

침입자로부터 안전한 XML문서 보호정책 방안

고철호[○], 이옥세^{*}

^{○*}한양대학교 컴퓨터공학과

e-mail: hommil@naver.com[○], oukseh@gmail.com^{*}

Safe XML Documents Protection Policy Method from Attacker

Chul-Ho Koh[○], Ouk-Seh Lee^{*}

^{○*}Dept. of Computer Science, Hanyang University

● 요약 ●

최근 XML 문서를 활용하여 다양한 분야에서 정보를 생성하여 사용하고 있다. 이에 따라 XML문서에 대한 보안이슈가 활발히 연구되고 있다. 본 논문에서는 익명의 침입자로부터 XML 문서에 대한 보호하는 정책을 제안한다. 이 기법은 XML 문서의 중요도에 따라 Count를 두어 설정한 Count 초과시 백업서버로 파일을 복제하여 전송한 후 파일을 삭제하기 때문에 익명의 사용자로부터 중요한 XML문서를 보호할 수 있다.

키워드: XML, XML 보호정책 (XML Documents Protection Policy)

I. 서론

XML를 활용하여 다양한 분야에서 정보를 활용하고 있다. 이에 따라 많은 분야에서 XML문서를 작성하여 정보를 공유함으로써 중요한 정보의 경우, 정보 보호에 대한 보안에 대한 인식이 커지고 있다. 웹 환경에서 정보는 공용 네트워크상에서 분산되고 공유된다. 따라서 민감한 정보에 대한 익명의 사용자가 접근하여 정보를 왜곡과 관련된 공격을 시도할 경우 안전하지 못하다.

본 논문에서는 익명의 사용자가 XML문서에 대해 공격을 시도할 경우, 이를 방지하고 XML문서를 보호하는 기법에 대해 제안한다. 기존 XML 문서에 대한 권한 설정, XML문서 암호화를 통해 익명의 사용자로부터 정보의 왜곡을 방지하는 연구들이 있었다. 그러나, 본 논문에서는 이러한 XML문서의 보호 연구들 수행하고도 정보왜곡이 가능한 상황이라 가정하고 중요한 문서에 대해 Count를 두어 익명의 사용자가 비정상적인 접근이 포착되면 파일을 복사하여 백업서버에 전송하고 기존 파일을 삭제하는 방법을 제안한다.

II. 관련 연구

1. 관련연구

박남제 외 4명은 안전한 전자 상거래를 위한 XML 정보보호기술 중 하나인 XML 키 관리 기술하며 W3C에서 진행 중인 표준안에 근거하여 XML 키 관리 구조와 처리절차에 대해 설명하고

있으며 국내의 제품 개발 동향을 분석하고 있다. 키 정보 서비스와 키 등록 서비스를 기반으로 문서를 교환할 때 사용하는 방법을 제시한다.[1]

박병철 외 4명은 웹 서비스의 보안 강화를 위해 XML 보안 기술을 현재 적용 가능하거나 향후 개발 및 적용될 XML 기반의 보안 기술을 설명하였다. 이에 XML 전자 서명, XML 암호화, XKMS SAM 등의 보안 기법에 대해 설명하였다. 이러한 기술을 적용하여 웹 서비스의 확장성 및 상호 운용성을 보장하는 보안 취약성 해결책을 제시하고 있다.[2]

조선문 외 2명은 접근 권한부여 정책들을 정의하여 접근 제어 시스템을 제시한다. XML문서를 생성할 때 문서에 대한 권한타입을 설정하여 문서를 생성한다. 그리고 권한을 설정한 문서들의 충돌에 대해 우선순위를 정의하여 권한충돌을 막는다. 기존 XML 문서의 접근제어 시간과 제안하는 접근 권한 부여 정책을 비교하여 기존보다 빠르게 접근하는 결과를 보여준다. 이러한 이유는 다양한 접근 권한 정책을 부여하기 때문에 기존 문서보다 빠르게 접근이 가능하다는 것을 보여주고 있다.[3]

III. 본론

본 논문에서는 암호화된 XML문서와 접근권한에 따라 불명확한 접근이 있을 경우, 중요도를 Count하여 명확하지 않는 접근이 발생할 경우, 접근된 XML문서를 복사하여 전송하는 기법을 제안한다. 따라서 익명의 사용자가 비정상적으로 XML파일에 접근할

경우, 문서를 백업서버에 전송한 후 기존 파일을 삭제하여 XML 문서를 보호할 수 있다. 이러한 메커니즘은 익명의 사용자가 XML파일을 접근하여 정보를 변환할 수 있다고 가정한다. 그리고 기존에 XML문서를 보호하는 기법을 사용하던 중 익명의 사용자가 접근이 가능하다고 가정한다.

제안하는 기법은 XML 문서의 중요도에 Count를 설정한다. 관리자 또는 문서작성자가 지정한 접근할 수 있는 Count를 넘길 경우, 익명의 사용자가 접근할 수 없도록 한다. 예를 들어, 문서 작성자가 회사의 중요한 문서를 XML문서를 저장하고 암호화하였다. 그리고 접근가능 Count를 1로 설정하였다. 그 후 익명의 사용자가 XML문서에 접근하기 위해 암호를 입력하였는데 틀렸을 경우, 문서에 지정한 Count가 1과 같아지기 때문에, 즉시 파일을 복사하여 백업서버에 전송하고 파일을 즉시 삭제하여 익명의 사용자가 접근할 수 없도록 한다. 이렇게 XML문서의 중요도는 문서 작성자 및 관리자가 지정하도록 한다.

제안하는 기법을 수행하기 위해서는 그림.1과 같은 구조의 흐름을 지닌다. XML문서는 DTD와 권한 정책 그리고 XML documents를 가지고 구성하여 정보를 제공하는데, 허용된 사용자가 정상적인 경로로 파일을 접근하여 수행할 경우, 명확한 정보를 확인할 수 있지만, 익명의 사용자가 파일을 접근하여 잘못된 암호 및 권한에 대한 불명확한 경로가 포착될 경우, 접근된 XML문서를 Count하여 관리자가 지정한 파일의 Count와 같아지면 파일을 복사한 후 백업서버에 전송하고 기존 파일을 삭제하여 익명의 사용자가 접근할 수 없도록 한다.

IV. 결 론

본 논문에서는 익명의 침입자로부터 XML 문서에 대한 보호하는 정책을 제안하였다. 이 기법은 XML 문서의 중요도에 따라 Count를 두어 설정한 Count 를 초과할 경우 백업서버로 파일을 복제하여 전송한 후 파일을 삭제하기 때문에 익명의 사용자로부터 중요한 XML문서를 보호할 수 있다. 따라서 이러한 정책은 XML 문서를 침입자로부터 안전하게 보호할 수 있을 것이라 예측된다.

참고문헌

- [1] Byung-chul Park et al., "A Study about Information Security Technology on XML for Web Service Security," Korean Institute of Information Scientists and Engineers 2003 fall Proceedings of the Conference announced, Book 30, No. 2, PP. 778-780, 2003.10
- [2] Bak, Nam Je et al, "XML key management for secure electronic transaction technology," Journal of Information Security, Book 13, No. 3, PP.72-82, 2003.6
- [3] Sun-Moon Jo et al., "Efficient Authorization Method for XML Document Security," Journal of the Korea Contents Association, Book 9, No. 8, PP.113-120, 2009.8

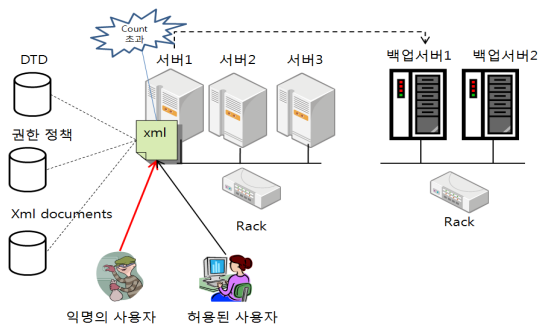


그림 1. XML 문서 보호의 흐름

Fig. 1. Flow of XML Document Protection