유니온 파일시스템에 대한 보안 위협 및 대응 방법

한성화

동명대학교

Security Treats about Union File System and Responce Methodology

Sung-Hwa Han

Tongmyung University

E-mail : shhan@tu.ac.kr

요 약

유니온 파일 시스템은 다양한 파일과 디렉토리를 통합하여 단일 파일 시스템으로 사용할 수 있는 기술로, 통합에 사용되는 Source File/Directory를 그대로 유지할 수 있는 장점이 있어 컨테이너 플랫폼 등의 많은 어플리케이션에서 사용되고 있다. 유니온 파일 시스템을 사용할 때, 사용자는 Write-able Layer에 접근하며, 여기에는 운영체제에서 제공하는 보안 기술을 적용할 수 있다. 그러나 유니온 파일 시스템 생성에 사용되는 Source File과 Directory에는 별도의 보안 기술을 적용하기 어려운 단점이 있다. 본 연구에서는 유니온 파일 시스템 사용 시 발생될 수 있는 Source File/Directory에 대한 보안 위협을 차단하기 위한 접근통제 메커니즘을 제안하고자 한다. 접근통제 메커니즘의 실효성을 검증하기 위해 실증 구현한 후 기능 테스트를 수행한 결과, 본 연구에서 제안한 접근통제 메커니즘은 유니온 파일 시스템의 장점을 유지하면서 Source File/Directory를 보호할 수 있는 것으로 확인되었다.

ABSTRACT

Union file system is a technology that can be used as a single file system by integrating various files and directories. It has the advantage of maintaining the source file/directory used for integration, so it is used in many applications like container platform. When using the union file system, the user accesses the write-able layer, to which the security technology provided by the operating system can be applied. However, there is a disadvantage in that it is difficult to apply a separate security technology to the source file and directory used to create the union file system. In this study, we intend to propose an access control mechanism to deny security threats to source file/directory that may occur when using the union file system. In order to verify the effectiveness of the access control mechanism, it was confirmed that the access control mechanism proposed in this study can protect the source file/directory while maintaining the advantages of the union file system.

키워드

유니온 파일시스템, 파일 보호, 접근통제, 쓰기 전용 계층, 컨테이너

Union Filesystem, File Protection, Access Control, Write-able Layer, Container Platform

Ⅰ. 서 론

서비스 제공 및 확대 편의를 위해, 많은 정보 서비스에서는 중요 파일을 배포하는 방식을 많이 활용한다. 여기서 중요 파일을 활용하되 최소한의 변경사항을 반영하기 위한 도구로 Union filesytem이 개발되었다[1]. Union filesystem은 중요 파일을 통합하여 하나의 view를 제공하며, 통합에 사용되는 source file/directory는 유지하는 장점이 있어, 다양한 서비스에서 사용되고 있다. 그러나 이 Union filesystem을 사용할 때 통합에 사용된 source file/directory을 임의 변조하면, 변조된 내용이 filesystem에 그대로 반영되는 취약점이 있다. 본 연구에는 Union filesystem 사용시 source file/directory를 보호하기 위한 방법을 제안한다.

Ⅱ. 관련 연구

2.1 Union filesystem

Union filesystem은 source file이나 directory를 통합하여 하나의 write-able layer을 제공하는 파일 시스템이다. 이를 활용할 경우, write-able layer 생성에 사용되는 file/directory의 무결성을 유지할 수 있는 장점이 있다[2]. 이러한 장점으로 인해 AUFS(advanced multi-layered unification filesystem)나 Overlay2 파일 시스템 등이 개발되었으며, Container Platform 등의 많은 서비스에서 사용되고 있다[3].

2.2 Union filesystem의 취약점

Union filesystem은 정보 제공을 위한 file이나 directory의 무결성을 유지하는 장점이 있으나, 보안적으로는 단점이 있다. Union filesystem을 mount 한 경우, mount에 사용되는 source file과 directory를 임의 변경한 경우, 변경한 사항이 union filesystem에 반영되는 보안 취약점이 있다. 이 취약점은 해당 file/directory를 사용하는 모든 union filesystem에 모두 반영되기 때문에, mount 수가 많을수록 그 피해가 커진다.

Ⅲ. Union filesystem 보호 메커니즘

3.1 Union filesystem 보호 전략

Union filesystem에 사용되는 source file/directory를 보호 하더라도, union filesystem의 장점은 유지해야 한다. 그러므로 union filesystem에 사용되는 source directory에 대한 여타 접근을 차단하는 방식을 적용해야 한다. 또한 union filesystem을 unmount 했을 때에는 해당 접근통제 기능을 중지하여, source file/directory의 변경을 허용해야 한다.

3.2 Union filesystem 보호 방법

본 연구에서는 Union filesystem의 source file/directory를 보호하기 위한 메커니즘을 제안한다. 제안하는 메커니즘은 figure 1과 같이 union filesystem mount 시 생성되는 source directory에 대한 정보를 수집하고, 해당 경로에 접근하는 사용자의 접근을 차단한다. 접근 차단 메커니즘은 kernel level에서 적용하기 때문에, 사용하는 이 접근통제 메커니즘을 우회할 수 없다. 목표하는 보안 기능의 정상 제공 여부를 확인한 결과, 접근통제 메커니즘은 union filesystem을 mount 하였을 때 source file/directory에 대한 접근을 차단하며, unmount했을 때에는 source file/directory에 대한 접근을 허용하는 것을 확인하였다.

Ⅳ. 결 론

Union filesystem은 장점이 매우 크기 때문에 활용되는 분야가 점진적으로 증가하고 있다. 그러나 활용 장점이 있는 만큼 정보는 보호되어야 한다.

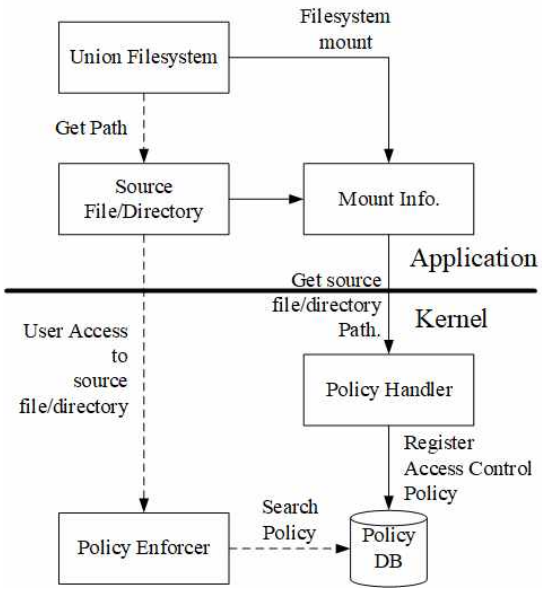

Fig. 1. Union filesystem source file/directory protection architecture

Union filesystem은 mount 한 이후의 write-able layer에 대한 보호는 가능하나, source file/directory를 보호할 수 없는 한계가 있다.

본 연구에서는 이러한 보안 취약점을 보완하기 위한 source file/directory 보호 방법을 제안한다. 제안하는 보호 방법의 기능을 확인한 결과, source file/directory을 보호할 수 있다고 확인되었다. 다만, 다중 union filesystem 생성 및 활용을 위한 접근통제 기능 제공 방법에 대한 추가 연구는 후속되어야 한다.

References

[1] WU, C., & CHEN, Q. A. (2013). Research on Union Filesystem for Linux and Its Performance Analysis. Computer Knowledge and Technology.

[2] Domaschka, J., & Seybold, D. (2020). Towards Understanding the Performance of Distributed Database Management Systems in Volatile Environments. An Automation-based Approach for Reproducible Evaluations of Distributed DBMS on Elastic Infrastructures.

[3] Tarasov, V., Rupprecht, L., Skourtis, D., Warke, A., Hildebrand, D., Mohamed, M., ... & Zhao, M. (2017, September). In search of the ideal storage configuration for Docker containers. In 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W) (pp. 199-206). IEEE.