다중 인증을 이용한 제로 트러스트 기반 VPN 인증 기술

곽승희[O], 이승주[*], 문정아[*], 전재호[*], 이재혁[**], 이경률[*]
[O]목포대학교 정보보호학과,
[*]목포대학교 정보보호학과,
[**]대구가톨릭대학교 컴퓨터소프트웨어학과
e-mail: {kwakshma, lo030ve, jeongah21, jjaihoo203920}@mokpo.ac.kr[O*],
gurtmggg@cu.ac.kr[**], carpedm@mnu.ac.kr[*],

Zero Trust-Based VPN Authentication Technology Using Multi-Factor Authentication

Seunghee Kwak[O], Seungju Lee[*], Jeongah Moon[*], Jaeho Jeon[*], Jaehyuk Lee[**], Kyungroul Lee[*]
[O]Dept. of Information Security, Mokpo National University,
[*]Dept. of Information Security, Mokpo National University,
[**]Dept. of Computer Software, Daegu Catholic University

● 요 약 ●

COVID-19 팬데믹으로 인하여, 재택근무와 같은 비대면 업무환경이 확대됨에 따라, 기업에서는 내부 보안을 위한 VPN 구축 및 사용률이 급격하게 증가하였다. 하지만, 기존의 대면 환경과는 다르게, 비대면 업무환경에서는 자신을 식별할 수 있는 수단을 제한적으로 활용하기 때문에, 사용자의 비밀번호가 노출되면, VPN에 접근하기 위한 사용자 인증이 무력화되는 심각한 문제점이 존재하며, 이러한 보안 취약점을 해결하기 위한 기술이 요구되는 실정이다. 따라서 본 논문에서는 기존 VPN 인증 기술에 내재된 보안 취약점을 해결하기 위하여, 사물 환경 인증, HIP 기술, 위치 인증, 상호 인증 기술을 활용한 다중 인증 기반의 제로 트러스트를 제공하는 VPN 인증 기술을 제안한다. 최종적으로는 본 논문에서 제안하는 기술을 통하여, 보다 안전성이 향상된 VPN을 제공할 것으로 사료된다.

키워드: VPN(Virtual Private Network), 보안 취약점(Security Vulnerability), MFA(Multi-Factor Authentication), 제로 트러스트(Zero Trust)

I. Introduction

2020년부터 COVID-19로 인하여, 많은 기업이 원격근무 인프라를 구축함으로써, 비대면 업무환경이 확대되었으며[1], 특히, VPN(Virtual Private Network) 도입 및 구축이 급격하게 증가하였다[2]. 비대면 업무환경이 도입되기 전, 대부분의 직장인들은 사원증과 같이 자신을 식별할 수 있는 수단을 활용하여 회사에 출입한다. 이는 일반적으로 사용자 인증 과정이라 할 수 있다. 인증이 완료되면, 자신에게 허가된 권한에 따라 회사 내 자원 및 자산에 접근하는 것이 가능하며, 이는 일반적으로 인가 과정이라 할 수 있다. 하지만 비대면 업무환경에서는 대면과는 다르게, 자신을 식별할 수 있는 수단을 제한적으로 활용하는 실정이며, 특히, 비밀번호 기반 인증을 활용하는 경우에는 사용자의 비밀번호가 노출됨으로써 인증이 무력화되는 심각한 문제점이 존재한다. 또한, 사용자 인증 방식의 취약점뿐만 아니라, 인증을 제공하는 프로그램, 혹은 VPN 자체적인 취약점으로 인하여, 허가되지 않은 공격자가 외부로부터 기업의 자산에 접근하는 심각한 문제점이 드러났으며[3], 실제로 최근 이러한 취약점을 이용한 해킹사건으로는 원자력연구원과 한국항공우주산업 사건이 있다.

이러한 이유로, VPN 환경에서 보안성이 더욱 향상된 사용자 및 장치 인증이 요구되는 실정이며, 본 논문에서는 다중 인증을 활용함으로써 제로 트러스트 개념을 도입한 보안성이 향상된 VPN 인증 기술을 제안한다.

II. The Proposed Scheme

본 논문에서 제안하는 다중 인증을 활용한 제로 트러스트를 제공하기 위하여, 사물 환경 인증, HIP(Human Interaction Proof) 기술, 위치 인증, 상호 인증 기술을 활용한다. 제안하는 방안을 활용한

VPN 환경에서의 다중 인증과정을 그림 1에 나타내었다.

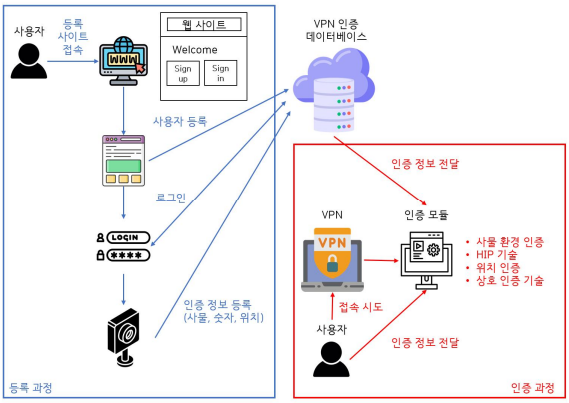

Fig. 1. 제안하는 방안을 활용한 VPN 환경에서의 사용자 등록 및 인증과정

● 사물 환경 인증 기술

사물 환경 인증 기술은 사용자가 지정한 사물이나 환경을 기반으로 인증하는 기술이다. 이 기술은 사용자를 식별할 수 있는 특정 사물을 이미지로 등록하거나 비대면 업무를 위한 전용 공간을 환경 이미지로 등록하며, 등록된 이미지를 기반으로 사용자를 인증한다. 사용자가 VPN으로 접속하기 위하여, 사용자 인증을 요청하면, 자신이 등록한 사물이나 환경 이미지를 실시간으로 확인함으로써 인증한다.

● HIP 기술

HIP 기술은 CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart.)와 같이 컴퓨터와 인간을 구별하기 위한 기술로, 본 논문에서는 사용자가 등록한 번호와 실시간으로 요구되는 정보와의 연관성을 검증함으로써 사용자를 인증한다. 사용자가 등록하는 번호로는 주민등록번호와 같이 사용자만이 아는 정보이며, 인증을 요청하는 경우에는 특정한 숫자를 화면에 출력하고, 사용자가 등록한 번호와의 계산 결과를 검증함으로써 사용자를 인증한다.

● 위치 인증 기술

위치 인증 기술은 사물 환경 인증 기술에서 사용자가 지정한 환경 이미지의 위치에 대한 GPS 정보를 저장한다. 저장된 GPS 정보를 기반으로, 환경 이미지에 해당하는 위치를 검증함으로써 사용자를 인증한다.

● 상호 인증 기술

상호 인증 기술은 악의적인 서버가 거짓된 정보를 인증 모듈로 전달하는 것을 방지하기 위하여, 인증 모듈에 서버만의 고유 정보를 미리 저장하여, 인증 정보를 전달받을 때, 서버의 신원을 확인하는 기술을 통하여 클라이언트와 서버의 상호 인증을 제공한다.

III. Conclusions

본 논문은 비대면 업무환경에서의 VPN 보안 위협을 방지하고 대응하기 위하여, 다양한 인증 방법 및 최소한의 인증 권한을 부여하는 다중 인증을 활용한 제로 트러스트 기반 기술을 제안하였다.

사용자 인증을 강화하기 위하여, 제안한 기술은 사물 환경 인증 기술, HIP 기술, 위치 인증, 상호 인증 기술이며, 상기 기술들을 기반으로, 사용자의 비밀번호가 노출됨으로써 인증이 무력화되는 문제점을 보완할 수 있을 것으로 사료된다.

향후 연구로는, 본 논문에서 제안하는 다중 인증을 활용한 제로 트러스트 기반 VPN 인증 기술을 제공하기 위하여, 제안한 기술들을 설계하고 구현함으로써, 기존 VPN과의 보안성과 관련된 성능을 비교하고 평가할 예정이다.

ACKNOWLEDGEMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2021R1F1A1050542).

REFERENCES

[1] S. Park, G. Kim, G. Son, W. Lee, and J. Park, "A study on a security model for the establishment of a non-face-to-face smart work working environment in a physical network separation environment of public institutions," Journal of The Korea Convergence Society, Vol. 11, No. 10, pp. 37-44, Oct. 2020.

[2] S. Park, "A study on the application of Zero Trust for security of remote office environment," Master's Thesis, Dongguk University, Jan. 2022.

[3] T. Bui, S. Rao, M. Antikainen, and T. Aura, "Client-side vulnerabilities in commercial vpns," In Nordic Conference on Secure IT Systems, Springer, Cham, pp. 103-119, Nov. 2019.