지만 이러한 값은 앞서 설명한 3.4.1 스캔 파일 탈취 공격과 같은 방법으로 부여 받기 때문에 악의적인 사용자는 똑같은 공격 방법으로 진행한다. 이렇게 다른 사용자의 문서함에 존재하는 파일에 접근 할 수 있는 이유는 앞서 3.2 재전송 공격에서 설명한 것처럼 사용자의 쿠키 정보가 전혀 바뀌지 않는다는 점이다.

본 논문에서는 Chrome 확장 프로그램[13] EditThisCookie를 이용하여 쿠키 값을 추출하여 쿠키 정보를 비교 해보았다. 서로 다른 사용자에서 추출한 쿠키 정보 Fig. 5와 Fig. 6에서 보는 것처럼 사용자의 ID만 다를 뿐 로그인과 관련된 다른 모든 쿠키 정보가 같다는 것을 발견하였다. 이는 악의적인 사용자에 의해 쿠키 정보가 탈취 당하거나 탈취 당하지 않아도 공격자 자신의 쿠키 정보를 활용하여 쿠키 정보와 HTTP URL 메타 데이터를 조작하여 다른 사용자의 권한과 파일을 탈취 할 수 있다.

```
GET /library/download.asp?bSeq=7&intSeq=162189&fileNum=1 HTTP/1.1
Host:
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8
```

Fig. 4. Example of documents file request message for member user.

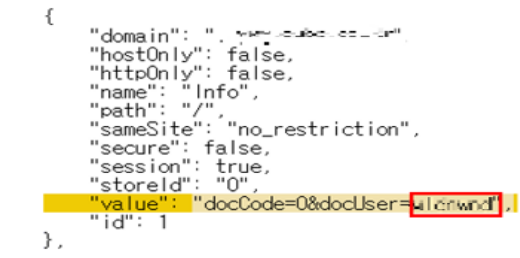

Fig. 5. Cookie information for A user.

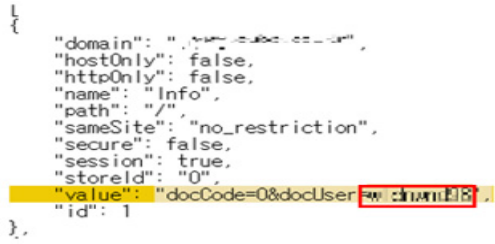

Fig. 6. Cookie information for B user.

V. 무인 복합 출력기 공격 실험 결과

본 장에서는 위에서 설명한 두 가지의 공격시나리오를 바탕으로 무인 복합 출력기 A사에 대해 실제 공격에 대한 결과를 설명한다.

5.1 무인 복합 출력기 회원 공격

Fig. 2에서는 비회원으로 USERID=GUEST로 되어 있지만 Fig. 7을 보면 USERID=해당 유저 ID를 볼 수가 있다. 유저 ID는 해당 솔루션 자유게시판 Fig. 8에서 보는 것처럼 쉽게 얻을 수가 있다. 이런 방식으로 악의적인 사용자는 자유게시판이나 다른 사용자가 올린 게시물에서 다른 사용자의 ID를 얻어와 해당 값을 변조하는 프로그램을 실행하여 악의적인 사용자는 IDX값과 USERID를 각각 변조해 변조된 HTTP URL 메타 데이터를 파일서버에게 재전송 공격을 수행하면 파일 서버는 이를 검증하지 않고 그대로 해당 스캔 파일을 넘겨주게 된다.

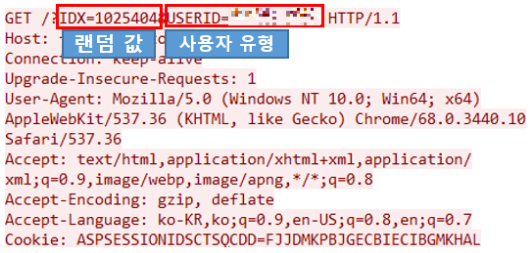

Fig. 7. A scan file download request packet of the member user.

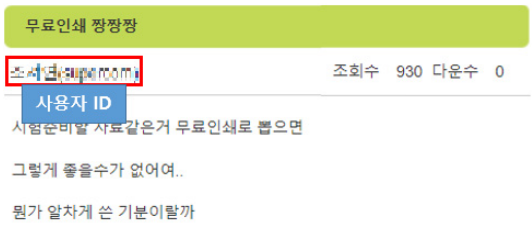

Fig. 8. User ID exposed on A company's free board.

5.2 비회원 공격

A사의 경우 회원가입을 하지 않고 회원가입 했을 때와 동일하게 서비스를 이용 할 수 있다. 다른점은 USERID에 회원 ID가 아닌 GUEST로 설정된다. IDX는 최대 10자리를 가지는 0부터 9까지의 정수이다. 우리는 이러한 랜덤한 값을 분석한 결과 7자리의 랜덤한 정수를 주로 사용하며 이는 10자리를 사용할 때보다 키 공간이 더 작아진다는 의미이다.

또 파일 서버 특성상 모든 파일을 계속해서 저장할

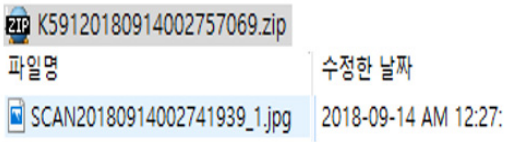

Fig. 9. Exposed scan files of users due to guest attacks.

수 없기 때문에 일정한 시간이 지나면 해당 파일을 삭제해 더 이상 다운로드 할 수 가 없다. 따라서 IDX가 가지는 전체적인 공간은 더 줄어들어 추측공격과 무차별공격[14]으로 인해 빠른 시간에 회원/비회원의 Fig. 9처럼 스캔 파일에 접근할 수가 있고 Fig. 10처럼 해당 스캔파일에는 여러 가지 개인정보들이 포함된 많은 문서들이 유출되었음을 확인하였다. 또 해당 파일의 이름이 생성될 때 사용자가 사용한 무인 복합 출력기의 기기 번호와 스캔한 시간으로 기본적으로 설정되어 스캔 파일 이름과 해당 개인정보가 유출된다면 사용자의 위치도 함께 노출이 때문에 각종 범죄의 대상이 될 우려가 높다.

Fig. 10. List of scan files of users exposed due to member attacks and guest attacks.

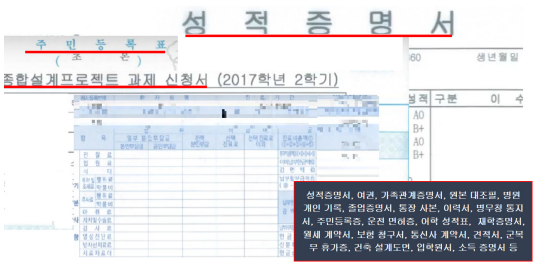

Fig. 10-1. List of scan files of users exposed due to member attacks and guest attacks.

5.3 문서함 파일 공격

본 절에서는 A사의 쿠키 정보가 사용자별로 ID만 다를 뿐 나머지 쿠키 정보는 같다는 취약점을 활용하여 다른 사용자의 문서함에 존재하는 파일을 탈취하는 공격에 대해 설명하겠다.

먼저 악의적인 사용자는 자기 자신의 계정으로 로그인을 한 후 자신의 내문서함에 아무런 파일을 내문서함에 업로드를 실시한다. 그런 다음 Fig. 11처럼 자신의 쿠키 정보를 이용하여 내문서함에 존재하는 파일 목록을 가져오는 악성 프로그램을 만든다.

악의적인 사용자가 성공적으로 자신의 내문서함의 파일 목록을 가져왔다면 Fig. 8처럼 자유게시판에 노출된 다른 사용자의 ID를 활용하여 로그인과 관련된 쿠키 정보를 변조하여 Fig. 12처럼 다른 사용자의 내문서함의 파일 목록 또한 탈취 할 수 있다.

악의적인 사용자는 다른 사용자의 파일을 탈취하기 위해 자신의 쿠키 정보에서 사용자의 ID 값만 변조하여 다른 사용자의 목록을 가져온 다음 bSeq와 intSeq 값을 획득한다. 여기서 bSeq의 값은 6, intSeq 값은 485407이다. 이렇게 다른 사용자의 bSeq 값과 intSeq 값을 획득한 악의적인 사용자는 Fig. 13처럼 다른 사용자의 파일 또한 탈취 할 수 있다.

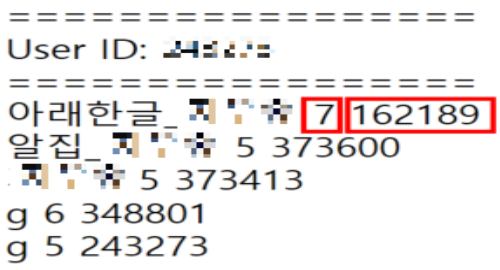

Fig. 11. List of malicious user's document box files.

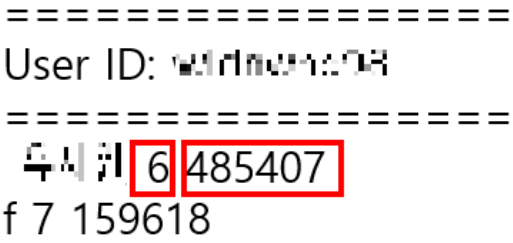

Fig. 12. List of the victim's document box file.

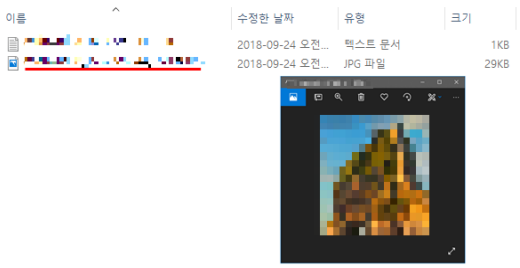

Fig. 13. Exposure of victim's document box file.

VI. 취약점 개선방안

발견된 3가지 취약점은 무인 복합 출력기 개발 업체에서 조금만 보안에 관심만 있었어도 막을 수 있는 간단한 취약점이다. 이러한 공격을 제일 간단하게 방어할 수 있는 기법은 해당 HTTP URL 메타 데이터를 해시함수를 통해 악의적인 사용자가 일반적인 사용자로 위장하여 위와 똑같은 방법을 사용하더라도 URL 메타데이터에는 추측 할 수 없는 해시값이 들어가 있기 때문에 큰 비용 없이 해당 취약점에 대한 공격을 막을 수가 있다. 자세히 설명하자면 악의적인 사용자에 의해 한번 탈취당한 HTTP URL 메타데이터에 대해서 서버 측에서는 고정된 메타데이터를 사용하지 않고 매번 다른 값을 생성한다. 즉 서버 측에만 사용하는 salt값과 서버 측의 시간을 함께 해시함수를 통해 URL 메타데이터를 구성한다면 한번 탈취당한 HTTP URL 메타데이터는 식별할 수 없는 데이터가 되기 때문에 악의적인 사용자는 URL 메타데이터를 이용하여 더 이상 공격 할 수가 없게 된다. 또 서버에서는 사용자의 쿠키 정보를 사용자별로 다르게 생성해야 하며 식별할 수 없는 값을 사용해야한다. 또한 서버에서 한번 발급된 쿠키 정보는 서버 측에서 일정한 시간이 지나면 로그인에 관한 쿠키 정보를 다시 재발급 받게 하여 악의적인 사용자에 의해 탈취당한 쿠키 정보를 재사용 할 수 없게 하여야 한다.

VII. 결 론

본 논문은 무인 복합 출력기에 대한 취약성을 알아보았다. 하지만 우리나라의 중, 소규모 기업들은 이런 취약점이 발견되었다고 하더라도 보안인력과 취약점을 개선할 때 발생하는 비용적인 측면 때문에 이를 확인하고도 묵인하고 있는 경우가 많다. 이와 마찬가지로 본 논문에서 소개한 무인 복합 출력기에 대한

취약성을 해당 기업에게 2017년 9월 20일에 해당 취약점을 발견하여 제보를 하였지만 2018년 9월 18일 현재까지도 패치가 되어있지 않은 상황이다. 해당 취약점은 HTTP URL 메타 데이터를 악의적인 사용자가 마음대로 조작할 수 있다는 점과 파일 서버에서 아무런 사용자의 인증을 거치지 않고 해당 스캔파일을 다운로드 할 수 있고 사용자 별로 로그인과 관련된 쿠키 정보가 같아 악의적인 사용자에 의해 각각의 사용자의 '내문서함'에 존재하는 파일을 탈취 할 수 있다는 것을 실제 사례를 통해 확인하였다.

References

〔1〕 Smith, B. (2008). Hacking the kiosk. Retrieved from. 〔website〕 〔2019. 02. 11〕 URL: https://pdfs.semanticscholar.org/8b4f/1b9cf984b25141f55670742816e0ea36a54c.pdf.

〔2〕 RSA CONFERENCE COMPUTERS SO FAUX SECURED. Wired Magazine. 〔website〕 〔2019. 02. 11〕 URL: https://www.wired.com/2007/02/rsa-conference-/.

〔3〕 Built-in Keylogger Found in MantisTek. 〔website〕 〔2019. 02. 11〕 URL:https://thehackernews.com/2017/11/mantistek-keyboard-keylogger.html.

〔4〕 In Flight Hacking System. 〔website〕 〔2019. 02. 11〕 URL: https://ioactive.com/in-flight-hacking-system.

〔5〕 Lim, D. B., & Park, J. C. (2011). Link-E-Param: A URL Parameter Encryption Technique for Improving Web Application Security. The Journal of Korean Institute of Communications and Information Sciences, 36(9B), 1073-1081.

〔6〕 Bau, J., Bursztein, E., Gupta, D., & Mitchell, J. (2010, May). State of the art: Automated black-box web application vulnerability testing. In 2010 IEEE Symposium on Security and Privacy (pp. 332-345). IEEE.

〔7〕 Berners-Lee, T., Masinter, L., & McCahill, M. (1994). Uniform resource locators (URL) (No. RFC 1738).

〔8〕 YoungJae Maeng, DaeHun Nyang. (2008). An Analysis of Replay Attack Vulnerability on Single Sign-On Solutions*. Journal of the Korea Institute of Information Security & Cryptology, 18(1), 103-114.

〔9〕 Syverson, P. (1994, June). A taxonomy of replay attacks 〔cryptographic protocols〕. In Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings (pp. 187-191). IEEE.

〔10〕 Jong-Phil Yang, Kyung-Hyune Rhee. (2002). The proposal of improved secure cookies system based on public-key certificate. The Journal of Korean Institute of Communications and Information Sciences, 27(11C), 1090-1096.

〔11〕 Lee, S., Kim, J., Ko, S., & Kim, H. (2016, August). A security analysis of paid subscription video-on-demand services for online learning. In Software Security and Assurance (ICSSA), 2016 International Conference on (pp. 43-48). IEEE.

〔12〕 Wireshark, 〔website〕 〔2019.02.11.〕 URL: https://www.wireshark.org/down lo a d.html.

〔13〕 EdithisCookie, 〔website〕 〔2019.02.11.〕 URL: http://www.editthiscookie.com.

〔14〕 Botelho, B. A. P., Nakamura, E. T., & Uto, N. (2012, December). Implementation of tools for brute forcing touch inputted passwords. In Internet Technology And Secured Transactions, 2012 International Conference F or (pp. 807-808). IEEE.

〈저자소개〉

지 우 중 (Woojoong Ji) 학생회원
2018년 2월: 중부대학교 정보보호학과 학사
2018년 3월: 성균관대학교 전자전기컴퓨터공학과 석사과정
〈관심분야〉 Network security, IoT security, Security Engineering

김 형 식 (Hyoungshick Kim) 종신회원
1999년 2월: 성균관대학교 정보공학부 학사
2001년 2월: KAIST 컴퓨터 과학과 석사
2012년 2월: University of Cambridge 컴퓨터공학과 박사
2013년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 조교수
〈관심분야〉 보안공학, 소셜 컴퓨팅