# 데이터 보안을 위한 제로 트러스트 아키텍처에 대한 연구

한성화[1] · 한주연[2,*]

[1]동명대학교 · [2]한국인터넷진흥원

# Study on Zero Trust Architecture for File Security

Sung-Hwa Han[1] · Joo-Yeon Han[2,*]

[1]Tongmyung University · [2]Korea Internet & Security Agency

E-mail : shhan@tu.ac.kr / jyhan@kisa.or.kr

## 요 약

정보 서비스에 대한 보안 위협은 갈수록 그 방법이 발전하고 있으며, 보안 위협으로 발생된 빈도와 피해도 증가하고 있다. 특히 조직 내부에서 발생하는 보안 위협이 크게 증가하고 있으며, 그 피해 규모도 크다. 이러한 보안 환경을 개선할 수 있는 방법으로 제로 트러스트 모델이 제안되었다. 제로 트러스트 모델은, 정보 자원에 접근하는 주체를 악의적 공격자로 간주한다. 주체는 식별 및 인증 과정을 통해 검증 후에 정보 자원에 접근할 수 있다. 그러나 초기 제안된 제로 트러스트 모델은 기본적으로 네트워크에 집중하고 있어, 시스템이나 데이터에 대한 보안 환경은 고려하지 않고 있다. 본 연구에서는 기존의 제로 트러스트 모델을 파일 시스템으로 확장한 제로 트러스트 기반 접근통제 메커니즘을 제안하였다. 연구 결과, 제안된 파일 접근통제 메커니즘은 제로 트러스트 모델 구현을 위해 적용될 수 있는 것으로 확인되었다.

## ABSTRACT

Security threats to information services are increasingly being developed, and the frequency and damage caused by security threats are also increasing. In particular, security threats occurring inside the organization are increasing significantly, and the size of the damage is also large. A zero trust model has been proposed as a way to improve such a security environment. In the zero trust model, a subject who has access to information resources is regarded as a malicious attacker. Subjects can access information resources after verification through identification and authentication processes. However, the initially proposed zero trust model basically focuses on the network and does not consider the security environment for systems or data. In this study, we proposed a zero trust-based access control mechanism that extends the existing zero trust model to the file system. As a result of the study, it was confirmed that the proposed file access control mechanism can be applied to implement the zero trust model.

키워드

제로 트러스트, 데이터 보안 위협, 접근통제, 정보 자원, 네트워크 보안

Zero Trust, Data Security Threats, Access Control, Information Resource, Network Security

## Ⅰ. 서 론

모바일 단말의 보급과 무선 네트워크의 발전으로 원격 근무 방식이 보편화되었으며, 이로 인해 RTE(Real-Time Enterprise)가 가능하게 되었다. 기관 내부에서만 접근할 수 있던 각종 정보서비스는 인터넷 망에 연결되었으며, 업무 효율성 증가를 위해 인터넷 망에 연결되는 정보 서비스는 더 증가하게 되었다.

그러나 정보 서비스의 발전에 따른 역효과도 있다. 대표적인 역효과는 정보 서비스를 인터넷 망에 직접 연결하면서 발생하는 보안 위협의 발생 증가이다.

## Ⅱ. 관련 연구

### 2.1 제로 트러스트 모델

경계 기반 접근통제 모델은, 적용되는 보안 기술

* corresponding author

및 보안 솔루션의 효율성이 가장 높기 때문에 많은 기관에서 채택하고 있다. 그러나 원격 근무 방식이 보편화되면서 경계 기반 보안 모델은 그 한계점이 지적되었다[1].

이에 따라 정보 서비스에 접근하는 모든 주체를 악의적 공격자로 간주하고 검증된 주체만 최소 권한만을 허용하는 제로 트러스트 모델이 제안되었다.

제로 트러스트 모델은 John Kindervarg가 제안한 접근통제 모델로, 정보 서비스에 접근하는 주체의 보안 환경 수준에 대한 검증을 요구한다. 만약 접근 주체의 보안 환경이 충분히 안전하다고 판단할 수 없을 경우에는 검증된 주체라도 접근할 수 없다[2].

### 2.2 제로 트러스트 모델의 한계

초기 제안된 제로 트러스트 모델은 네트워크 환경에 기반한다. 네트워크 계층에서, 조직 내부에 접근하는 정보 서비스에 대한 접근 주체 및 단말의 보안 환경을 검사하고, 인증된 주체 및 단말의 보안 환경이 충분이 안전할 경우에만 그 접근을 허용한다.

그러나 고도로 발달된 악성코드는 정보 서비스에 대한 접근 주체의 보안 환경에 은닉될 수 있다. 이러한 악성코드는 검증된 사용자 단말을 통해 엔터프라이즈 환경으로 유입될 수 있다.

## III. 제로 트러스트 모델의 확장

### 3.1 보안 환경에 대한 요구사항

검증된 사용자가 정보 서비스에 접근하였을 때, 악성코드는 인가되지 않은 데이터에 접근하여 정보를 유출하거나 변조 할 수 있다[3]. 이처럼 사용자의 권한을 넘어선 비인가 행위를 모니터링하고 차단하기 위해서는 제로 트러스트 모델을 네트워크 레벨뿐만 아니라 시스템, 어플리케이션, 데이터 레벨로 확대해야 한다.

### 3.2 데이터에 대한 제로 트러스트 접근 방법

본 연구에서는 시스템에 등록된 파일이나 디렉토리의 접근에 제로 트러스트 모델을 적용하기 위한 방법을 제안한다. 제안하는 제로 트러스트 모델 적용 방법은 Kernel 레벨에서 접근통제 기능을 제공하며, 보안 정책에 기반하여 동작한다. 접근통제 기능에 대한 우회를 차단하기 위하여 그림 1과 같이 LSM Interface에 연결시키는 방법을 적용하였다[4].

## IV. 결 론

제로 트러스트 모델은 분명 기존의 경계 기반 보안 모델의 한계점을 정확히 지적하며 그 문제점을 해결하기 위한 대안임에는 분명하다. 그러나 네트워크 레벨에 제로 트러스트 모델을 적용하는 것은 부적절하다. 본 연구에서는 파일이나 디렉토리에 대한 비인가 접근을 차단할 수 있는 제로 트러스트 기반 접근통제 방법을 제안하였다. 검증 결과 본 연구에서 제안하는 모델은 Zero-day attack 기반의 악성코드에 의한 비인가 파일/디렉토리 접근을 차단할 수 있다고 확인되었다.

다만, 각 계층 별 독립적인 운영은 그 효율성이 매우 떨어지므로, 통합 운영을 위한 추가 연구가 필요하다.

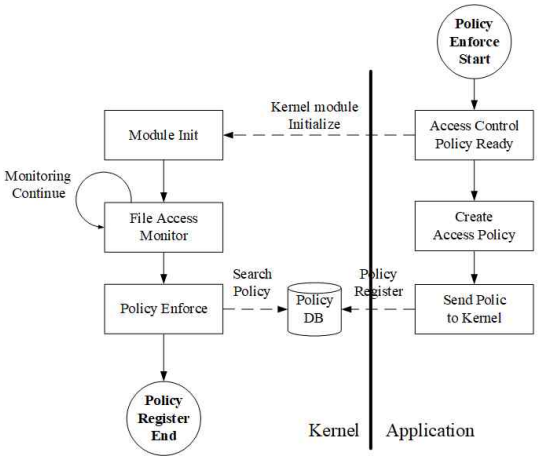


Fig. 1. Kernel level zero trust based File /Directory access control sequence

## Reference

[1] V. J. Gutierrez-Martinez, C. A. Cañizares, C, R. Fuerte-Esquivel, A. Pizano-Martinez and X. Gutierrez-Martinez, J. Victor, “Neural-network security-boundary constrained optimal power flow.” *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 63-72, 2010.

[2] Kindervag, John. “Build security into your network’s dna: The zero trust network architecture.” *Forrester Research Inc*, pp. 1-26, 2010.

[3] X. Sun, J. Dai, P. Liu, A. Singhal and J. Yen “Towards probabilistic identification of zero-day attack paths.” *2016 IEEE Conference on Communications and Network Security (CNS)., IEEE*, 2016.

[4] J. Morris, S. Stephen and G. Kroah-Hartman. “Linux security modules: General security support for the linux kernel.” *USENIX Security Symposium. ACM Berkeley, CA*, 2002.