https://doi.org/10.5392/JKCA.2018.18.09.141

다중 응용시스템용 앱기반 2-채널 사용자 인증방안

App-based 2-channel User Authentication Scheme for Multiple Application Systems

송태기, 조인준
배재대학교 사이버보안학과

Tae-Gi Song(taegi827@gmail.com), In-June Jo(injune@pcu.ac.kr)

요약

현재 사용자가 조직 내 다중의 응용시스템들에 접근하기 위해서 사용되는 사용자인증기술은 ID/PW 기반의 SSO기술이 적용되고 있다. 이러한 사용자 인증방안은 ID/PW와 SSO의 근본적인 단점을 그대로 지니고 있다. 즉, ID/PW의 보안 취약점 때문에 PW의 주기적 변경 및 잘못된 PW입력 횟수 제한 등을 들 수 있고, SSO는 중앙 집중적으로 인증정보를 저장하는 SSO서버가 추가되기 때문에 고비용, 가용성 확보, 해킹 타겟 명확화 등의 문제를 지닌다. 또한 SSO로 포탈 응용화면에 접근 후 자리를 비웠을 때, 다른 사람이 자유롭게 타인의 응용시스템을 사용할 수 있는 근본적인 취약성이 있다.

본 논문에서는 기존에 사용되고 있는 ID/PW기반의 SSO 사용자 인증기술이 지닌 문제점들을 근본적으로 제거하기 위해 앱 기반 2-채널 인증방안을 제안하였다. 이를 위해 SSO서버에 저장되는 중앙 집중적인 사용자 인증정보를 각 개인의 스마트폰으로 분산시켰다. 그리고 사용자가 특정 응용시스템을 접근할 경우 항상 자신의 스마트폰 앱을 경유하여 인증되도록 하였다.

■ 중심어 : | 식별 및 인증 | 스마트 디바이스 | 싱글사인온 | 인증시스템 |

Abstract

Currently, the user authentication technology used by users to access multiple applications within an organization is being applied with ID/PW-based SSO technology. These user authentication methods have the fundamental disadvantages of ID/PW and SSO. This means that security vulnerabilities in ID/PW can lead to periodic changes in PWs and limits on the number of incorrect PW inputs, and SSO adds high cost of the SSO server, which centrally stores the authentication information, etc. There is also a fundamental vulnerability that allows others to freely use other people's applications when they leave the portal application screen with SSO.

In this paper, we proposed an app-based 2-channel authentication scheme to fundamentally eliminate problems with existing ID/PW-based SSO user authentication technologies. To this end, it distributed centralized user authentication information that is stored on SSO server to each individual's smartphone. In addition, when users access a particular application, they are required to be authenticated through their own smartphone apps.

■ keyword : | Identification and Authentication | Smart Device | SSO | Authentication System |

* 본 논문은 2018학년도 배재대학교 교내학술연구비 지원에 의하여 수행된 것임
접수일자 : 2018년 07월 11일
심사완료일 : 2018년 08월 20일
수정일자 : 2018년 08월 20일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

I. 서 론

현재 특정기관이 개발하여 운영 중인 다수의 응용시스템들에 적용된 사용자 인증기술은 각 응용시스템별 ID/PW(IDentifier/PassWord)기술과 각 응용에 접근의 수월성을 제공하는 SSO(Single Sign On)기술로 분류할 수 있다. 전자의 ID/PW기술은 ID에 대응하는 PW를 일일이 기억해야하는 부담뿐만 아니라 그 자체가 지니는 보안상 취약점 때문에 주기적으로 PW를 변경해야 하는 번거로움이 상존한다. 후자의 SSO기술은 전자의 ID/PW인증기술이 적용될 경우에 다수개의 PW를 기억하여 입력해야 하는 부담을 줄이기 위해 조직 내의 응용시스템들을 대상으로 한번 ID/PW를 입력하면 등록된 모든 응용시스템에 ID/PW추가 입력 없이 접근이 가능하도록 만든 기술이다. 하지만 후자의 SSO인증기술 또한 SSO서버에 모든 사용자 인증정보가 집중되기 때문에 해킹의 타겟이 될 뿐만 아니라 SSO서버의 가용성 확보문제, 고비용 구축문제, 그리고 마지막으로 SSO로 포털로 접근한 후, 자리를 비웠을 때, 다른 사람이 포털에 등록된 응용시스템들에 자유롭게 접근하는 문제점을 들 수 있다. 따라서 ID/PW에서 번거롭게 PW를 주기적으로 변경하는 문제점과 상기의 SSO에 내제된 문제들을 해결할 수 있는 새로운 대체 사용자 인증기술이 필요한 것 또한 사실이다[1].

본 논문에서 제안하고자 하는 사용자 인증시스템은 조직 내 다수의 응용시스템들을 대상으로 첫째, 사용자는 응용시스템별 ID만을 제시하고 각 응용시스템에 대응되는 1회용 세션에서만 사용이 가능한 PW를 자동생성하여 PW를 사용자가 일일이 변경하는 번거로움을 제거하고 하였고, 둘째, SSO에서 SSO서버에 집중되는 모든 사용자인증정보를 각 사용자 개인의 스마트폰 앱 저장소로 분산시켜 인증 시 사용자 단말과 응용시스템 채널 그리고 응용시스템과 자신의 스마트폰 앱 채널을 경유하여 인증되는 2채널 기반의 새로운 인증시스템을 제안하여 상기에서 제시한 SSO의 문제점들을 제거하였다.

II. 제안 방안

현재 가장 많이 사용되고 있는 ID/PW기반의 사용자 인증시스템은 쉽게 구축이 가능하지만 무작위대입공격 및 사전공격, 악성코드, 파밍 사이트 등의 위협에 쉽게 노출이 되어있어 사용자들은 불편을 겪고 있지만 위의 위협에 대해 방지하기 위해서 사용자의 정보가 유출되지 않도록 주기적인 패스워드 변경 및 일정횟수 이상 입력오류금지 등을 권고 하고 있다[2-4].

SSO 인증기술에 내제된 단점들은 2가지 요인 때문에 발생한 것으로 판단된다. 하나는 조직 내 모든 응용에 등록된 모든 사용자 인증정보를 SSO서버에 중앙집중적인 유지가 요인이다. 이 요인으로 인해 SSO서버 비용, 가용성, 해킹의 취약성 등의 문제를 야기한다[5]. 두 번째는 SSO로 한번 포털에 접속에 성공하면 포털에 등록된 응용들을 ID/PW요구 없이 자유롭게 접근이 가능하다는 SSO의 장점이 문제의 요인이 된다. 즉, 조직 내에서 일시적으로 자리를 비운사이에 타인이 자신의 응용시스템을 자유롭게 접근하여 사용할 수 있다는 점이다. 본 논문에서 제안하는 “다중시스템용 앱기반 2-채널인증방안”은 첫째, SSO서버에 저장된 중앙집중적인 사용자인증정보를 각자의 사용자 스마트폰 앱 저장소로 분산 저장하여 SSO 서버를 제거하였다. 둘째, 사용자가 특정 응용시스템에 접근 시 접근하고자 하는 응용시스템을 경유하는 채널과 접근하고자 하는 응용시스템과 사용자의 스마트폰 앱을 경유하는 또 하나의 채널을 통한 2채널 인증기법을 사용하였다. 첫 번째 조치를 통해서 모든 인증정보를 중앙 집중적으로 저장하는 SSO서버가 제거되기 때문에 이로 인한 상기의 문제점들을 해결할 수 있다. 두 번째 조치를 통해 항상 자신의 스마트폰 앱을 통한 사용자 인증이 이루어지기 때문에 SSO로 접근한 포털화면에서 자리를 비웠을 때, 다른 사람이 불법적으로 포털화면의 응용에 자유롭게 접근하는 문제점을 해결할 수 있다[6-8].

1. 제안 시스템 구성

제안 시스템의 기본구성은 [그림 1]과 같다. 주요 구성요소는 사용자 단말, 사용자 스마트폰, 포털 지원 서

버, 그리고 다중응용시스템서버들로 이루어진다. 사용자단말은 사용자가 포털지원서버에 등록된 응용시스템들을 포털화면으로 불러오고 이들 중에서 하나의 응용시스템을 선택하여 사용자 등록 혹은 인증을 요구하는 역할을 한다. 사용자 스마트폰은 사용자 등록 혹은 인증 요구가 있을 경우 이를 처리한다. 즉, 해당 스마트폰 사용자의 모든 응용시스템들의 인증정보를 종합 관리하는 역할을 한다. 그리고 포털서비스서버는 본 논문에서 제시한 인증방법을 사용하는 모든 응용시스템들의 이름 및 주소정보를 종합적으로 유지 관리하는 역할을 한다. 마지막으로 각 응용시스템 서버들은 각각 자신을 요구하는 사용자등록 및 인증요구, 자신의 응용이름 및 주소를 포털관리 웹에 등록하고, 인증처리 및 정보관리, Log관리 등의 역할을 한다.

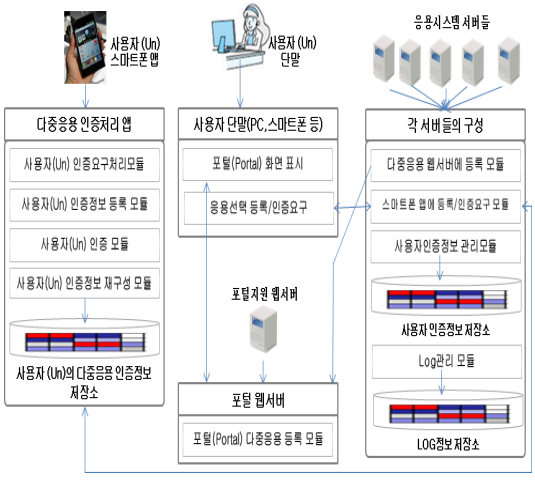

그림 1. 제안 시스템 구성도

[그림 1]의 제안시스템의 구성도를 기준으로 인증과정을 간략하게 설명하면 다음과 같다. 첫째, 사용자가 원하는 응용시스템에 접근을 위해 포털서비스 웹서버의 URL을 입력한다. 둘째, 자신의 단말에 나타난 응용시스템 이름 목록들 중에서 사용하고자 하는 응용시스템 이름을 선택하여 인증을 요구한다. 셋째, 사용자 단말로부터 인증을 요구 받은 해당 응용시스템 서버와 사용자가 소지하고 있는 스마트폰 앱으로 인증요구가 도착한다. 넷째, 해당 응용시스템 서버는 스마트폰 앱으로부터 인증허용 유·무신호가 도착할 때까지 일정시간 인증대기 모드상태로 유지한다. 다섯째, 인증요구를 받은 스마트폰 앱은 자신이 저장하고 있는 해당 응용시스템의 인증정보와 해당 응용시스템서버가 저장하고 있는 인증정보를 비교하여 동일하면 인증을 허용한다는 신호를 해당 응용시스템 서버에 보낸다. 그리고 다음세션에서 사용할 인증정보를 재구성하여 스마트폰 인증정보와 해당 응용시스템의 인증정보를 모두 갱신한다. 여섯째, 인증이 성공하면 해당 응용시스템을 사용자단말에서 접근하여 사용할 수 있게 된다.

2. 제안 시스템 상세 설계

제안시스템에서 핵심이 되는 인증정보생성, 사용자 인증, 인증정보 재구성 세 가지 모듈을 수행하기 위해 설계한 내용을 설명한다. 아래 절에서 사용되는 표기법은 다음 [표 1]과 같이 표기된다[9][10].

표 1. 표기법

부호	의미
Un_ID	사용자의 Un의 식별자
APLn_ID	응용시스템 APLn의 식별자
es_key	세션키를 암호화하는 대칭키
s_key	한 세션에서만 사용하는 세션키
En(m)	n이란 키로 m을 대칭 암호화
Dn(m)	n이란 키로 m을 대칭 복호화
(a+b+c+…)	a, b, c 항목으로 구성된 레코드
N	의사난수생성기(PRNG)가 생성한 난수
day	인증정보 생성/갱신 날짜
Nonce	재현공격 방지를 위한 비표

2.1 응용(APLn)에 사용자(Un) 등록

본 절에서는 스마트폰 앱에 사용자를 등록하여 특정 응용시스템을 시스템을 사용할 수 있도록 하는 절차에 대하여 설명한다.

Step 1) 사용자가 URL(Uniform Resource Location)를 통해서 포털지원서버로부터 포털화면을 표시하고 이로부터 특정 응용시스템(APLn)을 선택한다. 사용자가 등록되어 있지 않은 경우 등록에 필요한 정보입력 화면을 통해서 사용자 Un의 등록 요구 요구 메시지를 응용(APLn)시스템서버에 [그림 2]에서 ①과 같이 보낸다.

Step 2) 이를 수신한 응용시스템 APLn은 스마트폰 인증정보 등록요구 모듈을 통해서 사용자 스마트폰 앱에 등록요구 메시지를 보낸다([그림 2]에서 ②).

Step 3) 이를 수신한 스마트폰 앱은 의사난수생성기(PRNG)로 임의의 난수 N을 생성하고, ②메시지로부터 수신된 APLn-ID와 Un-ID와 생성된 난수 N를 일방향 해쉬함수에 입력하여 세션키(s_key)를 암호화하기 위한 키 es-key를 생성한다.

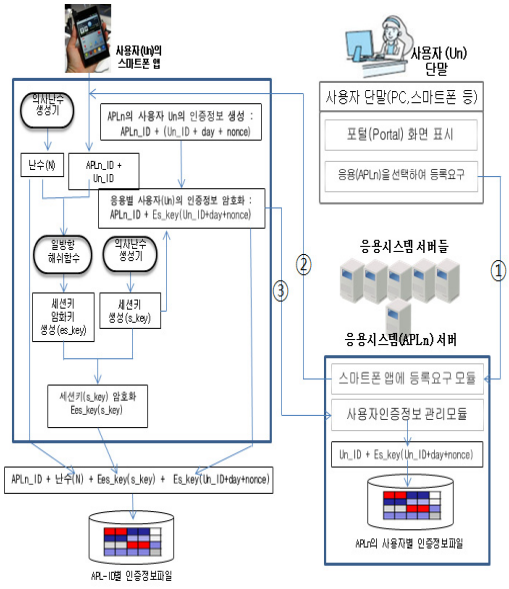

그림 2. 응용 APLn-ID에 사용자 Un등록 모듈

Step 4) 의사난수생성기(PRNG)를 사용하여 사용자의 인증정보를 암호화하기 위한 세션키(s_key)를 생성한다.

Step 5) 등록될 인증정보 암호화에 사용되는 세션키가 노출이 되지 않도록 세션키 암호화키(es_key)로 세션키(s_key)를 암호화한다[11].

= E_{es_key}(s_key)

Step 6) 사용자의 인증정보를 각 저장소에 저장하기 위해 사용자 인증정보 레코드를 생성한다. 즉 (APLn-ID + Un_ID + day + Nonce) 이다. 여기에서 비표 값(nonce)은 재현공격을 방어하기 위한 것이다.

Step 7) 위의 Step 6 과정에서 생성한 레코드 중 APLn_ID를 제외한 (Un_ID+day+Nonce)를 세션키 s_key로 암호화한다.

= Es_key(Un_ID+day+Nonce)

Step 8) 위의 Step 7 과정에서 암호화한 Es_key(Un_ID+day+Nonce)와 Un_ID을 [그림 2]에서 ③과 같이 응용시스템 APLn으로 보내어 인증정보파일에 저장한다.

= Un_ID+ Es_key(Un_ID+day+Nonce)

Step 9) 마지막으로 최초에 생성한 난수 N, Step 4에서 만든 암호화된 세션키(E_{es_key}(s_key)), 그리고 Step 7 과정의 암호화한 인증정보 (Es_key(Un_ID+day+Nonce))를 자신의 스마트폰 앱을 통해 내부 저장소에 저장한다.

= APLn_ID + Un-ID + N + (E_{es_key}(s_key)) + Es_key(Un_ID+day+Nonce)

2.2 응용(APLn)에 사용자(Un) 인증

본 절에서는 응용시스템 APLn에 사용자 Un이 2.1절의 절차에 따라 등록되었다는 전제하에서 사용자 Un이 응용 APLn에 접근을 요구할 경우 이루어지는 인증절차는 [그림 3]과 같다. 보다 상세하게 단계별절차를 살펴보면 다음과 같다.

Step 1) 사용자가 URL로 포털지원서버로부터 포털화면을 표시한다. 그리고 표신된 화면으로부터 특정 응용 시스템(APLn)을 선택한다. 사용자가 응용시스템 APLn에 등록되어 있을 경우 사용자 Un의 인증요구 메시지를 선택한 응용시스템(APLn)에 그림에서 ①과 같이 보낸다.

Step 2) 이를 수신한 응용시스템 APLn은 스마트폰 인증요구 모듈을 통해서 사용자 스마트폰 앱에 인증요구 메시지를 보낸다(그림에서 ②).

Step 3) 이를 수신한 스마트폰 앱은 자신의 저장소에 저장된 APLn_ID에 해당하는 레코드를 탐색하여 그 레코드로부터 난수 N과 ②메시지로부터 획득한 APL_ID와 Un_ID를 일방향 해수함수에 입력하여 세션키 암호화 키인 es_key를 생성한다.

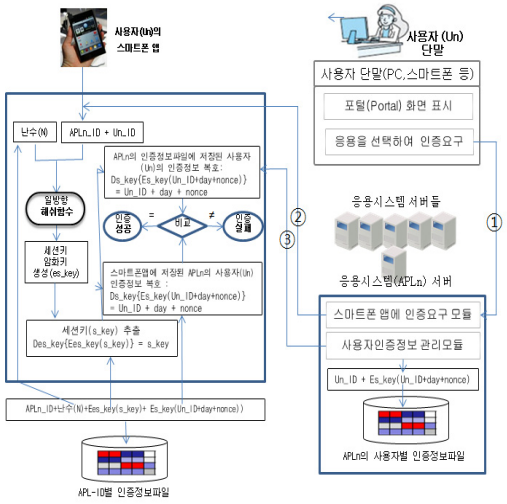

그림 3. 응용(APLn)에서 사용자(Un) 인증모듈

Step 4) 스마트폰 앱 저장소로부터 읽어온 암호화된 세션키(Ees_key(s_key))를 Step 3 과정에서 생성된 es_key로 복호화하여 세션키(s_key)를 구한다[11].

= D_{es_key}(Ees_key(s_key)) = s_key

Step 5) 스마트폰 내부 저장소로부터 읽어드린 암호화된 인증정보를 Step 4에서 얻은 세션키(s_key)를 사용하여 복호화하여 평문의 인증정보를 얻는다.

= Ds_key(Es_key(Un_ID+day+Nonce))

= Un_ID+day+Nonce

Step 6) 응용시스템 APLn로부터 그림에서 ③과 같이 APLn에 등록된 사용자 Un의 암호화된 인증정보 레코드를 전송받는다.

Step 7) Step 6에서 전송받은 암호화된 인증정보를 세션키(s_key)를 사용하여 복호화한다.

= Ds_key(Es_key(Un_ID+day+Nonce))

= Un_ID+day+Nonce

Step 8) Step 5 와 Step 7 과정에서 만들어진 복호화된 인증정보를 비교 인증하여 동일하면 인증 성공, 일치하지 않으면 인증실패 한다.

2.3 인증정보 재구성

본 절에서는 2.2.절의 인증이 성공되면 보안 강화를 위해 기존세션에서 사용된 인증정보를 모두 재구성하는 절차를 실행하게 된다. 다음 [그림 4]는 인증정보 재구성 모듈을 설명한 것이다.

Step 1) 사용자 Un의 스마트폰 앱은 의사난수생성기(PRNG)로 임의의 난수 N을 생성한다. 그리고 현재 인증이 성공한 응용시스템의 APLn_ID과 사용자의 Un_ID, 그리고 와 생성된 난수 N를 일방향 해수함수에 입력하여 세션키(s_key)를 암호화하기 위한 키 es-key를 생성한다.

Step 2) 다음으로 의사난수생성기(lPRNG)를 사용하여 사용자의 인증정보를 암호화하기 위한 세션키(s_key)를 생성한다.

Step 3) 등록될 인증정보 암호화에 사용되는 세션키가 노출이 되지 않도록 세션키 암호화키(es_key)로 세션키(s_key)를 암호화한다[11].

= E_{es_key}(s_key)

Step 4) 사용자의 인증정보를 각 저장소에 저장하기 위해 사용자 인증정보 레코드를 생성한다. 즉 (APLn-ID + Un_ID + day + Nonce) 이다. 여기에서 비표값(nonce)은 재현공격을 방어하기 위한 것이다.

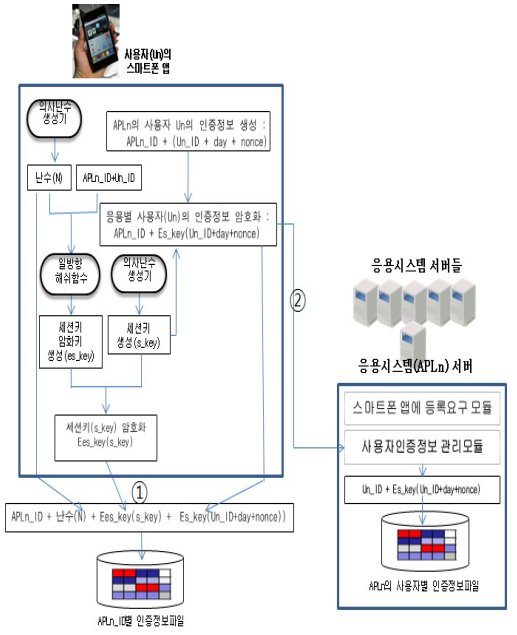

그림 4. 응용(APLn)에서 사용자(Un)인증정보 재구성 모듈

Step 5) 위의 Step 4 과정에서 생성한 레코드 중 APLn_ID를 제외한 (Un_ID+day+Nonce)를 세션키 s_key로 암호화한다.

= Es_key(Un_ID+day+Nonce)

Step 6) 위의 Step 5에서 암호화한 Es_key(Un_ID+day+Nonce)와 Un_ID을 [그림 4]에서 ②와 같이 응용시스템 APLn으로 보내어 인증정보파일에 저장한다.

= Un_ID+ Es_key(Un_ID+day+Nonce)

Step 7) 마지막으로 새롭게 생성한 난수 N, Step 3에서 만든 암호화된 세션키(E_{es_key}(s_key)), 그리고 Step 5 과정의 암호화한 인증정보 (Es_key(Un_ID+day+Nonce))를 스마트폰 앱을 통해 [그림 4]의 ①과 같이 내부에 저장소에 저장한다.

= APLn_ID + Un-ID + N + (E_{es_key}(s_key)) + Es_key(Un_ID+day+Nonce)

Ⅲ. 기존 방안과 비교 및 검토

이 장에서는 본 논문에서 제안한 스마트폰 앱기반 2-채널 인증방안을 기존의 ID/PW 인증방안 그리고 ID/PW기반 SSO 인증방안과 상호 비교하여 제안방안의 우수성을 도출하였다. 제안 방안의 비교에 있어서 전제는 특정조직내의 응용시스템들이 SSO시스템이 도입되지 않고 순수하게 각 응용시스템별 ID/PW기반으로 인증이 이루어진 경우, 그리고 사용자가 응용시스템에 접근할 때 마다 매번 ID/PW를 번거롭게 입력하는 것을 없애기 위해 SSO를 도입한 경우를 비교대상으로 하였다.

상기에서 제시한 기존의 인증방안과 본 논문에서 제안 인증방안의 상대적인 비교결과를 [표 2]에 정리하였다. [표 2]에서 본바와 같이 본 논문에서 제안한 스마트폰 앱에 기반한 2-채널 인증방안이 여러 비교요소들에서 우수성을 보이고 있다. 이는 ID/PW인증방안의 가장 큰 문제점인 PW의 입력부담 및 주기적 변경을 제거하기 위해 스마트폰 앱에서 세션 단위로 사용자의 인증정보를 자동으로 생성 및 갱신이 가능하도록 한 결과이다.

[표 2]에 따른 앱기반 2-채널 인증기술은 기존 인증방법들과 비교해 사용자 측면에서는 1회용 세션 PW를 자동 생성하기 때문에 PW를 기억하거나 주기적으로 변경할 필요가 없다. 또한 자동 생성되는 PW를 사용하는 것이기 때문에 ID 입력만으로도 로그인이 가능해 편의성이 뛰어나다. 인증을 위한 서버와 클라이언트 시스템 측면에서는 기존 SSO 서버 내의 인증정보들을 모두 저장했던 것에 비해 각 시스템 내에 인증정보들을 저장한다. 따라서 각 시스템의 인증정보와 사용자의 스마트폰의 인증정보들을 비교해 인증을 수행하고 SSO 서버의 구축 비용을 줄일 수 있게 된다. 나아가 SSO 내의 집중된 인증정보들을 분산시키게 되어 해킹 가능성이 낮아지고 보안 수준이 높아지게 된다.

표 2. 기존 인증방법과 제안시스템 비교분석

인증방법 / 비교요소	ID/PW 인증기술	ID/PW기반 SSO인증기술	앱 기반 2-채널 인증기술
인증 PW 특성	소유지식 (정적)	소유지식 (정적)	자동생성1회용 세션 PW(동적)
시스템 별 PW 기억	필요	필요	불필요(자동생성)
주기적 PW 변경	필요	필요	불필요(자동생성)
사용자 인증방법	(소유정보) : (각 시스템 인증정보) → 비교	(소유정보) : (SSO서버 내 인증정보) → 비교	(스마트폰 내 인증정보) : (시스템 내 인증) → 비교
사용자 편의성	저 (시스템 별 ID/PW입력)	고 (최소 한번 ID/PW 입력)	고 (ID만 입력 후 접근)
구축비용	저	고 (SSO서버 추가)	저
PW 해킹 가능성	고	고	저
자리를 비웠을 때 취약성	저	고	저
보안수준	하	하 (SSO서버에 인증정보 집중)	상 (스마트폰 앱으로 인증정보 분산)

이러한 우수성을 보인 요인은 SSO인증방안에서 문제가 되는 SSO인증서버에 모든 응용시스템의 모든 사용자의 인증정보를 중앙 집중적으로 지니는 문제를 제거하였기 때문이다. 즉, 각 사용자의 스마트폰 앱으로 그 사용자의 모든 응용시스템의 인증정보를 분산시켰기 때문에 SSO인증서버 때문에 발생되는 문제점들을 제거한 것이다. 또한 ID/PW기반 SSO인증방안은 1-채

널 형태로 인증이 이루어져 사용자가 자리를 비웠을 때 제 3자가 포털에 등록된 응용시스템을 자유롭게 접근하는 취약점을 지니고 있다. 본 논문에서 제안방안에서는 항상 추가적으로 스마트폰 앱을 경유하는 2-채널인증 방식을 채택했기 때문에 제 3자가 불법적으로 응용시스템에 접근할 수 없다.

본 논문에서 제안한 앱기반 2-채널 인증방안은 기존 OTP와 같은 2-채널 인증방안과 비교했을 때도 많은 장점을 확일할 수 있다. 우선 OTP를 비롯한 기존 2-채널 인증방안들은 ID/PW 시스템 자체에 추가적인 보안을 위해 사용하는 방식이다. 본 논문에서 제안하는 앱기반 2-채널 인증방안은 앞선 내용들에서 설명 했듯이 보안성뿐만 아니라 사용자의 편의성 구축비용의 효율성 등을 함께 고려한 것이다. 나아가 스마트폰의 자체 기술인 지문인식과 홍채인식 등과 같은 보안 솔루션들과 병합해 사용하면 뛰어난 보안성을 제공할 것이다. 또한 본 논문에서 제안한 스마트폰 앱기반 2-채널 인증방안을 사용하는 시스템은 OTP와 같은 2-채널 인증방안들과 마찬가지로 분실이나 도난 시 계정 잠금과 복구 방안을 제공해야 한다.

Ⅳ. 결 론

본 논문은 사용자가 조직 내에서 다수 응용시스템들을 사용할 경우 필수적으로 거치는 사용자 인증기술의 개선에 관한 내용이다. 본 논문에서 제안방안이 기존의 순수한 ID/PW인증기술에 내제된 문제점들이 해결됨을 보였고, 또한 ID/PW기반 SSO인증기술에 내제된 문제점들을 근본적으로 해결됨을 보였다. 물론 사용자인증이 항상 자신의 스마트폰에 설치된 앱에 연동되기 때문에 항상 스마트폰을 지녀야하는 부담이 존재할 수 있다. 하지만 이러한 부담에도 불구하고 기존의 ID/PW인증기술과 ID/PW기반 SSO인증기술들이 지니는 다양한 문제점들을 근본적으로 해결하기 때문에 충분히 유의미한 새로운 인증기술이라고 볼 수 있다.

새롭게 제안한 본 인증기술이 제품화되어 거의 대부분의 조직에서 활용 중인 기존의 SSO인증기술을 대체할 수 있는 대안기술로 자리매김 되길 기대한다.

참 고 문 헌

[1] N. Haller, C. Metz, P. Nesser, and M. Staraw, “A One-Time Password System” RFC 2289, IETF, 1998.

[2] 사희석, 최중섭, 주필환, “윈도우 악성코드 분류 방법론 설계,” 정보보호학회논문지, 제19권, 제2호, 2009(4).

[3] S. Gastellier-Prevost and M. Laurent, “Defeating pharming attacks at the client-side,” 2011 5th International Conference on Network and System security, IEEE. pp.33-40, Sept. 2011.

[4] 김영수, 나중찬, 손승원, “패스워드 인증 프로토콜 동향,” 전자통신동향분석, 제16권, 제6호, 2001(12).

[5] 이상민, “최근 인증기술 관련 현황,” 한국IT서비스산업협회, 2012.

[6] ISO/IEC 7816-1 (1998): “Identification cards - Integrated circuit(s) cards with contacts, part1 : Physical characteristics.”

[7] ISO/IEC 7816-3 (2006): “Identification cards - Integrated circuit(s) cards with contacts, part3 : Cards with contacts - Electrical interface and transmission protocols.”

[8] ISO/IEC 7816-12 (2005): “Identification cards - Integrated circuit(s) cards with contacts, part12 : Cards with contacts - USB electrical interface and operating procedures.”

[9] google android, (http://www.android.com).

[10] java cipher(http://docs.oracle.com/javase/8/docs/api/crypto/chiper.html)

[11] FIPS Pub. 197: Specification for the AES, Nov. 2001, availableat:http ://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

저 자 소 개

송 태 기(Tae-Gee Song) 준회원

- 2018년 2월 : 배재대학교 사이 버 보안학과 졸업
- 2018년 3월 : 배재대학교 사이버 보안학과 석사과정

<관심분야> : 정보보호, 모바일 보안, 보안 SW개발

조 인 준(In-June Jo) 정회원

- 1982년 2월 : 전남대학교 계산통계학과 졸업
- 1985년 2월 : 전남대학교 전자계산학과 석사
- 1999년 2월 : 아주대학교 컴퓨터공학과 박사
- 1983년 ~ 1993년 : 한국전자통신연구원 선임연구원
- 1994년 ~ 현재 : 배재대학교 사이버보안학과 교수

<관심분야> : 정보보호, 컴퓨터네트워크보안, 컴퓨터 시스템조직응용