Journal of The Korea Institute of Information Security & Cryptology
VOL.31, NO.5, Oct. 2021
ISSN 1598-3986(Print)
ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.5.941

침해된 웹 SSO 계정 보호를 위한 보안 조치 실험 연구*

남 지 현,[1†] 최 형 기[2‡]
[1,2]성균관대학교 (대학원생, 교수)

Measurement of Remediation for Compromised User Account of Web Single Sign-On (SSO)*

Ji-Hyun Nam,[1†] Hyoung-Kee Choi[2‡]
[1,2]Sungkyunkwan University (Graduate student, Professor)

요 약

계정 통합 시스템(SSO)은 다수의 웹사이트 계정 비밀번호를 통합 관리하기 때문에 높은 보안이 요구된다. 계정 통합 시스템을 이용하는 사용자는 웹사이트 로그인 시 주인증기관(IdP)을 통해 인증된다. 본 논문에서는 주인증기관 계정이 탈취된 사용자의 피해를 최소화하기 위하여 주인증기관이 취할 수 있는 보안 요구사항을 제시한다. 이를 만족하지 않을 시 발생하는 보안 위협을 설명한다. 실험을 통해 주인증기관이 보안 요구사항을 만족하지 않으면 사용자가 공격을 인지하더라도 공격자의 세션을 취소시킬 수 없음을 증명한다.

ABSTRACT

Single Sign-On (SSO) service manages user's account passwords from multiple websites so that security in a high level is required. Users who use the SSO service are authenticated through the Identity Provider (IdP) when logging into the website. We present the security requirements that IdP can take in order to minimize the user's risk whose IdP account is compromised. We describe the security threats that arise when the security requirements are not satisfied. Through evaluation, we prove that the attacker's session cannot be canceled even if the user recognizes the attack if the IdP does not satisfy the security requirements.

Keywords: SSO(Single Sign-On), Session Remediation, User Account Protection, Web Security, IdP(Identity Provider)

I. 서 론

웹서비스들이 다양해지면서 사용자들은 복수의 웹사이트의 계정 비밀번호를 관리하는 어려움을 겪고 있다. 어려움을 해결하기 위해 웹사이트는 계정을 통합 관리하는 서비스를 제공한다[1]. 계정 통합 시스템(SSO, Single Sign-On)은 주인증기관(IdP, Identity Provider)과 서비스기관(RP, Resource Provider)으로 구성된다. 주인증기관에서는 사용자 인증을 수행하고 서비스기관에서는 웹서비스를 제공한다. 서비스기관은 주인증기관의 사용자 계정을 위임받아 계정을 생성한다. 사용자는 주인증기관에서의 계정 로그인을 통해 서비스기관에 로그인할 수 있다. Facebook, Google, Microsoft 등 웹사이트는 주인증기관으로써 10억개 이상의 계정에 계정 통합 시스템을 지원한다[2][3].

서비스기관의 사용자 계정은 주인증기관의 사용자 계정에 종속적이다. 주인증기관에서 사용자 계정의 인증 정보가 변경되면 연동된 서비스기관 계정의 로

Received(07. 19. 2021), Modified(09. 01. 2021), Accepted(09. 06. 2021)
* 본 연구는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행하였습니다. (No.2020R1A2C1012708)
† 주저자, jhnam19@o365.skku.edu
‡ 교신저자, meosery@skku.edu(Corresponding author)

그인 상태가 변경되어야 한다. 로그인 상태 변경은 주인증기관 및 서비스기관에서 로그인된 사용자 계정을 로그아웃시키는 과정을 의미한다. 즉, 주인증기관의 이전 인증 정보로 로그인되었던 서비스기관 계정을 로그아웃시키고 새로운 인증 정보로 사용자를 다시 인증해야 한다.

주인증기관과 서비스기관은 독립된 웹사이트이다. 주인증기관이 사용자 계정의 인증 정보가 변경되었음을 연동된 서비스기관과 공유하지 않는 경우, 서비스기관은 사용자 계정의 로그인 상태를 변경해야 함을 알지 못한다. 로그인 상태가 변경되지 않으면 두 계정의 연동은 부분적으로 단절되어 보안 문제점을 야기한다. 예시로 본 논문의 실험에서 주인증기관의 사용자 계정이 삭제되더라도 연동된 서비스기관의 사용자 계정에 여전히 로그인되는 문제가 발생하였다.

본 논문은 사용자 계정 보호를 위해 주인증기관이 제공해야 하는 보안 요구사항을 제시하고, 이를 만족하지 않을 시 발생하는 보안 위협을 설명한다. 실제 주인증기관을 대상으로 보안 요구사항 만족 여부를 실험하기 위해 크롤러를 작성하여 Alexa 상위 1,000개 웹사이트에서 주인증기관과 서비스기관을 식별한다. 주인증기관에서 사용자 계정의 인증 정보를 변경한 뒤, 서비스기관에서의 로그인 상태 변경 여부를 실험한다. 실험 결과 26개 주인증기관 중 96% 주인증기관의 사용자 계정에서 연동된 서비스기관 계정과 부분적으로 단절되어 있음을 증명하였다. 주인증기관과 서비스기관 간 계정 단절 문제를 보완하기 위해 주인증기관이 서비스기관에게 계정의 로그인 상태 변경을 요청하는 프로토콜을 제안한다.

II. 배경 지식

서비스를 제공하는 웹사이트들은 개개인에 특화된 서비스를 제공하기 위해 사용자 별로 계정을 요구한다. 웹을 이용한 서비스들의 양과 수의 증가로 사용자들은 사이트 별로 서로 다른 계정 관리에 어려움을 겪고 있다. 이를 해결하기 위해 웹사이트는 SSO를 적용하여 사용자 편리성을 높였다. SSO는 단일 계정으로 복수의 웹사이트에 접속할 수 있는 서비스이다[1]. SSO를 실현하는 통합 인증 프로토콜로는 대표적으로 OAuth[4], OpenID Connect[5], SAML[6] 등이 있다.

OAuth는 사용자, 주인증기관인 IdP, 서비스기관인 RP로 구성된 주체 간의 인증 프로토콜이다.

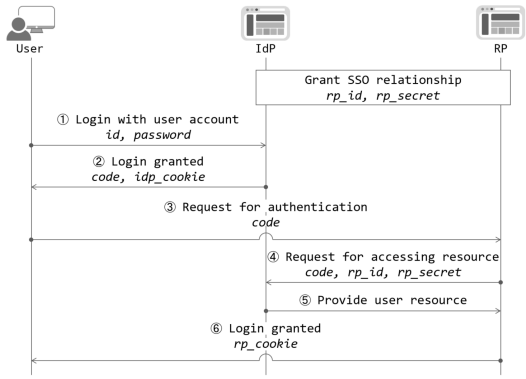

Fig. 1. User communicate with IdP to login into IdP and linked RP

IdP는 SSO 서비스 사용을 희망하는 사용자가 최초에 최소 한번 회원가입을 통하여 계정을 생성한 웹사이트이다. 사용자는 RP에 접속하여 서비스를 받기 전에 IdP의 도움을 받아 RP의 계정을 생성한다. RP의 계정은 전적으로 IdP 계정에 종속적이다.

Fig.1.은 OAuth에서 사용자가 IdP를 통해 RP에 로그인하는 과정이다. RP는 IdP와 SSO로 연동할 때 IdP가 RP를 식별하기 위한 값인 *rp_id*와 RP를 인증하기 위한 값인 *rp_secret*을 공유한다. RP에게 서비스를 받기 위해 사용자는 반드시 IdP에 로그인되어 있어야 한다. 사용자는 IdP에 로그인을 위해 계정 비밀번호를 입력한다(Fig.1.-①). IdP는 사용자를 인증한 뒤 인증 코드(*code*)와 *idp_cookie*를 발급한다(Fig.1.-②). IdP가 발급하는 인증 코드는 OAuth에서 IdP가 RP를 인증하기 위해 사용되는 정보이다. 이후 사용자는 IdP 접속 시 비밀번호를 재입력할 필요 없이 발급받은 *idp_cookie*를 제출하여 로그인한다. 사용자는 IdP로부터 발급받은 인증 코드를 RP에게 전달하며 서비스를 요청한다(Fig.1.-③). RP는 인증 코드와 *rp_id*, *rp_secret*을 제출하여 IdP에게 사용자 리소스에 대한 접근을 요청한다(Fig.1.-④). IdP는 *rp_id*와 *rp_secret*을 확인하여 자신과 SSO 관계를 맺은 RP로부터의 요청임을 검증한다. IdP는 인증 코드를 통해 사용자가 인가한 리소스 접근임을 확인한 뒤 RP에게 사용자 리소스를 제공한다(Fig.1.-⑤). RP는 IdP로부터 제공받은 사용자 리소스로 사용자에게 로그인된 페이지를 보여주고 *rp_cookie*를 발급한다(Fig.1.-⑥). 이후 사용자는 RP 접속 시 IdP에 다시 접속할 필요 없이 발급받은 *rp_cookie*

를 제출하여 로그인한다. IdP 및 RP는 쿠키로 인증된 사용자에게 세션을 발급하여 로그인 상태를 유지한다. 세션을 유지함으로써 사용자는 로그인된 사용자만 이용할 수 있는 서비스를 제공받는다. 사용자 계정은 IdP에서만 생성 및 관리되고 RP는 사용자 계정을 별도로 보관하지 않는다.

RP는 IdP로부터 가져오는 사용자 리소스의 종류에 따라서 약하게(loosely) 또는 강하게 결합된(strongly-coupled) RP로 구분이 된다. 강하게 결합된 RP는 IdP로부터 사용자 인증을 위임받으며 이후 사용자는 추가적인 작업없이 RP에 접속할 수 있다. 약하게 결합된 RP는 IdP로부터 아이디만을 가져오고 사용자로 하여금 별도의 비밀번호를 생성하여 향후 인증정보를 독립적으로 관리한다. 이 경우 RP는 IdP와 독립적으로 운영되므로 본 논문의 연구 범위에서 제외하고 이후 본문에서의 RP는 강하게 결합된 RP를 가리킨다.

III. 보안 요구사항

RP 보안은 IdP 보안에 절대적으로 종속된다. 공격자들은 이 점을 노려서 사용자들의 IdP 계정을 탈취하려는 시도를 한다. IdP 계정이 탈취된 사용자의 피해를 최소화하기 위하여 IdP가 취할 수 있는 보안 요구사항을 소개한다. IdP는 공격자가 임의로 사용자의 계정을 변경하지 못하도록 방어하고, 공격자를 사용자 계정에서 강제로 로그아웃시켜야 한다.

3.1 세션 차단

계정이 탈취된 사용자는 공격자의 로그인을 차단하기 위해 (1) 인증에 사용되는 아이디, 비밀번호, 전화번호 등 인증 정보를 변경하는 것과 (2) 인증에 사용되는 방식의 다변화를 수행할 수 있다. 인증방식 다변화는 기본설정인 비밀번호 외에 SMS 문자로 또는 별도의 애플리케이션이 생성한 코드들로 사용자를 인증하는 방식으로 보안 강도를 높일 수 있다. 더 나아가 사용자는 탈취된 IdP의 계정 사용을 중지하거나 IdP와 연동된 RP 계정을 해제할 수 있다. (1) 인증 정보 변경 및 (2) 인증 방식의 다변화를 통해 계정 변동 수행 시 공격자의 로그인을 차단할 수 있으나 이미 로그인된 세션 차단은 불가하다. 공격자의 세션 차단을 위하여 계정 변동이 발생하면 IdP는 IdP 및 RP의 모든 로그인 세션을 취소시켜야 한다.

3.2 계정 장악 방어

공격자는 탈취한 계정을 장악하기 위해 사용자 인증 정보를 변경할 수 있다. 이를 방지하기 위해 IdP는 인증 정보 변경 시 사용자를 재인증해야 한다. 정보 변경 전 사용자를 비밀번호로 다시 한번 확인하는 재인증은 쿠키를 탈취한 공격자는 방어할 수 있으나 비밀번호를 탈취한 공격자는 막을 수 없다. 해법으로는 비밀번호와는 다른 별도의 비밀을 IdP에 저장하고 재인증 시 사용하는 방법이 있다.

공격의 유효 시간을 제한하기 위해 IdP는 계정 변동 시 사용자에게 알림을 전송해야 한다. 계정 변동 알림을 사용자에게 전송함으로써 사용자가 공격을 인지하고 IdP에 계정 정지 등의 보안 조치를 요청할 수 있다. 이메일 및 SMS 등의 알림 통로를 공격자가 임의로 수정할 수 있는 경우 이 알림조차 차단이 가능하다. 방어를 위해서는 안전한 사용자 재인증을 함께 제공하여야 한다.

IV. 실 험

유명한 IdP와 RP들을 수집하고 IdP가 공격자의 세션을 차단하는지와 계정 장악 시도에 얼마나 안전한지를 실험을 통해서 알아본다. 분석 대상 IdP 및 RP의 선정 방법과 실험 방법 및 결과와 의미에 대하여 토론한다.

4.1 분석 대상 선정

실험을 위해 VMware workstation 16으로 가상환경을 구축하였으며 최신 버전인 Windows 10 운영체제 2004 버전과 Chrome 브라우저 83 버전에서 실험을 진행하였다. 실험은 2020년 6월부터 9월까지 약 4개월 간 진행되었다. 2020년 5월 29일을 기준으로 수집한 Alexa 상위 1,000개 웹사이트를 대상으로 크롤러를 동작시켜 RP 및 IdP를 식별하였다. Alexa는 지난 3개월 동안 사용자 조회 수가 가장 많은 웹사이트의 순위를 계산하는 서비스이다. 이용량이 많고 저명한 웹사이트를 대상으로 선정하기 위해 Alexa 리스트를 이용하였다. 크롤러는 크로미움 제어를 위해 자바스크립트 기반의 Puppeteer[7]를 기반으로 작성하였다.

크롤러는 1,000개 웹사이트의 URL을 입력받아 각 웹사이트의 메인 페이지를 파싱하여 모든 URL 문자열을 추출한다. 정규표현식을 통해 로그인과 관련된 단어가 포함된 URL을 식별한다. 식별한 URL을 모두 방문하여 ID와 비밀번호를 입력하는 input 태그가 존재하는 경우 로그인 페이지로 정한다.

논문에서 작성한 크롤러는 HTML 페이지에 포함된 텍스트를 기반으로 RP와 IdP를 식별하기 때문에 자바스크립트 등 HTML 외의 범위에서 SSO 서비스를 제공하는 경우는 식별하지 못한다. 정규표현식을 기반으로 동작하므로 정규표현식에 누락된 태그, 속성, 값으로 서비스를 제공하는 경우는 식별하지 못한다. 크롤러 동작 결과 35개의 IdP와 154개의 RP가 식별되었다. 식별된 웹사이트 중 분석 과정에서 계정 생성 시 서버 오류로 인해 웹사이트에 방문할 수 없는 경우, 앱에서만 인증 정보를 관리할 수 있는 경우, 웹에서 로그인 불가한 경우 등의 오류가 발생하는 웹사이트는 분석 대상에서 제외하였다. 자격이 되지 않는 웹사이트를 제외한 26개의 IdP와 133개의 RP를 분석 대상으로 선정한다. 선정된 IdP 및 RP의 리스트는 부록에 명시하였다. 분석 대상에 대해 총 162개의 계정을 새로 생성하여 로그인을 위한 이메일, 전화번호 등의 정보를 추가하였다.

4.2 세션 취소 결과

계정이 탈취된 후 사용자가 IdP 인증 정보를 변경하거나 계정 사용을 중지하면 공격자 세션을 포함해서 이 계정과 연동된 세션들의 취소 여부를 실험하여 SSO 운영의 안정성을 평가한다.

실험은 각 IdP 별로 Fig.2.의 과정을 수행하였다. 공격자는 IdP에 탈취한 비밀번호로 사용자 IdP 계정으로 로그인하고(Fig.2.-①) 이 계정과 연동된 RP에 로그인한다(Fig.2.-②). 사용자는 자신의 IdP 계정에 로그인 후 (Fig.2.-③) 인증 정보를 변경하거나 계정 사용을 중지한다(Fig.2.-④). 공격자는 IdP 쿠키를 제출하여 IdP에 로그인한 뒤 공격자의 IdP 세션이 취소되었는지 확인한다(Fig.2.-⑤). Fig.2.-⑤와 유사하게 공격자는 RP 쿠키로 로그인한 뒤 공격자의 RP 세션이 취소되었는지 확인한다(Fig.2.-⑥). IdP가 제공하는 인증 정보 변경 및 계정 사용 중지 기능이 복수이면 ④ ~ ⑥ 과정을 반복해서 각각의 기능 별로 실험한다.

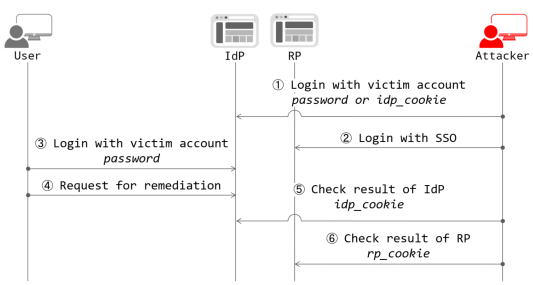

Fig. 2. Process of analyzation of session remediation between attacker and user PCs for each IdP

인증 정보 및 로그인 방식 변경 기능을 세분화하여 총 25개 기능에 대해 실험을 진행하였다. 이는 Table 1에 표기된 바와 같이 (1) IdP 인증 정보 변경 기능 8개, (2) IdP 로그인 방식 변경 기능 15개, (4) IdP 계정 비활성화 및 삭제 기능 2개로 구성된다. 25개 기능은 모두 IdP에서 제공하는 기능이며 본 실험은 사용자 인증을 담당하는 IdP를 중심으로 진행하였다. 공격자가 계정을 탈취하지 못하도록 방어하는 기능을 제외하였으며, 공격자가 계정을 이미 탈취한 상황에서 공격자의 로그인을 차단할 수 있는 기능만으로 선정하였다. Table 1의 숫자는 각 기능에 대한 실험 결과가 서로 동일한 IdP의 개수이며 그 수가 0이면 하이픈으로 표기한다. IdP에서 기능을 제공하지 않는 경우 N/A로 분류한다. RP 및 IdP에서 기능을 제공하나 웹사이트의 구현에 오류가 있어 실험 진행이 불가한 경우 에러로 분류한다.

Table 1에서 실험한 25가지 기능 중 24가지 기능에서 어떠한 IdP도 RP 세션을 취소시키지 않았다. RP 세션을 취소시킨 IdP가 존재하는 유일한 기능은 계정 삭제이다. 계정 삭제를 지원하는 IdP 중 Fanbyte만이 RP 세션을 취소시켰다. Fanbyte는 Tencent 사의 자매 웹사이트에만 SSO 서비스를 제공한다. 연동된 RP에서 Fanbyte의 ID로 새로운 계정을 생성 시도하면 이미 사용되고 있는 아이디라는 알림을 표시한다. 이는 Fanbyte가 자매 웹사이트와 사용자 데이터베이스를 공유하고 있다는 의미이다. Fanbyte는 IdP가 RP에게 사용자 정보를 제공해주는 일반적인 IdP가 아닌 특수한 IdP이다.

다음은 (3) IdP와 RP 계정의 연동 해제 실험 결과이다. 전체 26개 IdP 중 연동 해제를 제공하지 않는 6개 IdP와 RP의 구현 오류로 인해 실험을 진행할 수 없는 3개 IdP를 제외한 17개 IdP를 대상으로 실험을 진행하였다. 실험 결과 어떠한 IdP도

Table 1. Measurement result of RP and IdP session remediation after each account management actions. (M: Modify, A: Add, D: Delete, C: Change, AC: Activate, DA, Deactivate)

Unit: Number of IdPs(%)

Account management action				Action result (Session Remediation)						
				RP session			IdP session			N/A
				Delete	Maintain	Error	Delete	Maintain	Error	
Change account data		Username	M		5(19.2)	1(3.9)	-	5(19.2)	1(3.9)	20(76.9)
		Email	A	-	8(30.8)	1(3.9)	-	9(34.6)	-	17(65.4)
			M	-	13(50.0)	3(11.5)	2(7.7)	14(53.9)	-	10(38.5)
			D	-	5(19.2)	1(3.9)	-	6(23.1)	-	20(76.9)
		Phone number	A	-	13(50.0)	3(11.5)	-	14(53.9)	2(7.7)	10(38.5)
			M	-	10(38.5)	4(15.4)	1(3.9)	11(42.3)	2(7.7)	12(46.2)
			D	-	11(42.3)	3(11.5)	-	12(46.2)	2(7.7)	12(46.2)
		Password	M	-	22(84.6)	3(11.5)	19(73.1)	6(23.1)	-	1(3.9)
Change login method	2FA	All	C	-	8(30.8)	1(3.9)	2(7.7)	6(23.1)	1(3.9)	17(65.4)
		SMS	AC	-	12(46.2)	3(11.5)	2(7.7)	12(46.2)	1(3.9)	11(42.3)
			DC	-	11(42.3)	3(11.5)	-	13(50.0)	1(3.9)	12(46.2)
		OTP app	AC	-	11(42.3)	1(3.9)	1(3.9)	11(42.3)	-	14(53.9)
			DC	-	10(38.5)	1(3.9)	1(3.9)	10(38.5)	-	15(57.7)
		Call	AC	-	2(7.7)	-	-	2(7.7)	-	24(92.3)
			DA	-	1(3.9)	-	-	1(3.9)	-	25(96.2)
		Email	AC	-	3(11.5)	-	1(3.9)	2(7.7)	-	23(88.5)
			DA	-	2(7.7)	-	-	2(7.7)	-	24(92.3)
		Security alarm	AC	-	6(23.1)	1(3.8)	2(7.7)	4(15.4)	1(3.9)	19(73.1)
			DA	-	5(19.2)	1(3.9)	1(3.9)	4(15.4)	1(3.9)	20(76.9)
	Login w/o password	Security alarm	AC	-	3(11.5)	-	-	3(11.5)	-	23(88.5)
			DA	-	3(11.5)	-	-	3(11.5)	-	23(88.5)
		QR code login	AC	-	1(3.9)	-	-	1(3.9)	-	25(96.2)
			DA	-	1(3.9)	-	-	1(3.9)	-	25(96.2)
Delete account access		DA account		-	8(30.8)	1(3.9)	6(23.1)	3(11.5)	-	17(65.4)
		Delete account		1(3.9)	12(46.2)	3(11.5)	11(42.3)	5(19.2)	-	10(38.5)

RP 세션을 취소시키지 않았다.

(1) IdP 인증 정보 변경의 8개 기능 중 가장 높은 세션 취소율을 보이는 기능은 비밀번호 변경이다. 비밀번호 변경은 수행 시 73.07%의 IdP가 세션을 취소시킨다. 그 밖에 이메일 변경 시 7.69%, 전화번호 수정 시 3.85%의 IdP가 세션을 취소시키며 나머지 5개 기능은 수행 시 IdP 세션을 취소시키지 않는다. 일부 기능에서만 세션을 취소하는 IdP를 대상으로 추가적인 안정성 점검을 수행하였다.

실험 결과 다수의 인증 정보를 지원하는 IdP에서 각 정보에 대한 보안도가 동등하게 설정되지 않은 경우가 존재하였다. Payco의 경우 이메일과 전화번호를 모두 아이디로 사용하나 이메일 수정 시에만 IdP 세션을 취소시킨다. Payco는 아이디가 변경될 시 IdP 세션이 취소되어야 한다는 인식은 갖추고 있으나 일부 정보 변경 시에만 세션을 취소시키는 한계가 있다. 계정 보호를 위해서는 인증 정보로 사용되는 모든 정보들에 동등한 보안 조치를 제공해야 한다.

IdP가 세션 취소를 올바르게 구현하지 않는 문제도 발생하였다. T아이디의 경우 아이디를 변경할 때 모든 서비스에서 로그아웃한다는 알림을 표시한다. 그렇지만 아이디 변경 시 사용자의 IdP 세션만 취소되고 공격자의 세션은 유지된다. 이 경우 IdP는 공격자의 세션을 차단하였다고 생각하지만 구현 오류로 인해 공격자의 세션이 유지된다.

(2) IdP 로그인 방식 변경의 15개 기능 중 7개 기능 수행 시에만 IdP가 세션을 취소시키며 최대 취소율은 11.54%이다. 나머지 8개 기능은 수행 시 IdP 세션을 취소시키지 않는다. 일부 로그인 방식 변경 기능에서만 세션을 취소하는 IdP를 대상으로 추가적인 안정성 점검을 수행하였다.

실험 결과 다수의 로그인 방식을 지원하는 IdP에서 각 방식에 대한 보안도를 동등하게 설정하지 않는 경우가 발생하였다. Steam의 경우 OTP 앱과 이메일 모두 2FA로 지원하나 이메일을 2FA로 사용하도록 활성화할 시에만 IdP 세션을 취소시킨다. 보안도

의 불균형은 로그인 방식 활성 및 비활성 기능을 모두 지원하는 IdP에서도 발생한다. Kakao는 보안 알림을 2FA로 지원하나 보안 알림을 활성화할 시에는 IdP 세션을 취소시키고 비활성화할 시에는 IdP 세션을 취소시키지 않는다. Steam과 Kakao는 2FA 활성 시 IdP 세션이 취소되어야 한다는 인식은 갖추고 있으나 일부 2FA 활성시에만 세션을 취소시키는 한계가 있다. 계정 보호를 위해서는 로그인 방식으로 제공되는 모든 기능들에 대해 활성 및 비활성 시 모두 동등한 보안 조치를 제공해야 한다.

(4) IdP 계정 비활성화 및 삭제의 2개 기능 중 계정 비활성화는 23.08%, 계정 삭제는 42.31%의 IdP만 세션을 취소시킨다. 계정 비활성화 및 삭제 시 IdP에서 공격자의 세션을 취소시키지 않으면 사용자는 IdP 계정에 로그인할 수 없지만 공격자는 유지되는 세션을 통해 로그인 가능하다. 이 경우 공격자만이 IdP 계정 및 연동된 RP 계정에 로그인 가능하여 취약점이 발생한다. IdP 계정이 복구 유효기간 없이 즉시 삭제되는 경우 사용자가 IdP 계정에 영구적으로 접근할 수 없어 위험이 확대된다.

계정 비활성화 및 삭제 시 계정을 정지하지 않고 일정 기간동안 일반적인 로그인을 허용하는 경우에도 취약점이 발생한다. Apple의 경우 계정 삭제 요청 시 IdP 세션을 취소시키지 않으며 7일동안 일반적인 로그인을 허용하여 서비스를 제공한다. 이는 사용자가 공격자의 접근을 차단하기 위해 가장 강제성이 높은 계정 삭제를 수행하더라도 공격자는 최대 7일 동안 사용자 계정에 로그인 가능하다는 의미이다.

4.3 계정 장악 방어 결과

Table 2는 IdP 인증 정보 변경과 로그인 방식 변경 시 재인증 수행 여부와 수단을 분석한 결과이다. IdP가 제공하는 재인증 수단은 비밀번호, 전화 통화, SMS, 개인정보, 이메일, 앱이 있다. Table 2의 표기법은 Table 1과 동일하다. IdP가 재인증을 수행하지 않는 경우는 None으로 분류한다.

실험 결과 다수의 인증 정보를 지원하는 IdP에서

Table 2. Measurement result of re-authentication after each account management actions. (M: Modify, A: Add, D: Delete, C: Change, AC: Activate, DA, Deactivate)(Pass*: Password, PI**: Personal Information)

Unit: Number of IdPs(%)

Account management action				Action result (Re-authentication)								
				Pass*	Call	SMS	PI**	Email	App	None	Error	N/A
Change account data		Username	M	1(3.9)	-	-	-	-	-	4(14.4)	1(3.9)	20(76.9)
		Email	A	6(23.1)	-	-	-	-	-	5(19.2)	-	15(57.7)
			M	6(23.1)	1(3.9)	2(7.7)	1(3.9)	3(11.5)	-	6(23.1)	-	10(38.5)
			D	3(11.5)	-	-	-	-	-	4(14.4)	-	19(73.1)
		Phone number	A	4(14.4)	-	-	-	1(3.9)	-	9(34.6)	2(7.7)	10(38.5)
			M	2(7.7)	1(3.9)	3(11.5)	-	1(3.9)	-	7(26.9)	2(7.7)	12(46.2)
			D	2(7.7)	-	3(11.5)	-	1(3.9)	-	7(26.9)	2(7.7)	12(46.2)
		Pass*	M	22(84.6)	-	1(3.9)	-	-	-	2(7.7)	-	1(3.9)
Change login method	2FA	All	C	3(11.5)	-	1(3.9)	-	-	-	4(14.4)	1(3.9)	17(65.4)
		SMS	AC	5(19.2)	-	1(3.9)	-	-	-	8(30.8)	1(3.9)	11(42.3)
			DA	6(23.1)	-	1(3.9)	-	-	-	7(26.9)	1(3.9)	12(46.2)
		OTP app	AC	4(14.4)	-	2(7.7)	-	-	1(3.9)	5(19.2)	-	14(53.9)
			DA	4(14.4)	-	1(3.9)	-	1(3.9)	-	6(23.1)	-	15(57.7)
		Call	AC	1(3.9)	-	-	-	-	-	1(3.9)	-	24(92.3)
			DA	1(3.9)	-	-	-	-	-	-	-	25(96.2)
		Email	AC	1(3.9)	-	-	1(3.9)	-	-	2(7.7)	-	23(88.5)
			DA	1(3.9)	-	-	1(3.9)	1(3.9)	-	-	-	24(92.3)
		Security alarm	AC	4(14.4)	-	1(3.9)	-	1(3.9)	-	1(3.9)	1(3.9)	19(73.1)
			DA	4(14.4)	-	1(3.9)	-	-	1(3.9)	-	1(3.9)	20(76.9)
	Login w/o pass*	Security alarm	AC	-	-	-	-	-	1(3.9)	2(7.7)	-	23(88.5)
			DA	-	-	-	-	-	1(3.9)	2(7.7)	-	23(88.5)
		QR code login	AC	1(3.9)	-	-	-	-	-	-	-	25(96.2)
			DA	1(3.9)	-	-	-	-	-	-	-	25(96.2)

각 정보에 대한 보안도가 동등하게 설정되지 않은 경우가 존재하였다. Twitter의 경우 사용자 이름, 이메일, 전화번호를 모두 ID로 사용하나 이메일과 전화번호 수정 시에만 재인증을 수행한다. 다수의 로그인 방식 변경 기능을 지원하는 IdP에서도 각 변경 기능에 대한 보안도가 동등하게 설정되지 않은 경우가 존재한다. Microsoft는 SMS와 OTP 앱 모두 2FA로 지원하지만 OTP 앱을 활성화할 시에만 재인증을 수행한다.

보안도의 불균형은 로그인 방식 활성 및 비활성 기능을 모두 지원하는 IdP에서도 발생한다. IdP는 로그인 방식을 지원할 때 활성 및 비활성 시 모두 재인증을 수행해야 하며 재인증을 위해 제공하는 수단에도 주의해야 한다. Table 3은 SMS를 2FA로 지원하는 네 개의 IdP를 특성에 따라 분류한 예시이다. 재인증 수단의 중요성을 증명하기 위해 Table 3의 네 가지 IdP를 대상으로 공격자가 사용자 계정의 로그인 쿠키를 획득한 상황과 비밀번호를 획득한 상황에서의 로그인 가능성을 분석한다.

공격자가 사용자 IdP 계정의 로그인 쿠키를 획득하면 Twitter와 Google의 일부 기능을 변경 가능하다. Twitter는 2FA SMS가 활성화된 경우에도 제약없이 2FA를 비활성화할 수 있어 공격자가 IdP 계정의 비밀번호를 획득할 시 자유로이 로그인 가능하다. Google은 전화번호 등록 시 별도의 재인증 과정이 없어 공격자가 자신의 전화번호를 등록한 후 2FA SMS를 활성화시켜 사용자의 로그인을 차단할 수 있다. Linkedin과 Vkontakte는 재인증을 위한 값을 공격자가 획득할 수 없어 로그인 불가하다.

공격자가 사용자 IdP 계정의 비밀번호를 획득한 경우 2FA SMS가 활성화되어 있다면 네 개의 IdP 계정에 모두 로그인할 수 없다. 공격자의 로그인 가능성 분석을 위해 2FA SMS가 비활성화되어 있는 상황을 가정한다. 공격자가 사용자 IdP 계정 비밀번호를 획득하고 2FA SMS가 비활성화되어 있는 경우 Vkontakte의 SMS 활성 기능을 제외한 나머지 기능은 모두 변경 가능하다. 재인증 수단으로 비밀번호를 사용하면 공격자가 비밀번호 획득 시 재인증을 위한 값을 획득하게 되어 모든 기능을 변경 가능하다. 재인증 수단으로 자사 앱을 사용하는 경우 공격자가 획득한 비밀번호로 공격자의 디바이스에 설치된 앱에 로그인 가능하여 공격을 방어할 수 없다.

Table 3. Example of four IdP which provide re-authentication for SMS 2FA

IdP	Re-authentication for SMS 2FA	
	Activate	Deactivate
Linkedin	Password	Password
Twitter	Password	None
Google	None	Password
Vkontakte	Call/SMS	Password

실험 대상인 26개 IdP 중 23개(88.5%) IdP가 비밀번호를 재인증 수단으로 사용하고 있어 비밀번호를 획득한 공격자에 취약하다. 공격자가 계정을 변경할 수 없도록 SMS, 전화통화, 개인정보 페이지의 비공개된 개인정보 등 비밀번호 이외의 재인증 수단을 제공하는 것이 안전하다. 비밀번호 이외의 재인증 수단을 사용하는 경우에도 인증 수단에 대한 보호가 중요하다. 예시로 SMS 재인증 기능을 제공하나 전화번호 추가 및 수정에 제약이 없다면 공격자의 계정 변경을 방어할 수 없다. 공격자를 방어하기 위해서는 계정 생성 시 재인증을 위한 값을 별도로 입력하도록 하여 인증 정보 변경 시 등록된 재인증 값을 통해 사용자를 인증함이 안전하다. 예시로 Vkontakte는 계정 생성 시 사용자의 전화번호를 반드시 등록하도록 하여 SMS 활성 시 등록된 전화번호를 통해 SMS로 OTP를 제공하여 사용자를 재인증한다. 재인증 수단인 전화번호에 대한 변경은 수정 기능만 제공하며 전화번호 수정 시 SMS로 재인증을 수행함으로써 공격자의 계정 변경을 방어한다.

알림 전송 실험 결과 전체 IdP 중 9개(34.6%)만이 자신이 제공하는 모든 기능에서 알림을 전송하였다. 이외의 12개 IdP는 일부분의 기능 수행 시만 알림을 전송하였고, 4개는 모든 기능에서 알림을 전송하지 않았다. 나머지 1개 IdP는 계정 삭제 기능만 제공하여 실험에서 제외하였다. IdP가 사용하는 알림 수단은 이메일, SMS, 웹이 있다. 가장 많이 사용되는 수단은 20개(76.9%) IdP가 제공하고 있는 이메일이다. IdP가 사용자에게 전송하는 이메일은 확인 메일과 알림 메일로 분류된다. 이메일 변경 시의 알림 수단으로 이메일을 사용하는 경우 두 종류의 이메일을 용도에 따라 구분하여 전송해야 한다. 확인 메일은 IdP에 등록되는 새로운 이메일이 사용자의 소유인지 검증하는 용도이므로 새로운 이메일로 전송하여 검증해야 한다. 알림 메일은 기존 이메일 소유자에게 IdP 계정에 등록된 이메일에 변경이 발생하였음을 인지시키는 용도이므로 기존 이메일로 전송하여 검증해야 한다. 새로운 이메일로 알림 메일이 전

송되면 공격자가 사용자의 이메일을 공격자의 이메일로 수정할 시 새로 입력된 공격자 이메일로 알림이 전송되어 위험이 발생한다.

V. 해결 방안

분석 결과 26개 IdP의 96%가 인증 정보 변경 및 계정 사용 중지 시 연동된 RP의 세션을 취소시키지 않았다. 그 원인은 IdP 계정과 RP 계정이 부분적으로 단절되어 있는 것으로 밝혀졌다. IdP 세션 취소 시 로그인된 RP 계정을 알 수 없어 RP의 세션이 취소되지 않는다. 해결을 위해 IdP에서 RP 세션을 식별하고 관리하는 프로토콜이 필요하다. 본 장에서는 웹 SSO 서비스에 적용할 수 있는 RP 세션 취소 프로토콜을 설명하고 보완점을 제시한다.

최근 OpenID 재단에서는 RP 세션 취소 방안으로 OpenID connect back-channel logout[8]이라는 표준 초안을 작성 중이다. 사용자가 세션 취소를 요청하면 IdP는 연동된 RP에게 JWT(JSON Web Token) 형식의 로그아웃 토큰을 발급한다. 취소하는 RP 세션의 식별자를 파라미터로 추가할 수 있다. 로그아웃 토큰은 RP의 로그아웃 URI에 HTTP POST로 발급된다. RP는 로그아웃 토큰을 검증하고 토큰 발급자와 세션 식별자로 구분되는 RP 세션을 취소시킨다. IdP는 세션 취소를 요청하고 RP에서 직접 자신의 세션을 취소하는 방식이다. OpenID 이외의 프로토콜에서는 세션 취소 방안을 제시하고 있지 않아 IdP 구현 시 보안 허점을 발생시킬 수 있다.

OpenID의 방안은 1) 사용자 프라이버시, 2) 시스템 부하와 사용성, 3) IdP 계정 삭제 시 RP 계정 삭제, 4) 세션 취소 결과 검토를 고려하지 않았다. SSO를 구현하는 프로토콜에 OpenID 기반의 해결 방안을 적용하기 위해 보완점을 제시한다. 1) 프라이버시 보호를 위해 RP 세션에 대한 정보를 IdP에 노출을 방지해야 한다. IdP는 RP 세션을 식별하기 위해 RP의 로그인 요청마다 세션 식별자를 발급한다. 이는 RP 세션의 기본 정보로 IdP는 RP에서 수행된 사용자 작업을 추적할 수 없다. 2) 시스템 부하와 사용성을 고려하여 RP 세션을 취소하는 주기를 결정해야 한다. 사용자의 계정이 탈취된 경우에만 RP 세션을 취소하고 그 외의 경우는 사용성과 부하를 위해 RP 세션을 유지한다. 3) IdP는 계정을 삭제하기 전 연동된 RP들에게 삭제 사실을 통보해야 한다. 사용자가 IdP 계정을 삭제하면 IdP는 로그아웃 토큰에 계정 삭제 파라미터를 추가하여 RP에게 전달한다. 4) IdP는 RP가 정상적으로 세션 취소 요청을 완료하였는지 확인해야 한다. IdP는 로그아웃 토큰에 취소시킬 RP의 세션 식별자를 파라미터로 추가하여 발급한다. RP는 세션 취소 후 취소된 세션 식별자들을 HTTP 응답으로 전달한다. IdP는 누락된 세션 식별자가 존재하는지 검토한다.

VI. 관련 연구

기존 연구는 표준 문서를 기반으로 구현상의 취약점을 연구하였다. Zhou[9]와 Yang[10]의 연구는 OAuth 2.0[4]을 대상으로 취약점을 점검한다.

Zhou의 연구[9]는 Facebook을 대상으로 인증 정보 안정성을 점검한다. RP 인증값인 RP 비밀값과 사용자 인증값인 인증 코드는 서버에서 처리되어야 한다. 인증 정보가 브라우저를 통해 전송되면 악의적인 웹사이트에 노출된다. Zhou는 SSOScan 도구를 작성하여 Facebook을 IdP로 지원하는 1,660개 웹사이트를 자동으로 식별하고 인증 정보의 노출 여부를 분석하였다.

Yang의 연구[10]는 웹사이트를 대상으로 CSRF 공격에 대한 안정성을 검사한다. CSRF 공격을 방어하기 위해서는 state 파라미터를 추측할 수 없는 값으로 설정하고 사용해야 한다. 웹사이트는 인증 요청 시 임의의 state를 생성하여 사용자에게 보내고 사용자는 응답에 이를 포함함으로써 값의 유효성을 검사한다. Yang은 state에 대한 안정성을 점검하기 위해 OAuthTester 도구를 작성하여 405개 웹사이트를 대상으로 분석을 진행하였다.

SSO 구현 시 표준을 따르더라도 보안 허점이 발생함을 증명하는 기존 논문도 존재한다.

Mohammad[9]는 계정 보호를 위해 IdP가 탈취된 IdP 계정으로부터 생성된 RP 세션을 보편적으로 취소해야 함을 강조하였다. 연구는 Facebook과 연동된 95개 RP를 대상으로 진행되었으며 그 중 29개는 웹사이트이고 66개는 모바일 애플리케이션이다. 연구 결과 IdP 및 RP에서 사용자가 세션을 취소한 이후에도 공격자가 사용자 계정에 대한 세션을 유지할 수 있었다. 연구는 단일 IdP를 대상으로 연동된 RP에 초점을 맞춰 진행되었으며 IdP가 제공하는 일부 기능만을 실험하였다. 이는 IdP 로그아웃, RP 로그아웃, IdP 비밀번호 변경, RP 비밀번

호 변경, RP 연동 해제, 모든 RP 세션에서 로그아웃이다. 그 중 세 가지 로그아웃 기능은 IdP와 RP의 계정 연동에 관련 없이 단일 웹사이트 및 애플리케이션에서 세션을 취소하는 기능인 한계가 있다.

본 논문은 웹 상에서의 IdP와 RP 간의 세션 취소에 초점을 맞춰 진행하였으며 연구의 중심을 RP가 아닌 사용자 인증을 수행하는 IdP로 선정하였다. IdP 비밀번호 및 쿠키가 탈취된 공격 상황을 가정하여 IdP가 제공하는 26개 세션 취소 기능에서 보안 요구사항을 만족하는지 분석하였다. 26개 IdP를 대상으로 보안성 점검을 진행함으로써 단일 IdP에 대한 연구 결과에서 발생하는 바이어스를 절감하였다.

VII. 결 론

웹사이트 별로 사용자 계정을 관리하는 어려움을 해소하기 위해 웹사이트는 SSO를 적용하여 사용자 편리성을 높이고 있다. SSO 이용 시 IdP에서 사용자 인증이 이루어지며 계정 보안의 핵심 역할을 수행한다. 본 논문에서는 IdP가 사용자 계정 보호를 위해 제공해야 하는 보안 요구사항을 규정하였다. IdP는 공격자가 계정을 탈취한 상황을 가정하여 1) 세션 차단과 2) 계정 장악 방어를 제공해야 한다. 실제 IdP가 보안 요구사항을 만족하고 있는지 점검하기 위해 실태조사를 수행하였다. 1) 세션 차단은 IdP 인증 정보가 변경되거나 계정 사용 중지 시 해당 계정과 연동된 모든 세션을 취소하는지 실험하였다. 2) 계정 장악 방어는 IdP 인증 정보 변경 시 사용자 재인증을 수행하고 알림을 제공하는지 실험하였다. 실험 결과 26개 IdP 중 96%가 보안 요구사항을 만족하지 않았다. IdP가 보안 요구사항을 만족하지 않으면 사용자가 공격을 인지하더라도 공격자의 세션을 취소시킬 수 없다. 해결을 위해 IdP에서 RP 세션을 식별하고 관리하는 프로토콜을 제안하였다.

VIII. 부 록

본문에서 실험한 IdP 도메인 리스트를 제시한다.

Table 4. List of IdP websites and number of RPs authenticated by each IdP.

IdP	Number of RPs
Facebook	30
Google	30
Twitter	25
Apple	17
Linedin	6
Microsoft	5
Vkontakte	5
Yahoo	3
Github	2
Naver	2
Mail.ru	2
Kakao	2
Battle.net	2
Office365	2
Slack	2
Docomo	1
Steam	1
Twitch	1
Payco	1
Fanbyte	1
Ocn	1
Firefox	1
TID	1
ok.ru	1
Instagram	1
Bosspay	1

References

[1] J.D. Clercq, "Single sign-on architectures," Proceedings of International Conference on Infrastructure Security, LNCS 2437, pp. 40-58, Oct. 2002.

[2] S.T. Sun and K. Beznosov, "The devil is in the (implementation) details: An empirical analysis of OAuth SSO systems," Proceedings of 2012 ACM Conference on Computer and Communications Security, pp. 378-390, Oct. 2012.
[3] C. Yue, "The devil is phishing: rethinking web single sign-on systems security," Proceedings of 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats, Aug. 2013.
[4] D. Hardt, "The OAuth 2.0 authorization framework," RFC 6749, Oct. 2012.
[5] OpenID.net, "OpenID connect core 1.0 incorporating errata set 1," https://openid.net/specs/openid-connect-core-1_0.html, Sep. 2021.
[6] OASIS, "Assertions and protocols for the OASIS security assertion markup language (SAML) V2.0," http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, Sep. 2021.
[7] Github, "Puppeteer," https://github.com/puppeteer/puppeteer, Sep. 2021.
[8] OpenID.net, "OpenID connect back-channel logout 1.0 - draft 06," https://openid.net/specs/openid-connect-backchannel-1_0.html, Sep. 2021.
[9] M. Ghasemisharif, A. Ramesh, S. Checkoway, C. Kanich, and J. Polakis, "O single sign-off, where art thou? An empirical analysis of single sign-on account hijacking and session management on the web," Proceedings of 27th USENIX Security Symposium, pp. 1475-1492, Aug. 2018.
[10] R. Yang, G. Li, W.C. Lau, K. Zhang, and P. Hu, "Model-based security testing: an empirical study on OAuth 2.0 implementations," Proceedings of 11th ACM on Asia Conference on Computer and Communications Security, pp. 651-662, May 2016.

〈저자소개〉

남 지 현 (Ji-Hyun Nam) 학생회원
2019년 2월: 성신여자대학교 융합보안학과 졸업
2021년 2월: 성균관대학교 전자전기컴퓨터공학과 석사
2021년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 박사과정
〈관심분야〉 리버스 엔지니어링, 보안공학

최 형 기 (Hyoung-Kee Choi) 정회원
1992년 2월: 성균관대학교 전자공학과 졸업
1996년 2월: Polytechnic University in Brooklyn, NY 석사
2001년 2월: Georgia Institute of Technology in Atlanta, GA 박사
2001년 1월~2004년 12월: Cisco 근무
2004년 3월~현재: 성균관대학교 소프트웨어대학 교수
〈관심분야〉 네트워크 보안, 리버스 엔지니어링