http://dx.doi.org/10.3745/KIPSTC.2012.19C.4.231

스마트기기 사용 증거 확보를 위한 로깅 연구

신 원†

요 약

일반적으로 로깅은 안전한 컴퓨터 시스템을 위한 중요한 요소인데, 이러한 로그를 분석함으로써 컴퓨터 내부에서 발생하는 다양한 문제를 식별하거나 침입을 발견할 수 있다. 따라서, 로그 내의 정보를 잘 활용한다면, 각종 사이버 침해에 대한 스마트 기기의 증거자료를 확보는 물론 사이버 수사에서 포렌식 관점의 효력을 가지도록 할 수도 있다. 본 논문은 스마트기기를 위한 새로운 로깅 방안을 제안한다. 제안 방안은 스마트기기용 로깅의 요구사항을 모두 만족하므로, 스마트기기의 디지털 증거를 수집하기 위한 안전한 로깅 방안을 개발하는데 도움이 될 것이다.

키워드 : 로깅, 스마트기기, 디지털 증거

A New Logging Scheme in Smart Devices for Digital Evidences

Shin, Weon†

ABSTRACT

Logging is an important part of any secure computer system. By analyzing logs in computer systems, you can identify early various problems and detect intrusions by attackers. Also logs can use to collect digital evidences in smart devices and to be forensics value for cybercrime investigations. In this paper, we propose a new logging scheme for smart devices and improve it to apply various environments. The proposed scheme satisfies the requirements of logging for smart devices. Thus it will help to develop a better logging in smart devices for digital evidences.

Keywords : Logging, Smart Device, Digital Evidence

1. 서 론

2011년 국내 스마트폰 사용자는 2,000만명을 이미 넘어섰으며, 휴대전화 사용자 중 40%이상이 스마트폰을 사용한다는 통계자료도 나와 있다[1]. 국내외 스마트폰 및 태블릿PC 사용자는 웹 서핑, 음악감상, 채팅 및 메신저, 스케줄링, 게임 및 지도 이용 목적으로 사용하고 있는 것으로 조사되어, 기존의 PC를 기반으로 하는 간단한 인터넷 검색, 일정관리, 채팅 등은 이미 스마트기기로 대체되는 추세에 있다. 그러나 스마트기기 사용자의 폭발적 증가와 새로운 서비스의 경쟁적 도입에 따라 이를 이용한 역기능 또한 함께 증가하고 있는 추세이다. 즉, 유명 어플리케이션 위장을 통한 정보 유출, 스마트기기 악성코드를 통한 정보 변조와 피해, 분산서비스거부(DDoS) 공격을 위한 좀비 역할 수행 등이 증가하는 것으로 보고되고 있다[2].

스마트기기에서 발생하는 다양한 침해를 분석하기 위해서는 무형의 정보를 디지털 증거물로 수집하여 법적 효력을 갖는 증거물로 제시하는 절차인 디지털 포렌식이 필수적이다. 즉, 사이버범죄 등에 대하여 컴퓨터 등 정보기기 장치에 내장된 디지털 자료를 근거로 그 장치를 매개체로 발생한 행위의 사실 관계를 규정·증명하는 기술 또는 일련의 절차가 바로 디지털 포렌식이다[3]. 디지털 포렌식은 보안 서비스의 한 분야로 검찰, 경찰 등의 국가 수사 기관에서 범죄 수사에 활용하고 있으며 일반 기업체 및 금융 회사 등의 민간 분야에서도 필요성이 증가하고 있는 추세이다. 이러한 디지털 포렌식을 수행하기 위해서는 컴퓨터 및 스마트기기에 저장된 디지털 증거 분석이 필수적인데, 기본이 되는 자료가 바로 로그이다. 즉, 로그를 어떻게 확보하느냐에 따라 디지털 범죄에 대한 수사의 향방이 결정되므로 로그의 수집은 디지털 포렌식에서도 중요한 작업이라 할 수 있다.

본 논문에서는 스마트기기를 위한 안전한 로깅 방안을 제안하고자 한다. 먼저 2장에서는 스마트기기에서 로그에 대한 내용과 기존 연구, 스마트기기용 로깅의 요구사항에 대하여 살펴본다. 3장에서는 안전한 로깅 방안을 제안하고 안전성 분석과 기존 방안과의 성능을 분석한 후, 마지막 4장에서 결론을 맺는다.

† 종신회원 : 동명대학교 정보보호학과 부교수
논문접수 : 2012년 3월 30일
수 정 일 : 1차 2012년 5월 18일
심사완료 : 2012년 7월 10일
* Corresponding Author : Shin, Weon(shinweon@tu.ac.kr)

2. 로깅 개요

2.1 스마트기기에서 로깅

컴퓨터에서 로깅(Logging)은 프로그램 개발이나 시스템 운영 시 발생하는 문제점을 추적하거나 운영상태를 모니터링하기 위한 텍스트 형식의 데이터를 남기는 것을 말한다[4]. 스마트기기에서 로그는 그림 1과 같이 스마트기기의 부팅 및 종료, 망접속 상태, GPS 및 카메라 등 주변기기 사용, 어플리케이션의 설치와 삭제 등이 포함될 수 있다. 따라서, 로깅은 스마트기기 동작 중 발생하는 각종 이벤트를 저장하는 기록 과정이므로, 기록된 로그는 관리 관점에서는 스마트기기의 동작을 기록하여 각종 문제점을 파악할 수 있는 재료를 제공할 뿐만 아니라 보안 관점에서는 스마트기기의 침해 여부를 판단하게 해주고 해당 침해의 증거 자료로써 법적인 효력을 가지기도 한다. 그러나 대부분의 스마트기기 로그는 평문으로 되어 있어 누구나 열람할 수 있을 뿐 아니라 특정 이벤트 로그의 삭제, 추가, 삽입 등의 조작에 매우 취약한 상태이다.

Log

Time		pid	tag	Message
01-04 23:00:07.484	D	526	PhoneWindow	DebugMonitor.class*c
01-04 23:00:07.504	I	80	HtcLockScreen	loadImage - system/c
01-04 23:00:07.504	I	80	HtcLockScreen	loadWallpaper = resu
01-04 23:00:07.584	D	80	WifiService	ACTION_SCREEN_OFF
01-04 23:00:07.624	I	115	wpa_supplicant	wpa_driver_tista_dri
01-04 23:00:07.634	I	115	wpa_supplicant	wpa_driver_tista_dri
01-04 23:00:07.634	D	80	WifiService	setting ACTION_DEVICI
01-04 23:00:07.744	D	61	AK8973	Compass CLOSE
01-04 23:00:07.774	I	115	wpa_supplicant	wpa_driver_tista_dri
01-04 23:00:07.784	I	115	wpa_supplicant	wpa_driver_tista_dri
01-04 23:00:12.844	D	181	dalvikvm	GC freed 498 objects
01-04 23:00:21.994	D	80	KeyguardUpdat	receive ACTION_BATTE
01-04 23:00:21.994	D	80	WifiService	ACTION_BATTERY_CHANG
01-04 23:00:21.994	D	80	StatusBar	performAddUpdateIcon
01-04 23:00:22.004	D	269	NetSharing_NS	onReceive : android
01-04 23:00:22.004	D	269	NetSharing_NS	USB = true netstate
01-04 23:00:22.024	D	334	UsbConnectedR	ACTION_BATTERY_CHANG
01-04 23:00:22.044	D	80	HtcLockScreen	onRefreshBatteryInfo
01-04 23:00:22.044	I	80	HtcLockScreen	updateStatusViewByFr
01-04 23:00:22.074	D	334	UsbConnectedR	unplugged = 2
01-04 23:00:22.074	D	334	UsbConnectedR	Current type is same

그림 1. 스마트폰 이벤트 로그 예제
Fig. 1. Example of event logs on smartphone

2.2 기존 연구

로깅에 대한 연구는 일반적으로 컴퓨터 시스템에서 기존 로깅을 수정하여 암호학 기반의 부가 정보를 추가함으로써 로그의 불법 수정을 검출하거나 수정 자체를 방지하는 쪽으로 초점을 맞추어져 진행되었다. 대표적으로 syslog-sign[5], Schneier-Kelsey 방안[6], Ma-Tsudik 방안[7] 등이 있다. 단, 본 논문에서 언급된 로깅 방안은 다음과 같은 가정에 기반한다.

<가 정>

① 로깅 방안에서 사용하는 해쉬 함수는 안전하므로, 공격자가 해쉬 함수 자체를 공격하는 것은 계산적으로 불가능하다.

② 로깅 방안에서 사용하는 MAC(Message Authentication Code)는 안전하므로, 공격자가 MAC 자체를 공격하는 것은 계산적으로 불가능하다. 단, 키를 아는 경우는 쉽게 공격할 수 있다.

③ 로깅 방안의 암호화에 사용하는 알고리즘은 안전하므로, 공격자가 암호화 알고리즘 자체를 공격하는 것은 계산적으로 불가능하다. 단, 키를 아는 경우는 쉽게 복호화할 수 있다.

④ 로깅 방안의 암호화 및 MAC에서 사용하는 비밀키는 안전하게 보관된다. 단, 사용자 부주의 등으로 인해 공격자에게 노출될 수 있다.

⑤ 공격자가 임의의 난수값을 정확히 추측하는 것은 계산적으로 불가능하다.

syslog-sign[5]은 개별 로그 데이터를 각각 해쉬시킨 다음 이들을 전자서명하고, 다시 순서대로 모아서 만든 해쉬값에 전자서명을 수행하여 전자서명 값을 첨부하는 방식으로 이루어진다. 이 방안은 전자서명을 통하여 로그에 대한 인증성을 보장하지만 특정 로그가 불법 수정된 경우, 로그가 수정되었다는 사실은 확인할 수 있으나 어떤 로그가 수정되었는지 찾기가 힘든 문제점을 가지고 있다. 특히, 스마트기기 환경에서 전자서명을 사용함으로써 계산량이 복잡하고, 성능이 저하되는 문제점도 있다.

Schneier-Kelsey 방안[6]은 로그 데이터를 특정 키와 함께 해쉬시킨 후 이를 이용하여 암호화하고, 이전 로그 데이터에 의한 해쉬값을 현재 로그에도 반영하는 형태를 취한다. 즉, 이들이 해쉬 체인을 구성함으로써 로그 삭제 및 삽입과 같은 수정 공격을 검출할 수 있다. 그러나, 이 방안은 로그 데이터에 대한 암호화를 제공할 뿐만 아니라 해쉬 체인에 비밀값 $A_i = H(A_{i-1})$을 이용하여 안전성을 보장하는데, 공격자에게 A_x이 노출되면 A_{x+1}를 계산할 수 있으므로 전방향 무결성을 보장하지 못한다.

Ma-Tsudik 방안[7]은 로그 데이터에 메시지 인증을 위한 MAC 체인을 구성하여 삭제 및 삽입과 같은 수정 공격을 검출할 수 있다. 또한, 검증자에 의한 부정 방지까지 포함한다. 그러나, MAC의 비밀키를 $A_i = H(A_{i-1})$로 계산하므로 공격자에게 A_x가 노출되면 A_{x+1}를 계산할 수 있으므로 역시 전방향 무결성을 보장하지 못한다.

2.3 스마트기기용 로깅의 요구사항

로그 데이터는 각종 이벤트를 저장함으로써 특정 이벤트 발생 당시에 일어난 일들에 대한 근거를 제공한다. 일반 컴퓨터 시스템의 로깅 방안은 로그 데이터 수정 방지, 작은 오버헤드, 전방향 무결성을 만족하면 되지만[8], 스마트기기에 적용가능한 로깅 방안은 그 특성에 따라 로그 데이터 수정 방지, 전방향 무결성, 구현의 용이성, 작은 저장공간의 조건을 만족하여야 한다. 요구사항의 구체적인 내용은 다음과 같다.

① 로그 데이터 수정 방지 : 스마트기기의 공격자 입장에서는 자신의 범행에 대한 증거가 되는 로그 데이터 수정에 대한 동기를 가진다. 반대로 스마트기기의 사용자 입장에서는 이를 방지하기 위하여 로그 데이터가 수정/삽입/삭제 공격에 안전하여야 한다.

② 전방향 무결성(Forward Integrity) : 전반향 무결성이란 이전의 모든 키가 노출되어 공격자가 그것을 알고 있다 하여도 과거의 데이터를 위조할 수 없는 성질[9]로, 이미 한번 작성된 로그 데이터는 설사 본인이라 할지라도 추후에 이를 수정할 수 없다. 각 로그 데이터는 전방향 무결성을 만족하여야 한다.

③ 구현의 용이성 : 스마트기기는 PC에 비교하여 저성능의 CPU와 메모리, 저용량 저장장치를 가지고 있으므로, 스마트기기에서 사용하는 로그 데이터는 경량으로 구현이 가능하고 계산량이 충분히 작아서 스마트기기에 부담을 주지 않도록 효율적으로 생성할 수 있어야 한다.

④ 작은 저장공간 : 로그 데이터의 무결성과 안전성을 보장하기 위해서는 로그 데이터 이외에 이를 위한 부가 정보가 필수적이다. 이 부가 정보들은 스마트기기의 저장 공간을 가능한 작게 차지하여 쉽게 저장될 수 있어야 한다.

3. 스마트기기에 적용가능한 로깅 방안의 제안

본 장에서는 스마트기기를 위한 로깅의 요구사항을 만족하고, 다양한 스마트기기에 적용할 수 있는 보다 효율적이며 안전한 방안을 제안한다. 본 논문에서 사용되는 표기법은 다음과 같다.

l_i : i번째 로그
$h(m)$: 메시지 m에 대한 해쉬값
$mac(K, m)$: K를 이용한 m에 대한 메시지 인증값
$e(K, m)$: K를 이용하여 메시지 m을 암호화
r_A : A가 생성한 임의의 난수값

3.1 로깅 방안의 제안

스마트기기를 위한 로깅의 요구사항을 만족하는 새로운 로깅 방안은 아래와 같다.

$$S=\{(l_1 \| v_1), (l_2 \| v_2), \cdots, (l_n \| v_n)\}$$
$$v_i = mac(K_i, (l_i \| v_{i-1})),\ v_0 = mac(K_0, \text{Device})$$
$$K_i = h(r_{\text{User}} \| v_{i-1}),\ K_0 = h(r_{\text{Device}})$$

제안 로깅 방안은 $S=\{(l_1 \| v_1), (l_2 \| v_2), \cdots, (l_n \| v_n)\}$로 구성되고, 각 로그는 $(l_i \| v_i)$, $1 \le i \le n$이다. 여기서, l_i는 로그 데이터이고, v_i는 각 로그의 안전성과 무결성을 보장하기 위해 삽입되는 부가 정보로써 다음과 같이 생성된다.

$$\begin{aligned} v_i &= mac(K_i, (l_i \| v_{i-1})) \\ &= mac(K_i, (l_i \| mac(K_{i-1}, (l_{i-1} \| v_{i-2})))) \\ &= mac(K_i, (l_i \| l_{i-1} \| \cdots \| mac(K_1, (l_1 \| v_0)) \cdots)) \end{aligned}$$

단, v_0는 스마트기기 이름을 특정한 키 K_0로 MAC한 값을 사용한다. 또한, MAC에서 사용하는 키 K_i는 다음과 같다.

$$K_i = h(r_{\text{User}} \| v_{i-1}),\ K_0 = h(r_{\text{Device}})$$

여기서, r_{Device}는 스마트기기가 생성한 임의의 난수값이다. K_i는 사용자 자신이 생성한 난수값 r_{User}과 함께 이전 v_{i-1}과 함께 자체적으로 생성한다.

특히, r_{Device}과 r_{User}은 스마트기기와 사용자가 생성한 임의의 난수값으로 각각 안전하게 보관한다. 결국 로그 데이터 l_i와 이를 해쉬한 후 하나의 키를 사용하여 메시지 인증한 v_i이 제안 방안의 로그가 되는데, 공격자에게 키 K_x가 노출된다 하더라도 r_{User}를 모른다면 키 K_{x+1} 계산이 불가능하므로 v_{x+1}을 만들 수 없다.

3.2 안전성 분석과 수정

새로운 제안 방안의 (l_i, v_i)에서 v_i은 $m_i = mac(K_i, (l_i \| v_{i-1}))$를 통해서만 계산할 수 있으므로, K_0가 비밀로 유지된다면 공격자는 위조 로그 (l_x, v_x)를 만들 수 없다. 또한 공격자가 로그 (l_i, v_i)를 임의로 삭제한 경우, 로그 (l_{i-1}, v_{i-1})와 로그 (l_{i+1}, v_{i+1})와의 관계에서 $m_{i+1} \neq mac(K_{i+1}, (l_{i+1} \| v_{i-1}))$가 성립하므로 사용자는 공격자가 삭제한 로그를 찾아낼 수 있게 된다. 또한, 공격자가 (l_i, v_i)를 알고 있고 심지어 K_i를 알아냈다고 하더라도, K_0가 비밀로 유지된다면 공격자는 로그 (l_{i+1}, v_{i+1})를 만들 수 없으므로 전방향 무결성이 보장된다.

제안 방안과 각 로깅 방안의 요구사항 만족 여부와 특징을 상대적으로 비교하면 표 1과 같다.

표 1. 각 로깅 방안의 특징 비교
Table 1. Comparison of logging schemes

분류	특징	로그 수정 방지	전방향 무결성	구현	저장 공간
syslog-sign	해쉬와 전자서명을 함께 사용	제공	비보장	구현 복잡	작지 않음
Schneier-Kelsey 방안	해쉬 체인과 암호화를 함께 사용	제공	비보장	구현 복잡	작음
Ma-Tsudik 방안	MAC 체인 사용	제공	비보장	구현 용이	작음
제안 방안	해쉬 기반 MAC 체인 사용	제공	보장	구현 용이	작음

또한, 제안 방안은 로그 데이터를 암호화하거나 성능을 향상시키기 위하여 다음과 같이 수정할 수도 있다.

첫째, 제안 방안은 로그 데이터 자체를 암호화하지 않는데, 안전 상의 이유로 스마트기기 내의 로그 데이터에 접근 제어가 필요하다면 다음과 같이 암호화를 적용할 수 있다.

$$(e(K_0, l_i), v_i),\ 1 \le i \le n$$

여기서, K_0는 스마트기기만이 알고 있으므로 로그 데이터를 복호화하여 열람할 수 있는 대상은 스마트기기 사용자뿐이다.

둘째, 제안 방안을 스마트폰과 같은 시스템에 사용하는 경우, 다음과 같이 성능을 향상시킬 수 있다. 저성능의 스마트기기에서 각 로그 데이터마다 해쉬와 MAC을 적용한다는 것이 오버헤드를 야기할 수 있으므로 이를 위하여 다음과 같이 수정하여 사용한다.

$$S=\left\{\begin{array}{l}(\{l_{1,1},l_{1,2},\cdots,l_{1,k}\},\ v_1),\\(\{l_{2,1},l_{2,2},\cdots,l_{2,k}\},\ v_2),\\\cdots,\\(\{l_{n,1},l_{n,2},\cdots,l_{n,k}\},\ v_n)\end{array}\right\}$$

즉, 로그 데이터를 1개 단위가 아니라 k개 단위로 묶은 후 함께 MAC을 적용하여 성능을 향상시키는 것이다. 여기서, k는 스마트기기에서 적합한 단위 개수 또는 단위 시간에 따라 선택한다.

3.3 제안 방안의 성능과 적용

제안 로깅 방안과 기존의 방안을 1.2GHz 듀얼코어 프로세서, Android 2.3 버전의 스마트기기에서 직접 구현하여 성능을 비교한 자료는 그림 2와 같다. 제안 방안과 Ma-Tsudik 방안은 거의 비슷한 성능을 가지고 있음을 확인할 수 있다. 또한, 제안 방안을 수정($k=20$)한 방안이 가장 성능이 높아 보이지만, 타 방안에 비해 안전성은 떨어질 수 있다.

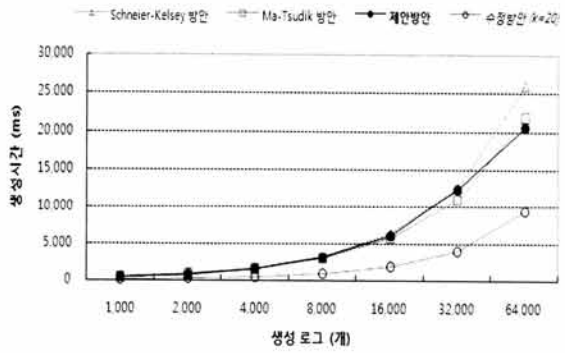

그림 2. 로깅 방안의 성능 비교
Fig. 2. Performance comparison of logging schemes

또한, 제안 방안은 작은 오버헤드를 가지고 있으며 로그 수정 방지는 물론 전방향 무결성의 성질도 함께 가진다. 해쉬 함수 기반의 MAC를 사용한다면, 각 로그 당 160비트(20바이트) 또는 256비트(32바이트)가 추가되어야 하는데, 로그 크기가 512바이트인 경우 각각 3.91%와 6.25%, 1,024바이트인 경우 각각 1.95%와 3.13%의 오버헤드를 가지므로 일반적인 스마트기기에서 충분히 수용가능한 크기라 할 수 있다.

4. 결 론

이제는 스마트기기를 통하여 손가락만으로도 원하는 정보를 얻고, SNS 등을 활용하여 개인화된 서비스를 사용할 수 있다. 그러나 스마트기기를 대상으로 하는 해킹, 악성코드 등의 새로운 위협으로 인한 피해도 해마다 증가하고 있는 추세이다. 이에 대해 스마트기기에 저장된 로그를 이용한다면, 각종 위협에 대한 증거자료를 확보할 수 있고 대응방안을 마련할 수도 있다. 본 논문에서는 스마트기기를 위한 로깅의 요구사항을 만족하는 새로운 로깅 방안을 제안하였다. 제안 방안은 기존 방안과 비교하여 안전성과 함께 전방향 무결성을 제공하고, 오버헤드가 작아서 스마트기기에도 효율적으로 구현할 수 있다. 따라서, 제안 방안은 스마트기기를 이용한 각종 위협에 대한 디지털 증거자료 확보에 직접적인 도움을 줄 수 있을 것이다.

참 고 문 헌

[1] "Korea Internet White Paper", Korea Internet & Security Agency, 2011.
[2] "Korea Internet Incident Trend Report, December 2011", Korea Internet & Security Agency KrCERT/CC, 2011.
[3] Digital forensics, http://en.wikipedia.org/wiki/Digital_forensics
[4] Computer data logging, http://en.wikipedia.org/wiki/Computer_data_logging
[5] J. Kelsey and J. Callas, "Signed syslog messages," IETF Internet Draft, 2005, http://www.ietf.org/internet-drafts/draft-ietf-syslog-sign-16.txt
[6] B. Schneier and J. Kelsey, "Security audit logs to support computer forensics," ACM TISSEC, Vol.2, No.2, pp.159-176, 1999.
[7] D. Ma and G. Tsudik, "A new approach to secure logging," ACM Trans. on Storage, Vol.5, No.1, pp.1-21, 2009.
[8] Weon Shin, "A Secure Logging for Collection of Digital Evidences", Journal of the Korea Institute of Marine Information & Communication Sciences, Vol.14, No.7, pp.1610-1616, 2010.
[9] M. Bellare and B. Yee, "Forward integrity for secure audit logs," University of California, San Diego, Dept. of Computer Science & Engineering, Tech. Rep., 1997.

신 원
e-mail : shinweon@tu.ac.kr
1996년 부경대학교 전자계산학과(이학사)
1998년 부경대학교 전자계산학과(이학석사)
2001년 부경대학교 전자계산학과(이학박사)
2002년~2005년 (주)안철수연구소 선임연구원
2005년~현 재 동명대학교 정보보호학과 전임강사, 조교수, 부교수
관심분야 : 소프트웨어 보안, 악성코드 확산, 디지털 포렌식