제로 트러스트를 위한 신뢰점수 기반 클라이언트 접근 제어 기법

윤아영 [1], 유헌창 [2]
[1] 고려대학교 SW · AI 융합대학원 소프트웨어보안학과
[2] 고려대학교 정보대학 컴퓨터학과 교수

yoon-a0@korea.ac.kr, yuhc@korea.ac.kr

Trust Score-Based Client Access Control for Zero Trust

Ah-Young Yoon[1], Heonchang Yu[2]
[1] Dept. of Software Security, Graduate School of SW · AI Convergence, Korea University
[2] Dept. of Computer Science & Engineering, Korea University

요 약

기존 경계형 보안 모델의 한계로 인해 제로 트러스트 아키텍처의 도입이 기업의 필수 과제로 부상하고 있다. 그러나 제로 트러스트 아키텍처로의 전환은 장기적인 과제이며, 빅뱅 방식으로 접근할 경우 큰 리스크와 높은 비용이 발생할 수 있다. 본 논문에서는 신뢰점수(Trust Score)기반 클라이언트 접근제어 기법을 제안함으로서 기존 구축된 인프라와 제로트러스트 아키텍처 간의 가교가 되는 점진적인 전환을 시도하고자 한다. 제안된 기법이 제로트러스트 패러다임에 적합하며 적용 후 제로트러스트 성숙도 수준이 향상되는 것을 확인하였다.

1. 서론

최근 경계 기반 보안의 한계가 부각됨에 따라, 모든 것을 신뢰하지 않는 제로트러스트 아키텍처가 각광받고 있다. 기존 경계 기반 보안 모델은 네트워크 단위의 신뢰를 허용함으로써 공격표면(Attack Surface)을 넓히고, 최초 허가된 사용자에 대하여 연결이 지속되는 동안은 신뢰검사를 하지 않음으로써 허가된 사용자의 비정상적 행위에 대해서는 탐지 및 제한을 할 수 없다는 보안적 취약성을 갖게 된다. 또한 원격근무와 클라우드 기술들은 데이터와 자원 접근에 대한 위치적 제약이 사라지게 만들어 더이상 접속지에 따른 보안 제어는 신뢰할 수 없게 되었다.

이런 흐름에서 제로트러스트 보안 모델은 기업, 스마트 시티, 스마트 팩토리 등 다양한 환경에서의 공격표면을 줄이고 보안성을 향상 시키는 새로운 패러다임으로 부각되어 구축의 요구는 커지고 있으나, 실제로 구축에는 전반적인 인프라 재설계에 따른 막대한 비용과 기간이 필요한 상황이다. 모든 것을 한번에 전환하는 빅뱅방식은 현실적으로 불가능한 사항이기 때문에 제로트러스트 아키텍처로의 점진적인 접근이 필요한 상황이다.

본 논문에서는 경계 기반 보안모델에서 제로트러스트 기반 보안모델로 넘어가기 위한 선 과제로 신뢰점수 기반 클라이언트 접근 제어 기법을 제안하고자 한다. 이러한 기법의 적용으로 기업의 제로트러스트 성숙도 레벨을 향상시킬 수 있을 것을 기대한다.

2. 관련 연구

2.1 ZTNA (Zero Trust Network Access)

"Zero Trust"는 위협이 네트워크 내부와 외부 모두에 존재한다고 가정하는 IT 보안 모델이다. 자원에 접근하려는 모든 사용자 엄격한 검증이 필요하며, 유연한 접근제어를 수행하여야 한다. 제로트러스트 가이드라인에 따르면 제로트러스트 아키텍처의 세 가지 주요 접근 방법[1]은 <표 1>에서 보여 준다.

<표 1> 제로트러스트 아키텍처 접근 방법

접근방법	세부 설명
인증 체계 강화	행위자의 식별자를 핵심 요소로 설정하여 정책 작성
마이크로 세그멘테이션 (Micro-Segmentation)	보안 게이트웨이로 보호되는 단독 네트워크 구역(segment)에 개별 리소스 (혹은 리소스 그룹) 배치
네트워크 인프라 및 소프트웨어 정의 경	소프트웨어 정의 경계 기법을 활용하여 정책 엔진의 결정에 따라 컨

계	트롤러가 네트워크를 재구성

ZTNA 는 제로트러스트 아키텍처를 구현하기 위한 핵심 기술로 네트워크 내·외부의 모든 사용자를 검증하고 권한을 부여하는 접근 제어 기술이다.

ZTNA 2.0 의 주요 요건[2]은 <표 2> 에서 보여준다.

<표 2> ZTNA 주요 요건

주요 요건	설명
최소 권한 접근	네트워크 계층에서 애플리케이션 계층까지 엄격한 권한 관리
연속적인 신뢰 검증	사용자 행동, 애플리케이션 변화, 디바이스 상태 등의 변화의 실시간 모니터링, 신뢰 수준을 지속적으로 검증
연속적인 보안 검사	모든 트래픽에 대해 지속적으로 보안 검사를 수행하여 위협 차단
모든 데이터의 일관된 보호	모든 애플리케이션에서 동일한 데이터 보호 정책을 적용하여 데이터 유출이나 손실 방지
모든 애플리케이션에 대한 일관된 보안	사설 애플리케이션, 클라우드 애플리케이션, SaaS 등을 포함하여 일관된 보안 제공

2.2 제로트러스트 아키텍처 성숙도

제로트러스트 아키텍처 성숙도는 조직이 제로트러스트 보안모델을 얼마나 잘 구현하고 있는지 평가하는 기준이 된다. <표 3>은 제로트러스트 가이드라인 1.0에서 정의하는 제로트러스트 성숙도 모델 3 단계[1]를 보여준다.

<표 3> 제로트러스트 성숙도 모델

단계	의미
기존 수준	아직 제로트러스트 아키텍처를 적용하지 않은 수준
향상 수준	제로트러스트 철학을 부분적으로 도입한 수준
최적화 수준	제로트러스트 철학이 전사적으로 적용된 상태

제로트러스트 성숙도 수준별 보안 기능은 식별자·신원, 기기 및 엔드포인트, 네트워크, 시스템, 응용 및 워크로드, 데이터 등 6 개의 항목에서 제시되고 있다. 이 논문에서는 ZTNA 구현을 목표로 하기 때문에 <표 4>, <표 5>, <표 6>에서 식별자·식원, 기기 및 엔드포인트, 네트워크 항목에서의 성숙도 수준별 특징[1]을 수용한다.

<표 4> 식별자·신원에 대한 성숙도 수준별 특징

기능	기본	향상	최적화
식별자 관리	온프레미스 ID	클라우드와 온프레미스 ID	클라우드 및 온프레미스 글로벌 ID
인증	패스워드, MFA	MFA	지속적인 신원 검증
위험도 평가	제한된 결정	정적 규칙 기반	기계학습 기반 실시간 분석
가시성 및 분석	정적 요소 기반	가시성 집계 후 분석	요소, 사용자, 행동 분석 및 중앙 집중화
자동화 및 통합	ID 와 자격증명 기반 수동	자동화 통합	ID 생명주기 통합

<표 5> 기기 및 엔드포인트에 대한 성숙도 수준별 특징

기능	기본	향상	최적화
정책준수 모니터링	제한된 정보 제공	대부분의 기기에 정책 시행	지속적인 기기 모니터링
데이터 접근제어	기기에 대한 정보 미의존	첫 데이터 접근 시 고려	실시간 위험 분석
자산관리	단순하며 수동으로 추적	자동화된 자산 관리	클라우드, 원격 자산 포함
가시성 및 분석	기기 수동 검사	정책 미준수 구성요소 파악/격리	지속적 기기 상태 평가
자동화 및 통합	정적 용량 할당 기기 수동 관리	사후 조정, 자동·반복적 방법 사용	동적 조정, CI/CD 적용

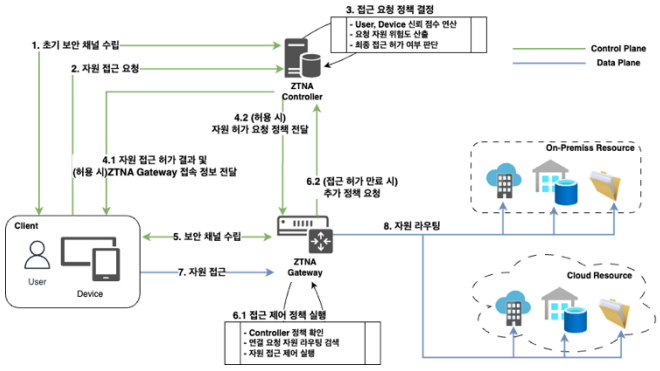
<표 6> 네트워크에 대한 성숙도 수준별 특징

기능	기본	향상	최적화
네트워크 세분화	대규모 경계 분리	일부 세분화	완벽히 분산된 세부 경계
위협 대응	정적 트래픽 필터링	사전 분석 포함	컨텍스트 기반 기계학습 필터링
암호화	최소한의 내외부 트래픽 암호화	모든 내부 트래픽 암호화, 일부 외부 트래픽 암호화	내외부 모든 트래픽 암호화
가시성 및 분석	중앙집중식 수집 기반 경계 가시성	수동 정책 기반 통합 분석	자동화된 통합 분석
자동화 및 통합	수동화된 네트워크 및 환경 변경	일부 자동화된 워크플로우	CI/CD, 자동화 코드로서의 인프라 사용

3. 클라이언트 접근제어 기법 및 신뢰도 평가

3.1 제안하는 기법

본 논문에서 제안하는 기법은 ZTNA Controller 에서 신뢰점수 산정 및 접근제어 허용 여부를 결정하며, ZTNA Gateway 는 클라이언트의 접근제어를 실행한다. (그림 2)는 신뢰점수에 기반하여 클라이언트 접근제어가 일어나는 흐름을 보여준다.



(그림 2) 클라이언트 접근제어 동작 과정

ZTNA 환경에서 사용자(User)는 접근하려는 자원에 대한 정보를 초기에 알 수 없으며 ZTNA Controller 에 의한 신뢰점수에 기반한 접근 허가를 받은 후 자원에 접근할 수 있다.

제안하는 기법의 동작 순서는 다음과 같다.

1. 클라이언트(사용자, 접근장치)는 ZTNA Controller 와 초기 보안 채널을 수립한다.
2. 클라이언트는 접근하려는 자원에 대한 정보를 요청한다.
3. ZTNA Controller 는 클라이언트 정보(사용자 정보, 접속 환경 등)을 이용하여 신뢰 점수를 확인하여 클라이언트의 접근 허가 여부를 판단한다.
   3.1 클라이언트가 접근을 요청한 자원의 접근 위험도를 확인하고, 연산한 클라이언트의 신뢰점수와 비교한다.
   3.2 신뢰점수가 더 높은 경우 접속을 허가하고, 그 외에는 접속을 거부한다.
4. 접근 허가 여부에 따른 정보를 전달한다.
   4.1 접근이 허용 된 경우, 클라이언트에게 ZTNA Gateway 접근 정보 및 보안채널 수립 정보를 전달한다.
   4.2 ZTNA Gateway 에게 접근이 허가된 클라이언트 접근 정보와 요청하려는 자원 정보에 대한 정책을 전달한다.
5. 클라이언트는 ZTNA Controller 로부터 전달 받은 정보를 이용하여 ZTNA Gateway 와 보안채널을 수립한다.
6. ZTNA Gateway 는 Controller 로부터 전달받은 정책을 실행하여 클라이언트의 접근을 제어한다.
   6.1 연결 요청이 들어온 허가된 자원에 대한 트래픽 라우팅을 실행한다.
   6.2 접근 허가가 만료되었거나, 허가된 클라이언트로부터 새로운 자원 연결 시도가 들어오는 경우 ZTNA Controller 에게 추가 정책을 요청한다.
7. 클라이언트는 ZTNA Gateway 를 통하여 원하는 자원에 접근한다.
8. ZTNA Gateway 는 자원에 위치와 요소에 따라 클라이언트 트래픽을 라우팅 한다.

3.2 신뢰 점수 기반 신뢰도 평가

신뢰점수(Trust Score)는 클라이언트의 접근을 허가를 판단하기 위한 신뢰도 평가 기준이다. 클라이언트의 신뢰도를 평가하기 위해서는 접근 정보에 기반한 정적 스코어링 방식과 컨텍스트 기반 동적 스코어링 방식이 존재한다. 제안하는 기법에서는 구현의 현실성 및 측정 성능 등을 고려하여 정적 스코어링 기반에 일부 컨텍스트 기반 정보를 적용한다. 클라이언트의 신뢰점수는 사용자 신뢰요소, 기기 신뢰 요소에 따라 측정된다. 신뢰점수가 위험요소 점수보다 높은 경우 자원에 대한 접근이 허가된다.

Trust Score 를 산출하기 위한 수식[3]은 다음과 같다.

$$Trust\ \ Score = \frac{(w_1 \times p_1) + (w_2 \times p_2) + \ldots + (w_n \times p_n)}{p_1 + p_2 + \ldots + p_n}$$

$p_1, p_2, \ldots p_n$: 신뢰를 평가하는 여러 요소 (예: IP 주소, 사용자 이름 및 역할, 위치, 시간, 장치 상태 등).

$w_1, w_2, \ldots w_n$: 각 요소에 할당된 가중치로, 해당 요소가 신뢰점수에 미치는 상대적인 중요도를 나타냄.

클라이언트의 신뢰 점수로 사용되는 주요 요소은 사용자/장치/통신채널 별로 <표 7>, <표 8>, <표 9>에 서술되었다. 기존 연구[3][4]에서는 제한적인고 정적인 항목만 신뢰 점수 요소로 사용한 것에서 사용자/장치/통신채널 항목으로 요소를 세부 정의하고, 사용자 히스토리에 기반한 정보를 추가하여 컨텍스트 기반 사용자 신뢰 항목을 추가하였다.

<표 7> 사용자 신뢰 주요 요소

요소	설명
인증 요소	사용자가 제시하는 각 인증 요소별 요소. (ex, 비밀번호, FIDO, OTP 등)
기본 권한	사용자가 갖고 있는 기본 권한
접근 시간	자원 요청에 대한 사용자의 접근 시간
사용자 DB 갱신 날짜	DB 의 사용자 데이터의 최신 여부
자원 사용	사용자가 일반적으로 사용하는 자원여부
신뢰 기록	사용자의 이전 자원 접근 요청 시의 신뢰 점수

사용자의 히스토리 기반한 정보(사용자 DB 갱신 날짜, 자원 사용, 신뢰 기록 등)를 기록하여 컨텍스트에 기반 사용자 신뢰 점수를 산정한다.

<표 8> 장치 신뢰 주요 요소

요소	설명
장치 SW	접근 장치의 OS 버전, 소프트웨어 패치 수준 등
장치 유형	PC, 모바일폰, 태블릿 등
관리 장치	사전에 접근이 허가된 장치 여부 확인
장치 위치	기기의 현재 위치가 일반적인 위치와 일치하는지
취약성 검사	마지막 백신 검사 결과, 백신 실행 여부 등

장치의 관리 정보와 소프트웨어/하드웨어 정보. CVE, CVSS 정보를 통하여 장치의 신뢰 점수를 산정한다.

<표 9> 통신 채널 신뢰 주요 요소

요소	설명
인증	통신 채널의 인증 방법
채널 유형	유선, WiFi, 셀룰러 등

WiFi 채널의 보안강도는 약하므로, 높은 보안 등급의 자원에 접근할 시 낮은 신뢰점수로 산정하거나, Cellular 를 사용하도록 유도한다.

4. 결과 분석 및 보안성 평가

4.1 결과 분석

제안 기법을 적용하여 제로트러스트 성숙도 향상도를 측정한다. 제로트러스트 성숙도는 점진적인 제로트러스트 아키텍처 구축에 얼마나 적합한지를 가늠하며, <표 3> 제로트러스트 성숙도 모델에 기반하여 제안하는 기법이 적용전에 비해 제로트러스트 수준을 어느 수준으로 높이는지를 확인할 수 있다.

제로트러스트 가이드라인 기능별 성숙도 수준별 특징에 시스템의 기능을 매핑하여 <표 10>, <표 11>, <표 12>와 같이 성숙도 수준을 평가하였다.

<표 10> 식별자 · 신원에 대한 성숙도 수준 평가

기능	적용 후	성숙도 수준
식별자 관리	구축 조직 ID 체계	향상 수준
인증	다중 인증 및 지속적 신원 검증.	최적화 수준
위험도 평가	정적 규칙 기반 식별자 위험성 판단	향상 수준

<표 11> 기기 및 엔드포인트에 대한 성숙도 수준 평가

기능	적용 후	성숙도 수준
정책 준수 모니터링	장치에 정책 준수 시행 매커니즘 적용	향상 수준
데이터 접근제어	첫 데이터 접근시 기기 상태 고려	향상 수준
자산 관리	수동으로 추적되는 목록	기존 수준

<표 12> 네트워크 대한 성숙도 수준 평가

기능	적용 후	성숙도 수준
네트워크 세분화	일부 내부적 세분화	향상 수준
위협 대응	위험을 사전에 발견하기 위한 분석	향상 수준
암호화	모든 트래픽 암호화	최적화 수준

해당 기법에서는 다루지 않는 가시성 및 분석과 자동화 및 통합 항목은 제외하였다. 식별자/기기/네트워크 기능에 대해서 향상 ~ 최적화의 성숙도 수준으로 책정되었다. 다만 자산관리 영역에서는 도입하는 조직 자산에 대한 적용이 필요하기 때문에 해당 기법의 제안 범위에서는 벗어나 기존 수준으로 책정하였다.

4.2 제로트러스트 적합성 평가

제안한 기법이 얼마나 제로트러스트 패러다임에 부합하는지와 ZTNA 의 주요 요건을 기준으로 판단하였다. ZTNA 의 최소 권한 접근 요건은 자원 별 신뢰 점수 기반의 권한 할당으로 만족한다 볼 수 있다.

연속적인 신뢰 검증 요건은 정적인 요소과 컨텍스트적 요소을 고려한 신뢰점수 책정을 통하여 만족한다고 볼 수 있다.

연속적인 보안 검사 요건은 논문에서 제안하는 기법의 범위는 아니나 ZTNA Gateway 와 추가 인프라(IPS, IDS, NG-Firewall)을 연계하여 만족 할 수 있다.

모든 데이터와 애플리케이션에 대한 일관된 보안은 ZTNA Gateway 의 추가 기능 구현이 필요한 사항이다.

5. 결론

본 연구는 신뢰점수기반 클라이언트 접근제어 기법을 제안함으로써 기존 경계형 기반 보안 모델 대비 제로트러스트 성숙도를 높이고자 하는 시도를 하였다. 이를 위하여 경우 기존 인프라 구조를 크게 변형하지 않는 상태에서 ZTNA Controller 에서 신뢰점수 기반의 클라이언트 접근제어 정책 결정을 하였고, ZTNA Gateway 에서는 정책에 의한 클라이언트 접근제어의 실행을 수행하였다. 또한 사용자/장치/통신채널 기반으로 신뢰점수를 산정하여 접근제어 판단의 기준을 수립하였다. 결과적으로 제로트러스트 성숙도 수준을을 기존 인프라에 향상 수준으로 도입할 수 있었다. 또한 제로트러스트 패러다임 도입에 어려움을 겪고 있는 기업들에 점진적 변환의 시발점에 도움을 줄 수 있을 것으로 기대한다.

참고문헌

[1] 과학기술정보통신부, “제로트러스트 가이드라인 1.0” 2023

[2] Palo Alto Networks, “ZTNA 2.0: The New Standard for Securing Access” 2022

[3] Aleena Terese George et al., “A Trust Score calculation approach for Zero Trust Access System”, 2023 IEEE 20th India Council International Conference

[4] Leonard Bradatsch et al., “Zero Trust Score-based Network-level Access Control in Enterprise Networks”, 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications