분산된 로그 정보의 실시간 암호화 백업모델을 통한 법적 신빙성 획득에 관한 연구

박종성[0], 문종섭 ,손태식
고려대학교 정보보호기술연구센터
p19j78s@korea.ac.kr

A Study on Real-Time Encryption Backup Model of Decentralized log data for acquiring completeness in court

Jong-Seong Park[0] , Jong-sub Moon , Tae-shik Sohn
*CIST Korea Univ

요 약

최근 악의적인 해킹이나 산업 스파이에 의한 정보유출 등이 날로 늘어남에 따라 정부 차원에서의 관련 법제도 강화나 적극적인 대응에 대한 방법론 등이 크게 대두되고 있다. 이에 컴퓨터 내에 남아있는 전자적 증거들을 실제 법적인 효력을 가지도록 하는 연구가 활발하게 이루어지고 있는 실정이다. 이러한 전자적 증거로서 가장 많이 사용되어지는 것이 로그 정보라 할 것이다. 기존의 로그정보는 분산된 호스트에 따른 관리의 문제와 무결성과 인증의 문제를 지니고 있다. 이 논문에서는 이러한 문제를 해결하기 위해 분산된 로그 정보를 실시간으로 암호화 하여 중앙의 특정 서버에 저장하는 방법을 사용한다. 이를 통해 무결성과 출처의 인증이 보장된 실시간정보에 의한 법적 신빙성을 획득할 수 있다.

1. 서론

컴퓨터 관련 범죄가 일어났을 때, 우리가 제일 먼저 취하는 행동은 해커의 흔적을 찾는 행위이다. 이러한 행위에 가장 흔히 사용되는 정보가 컴퓨터 내에 남아있는 로그정보라 하겠다. 이러한 이유로 로그정보는 해커의 악의적 행위에 대한 법적인 증거로 사용되어지고 있다. 그러나 이러한 로그정보는 위·변조 가능성이나 그 정보의 출처에 대한 인증의 부재로 인하여 법정에서 참고로서의 효력 밖에 가지지 못하고 있다.

이러한 로그정보에 무결성이나 정보출처에 대한 인증을 추가함으로써, 법적 신빙성을 가지는 시스템을 구성해보고 데이터 교환의 상호 동작을 살펴보도록 하자. 먼저 포렌식 관점에서의 로그의 의미와 기존 수집 방법에 의한 로그정보의 문제점에 대해 알아보고, 그 후 이 논문에서 제안하는 실시간 암호화 백업 모델을 살펴보도록 하자.

2. 포렌식 관점에서의 로그의 의미

컴퓨터 시스템에 불법으로 침입한 공격자는 흔적을 남기게 되는데 이러한 흔적이 저장되어 자는 곳을 로그 파일이라 할 수 있다. 이러한 로그파일에는 시스템에 대한 스캔 행위, exploit 툴을 이용한 공격, 특정 사용자 계정으로의 접속, root 권한의 획득, 트로이 목마 설치, 자료 유출 및 삭제 등 공격자의 행위들이 기록되어 진다. 이미 시스템에는 이러한 로그가 다량 존재하며, 이를 분석하고 조합하고 추리하여 공격자의 행동을 추적하는 것이 포렌식 관점에서의 로그의 의미라 할 수 있을 것이다. 이렇게 모아진 로그 정보는 법적인 증거자료로도 신빙성을 가질 수 있다.

3. 기존의 로그 수집 방법과 문제점

데이터베이스 서버에서 고객정보가 유출된 것을 관리자가 알았다고 가정하자. 서버 관리자는 공격의 흔적을 찾기 위해 먼저 정보유출 컴퓨터에 남아있는 로그 정보를 일일이 모으는 작업을 하게 된다. 뒤이어 정보유출 컴퓨터에 도착하기까지 경유하는 각종 네트웍 및 보안 장비(라우터, 침입차단시스템, 침입탐지시스템)의 로그 정보를 모으는 작업을 하게 된다. 마지막으로 관리자는 로그를 얻은 네트웍 및 보안 장비나 호스트에 대한 네트웍의 위치와 각 로그의 시간정보를 근거로 종합적인 분석을 수행하게 된다. 이러한 절차적 분석을 통해 관리자는 여러 위치의 장비들이 지닌 로그가 공통적으로 나타내는 핵심 이벤트를 찾을 수 있고, 이는 해커에 대한 추적이나 법적인 증거로 사용되어 지게 된다.

이러한 기존의 로그수집 방법은 크게 2가지의 문제를 가지고 있다. 관련된 로그 정보를 얻기 위해 각 호스트에 접근하여 로그정보를 일일이 수집하는 비효율성이 첫 번째 문제이고, 정보 유출이나 공격행위 이후에 관련 로그정보에 대한 위·변조 가능성이 존재한다는 것이 두 번째 문제이다. 이 중 두 번째 문제는 로그 정보의 법적인 효력과 직접적으로 관련이 있으며 법적인 신빙성을 위해서는 해커 뿐만 아니라 관리자 조차도 로그정보를 위·변조하지 않았다는 완벽한 무결성의 증명이 필요하다.

4. 실시간 암호화 백업 모델

기존의 로그정보 수집상의 문제점을 해결하기 위해 실시간 암호화 백업 모델을 제안 하고자 한다. 이 모델은 서버-클라이언트 모델로서 동작하게 되는데, 서버 측은 실시간으로 로그정보를 획득하고 획득된 정보를 시나리오 별로 분류하여 무결하게 유지하는 역할을 한다. 그리고 클라이언트 측(주요 네

트윅 및 보안 장비나 호스트)은 센서가 설치되어 통합 서버로 공유될 세션키를 보내고 그렇게 공유된 세션키를 사용해 로그 정보를 암호화 하여 보내는 역할을 하게 된다. 실시간 암호화 백업 모델에 대해 구체적으로 살표보도록 하자. 이 모델은 크게 2가지 동작으로 나뉘어진다. 사전에 세션키를 교환 하는 동작과 이 세션키를 사용하여 암호화된 로그 정보를 교환하는 동작이다.

가. 구체적 동작

그림 1은 그 첫 번째인 세션키를 교환 하는 동작이다. 이 동작은 통합 서버에서 PKI 서버를 이용하여 센서를 지닌 각 호스트를 인증함과 동시에 각 호스트에서 보내는 {세션키, 호스트 명칭}정보을 받는다. 그리고 통합 서버는 내부적으로 각 호스트의 명칭과 세션키 그리고 PKI 서버로부터 받는 각 호스트의 네트웍 위치에 따른 위치 값을 저장해 두게 된다.

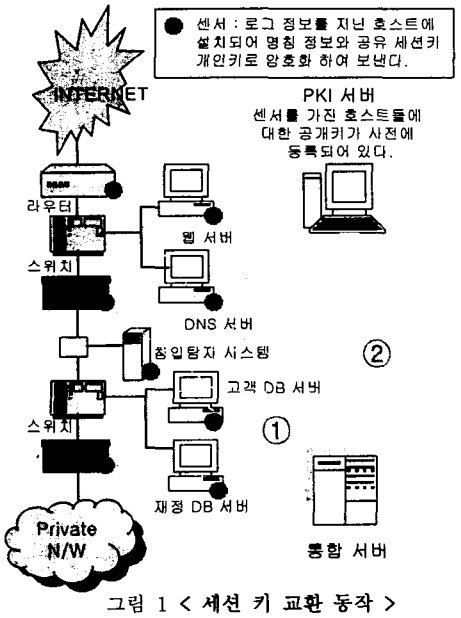

그림 1 < **세션 키 교환 동작** >

진행 절차는 다음과 같다.

(1) 센서를 설치하게 될 새로운 호스트의 등록 시, PKI 서버에 명칭정보와 공개키 정보 그리고 네트웍 위치 값에 대한 등록이 먼저 이루어진다.

(2) 호스트에 센서가 설치됨과 동시에 센서는 임의의 세션키를 생성한다.

(3) 이 세션 키를 자신의 명칭과 함께 개인키로 암호화하여 통합서버에 보내게 된다.(무결성 획득) ①

(4) 이 정보를 받은 통합 서버는 PKI 서버로 부터 인증서를 요구하고 인증서 내의 공개키를 사용해 복호화를 진행한다.(출처에 대한 인증 획득) ②

(5) 호스트로부터 받은 {세션키, 호스트 명칭}정보와 PKI 인증서로부터의 네트웍 위치 값 정보를 통해 다음과 같은 센서들의 목록를 생성한다.

라우터	11010..	1
웹 서버	01011..	1.5.1
외부방화벽	00110..	2
...	...	...

표 1 < **센서 목록** >

이와 같은 목록 정보는 로그 센서를 필요로 하는 호스트가 늘어남에 따라 자동적으로 통합서버에 업데이트 되어진다.

그림 2는 교환된 세션키를 사용하여 각 호스트에 로그 정보가 생길 때 마다 실시간으로 정보를 암호화해 보내는 동작을 보이고 있다. 전송되는 데이터의 앞부분에서 추출되는 네트웍 위치 정보와 거기에 해당하는 세션키를 사용하여 복호화해 봄으로써 출처 호스트에 대한 인증이 획득되고 데이터를 6라운드 DES 방식의 세션키를 사용함으로써 무결성이 보장된다.

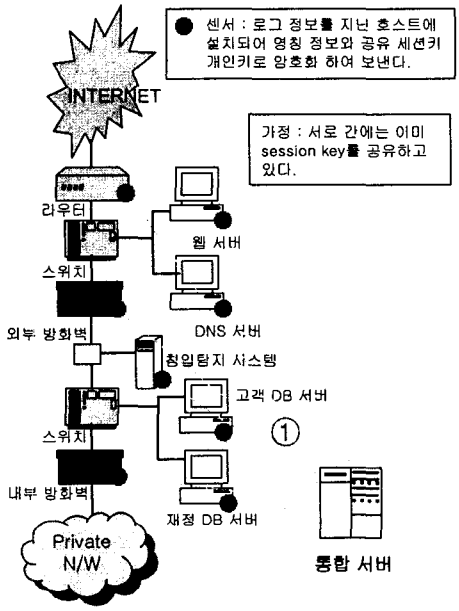

그림 2 < **암호화된 로그 정보 교환 동작** >

진행 절차는 다음과 같다.

(1) 각 호스트에서는 키 교환 과정을 통해 공유된 세션키를 이용해 실시간으로 생성되는 로그 정보를 암호화 한다.

(2) 암호화된 로그정보 앞부분에 명칭 정보 대신 자신을 인증시켜줄 네트웍 위치 값을 덧붙인다.

(3) 이렇게 생성된 데이터를 통합서버에게 보낸다. ①
이 때, 보내지는 네트웍 위치 값은 전송 도중 위·변조 되지 않는다고 가정한다.

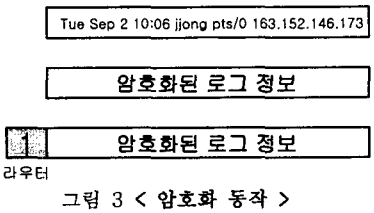

그림 3 < **암호화 동작** >

(4) 통합서버에서는 데이터의 앞부분에 덧붙여진 네트웍 위치 값에 해당하는 세션키를 센서 목록에서 구한다.

(5) 구해진 세션키로 암호화된 로그정보를 복호화 한다.

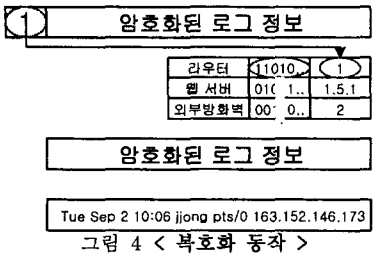

그림 4 < 복호화 동작 >

(6) 끝으로, 네트웍 위치 값과 로그 파일의 발생시간 정보를 시나리오별 분류 모듈에서 분석하여 시나리오에 맞게 로그 파일을 위치시키게 된다.

지금까지 실시간 암호화 백업의 동작에 대해서 알아보았다. 마지막으로 시나리오별 분류나 인증에 사용되어지는 네트웍 위치 값의 등번 생성 원칙에 대해 알아보자.

나. 등번생성원칙

네트웍 위치 값은 네트웍에 위치한 네트웍 및 보안 장비들의 연결순서에 따른 값으로서 시나리오별 로그파일 분석에서 이용된다.

등번 생선 원칙은 다음과 같다.

(1) 이러한 네트웍 위치 값은 외부에서 패킷이 내부로 들어온다고 가정했을 때 거치게 되는 장비의 순서에 따라 값을 매긴다.

(2) 정보유출이나 해킹의 직접적인 대상이 되지 않는 네트웍 장비나 보안 장비의 경우 양의 정수로 표기한다.

(3) 해킹의 대상이 되는 중요 서버들의 경우, { 위에 위치한 장비 < X < 아래에 위치한 장비 } X 라는 사이 값으로 표기하되 만약 동등한 위치에 서버들이 여럿 존재한다면 식별을 위해 ".x" 의 값을 덧붙인다.

다음의 표 2는 등번 생성의 한 예로 그림 1과 2에서 제시된 네트웍 구성도의 네트웍 위치 값을 보이고 있다.

라우터	1
웹 서버	1.5.1
DNS 서버	1.5.2
외부 방화벽	2
침입탐지시스템	3
고객 DB 서버	3.5.1
재정 DB 서버	3.5.2
내부 방화벽	4
내부 호스트	4.5.x

표 2 < 네트웍 위치 값 >

다. 정리 및 통합서버의 작업

지금까지 살펴본 (가), (나)의 과정을 통해, 제안된 실시간 암호화 백업모델이 로그정보의 출처에 대한 인증과 무결성을 보장함을 볼 수 있었다. 그리고 로그정보는 실시간으로 통합서버에 저장이 되므로 통합서버에 저장되어 있는 로그정보는 각 호스트에서 발생했던 로그정보들이 위·변조 되지 않고 그대로 통합서버에 옮겨져 있다고 생각 할 수 있을 것이다.

마지막으로 실시간 암호화 백업모델에서 핵심이 되는 통합서버의 작업들을 정리해 보도록 보자.

♠ 통합서버의 작업 :

(1) 새로운 센서가 등록 되었을 시 PKI 와 연동하여 로그정보를 지닌 각 호스트의 센서목록(명칭, 세션키, 네트웍 위치 값)을 저장한다.

(2) 각 호스트로부터 받은 실시간 로그 정보에 대해 복호화를 수행하고 네트웍 상의 호스트들의 위치와 로그의 발생시간 정보를 근거로 로그들을 시나리오별로 분류한다.

(3) 시나리오별로 분류되어진 로그 정보들에 대한 완전 무결성을 보장한다.(읽기 권한만이 주어진 data 저장공간에 정렬된 로그정보를 저장한다.)

위와 같은 통합서버의 작업을 통해 우리는 로그정보들의 시나리오별 분류에 따른 관리상의 효율성과 법적 증거자료로서의 신빙성을 획득할 수 있다.

5. 결론

위의 제안된 모델은 여러 호스트에 남겨진 로그정보를 시나리오 별로 자동 관리할 수 있고 일목요연하게 확인할 수 있는 이점 뿐 아니라 법정에서 신빙성을 더할 수 있다는 이점 또한 지니게 된다. 이러한 이점은 실시간 암호화 백업 모델의 두 동작 중 호스트에 대한 인증과 데이터의 무결성에 의해 보장된다.

아직 실제적인 구현과 성능 테스트가 없었기 때문에 이 후 구현 시에 돌발적인 문제들이 생길 것이라 생각한다. 하지만 가장 큰 문제로 대두 될 것이라고 생각되어지는 각 센서를 지닌 각 호스들의 성능과 통합 서버에 대한 성능만 안정적으로 유지가 된다면 지금까지 살펴본 것처럼 로그 정보의 법정에서의 신빙성을 획기적으로 향상시킬 수 있고 관리자의 로그정보에 대한 명확한 관리가 가능하다는 이점을 획득할 수 있을 것이다.

참고문헌

[1] Eoghan Casey. Digital Evidence and Computer Crime. ACADEMIC PRESS. 2000

[2] Eoghan Casey. Handbook of Computer Crime Investigation. ACADEMIC PRESS. 2002

[3] Warren G. Kruse II , Jay G. Heiser. Computer Forensics: Incident Response Essentials. Addison-Wesley .2002

[4] Albert J. Marcella, Robert S. Greenfield. Cyber Forensics[A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes]. Auerbach publications. 2002

[5] The Honeynet Project. Know Your Enemy: Revealing The Security Tools, Tactics, and Motives of the Blackhat Community. Addison-Wesley. 2002

[6] Douglas R. Stinson. Cryptography: Theory and Practice. CRC Press. 1995

[7] Alfred J. Menezes, Paul C. van oorschot, Scott A. Van stone. Handbook of Applied Cryptography. CRC Press

[8] Casey E, Garrity J. Internet Misuse in the Workplace : A Lawer's Primer. The Florida Bar Journal. 1998

[9] Diffie W, Landau S. Privacy on the Line: The Politics of Wiretapping and Encryption. The MIT Press

[10] 정현철. Unix_log_analysis. certcc.or.kr 문서. 2001