하드웨어 인증을 이용한 디지털 증거 보호 기법 설계

김지영*, 정병옥*, 최용락*

*대전대학교 컴퓨터공학과

A Design of Digital Evidence Integrity Assurance Techniques Using Hardware Authentication

Ji-Young Kim*, Byung-Ok Jeong*, Yong-Rak Choi*

*Department of Computer Engineering, Daejeon University.

요 약

보안 침해사고시 수집된 디지털 증거를 법적 증거로써 제출하기 위해 신뢰성이 확보되어야한다. 이를 위한 디지털 증거 무결성 보증 기법들중 MDC를 사용한 디지털 증거 무결성 보증 기법은 MDC값을 공격자가 위조·변조 할 수 있다는 단점이 있다. 또 PKI 를 이용한 공증 방식은 기존의 증거 수집 시스템을 수정해야 하는 단점과 새로 시스템을 도입하기 위한 비용이 많이 드는 단점이 있다. 따라서 본 논문에서 제안하는 디지털 증거 보호 기법은 Diffie-Hellman(DH) 키 교환 알고리즘을 이용하여 생성된 비밀키와 디지털 증거 수집 대상 시스템(Collecotion System-CS)의 하드웨어 정보(HW_{CS})로 디지털 증거(D), 디지털 증거에 대한 해쉬값(H(D))과 타임스탬프(Time)를 암호화해서 디지털 증거에 대한 기밀성, 인증 및 무결성을 보증하는 기법을 제안하였다.

I. 서론

사이버 범죄의 증가는 공공기관, 기업, 개인의 물적·경제적 손실을 초래하고 있다. 심각한 사회적 혼란의 주범인 해커들을 잡기 위해서는 시스템에 남아있는 침입의 흔적이나 악의적인 행위들에 대한 디지털 증거들을 확보해야 한다. 이 디지털 증거는 실생활에서 수사관들이 범죄현장에서 수집하는 범죄행위들에 대한 각종 증거물들로 생각할 수 있다. 수집된 증거물들은 법정에 가서 범인의 범죄행위에 대한 증거가 된다. 마찬가지로 디지털 증거들도 해커들의 악의적인 행위들에 대한 증거로 사용하기 위해 수집된다. 그러나 디지털 증거들은 삭제 및 위조·변조가 용이하고 그 출처에 대한 인증 부재로 인해 법적 증거로써 효력을 갖지 못하는 특징이 있다. 그러므로 디지털 증거의 보관 및 수집에 있어서 신뢰성이 확보 되어야만 법적 증거로써 효력을 갖는다. 이를 위해 디지털 증거에 대한 무결성 보증 및 출처 인증이 요구된다[1][2].

디지털 증거의 법적 효력을 갖도록 하기 위한 요구사항을 표 1에서 보인다.

[표 1] 제안 기법의 요구사항

요구사항	
디지털 증거의 보호	기밀성
디지털 증거의 출처 인증	인증
디지털 증거의 삭제 및 위조/변조 방지	무결성

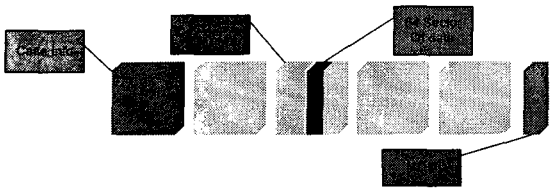
본 논문에서는 표 1과 같은 요구 사항을 만족하는 기법으로 Diffie-Hellman(DH) 키 교환 알고리즘을 이용하여 생성한 비밀키와 디지털 증거 수집 대상 시스템(Collection System-CS)의 하드웨어 정보(HW_{CS})로 디지털 증거(D)와 디지털 증거에 대한 해쉬값(H(D)), 타임스탬프(Time)를 암호화하는 기법을 설계하였다.

II. 관련 연구

1. MDC를 사용한 디지털 증거 무결성 보증 기법

대표적인 통합 포렌식 도구중 하나인 Encace의 이미지 구조를 보면 MDC(Manipulation Detection

Code)를 사용하여 디지털 증거의 무결성을 보증하고 있다. 그림 1은 Encase의 이미지 구조를 나타낸다.



<그림 1> EnCase의 이미지 구조

이미지의 머리 부분은 원본 저장 매체의 전체 개요 및 사건 정보를 포함하고 있다. 이미지의 몸통 부분은 저장매체의 정보를 저장한다. 그리고 64 섹터마다 CRC 값을 계산하고 이를 저장하여, 데이터의 오류 발생 여부를 확인한다. 이미지의 꼬리 부분은 MD5 해쉬값을 기록한다. Encase를 실행하면 S/W 자체에 이미지를 마운트 하고, 이미지의 몸통부분에 저장된 CRC 값과 꼬리 부분에 저장된 MD5 값을 검증한다. 이런 방식이 디지털 증거 무결성 보증 부분에서 거의 표준으로 알려져 있다. 그러나 이 방식은 이미지 정보를 위조하고 위조한 섹터의 CRC 값을 재 계산한 후 기존 CRC 값과 변경할 수 있다. 그리고 조작된 이미지 파일의 해쉬값을 재계산한 후 기존 해쉬값과 변경하면 디지털 증거의 무결성에 대해 주장할 수 없는 문제점이 있다.

하드디스크 정보를 H, 이미지의 정보를 I, MDC 값을 V라 했을 때, H = I이며, V = h(H) = h(I)이다. 이때, 위조자가 H, I, V 모두 변경할 수 있기 때문에, V′ = h(H′) = h(I′)로 위조·변조가 쉬워 법적 증거로 제출하기 위한 디지털 증거의 무결성을 갖지 못한다[2][3].

2. PKI를 이용한 공증 방식

PKI를 이용한 공증 방식은 공인된 디지털 증거 수집자가 디지털 증거의 MDC가 포함된 요약 정보에 전자서명을 하고, 신뢰성 있는 제 3자가 운영하는 온라인 공증 시스템에 원격으로 공개키 기반의 공증을 요청한다. 온라인 공증 시스템은 전자 서명을 확인하고, 공증 내용에 Time Stamp를 실시하여, 안전한 DB에 저장하고 공증 내용을 재전송 하는 방식이다.

이 방식은 공격자가 정당한 서명 값 및 Time Stamp를 작성할 수 없고, 공증 DB의 내용을 위조할 수 없으므로, 위변조가 암호학적으로, 시스템적으로 불가능 한 특징과 증거 수집자가 MDC의 내용을 확인하고 전자서명을 실시하므로, 디지털 증거 무결성의 이의 제기를 사전에 방지하는 부인봉쇄 기능을 제공한다. 그러나 이 방식은 기존 증거 수집 시스템을 수정해야 하고 새로운 시스템을 도입하기 위한 비용이 많이 드는 단점이 있다[3][4].

III. 제안하는 디지털 증거 보호 기법

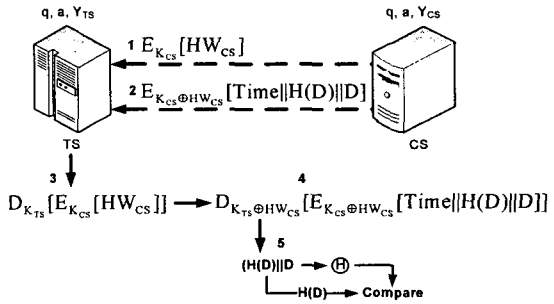
본 논문에서는 디지털 증거를 통합관리하는 신뢰 시스템(Trusted System-TS)은 CS 하고만 연결이 되어 있어 안전하고 TS에 등록된 CS만 접근 허용된다고 가정한다.

제안하는 디지털 증거 보호 기법은 암호화에 사용되는 키를 안전하게 교환하기 위해 DH 알고리즘을 사용하여 비밀키를 공유한다.

DH 알고리즘을 사용하여 비밀키를 공유하는 이유는 TS와 CS가 상호 동일한 키를 공유해야 하는데 키 전송상의 취약성과 상대방의 인증문제에 대한 대안으로 공개키 시스템을 응용한 암호화 프로토콜인 DH 키 교환 알고리즘을 사용한다.

그리고 정당한 CS라는 것을 확인하기 위해 HW_{CS}를 사용한다. CS는 CS의 비밀키(K_{CS})와 HW_{CS}를 XOR연산을 통해 얻은 키로 D, H(D)와 Time를 암호화하고 TS에 전송한다.

제안 기법은 TS에서만 디지털 증거를 복호화 할 수 있기 때문에 디지털 증거의 기밀성, 인증, 무결성을 보증할 수 있다. 제안 기법은 그림 2와 같은 수행절차를 따른다.



TS	디지털 증거 통합 관리하는 신뢰 시스템(Trusted System)
CS	디지털 증거 수집 대상 시스템(Collection System)
q	숫수
a	a < q 그리고 q의 원시근 a
Y_{TS}	TS의 공개키
Y_{CS}	CS의 공개키
K	TS, CS의 비밀키
HW_{CS}	시스템의 하드웨어 정보
Time	타임스탬프
H(D)	디지털 증거 해쉬 값
D	디지털 증거(Digital Evidence)

<그림 2> 제안하는 디지털 증거 보호 기법

○ 제안 기법 수행 절차

1. TS와 CS는 DH 키 교환 알고리즘을 사용하여 비밀키를 생성한다. CS는 이 비밀키 K_{CS}로 SEED 알고리즘 또는 AES 알고리즘, 등을 선택하여 HW_{CS}를 암호화시켜 TS에 전송한다.

2. CS는 Time, 디지털 증거에 대한 해쉬값(H(D))와 디지털 증거(D)를 K_{CS}와 HW_{CS}를 XOR 연산을 통해 얻은 키로 암호화 해서 TS로 전송한다.

3. TS는 1번에서 전송 받은 CS의 HW_{CS}를 TS에서 계산된 비밀키(K_{TS})로 복호화한다.

4. TS는 2번에서 전송 받은 디지털 증거를 K_{TS}와 3번에서 얻은 CS의 HW_{CS}를 XOR연산을 하여 얻은 키로 복호화 한다.

5. 복호화를 통해 얻은 Time는 디지털 증거의 현재성이 정당함을 확인하는데 사용된다. 그리고 D를 해쉬값 계산한 후 H(D)와 비교하여 디지털 증거의 변조 유무를 확인한다.

○ 제안 기법의 특징을 보면,

1. 제안 기법은 디지털 증거를 암호화하는데 사용하는 비밀키를 안전하게 공유할 수 있다.(키 교환)

2. TS와 CS만이 키를 정할 수 있기 때문에 공격자가 디지털 증거를 볼 수 없다.(기밀성)

3. TS는 오직 CS만이 이 비밀키와 하드웨어 정보를 사용하여 디지털 증거를 암호화 했다는 것을 안다.(인증)

4. TS는 타임스탬프값을 통해 전송 받은 디지털 증거가 오래된 것이 아님을 안다.(재전송 공격 방어)

5. TS는 HW_{CS}를 확인하여 D를 전송 받기 때문에 정당한 CS와 통신할 수 있다.(제 3자 개입 공격:Man In The Middle Attack 방어)

6. TS는 CS로부터 전송된 D를 해쉬값을 계산한 후 H(D)와 비교하여 디지털 증거의 변조 유무를 확인함으로써 디지털 증거의 변조 유무를 확인할 수 있다.(무결성)

1. 하드웨어 정보

하드웨어 정보를 이용하여 CS를 인증하는 것은 공격자가 TS와 CS 사이에서 정상적인 CS에서 오는 디지털 증거인것처럼 속이고 TS에 디지털 증거를 전송했을 경우 TS는 전송된 디지털 증거에 대해 신뢰할 수 없기 때문에 제 3자 개입 공격에 취약하다. 이를 예방하기 위해 CS의 하드웨어 정보를 TS에 등록해 놓고 CS에서 디지털 증거를 전송하기전 등록된 CS인지 비교하여 등록된 CS가 맞는지 확인하는 절차가 필요하다.

CS에서 추출될 하드웨어 정보는 <하드디스크 일련번호>, <CPU ID>, <CPU Vender>, <CPU Product ID>, <Mac Address>, 등 이다.

다음은 정상적인 CS인지 확인 하는 절차이다.

1. HW_{CS}는 TS로 TS와 CS가 공유한 비밀키로 암호화되서 전송된다.

2. TS에서는 HW_{CS}를 복호화해서 정상적인 CS인지 등록된 CS와 비교하여 확인한다.

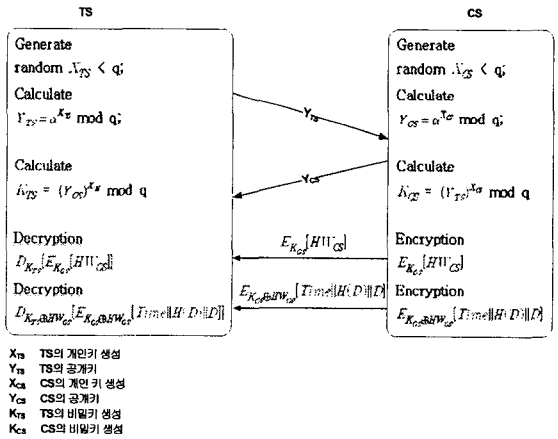
3. 등록되어 있는 CS의 HW_{CS}가 아니면 CS와의 세션을 종료한다.

TS는 HW_{CS}을 이용해서 정상적인 CS에 대해서만 디지털 증거를 전송받아 CS의 출처를 인증하고제 3자 개입 공격에 대해 방어할 수 있다.

2. 디지털 증거 보호 알고리즘

본 절에서는 DH 키 교환 알고리즘을 사용하여 TS와 CS의 비밀키를 안전하게 교환하고 CS의 HW_{CS}를 통해 정당한 CS인지 확인하고 디지털 증거의 출처에 대한 인증을 한다. Time은 전송된 디지털 증거의 현재성을 확인해준다. CS에서 계산된 H(D)값은 TS에서 전송받은 D를 해쉬값 계산한 후 비교하여 디지털 증거의 무결성을 보증한다.

그림 3은 TS와 CS 사이에 비밀키를 교환하고 이 키로 HW_{CS}를 암호화해서 TS로 전송하고 이 비밀키와 HW_{CS}를 XOR 연산하여 얻은 키로 디지털 증거를 암호화 하고 TS에서 복호화 하는 절차를 보여준다.



<그림 3> 디지털 증거 보호 프로토콜

먼저 DH 키 교환 알고리즘으로 TS는 비밀키 K_{TS}를 계산하고 CS는 비밀키 K_{CS}를 계산한다. 계산된 K_{TS}와 K_{CS}는 동일한 키로써 TS와 CS가 비밀키를 공유하게 된다.

다음은 공유된 비밀키를 사용하여 CS에서 생성된 디지털 증거를 TS에 보안 요구사항을 만족하도록 전송하는 절차이다.

1. CS는 HW_{CS}를 추출하여 K_{CS}로 암호화해서 TS로 전송한다.

2. TS는 전송받은 HW_{CS}를 K_{TS}로 복호화한다.

3. TS는 HW_{CS}로 사전에 등록된 CS인지 확인한다. 등록된 CS가 아니면 CS와의 세션을 종료하고 등록된 CS가 맞으면 계속 세션을 연결한다.

4. 디지털 증거가 현재 생성된 것임을 확인 할 수 있도록 Time을 만든다.

5. 디지털 증거가 위조·변조 되지 않았음을 증명하기 위해 H(D)를 계산한다.

6. CS는 K_{CS}와 HW_{CS}를 XOR연산을 하여 얻은 키로 Time, H(D)와 D를 암호화하여 TS로 전송한다.

7. TS는 전송받은 디지털 증거를 K_{TS}와 HW_{CS}로 XOR연산을 하여 얻은 키로 복호화한다.

제안된 알고리즘은 공격자가 TS에게 CS인 것처럼 속이고 비밀키를 공유하고 하드웨어 정보를 TS에 전송하면 TS는 등록된 HW_{CS}와 비교해서 정상적인 CS가 아님을 확인하고 세션을 종료하여 제 3자 개입 공격에 대해 방어한다. 또한 Time은 디지털 증거가 전송될 때 타임 스탬프값이다. 즉 Time은 디지털 증거의 현재성을 증명해주기 때문에 공격자가 CS에서 전송되는 증거를 가로채어 TS에 지속적으로 전송하여 TS에 부하를 줘서 더 이상 CS로부터 디지털 증거를 받지 못하도록 하는 재전송 공격에 대해 방어할 수 있다. 그리고 TS에서 D에대해 해쉬값을 계산하여 H(D)와 비교함을 통해 디지털 증거가 위조·변조되지 않았음을 증명할 수 있다.

IV. 결론

보안 침해사고시 수집된 디지털 증거를 법적 증거로써 제출하기 위해 디지털 증거에 대한 무결성 보증을 해야 한다.

본 논문에서 제안한 기법은 TS와 CS만이 알고 있는 비밀키와 CS의 하드웨어정보를 사용하여 디지털 증거와 디지털 증거에 대한 해쉬값, 타임스탬프를 암호화하므로 기존 디지털 증거 수집 시스템들로부터 생성된 증거들에 적용 가능하고 디지털 증거에 대한 요구사항인 기밀성, 인증, 무결성을 만족한다. 또한 공격자로부터 재전송 공격과 제 3자 개입 공격에 대해 방어할 수 있다.

향후 연구에서는 디지털 증거를 불법적 접근하여 삭제 하는 행위에 대한 접근 통제에 대해 연구하려 한다.

[참고문헌]

[1] Warren G. Kruse II, Jay G. Heiser, "Computer Forensics: Incident Response Essentials", Addson-Wesley, 2002.

[2] "Eoghan Casey, Handbook of Computer Crime Investigation", p.179~p.182.

[3] 김현상, 최재민, 이상진, 임종인, "무결성을 보장하는 디지털 증거 수집 절차", 한국정보보호학회 하계학술발표 논문집 Vol.15, No.1, 2005. 6.

[4] 박종성, 문종섭, 손태식, "분산된 로그 정보의 실시간 암호화 백업모델을 통한 법적 신빙성 획득에 관한 연구", 한국정보과학회지 Vol. 30 No. 2, 2003.

[5] 이영란, 이향숙, "인증서 기반이 아닌 효율적인 공개키 암호화 기법", 한국정보보호학회논문집 제14권 제5호, 2004. 10.

[6] William Stallings, "Cryptography and Network Security Principles and Practices Fourth Edition", p. 298~p.301.

[7] 김승주, 박성준, 이임영, 원동호, "암호 알고리즘과 암호 프로토콜", Telecommunications Review, p. 901-914, 2000. 10.