논문 20-45-11-15 The Journal of Korean Institute of Communications and Information Sciences '20-11 Vol.45 No.11
https://doi.org/10.7840/kics.2020.45.11.1921

네트워크 접근제어를 위한 사용자 인증인가 시스템의 개발

조 진 용◆, 채 영 훈°, 공 정 욱*

Development of User Authentication and Authorization System for Network Access Control

Jinyong Jo◆, Yeonghun Chae°, JongUk Kong*

요 약

Guest 사용자의 인터넷 접근을 제어하는 NAC(Network Access Control) 시스템은 편의성과 보안성 간에 트레이드오프(Tradeoff)가 존재한다. 본 논문은 Captive 포털 방식의 NAC 시스템에 표준규격의 연합인증을 적용함으로써 사용자 계정관리에 대한 부담을 완화하고 NAC 서비스의 이용 편의성을 높인 연합인증형 NAC 시스템을 소개한다. 사용자 속성 기반의 인터넷 접근제어를 위해 허브형 인증인가(Authentication and authorization) 시스템을 개발하고 공개 NAC 소프트웨어와 표준 인증규약을 이용해 연동함으로써 계정관리에 대한 보안성을 높인다. 또한, 별도의 계정을 생성하지 않아도 소속기관에서 이용하는 사용자 본인의 크리덴셜을 통해 인터넷 접근권한을 획득케 함으로써 높은 편의성을 기대할 수 있다. 개발한 시스템의 접근제어 기능과 동시 사용자 수 및 전송성능을 구축된 테스트환경에서 정성·정량적으로 검증함으로써 시스템의 실 환경 적용가능성이 높음을 확인했다.

키워드 : 연합인증, SAML, AA, 네트워크 접근제어, Captive 포털
Key Words : Federated IAM, SAML, AA, NAC, Captive Portal

ABSTRACT

The Network Access Control (NAC) system that handles users' Internet access generally has a tradeoff between usability and security. This paper proposes a NAC system which reduces the burden on user account management and improves the convenience of using NAC service by applying a standard authentication specification to the captive portal of the NAC system. Security for account management is enhanced by leveraging federated authentication with a hub-type AA (Authentication and Authorization) system and adopting a standard to facilitates the exchange of security information. In addition, it is possible to achieve high usability because users can obtain access rights to Guest Internet through their home institutional credentials. We established a networking test-bed to verify the feasibility of the NAC system and evaluate its performance such as the capacity of concurrent users and the throughput of TCP/UDP packet streams.

※ 본 연구는 한국과학기술정보연구원(과제번호: K-20-L02-C02)의 지원으로 수행되었습니다.
◆ First Author : Korea Institute of Science and Technology Information, jiny92@kisti.re.kr, 책임연구원, 정회원
° Korea Institute of Science and Technology Information, proin@kisti.re.kr, 연구원, 정회원
* Korea Institute of Science and Technology Information, kju@kisti.re.kr, 책임연구원, 정회원
논문번호 : 202007-169-D-RU, Received July 28, 2020; Revised August 24, 2020; Accepted August 28, 2020

Ⅰ. 서 론

산·학·연의 공동 연구가 일반화[1]되는 추세로 인해 연구자들이 장·단기적으로 공동연구기관을 방문해 협력하는 기회가 많아지고 있다. BYOD(Bring Your Own Device) 환경에서 협력의 시작점은 방문기관에서 인터넷을 활용할 수 있도록 Guest 접근권한을 확보하는 것이라 해도 과언이 아니다. 하지만, Guest 접근을 불허하거나 특정 장소(예, 강당 등)에서만 허용하는 등 다수의 연구기관은 Guest 접근에 대해 보수적인 또는 폐쇄적인 성향을 보이는 측면이 있다. 이는 망분리를 시행토록 하는 정부 정책, 보안침해에 대한 우려와 보안시스템의 구축에 소요되는 비용 및 접근권한의 관리를 위한 시스템 유지비용 등이 전체적으로 결합된 결과로 볼 수 있다.

NAC(Network Access Control)은 외부로부터의 보안침해를 방지하거나 내부정보의 보호를 위해 공공기관이 필수적으로 갖춰야 하는 보안시스템 중 하나이다[2]. 교육기관은 주로 eduroam[3]을 활용해 무선 인터넷에 대한 Guest 접근을 관리한다. eduroam은 RADIUS 인증서버의 계층구조를 활용하는 802.1x 기반의 인증방식으로서 유무선 환경에 적용될 수 있지만 일반적으로는 무선 인증을 위해서 사용되고 있다. Captive 포털도 연구기관이나 교육기관에서 Guest 접근을 제어하기 위해 사용하는 일반적인 인증방식이다[4],[5],[6]. 인증받지 않은 모든 유무선 단말을 Captive 포털로 리디렉트(Redirect)시켜 인터넷 접속을 차단하거나 허용하는 방식으로 Wi-Fi Hotspot의 증가로 인해 Captive 포털의 사용이 확대될 것으로 예상된다[7]. NAC은 802.1x나 Captive 포털을 포함하는 광의의 개념으로써 연결된 유무선 단말의 검역이나 특정 네트워크 영역으로의 격리 등 확장된 기능을 포함한다.

응용계층에서 인증이 이루어지는 Captive 포털은 링크계층에서 인증하는 802.1x에 비해 보안성이 낮은 것으로 평가된다[8]. 하지만, 유무선 단말에 환경설정이 필요하지 않고 에이전트를 이용하지 않으므로 높은 편의성을 제공한다. 또한, 응용계층에서 연합인증(Federated identity management[9])과 쉽게 연동될 수 있으므로 사용자 인증이나 접근권한의 관리를 기관 외부의 계정관리시스템에 위임할 수 있다. eduroam도 사용자 인증을 기관외부의 개체에게 위임하지만 RADIUS 계층구조를 이용하기 때문에 RADIUS 인증 인프라의 구축이 필요하다.

Captive 포털과 연합인증을 활용해 유무선 단말의 Guest 접근을 제어하는 기존 연구[4-6]들은 사용자 인증(Authentication)에 한정해 외부 시스템에 권한을 위임했기 때문에 권한부여(또는 인가, Authorization)의 제어가 어려운 문제가 있다. 또한, 인증·인가 권한의 관리와 접근제어의 실행이 구조적으로 분리되지 않았기 때문에 인증·인가 기능의 적용을 다양한 OSS(Open Source Software) NAC으로 확장하는데 한계가 있다.

본 논문은 BYOD 환경에서 연구기관이나 교육기관을 방문하는 사용자가 소속기관에서 사용자 인증을 받으면 방문기관에서 제공하는 인터넷에 접속할 수 있도록 하는 허브형 AA(Authentication and Authorization) 시스템을 개발하는데 목적이 있다. 또한, OSS NAC과 허브형 AA를 연동하고 양자의 성능과 기능을 분석함으로써 개발한 시스템의 실행가능성(Feasibility)을 검증하는데 있다.

개발한 시스템은 인증·인가 권한의 관리와 접근제어의 실행을 구조적으로 분리함으로써 다양한 OSS NAC에 쉽게 적용할 수 있다. 본 논문의 기여 점은 다음과 같다. 1) 사용자 인가기능의 일부를 위임받은 허브형 AA 시스템을 개발하고 OSS NAC과 연동한 최초의 논문으로써 2) 허브형 AA 시스템이 갖는 사용자 권한관리 기능과 OSS NAC의 전송성능을 분석함으로써 개발 시스템들의 운용환경 적용 가능성을 확인했다. 개발된 시스템은 Guest 접근을 이용하는 연구기관과 교육기관의 구성원들에게 편의성을 제공하고 Guest 접근의 제어가 필요한 NAC 운용기관에게 비용효율적인 NAC 시스템의 구축과 관리를 가능케 한다.

본 논문은 다음과 같이 구성되어 있다. 제2장은 NAC과 연합인증에 대해 소개하고 관련 연구를 살펴본다. 제3장에서는 허브형 AA 시스템과 OSS NAC의 연동을 위해 고려되어야 할 요구사항을 정리하고 구현 내용을 세부적으로 설명한다. 제4장에서는 테스트베드에서 수행한 실험을 통해 제안한 시스템의 성능을 정성적·정량적으로 평가하고 제5장에서 결론을 맺는다.

Ⅱ. 배경 및 관련 연구

2.1 배경

NAC은 유무선 단말이 특정 네트워크 영역에 접근할 때 보안정책을 적용하기 위한 네트워킹 솔루션이다. NAC 시스템은 구조적으로 In-line 방식과 Out-of-band방식으로 구분할 수 있다. In-line 방식은 데이터 패킷이 NAC 장비를 통해 포워딩되는 형태로써 시스템의 구축과 관리가 쉽지만 단일 실패점

(Single point of failure)으로 작용할 가능성이 있다. Out-of-band 방식은 데이터 패킷이 이동하는 스위치나 라우터를 NAC 장비에서 제어하는 구조로써 일반적으로 VLAN 설정을 통해 허가 영역과 비허가 영역을 구분하고 SNMP(Simple Network Management Protocol) 명령을 이용해 스위치나 라우터를 제어하는 방식이다. 비허가 네트워크 영역을 분리해 관리하기 때문에 보안성이 높으며 유무선 단말의 전송성능이 저하되지 않는다는 장점이 있다. 하지만 환경설정이 복잡하고 유지비용이 높아질 수 있는 점 및 In-line 방식에 비해 접근제어 규칙이 NAC에 적용되는 시간이 더 걸린다는 문제점이 있다[10].

유무선 단말을 인증하기 위해서 802.1x나 MAC과 같은 2계층 인증과 Captive 포털이나 VPN과 같은 3계층 인증방법이 일반적으로 사용된다. 본 논문에서는 인증방식의 복잡성(예, Radius/802.1x의 계층 구조)을 낮추기 위해 Captive 포털을 활용하고 사용자 식별자나 비밀번호가 방문하는 기관의 네트워크(Visited network)에 노출되지 않도록 SAML 기반의 연합인증 통해 사용자를 인증한다. Captive 포털은 유무선 단말이 인터넷에 접근할 때, 접근 허가를 얻기 위해 리디렉트되는 특정 웹 페이지를 의미한다. Captive 포털에서 인증된 사용자만 인터넷 접근이 허가된다.

연합인증은 다수의 보안도메인 간에 적용되는 표준화된 사용자 인증·인가 체계이다[11]. 단일 보안도메인에 적용되는 통합인증(Single Sign One)을 멀티도메인으로 확장한 개념이다. 사용자를 인증하는 식별정보제공자(Identity provider)와 식별정보제공자로부터 전달받은 인증정보와 속성정보를 분석해 응용서비스에 전달하는 서비스제공자(Service provider)로 구성된다. 표준 메시지규약으로 SAML(Security Assertion Markup Language)을 사용하며 물리적으로 분리된 식별정보제공자와 서비스제공자를 네트워킹하기 위해 HTTP나 SOAP(Simple Object Access Protocol)를 전송규약으로 활용한다. 연합인증 환경 하에서 사용자들은 소속기관의 식별정보제공자에 로그인해야 계정연합(Identity federation)에 포함된 응용서비스에 접속할 수 있다.

계정연합은 동일한 연합인증 정책을 공유하는 SAML 개체(식별정보제공자 또는 서비스제공자)의 집합으로써 SAML 메타데이터를 서로 교환함으로써 신뢰관계를 구축한다. SAML 메타데이터는 개체식별자, 암호화/서명키, 앤드포인트 URL 및 개체정보 등을 포함하는 XML 형태의 정보이다. 계정연합 내에서 수립한 정책(보안규정 등)의 준수 여부를 메타데이터에 자가 주장(Self-assertion)하면 계정연합 내의 개체들이 해당 주장을 신뢰하기 때문에 신뢰네트워크라고도 한다. 계정연합에 속한 개체들의 모든 메타데이터를 수집과 검증 및 배포하는 중앙형 정보시스템이 존재하기 때문에 식별정보제공자들과 서비스제공자들은 메타데이터를 직접 교환하지 않아도 신뢰네트워크가 형성된다.

2.2 관련 연구

OpenNAC, PacketFence 및 FreeNAC 등 다양한 OSS NAC 솔루션이 존재하지만 본 절에서는 연합인증과 Captive 포털을 지원하는 일부 솔루션에 대해서만 소개한다.

CNR Captive 포털[4]은 무선 인터넷에 대한 사용자 접근을 제어하기 위해 Captive 포털과 연합인증을 연동한 NAC 시스템을 소개했다. 상용 솔루션의 Captive 포털을 대체하기 위해 무선인증과 Captive 포털을 지원하는 OSS를 활용했다. 무선인증을 위해 FreeRADIUS를 사용하고 사용자 인증을 위해서는 공개 SAML 소프트웨어인 simpleSAMLphp를 활용했다. NAC 소프트웨어로 Coovachilli를 이용했으며 IP 주소를 기반으로 사용자의 인터넷 접근을 제어한다.

Opengate[5]는 Captive 포털을 활용해 무선인터넷의 접근을 제어하는 시스템이다. Opengate는 MAC 또는 IP 기반의 NAC 시스템이고 In-line 방식으로 동작한다. 공개 SAML 소프트웨어인 Shibboleth를 이용해 사용자를 인증하며 Watch 프로세스를 통해 사용자 단말의 TCP 연결 상태를 검사한다. 접근제어를 위해 소프트웨어 방화벽을 이용한다. Watch 프로세스가 TCP 연결종료를 인지하면 소프트웨어 방화벽에서 해당되는 접근허가 규칙을 제거함으로써 접근을 차단한다.

HUPnet[6]은 Opengate와 매우 유사한 처리방식과 구조를 갖는 네트워크 접근제어 시스템이다. Shibboleth를 이용해 사용자를 인증하며 소프트웨어 방화벽을 활용해 IP/MAC 기반의 접근제어를 수행한다. 사용자의 접근권한을 세분화하기 위해 속성기반 접근제어(Attribute Based Access Control)를 활용한다.

표 1은 관련 연구와 제안하는 시스템의 주요 유사점과 차이점을 보여주는 비교표이다. CNR Captive 포털과 Opengate 및 HUPnet은 1) Captive 포털의 지원, 2) 연합인증의 적용, 3) In-line 방식, 4) 소프트웨어 방화벽의 사용 등에서 본 논문이 제안하는 NAC 시스템과 유사하다. 하지만 개발한 시스템은 1) 각 구성요소들을 모듈화해 OSS NAC들과 쉽게 연동·확장(Portability)할 수 있고 2) 허브형 AA 구조를 채택함

표 1. 관련 연구의 비교
Table 1. Comparison of related work.

	CNR	Opengate	HUPnet	Proposed
Captive portal	○	○	○	○
SAML	○	○	○	○
Centralized ACL	×	×	×	○
Portability	low	low	low	high

으로써 Guest 인터넷에 접근하는 사용자를 세밀하게 제어한다는 점에서 차이가 있다.

CILogon[12]과 SCZ(Science Collaboration Zone[13])는 대표적인 허브형 AA 시스템이다. CILogon은 OSS 기반의 연합인증 인프라로써 협업조직(또는 그룹) 관리 소프트웨어인 COManage와 연동되어 사용자의 속성정보를 관리한다. SCZ도 COManage를 통해 협업조직을 관리하는 허브형 AA 시스템이다. 하지만 우리가 아는 한 CILogon과 SCZ는 1) 서비스에 대한 접근제어를 허브형 시스템에서 수행할 수 없고, 2) 네트워크 접근제어를 위한 별도의 소프트웨어를 구현·연동하지 않았으며 3) 시스템 구조와 이용한 OSS가 다르다는 점 등에서 개발한 시스템과 차이가 있다.

Ⅲ. 설계 및 구현

본 논문은 인터넷 연결을 시도하는 Guest 사용자의 접근을 제어하기 위해서 허브형 AA 시스템을 개발하고 Captive 포털 기반의 OSS NAC 시스템에 허브형 AA 시스템을 연동하는데 목적이 있다. 본 논문에서 연합인증형 NAC 시스템은 허브형 AA 시스템과 연동된 NAC 시스템을 의미한다.

NAC 시스템을 운용환경에 빠르게 적용하고 유지관리의 편의성을 확보하기 위해서 필요한 시스템 요구사항은 다음과 같다. 기술개발 소요를 제기한 기관의 운용부서에서는 학술행사 등 특정 이벤트가 있는 경우에 네트워크 관리자가 방화벽을 수동으로 설정하거나 일회성 비밀번호를 발급해 접근제어를 수행하고 있어 관리가 불편한 상황이다.

3.1 시스템 요구사항

• **Fast deployment**: 새로운 NAC 시스템을 개발하고 검증하는데 소요되는 비용과 시간을 줄이고 기존에 수동으로 설정해 왔던 접근제어 방식을 빠르게 대체하기 위해서 OSS를 활용한다. OSS NAC 시스템은 유무선 인터넷 환경에 모두 적용할 수 있어야 하며 사용자 입장에서 유무선 인터넷 활용을 위해 요구되는 접속단말의 환경설정을 최소화할 수 있는 방식이어야 한다. NAC 시스템의 관리자도 직관적이고 편리하게 운용환경을 제어할 수 있어야 한다.

• **Delegated Authentication and Authorization**: Guest 접근을 요구하는 사용자에게 접근권한을 부여하기 위해서는 일반적으로 NAC 시스템에 사용자 계정을 생성하고 관리해야 한다. 802.1x 기반의 NAC을 사용하면 인증을 위해 RADIUS 인프라가 필요하다. 또한, EAP(Extensible Authentication Protocol)나 PEAP(Protected EAP)를 통해 전달되는 비밀번호의 암호화 방식(에, 평문, SHA1, MD5 등)은 SHA2의 적용을 강제하는 '개인정보의 안전성 확보조치[14]'를 위반할 가능성이 높다. 계정관리에 대한 부담을 줄이고 지침을 준수하기 위해 사용자 인증과 일부 권한부여 기능을 표준화된 외부 AA 시스템에 위임할 필요가 있다.

• **High Performance**: 사용자의 인터넷 이용환경(주로 웹 브라우징)을 고려하면 NAC 시스템은 1 Gbps 내외의 전송성능을 보장해야 한다. Guest 접근이 가능한 인터넷의 일반적인 접속속도가 100 Mbps 또는 1 Gbps 이하이며 동영상이 포함된 웹 브라우징 등 비교적 가벼운 목적으로 Guest 접근이 활용되기 때문에 1 Gbps의 전송속도면 충분할 것으로 예상한다. 공개 NAC 시스템이 내부적으로 병목지점을 가지고 있지 않다면 패킷처리 성능이 NIC(Network Interface Card)과 서버시스템의 성능에 비례하기 때문에 고사양 서버시스템을 활용함으로써 1 Gbps 이상의 속도를 기대할 수 있다.

위와 같은 시스템 요구사항을 충족시킴으로써 개발한 시스템을 다양한 OSS NAC에 적용할 수 있을 것으로 기대한다.

그림 1은 제안하는 시스템에서 Guest 사용자에 대한 접근제어 절차를 간략하게 보여준다(배경색을 갖는 절차는 NAC 시스템이 처리한다). 사용자가 유무선 인터넷에 접근하면 NAC 시스템이 패킷을 가로채고 해당 패킷의 IP/MAC 주소를 기반으로 사용자의 등록 여부를 검사한다. 사용자가 등록되어 있으면 업링크로 패킷을 포워딩한다. 사용자가 NAC 시스템에 등록되어 있지 않으면 사용자의 웹 브라우저를 실행해 Captive 포털로 리디렉트한 후, 사용자가 로그인을 요청하면 소속기관으로 다시 리디렉트한다. 그림 1에는 사용자가 소속기관을 선택하는 과정이 생략되어 있다. 소속기관에서 제공하는 인증시스템에 성공적으

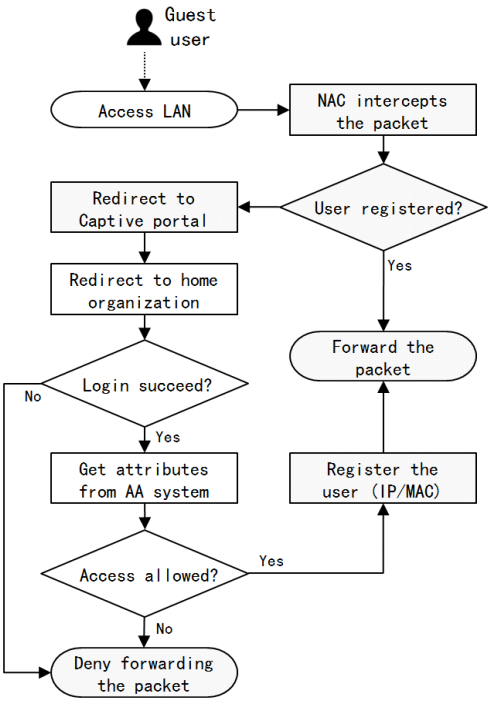


그림 1. 제안하는 접근제어 방식의 플로우차트
Fig. 1. Flow chart of the proposed access control.

로 로그인하면 해당 사용자의 속성정보가 AA 시스템으로 전달된다. AA 시스템이 해당 사용자의 부가 속성정보를 저장하고 있으면 소속기관으로 부터 획득한 속성정보와 취합하고 사용자가 LAN 접속권한이 있는지 확인한다. 사전에 정의된 속성정보와 값을 이용해 Guest 사용자의 접속 허용 또는 거부 여부를 결정한다.

3.2 시스템 구현

NAC 시스템을 신속하게 운용환경에 적용하기 위해 OSS인 PacketFence[15]를 활용했다. PacketFence는 웹 기반의 관리자 콘솔을 제공하고 Snort[16] 등 공개 침입탐지 시스템들과 쉽게 통합될 수 있다. 또한, 대역폭 관리(예, Traffic shaping)가 가능하고 접속단말의 보안 상태를 평가(Posture assessment. 예, 접속단말의 백신소프트웨어 설치여부 검사 등) 할 수 있는 등 OpenNAC[17]이나 FreeNAC과 같은 OSS NAC에 비해 다양한 관리기능을 제공한다. 자세한 기능비교는 리뷰논문[18]을 참조한다.

PacketFence는 In-band 방식 또는 Out-of-band 방식의 접근제어가 가능하며 통합인증을 활용할 수 있도록 SAML 표준규약을 지원한다. PacketFence의 통합인증은 하나의 식별정보제공자만 수용하므로 연합인증을 통해 다수의 식별정보제공자가 PacketFence와 연동될 수 있도록 시스템을 설계해야 한다. 빠른 운용환경 적용을 위해 본 논문에서는 In-band 방식을 채택하고 Captive 포털에서 SAML 규약을 이용해 사용자를 인증하도록 시스템을 개발했다. In-band 방식에서 PacketFence는 인증된 사용자의 단말이 갖는 MAC/IP 튜플 정보를 이용해 접근제어를 수행한다.

제안하는 허브형 AA 시스템은 사용자가 NAC 시스템에 계정을 생성하지 않거나 시스템 운영자가 사용자 계정들을 관리하지 않아도 되는 등 사용자 편의성과 계정관리의 효율성이 높은 장점이 있다.

그림 2는 사용자 인증과 인가를 각각 식별정보제공자와 식별정보교환자(IDeX, IDentity eXchange)에게 위임하기 위한 연합인증형 NAC 시스템의 개념도이다. 서비스제공자(즉, NAC)가 표준 인증규약을 사용해 식별정보제공자에게 사용자 인증을 위임함으로써 계정관리에 대한 부담을 줄일 수 있다. 본 논문에서는 속성관리자(Attribute Authority)와 속성제어자(Attribute Controller)를 포함하는 IDeX를 설계하고 운용환경에 적용함으로써 응용서비스가 담당하는 사용자 권한부여(즉, 인가)까지 외부 AA 시스템에 위임할 수 있는 방법을 제안한다.

연합인증형 NAC 시스템은 PacketFence의 소스코드를 수정하지 않아도 PacketFence가 가지고 있는 다음과 같은 문제점을 극복할 수 있도록 개발되었다. 아래에 기술한 문제점들은 OSS NAC의 Captive 포털에 연합인증을 적용하기 위해 필요한 기능들 중 PacketFence가 지원하지 않는 기능들이다.

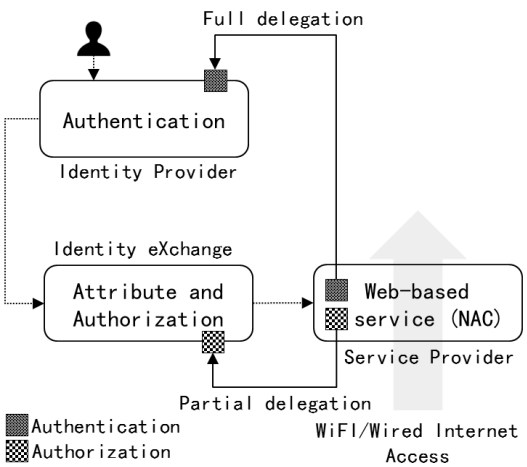


그림 2. NAC을 위해 제안하는 AA 시스템의 개념도
Fig. 2. Conceptual overview of the proposed AA system for NAC.

• PacketFence의 Captive 포털이 갖는 SAML 개체(즉, 서비스제공자)는 식별정보제공자와 1:1로만 연동될 수 있다. 즉, 하나의 식별정보제공자를 통해서만 인증을 받을 수 있다. 하지만 연합인증 환경에서는 다수의 식별정보제공자가 존재하기 때문에 식별정보제공자들과 서비스제공자(즉, PacketFence)가 N:1로 연동될 수 있어야 한다.

• PacketFence는 역할기반 접근제어(Role Based Access Control)을 지원하며 인증 받은 사용자는 Guest 접근권한을 갖게 된다. PacketFence는 SAML 속성 중 username만 수용하기 때문에 세분화(예, A 기관의 학생과 교수에게만 접근을 허용하고 B 기관은 학생에게만 허용)된 접근제어가 어려운 측면이 있다. 속성기반 접근제어와 역할기반 접근제어를 선택해 활용할 수 있게 함으로써 접근관리의 유연성을 높일 필요가 있다[19].

• 식별정보제공자를 포함해 연합인증에 필요한 AA 시스템들은 기관의 보안경계선(Perimeter) 외부에 존재한다. 따라서 경계선에 존재하는 NAC 시스템과 외부의 AA 시스템이 서로 통신할 수 있도록 즉, NAC을 회피(Passthrough)할 수 있도록 NAC 시스템이 구성되어야 한다. NAC을 회피해야 할 AA 시스템들의 수는 동적으로 증가하거나 감소할 수 있다.

위에 열거된 PacketFence의 미비점을 보완할 수 있도록 IDeX와 PCon(Passthrough Configurator)가 개발되었다. 특히, IDeX는 NAC 등 특정 응용서비스에 종속되지 않고 범용으로 활용될 수 있도록 설계되었다. IDeX와 PCon의 구성도는 그림 3과 같다. 그림 3

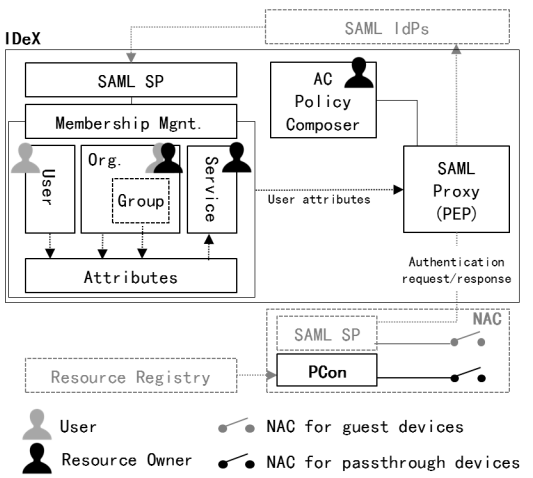


그림 3. NAC을 위해 제안하는 AA 시스템의 구조
Fig. 3. High-level architecture of the proposed AA system for NAC.

에서 점선으로 표시된 부분은 IDeX 외부에 존재하는 인증관련 시스템들이거나 PacketFence에 내장된 소프트웨어 모듈을 보여준다. IDeX는 User, Group, Organization 및 Service 개체를 생성하고 관리하는 회원관리자(Membership management)와 접근제어 정책을 구성하는 정책구성기(Policy composer) 및 N:1 메시지 교환이 가능한 SAML 프록시(Proxy)로 구성된다.

SAML 프록시는 식별정보제공자 및 서비스제공자의 기능을 동시에 제공하는 네트워킹 요소로써 정책구성기의 PEP(Policy Enforcement Point) 역할을 수행한다. 프록시는 다수의 식별정보제공자와 N:1로 연동되고 다수의 서비스제공자와 1:N으로 연동함으로써 N:N 메시지 교환을 가능케 한다. 프록시 내에서 메시지교환을 위해 공유메모리를 이용한다. 식별정보제공자는 사용자의 소속기관에 구축된 로그인 시스템을 의미하며 회원관리자는 가상의 조직(예, 연구프로젝트나 커뮤니티)에 속한 사용자의 속성정보를 관리한다. 기관에서 관리하는 속성정보와 조직에서 관리하는 속성정보가 서로 다르기 때문에 회원관리자가 필요하다. 예를 들어, 소속기관이 서로 다른 사용자들의 속성정보는 특정기관에서 관리하지 않으므로 회원관리자에서 관리해야 한다.

속성관리자에서 접근제어 규칙을 설정하면 SAML 프록시는 회원관리자가 제공하는 속성정보를 이용해 접근제어를 수행한다. 역할기반 접근제어와 속성기반 접근제어는 각각 PacketFence와 IDeX에서 선택적으로 수행될 수 있다. 사용자가 로그인에 성공하면 IDeX는 식별정보제공자로부터 속성 값의 집합, A_i을 획득한다. 또한, 회원관리자로부터 부가속성 값의 집합, A_m을 확보한다. A_m은 사용자가 스스로 생성한 속성 값(예, SSHPubkey)이나 조직 또는 그룹 관리자가 생성해 사용자에게 할당한 속성 값(예, 자격정보)을 포함한다. IDeX의 최고관리자(Superuser)는 특정 사용자에게 조직(O)이나 서비스(S)의 관리권한을 부여할 수 있다. 최고관리자 및 하위 관리자들은 일반 사용자를 초대하거나 등록할 수 있는 권한을 갖는다. 또한, O나 S에서 사용할 속성들을 정의할 수 있다. 임의의 조직(O_i)은 해당 조직에 속한 그룹(G_i)을 갖지 않거나 하나 이상의 그룹 ($O_i = \{G_i^1, ..., G_i^m\},\ n \geq 1$)을 가질 수 있다. 시스템 복잡도를 낮추기 위해 그룹은 하위 그룹을 가질 수 없도록 설계했다.

임의의 서비스 S_j는 임의의 O_i나 G_i에게 종속된

다. S_j가 독립적으로 존재할 수는 있지만 사용자를 등록할 수는 없다. 즉, S_j가 접근제어에 활용되기 위해서는 항상 O_i 또는 G_i와 연동되어야 한다. 임의의 서비스 S_j가 O_i 또는 O_i에 속한 그룹(G_i^m)과 연동되기 위해서는((S_j, O_i) 또는 (S_j, G_i^m)) 개체(S_j, O_i 또는 G_i^m) 관리자들의 상호승인이 필요하다. 시스템의 복잡도를 낮추기 위해서 임의의 서비스 S_j는 임의의 조직 O_i만 연동할 수 있도록 구현했다(S_j와 G_i는 연동불가). 임의의 S_j는 $O=\{O_1,...,O_n\}$와 $1:n$으로 연동될 수 있다.

정책구성기는 임의의 서비스 S_j에서 정의한 속성정보를 이용해 S_j와 연동된 응용서비스에 대한 사용자 접근을 제어할 수 있다. 임의의 S_j($S_j \in S$, $S=\{S_1,...,S_n\}$)는 개별적인 접근제어 정책 P_i^s ($P_i^s \subseteq P$, $P=\{P_1,...,P_m\}$)을 가질 수 있다. 서비스 S_j에 대한 정책 P_j^s는 S_j에서 사용하는 속성들의 집합 A_j($A_j=\{a_1=v_1,...,a_n=v_n\}$)를 이용해 정의한다. 즉, 정책제어기는 $P_j^s \subseteq A_j$인 속성 명(예, a_k)과 속성 값(예, v_k)의 집합을 이용해 접근제어 규칙을 설정한다. 예를 들어, 기관을 나타내는 속성 명이 a_1이고 속성 값이 v_1, 로그인한 사용자의 직무정보를 나타내는 속명명과 속성 값이 각각 a_2과 v_2라면 $P_j^s=\{p_1=(v_1='my.univ'), p_2=(v_2='student')\}$와 규칙 $p_1 \wedge p_2$을 통해 $my.univ$ 대학의 학생($student$)들만 접근을 허가하거나 거부할 수 있다.

접근제어 정책의 구성은 정책구성기가 담당하지만 실행은 SAML 프록시에서 수행한다. 정책구성기와 SAML 프록시 간의 규칙공유를 위해 SQL 데이터베이스를 이용했다. 정책구성기에서 규칙을 설정해 데이터베이스에 저장하면 SAML 프록시는 SAML 응답(Response) 메시지가 서비스제공자에게 전달 될 때마다 규칙을 검사하고 조건규칙에 맞을 경우 실행규칙(예, 허용이나 거부 등)을 적용하는 방식으로 동작한다.

규칙의 실행과 함께 SAML 프록시는 개별 서비스 제공자가 다수의 식별정보제공자와 연동될 수 있도록 프록시 기능을 제공한다. PacketFence는 식별정보제공자와 1:1로만 연동되기 때문에 OSS를 수정하지 않는 한 다수의 식별정보제공자와 연동될 수 없다. 본 논문에서는 공개 SAML 소프트웨어인 simpleSAMLphp[20]를 이용해 SAML 프록시를 구축했으며 기관단위 접근제어를 위한 탐색서비스(Discovery service)와 규칙의 실행을 담당하는 정책적용기를 simpleSAMLphp의 소프트웨어 모듈로 구현했다. 탐색서비스가 식별정보제공자들의 목록을 제공하기 때문에 사용자는 탐색서비스를 통해 자신의 계정정보를 저장하고 있는 식별정보제공자를 선택할 수 있다.

보안경계선의 외부에 존재하는 SAML 프록시와 식별정보제공자들은 경계선 내부에 위치한 Guest 사용자의 단말과 SAML 메시지를 교환해야하기 때문에 NAC을 회피할 수 있어야 한다. 관리자가 외부 AA 시스템들의 도메인이나 IP 주소를 PacketFence의 접근허가 목록에 수동으로 등록함으로써 NAC을 회피할 수 있다. 하지만, 식별정보제공자들의 수가 동적으로 증감하므로 수동으로 등록하면 관리비용이 증가한다. 따라서 외부 AA 시스템들의 도메인이나 IP 주소를 PacketFence의 접근허가 목록에 자동으로 등록할 수 있어야 한다. 그림 3의 PConf(Passthrough Configurator)는 자원등록기(Resource Registry)로부터 SAML 메타데이터를 주기적으로 내려 받고 식별정보제공자의 앤드포인트 URL 주소에서 도메인명을 추출한 다음에 IP 주소로 변환한다. 변환된 IP 주소를 PacketFence에서 제공하는 API(/ipset/passthrough)를 이용해 회피주소로 등록함으로써 외부 AA 시스템들의 동적 증감에 대응한다. 자원등록기는 식별정보제공자와 서비스제공자의 메타데이터를 등록하고 배포하는 저장소이다.

IDeX와 PCon을 개발해 OSS NAC 시스템에 연동·적용함으로써 OSS인 PacketFence의 소스코드를 수정하지 않아도 요구기능을 충족시킬 수 있다. 마지막으로, 성능에 대한 요구사항은 4장에서 실험을 통해 검증한다.

Ⅳ. 성능 평가

본 장에서는 제안한 연합인증형 NAC 시스템의 기능과 성능을 정성적 및 정량적으로 평가한다.

성능평가를 위해서 그림 4와 같은 네트워크 테스트베드를 구성했다. 식별정보제공자와 허브형 AA 시스템인 IDeX은 캠퍼스 네트워크의 외부에 위치한다. 구축된 NAC 시스템의 업링크는 캠퍼스 네트워크와 연동되며 다운링크는 2계층 사설망으로 구성했다. 사설망의 최대 가용대역폭은 1 Gbps이다. NAC의 다운링크는 1 Gbps 스위칭 허브와 연결했으며 허브를 통해 무선 AP(Access Point)와 실험용 Laptop(그림 4의

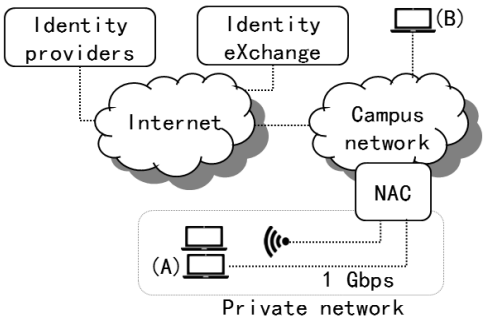


그림 4. 성능평가를 위한 테스트베드
Fig. 4. Test-bed for performance evaluation.

(A))을 연결했다. 또한, 성능측정을 위해 캠퍼스 네트워크 내부에 위치하는 Desktop PC(그림 4의 (B))를 이용했다. (A)와 (B) 사이의 병목 대역폭은 1 Gbps 이며 백그라운드 트래픽은 500 Kbps 이하이다.

그림 5는 NAC을 포함해 사설망에 구축된 시스템들을 보여준다. Laptop과 Desktop PC의 운영체제는 MS Windows 10이다. NAC 시스템은 3GHz CPU(2 cores), 12GB RAM, 100GB HDD 및 2-port 1 Gbps NIC을 갖는다.

그림 6은 IDeX에 구축된 NAC을 서비스로 등록하는 화면이다. NAC에 포함된 SAML 개체의 고유 식별자(Entity ID)를 등록하고 eudPersonEntitlement 속성을 AA 시스템들에게 제공할 수 있도록 설정했다. eduPersonEntitlement는 자원에 대한 이용권한을 표기할 수 있는 사용자 속성이다. SAML 프록시는 해당 속성 값을 활용해 Guest 사용자의 인터넷 접속을 제어한다.

그림 7은 조직 O_{nac}을 생성하고 그림 6에서 만든 S_{nac} 개체에 O_{nac}을 연동하는 화면을 보여준다. S_{nac}에서 생성한 개체의 고유 식별자(https://pf.kafe.or.kr/sp/user_saml)를 이용해 O_{nac}와 S_{nac}을 연동함을 알 수

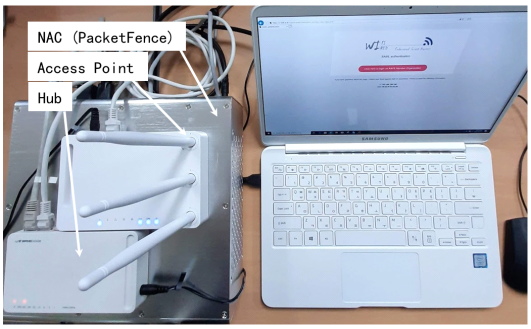


그림 5. 테스트베드에 구축된 NAC
Fig. 5. Deployed NAC in the test-bed.

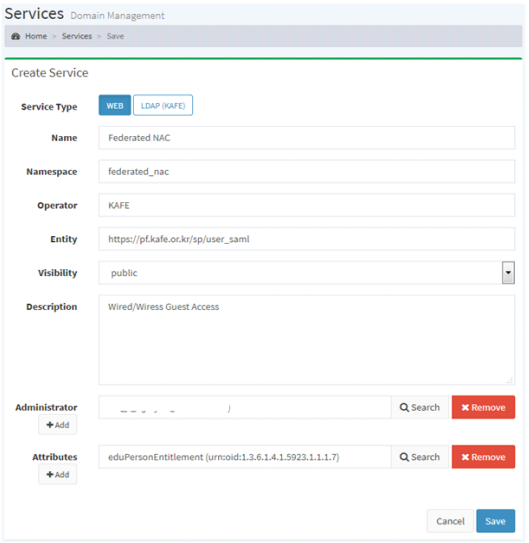


그림 6. Service의 생성
Fig. 6. Creation of a Service.

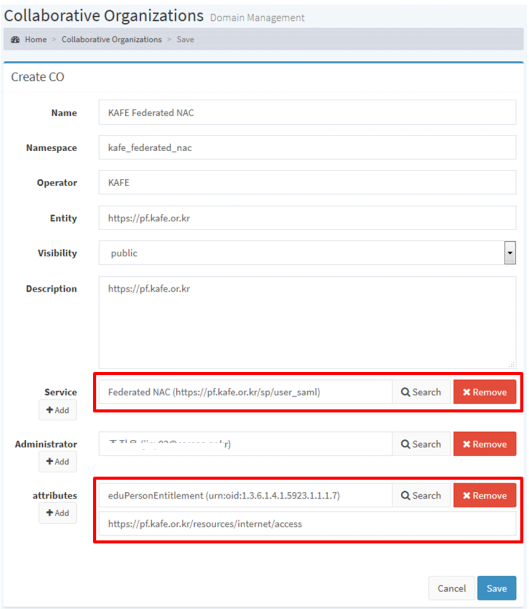


그림 7. CO의 생성
Fig. 7. Creation of a CO.

있다. O_{nac}에서 S_{nac}에 제공할 사용자 속성 명(a_1)으로 eduPersonEntitlement를 입력했고 속성 값(v_1)으로 https://pf.kafe.or.kr/resources/in ternet/access를 갖도록 설정했다. 따라서 O_{nac}의 관리자가 해당 속성 값을 변경하지 않는 이상, O_{nac}에 참여하는 모든 사용자는 설정된 eduPersonEntitlement 값을 갖게 된다.

그림 8은 생성한 O_{nac}에 사용자를 등록한 화면이다. 관리자는 ID 2에 해당하는 사용자를 신규로 등록했다. 따라서 그림 8의 ID 1과 ID 2에 해당하는 사용자는 S_{nac}에서 생성된 개체를 통해 SAML 프록시의 요청이 있을 경우에 설정된 eduPersonEntitlement 값을 제공하게 된다.

그림 9는 S_{nac}이 제공하는 속성 값을 이용해 사용자의 Guest 접근을 제어하기 위한 규칙설정 화면을 보여준다. 2개의 규칙이 생성되어 있다: a_1 값이 v_1인 사용자는 모두 Guest 접근이 허용되고 값을 갖지 않거나 다른 값을 갖는 사용자는 모두 거부된다. SAML 프록시는 S_{nac}에 등록된 사용자를 식별하기 위해서 eduPersonPrincipalName(a_e)을 이용한다. 즉, SAML 프록시를 통해 로그인 중인 사용자의 a_e를 이용해 S_{nac}에 저장된 해당 사용자의 e_1을 얻을 수 있다.

그림 10은 설정된 e_1 값을 갖지 않는 사용자가 PacketFence의 Captive 포털에 로그인을 시도하면 나타나는 접근거부 화면을 보여준다. SAML 프록시에서 사용자 인증을 차단함으로써 해당 사용자의 Guest 접근을 거부함을 예상할 수 있다. 즉, 사용자 인증이 차단되면 해당 사용자 단말의 MAC/IP 튜플이 PacketFence에 등록되지 않는다.

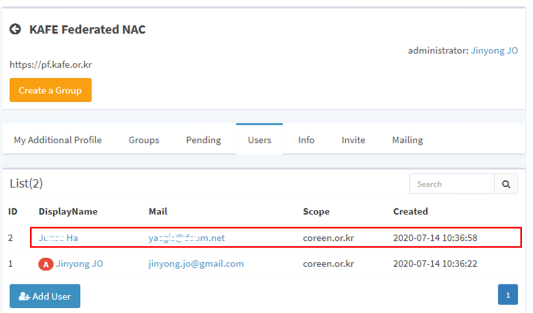


그림 8. O_{nac}에 참가한 신규 사용자
Fig. 8. User newly joined in O_{nac}.

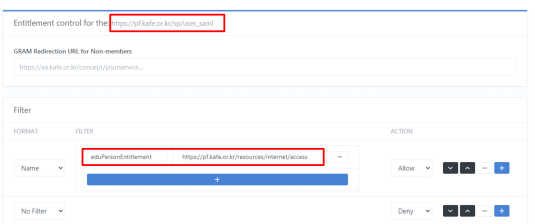


그림 9. 접근제어를 위해 설정된 규칙
Fig. 9. Configured rule for access control.

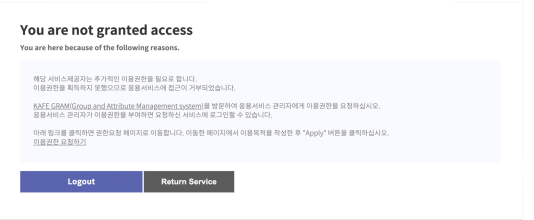


그림 10. 접근 거부
Fig. 10. Access denied.

Guest 사용자의 단말정보가 PacketFence에 등록되기 위해서는 Captive 포털에서 로그인에 성공해야 한다. Captive 포털의 성능을 확인하기 위해 동시접속자 처리수준을 측정했다. 그림 11은 n명의 Guest 사용자가 Captive 포털에 동시 접근했을 때, 웹 페이지 요청에 대한 평균 응답시간을 측정한 그래프이다. 측정도구로는 Apache Benchmark(ab[21])를 이용했다. 약 5,000명의 Guest 사용자가 Captive포털에 동시 접속했을 경우에 평균 웹 응답시간은 약 1.74초이고 최대 3.21초 걸리는 것으로 측정되었다. 사용자가 2초 이하의 페이지 로딩시간을 인내할 수 있다고 가정[22]하면 실험에 사용된 PacketFence 장치는 5,000명 이하의 동시접속자를 수용할 수 있을 것으로 판단된다.

마지막으로, PacketFence의 다운링크에 연결된 랩톱과 보안경계선 내부에 존재하는 데스크톱 PC를 연동하고 Iperf[23]를 이용해 TCP/UDP 전송성능을 측정했다. 랩톱과 데스크톱 PC는 동일한 2계층 스위치에 연결되어 있으며 병목 대역폭은 1 Gbps이다. 그림 12는 전송률에 따른 TCP 및 UDP 전송성능(Throughput)을 보여준다. NAC 시스템이 존재하지 않으면 PacketFence를 적용했을 때보다 UDP와 TCP

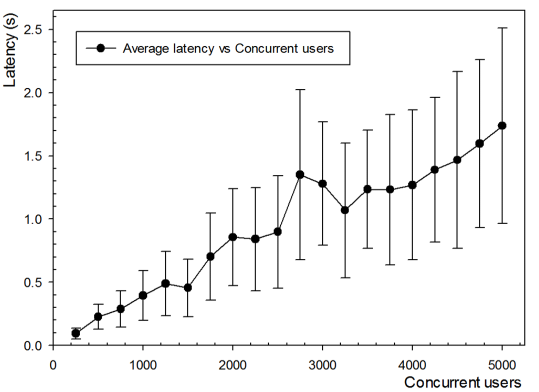


그림 11. 페이지 당 평균 처리시간(평균, 표준편차)
Fig. 11. Average processing time (mean, std.) per page request.

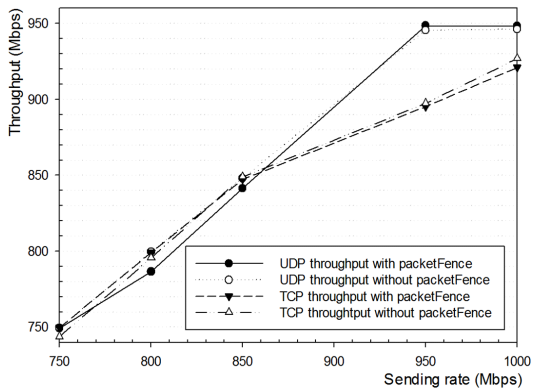


그림 12. TCP/UDP 전송성능
Fig. 12. TCP/UDP throughput.

의 전송성능이 평균적으로 각각 0.37 Mbps와 0.12 Mbps가 높아지는 것으로 나타났다. 평균 지연변이(Jitter)는 PacketFence를 사용했을 경우에 약 0.4 ms로써 사용하지 않았을 때의 0.16 ms 보다 평균 0.24 ms가 높았다. PacketFence의 적용여부가 TCP와 UDP의 전송성능에 크게 영향을 주지 않음을 확인할 수 있다.

V. 결 론

본 논문은 연합인증형 NAC 시스템을 개발하고 성능평가를 통해 개발한 시스템이 실제 운용환경에 적용가능한지를 살펴보았다. 안전한 표준 인증규약의 사용으로 NAC 시스템의 보안성을 높이고 계정관리에 대한 관리자 부담을 줄일 수 있을 것으로 기대한다. 또한, 일반 사용자들은 유무선 인터넷에 대한 Guest 접근권한을 빠르고 편리하게 획득할 수 있을 것으로 예상한다. 향후, Captive 포털에 기록된 브라우저 지문(Browser fingerprint)을 활용해 MAC/IP Spoofing 문제를 해결할 수 있도록 추가적인 연구를 진행할 계획이다.

References

[1] *Apache Software Foundation: Apache Benchmark*, Retrieved Jul. 27, 2020 from http://httpd.apache.org/docs/2.0/programs/ab.html.

[2] *Guide of Network separation for national institutions* (Korean), National Information Society Agency, Ministry of the Interior and Safety.

[3] L. Florio and K. Wierenga, "Eduroam, providing mobility for roaming users," in *Proc. EUNIS 2005 Conf.*, Manchester, 2005.

[4] I. Luca and P. Augusto, "Accesso wi-fi con authenticazione federata," *Smart eLab,* vol. 8, pp. 9-13, 2016.

[5] K. Watanabe, M. Otani, S. Tadaki, and Y. Watanabe, "Opengate on cloud," in *Proc. 26th Int. Conf. Advanced Information Networking and Appl. Wkshps.*, pp. 1027-1030, 2012.

[6] M. Linden and V. Viitanen, "Roaming network access using Shibboleth," in *Proc. TERENA Netw. Conf.*, p. 1, 2004.

[7] Cisco Visual Networking Index, "*Global mobile data traffic forecast update 2017-2022*," Cisco White paper, 2019.

[8] N. Marques, A. Zúquete, and J. P. Barraca, "Integration of the captive portal paradigm with the 802.1x architecture," *arXiv preprint arXiv:1908.09927*, 2019.

[9] S. Shim, G. Bhalla, and V. Pendyala, "Federated identity management," *Computer*, vol. 38, no. 12, pp. 120-122, 2005.

[10] *NAC White Paper* (Korean), Technical Report, Endpoint Lab., 2016.

[11] J. Jo, H. Jang, J. Kong, and Y. Chae, "Federated IAM service of KAFE identity federation," *J. KICS*, vol. 43, no. 12, pp. 2200-2214, 2018.

[12] J. T. Fleury and J. Gaynor, "Cilogon: A federated x.509 certification authority for cyberinfrastructure logon," *Concurrency and Computation: Practice and Experience*, vol. 26, no. 13, pp. 2225-2239, 2014.

[13] *SURF*, Retrieved Jul., 27, 2020 from https:nnwiki.surfnet.nlndisplaynSCZnScience+Collaboraton+Zone+Home.

[14] Ministry of the Interior and Safety, *Measures to ensure the safety of personal information* (Korean), 2019.

[15] R. Balzard and D. Gehl, "Packetfence revisited," *Linux J.*, vol. 2008, no. 165, p. 4, 2008.

[16] M. Roesch, et al., "Snort: Lightweight

intrusion detection for networks," in *Proc. Lisa*, vol. 99, pp. 229-238, 1999.

[17] openNAC, *Opensource NAC solution*, Retrieved Jul. 27, 2020 from http://www.opennac.org/opennac/en.html.

[18] H. Nunoo-Mensah, E. K. Akowuah, and K. O. Boateng, "A review of opensource network access control (NAC) tools for enterprise educational networks," *Int. J. Comput. Appl.*, vol. 106, no. 6, 2014.

[19] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," *Computer*, vol. 43, no. 6, pp. 79-81, 2010.

[20] *SimpleSAMLphp*, Retrieved Jul. 27, 2020 from https://simplesamlphp.org/.

[21] *Apache Software Foundation: Apache Benchmark*, Retrieved Jul. 27, 2020 from http://httpd.apache.org/docs/2.0/programs/ab.html.

[22] F. F. Nah, "A study on tolerable waiting time: how long are web users willing to wait?," *Behaviour & Inf. Technol.*, vol. 23, no. 3 pp. 153-163, 2004.

[23] A. Tirumala, L. Cottrell, and T. Dunigan. "Measuring end-to-end bandwidth with Iperf using Web100," in *Proc. Web100 Passive and Active Measurement Wkshp.*, 2003.

조 진 용 (Jinyong Jo)

2003년 : 광주과학기술원 정보통신공학과 석사
2013년 : 광주과학기술원 정보통신공학과 박사
2003년~현재 : 한국과학기술정보연구원
2016년~현재 : eduGAIN 운영그룹 위원

<관심분야> Authentication and authorization, Federated identity

[ORCID:0000-0001-6830-3604]

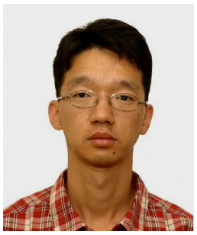
채 영 훈 (Yeonghun Chae)

2015년 : 고려대학교 전자 및 정보공학과 학사
2017년 : 과학기술연합대학원대학교 빅데이터과학 석사
2017년~현재 : 한국과학기술정보연구원

<관심분야> 딥러닝, 연합인증

[ORCID:0000-0002-6860-7533]

공 정 욱 (JongUk Kong)



1998년 : 포항공과대학교 석사
2015년 : 충남대학교 정보통신공학과 박사
2002년~현재 : 한국과학기술정보연구원

<관심분야> 네트워크 자원제어, 사용자정의 네트워킹

[ORCID:0000-0002-8703-2798]