내부 사용자에 의한 불법 데이터 유출 방지를 위한 안전한 지식관리 시스템☆

Secure Knowledge Management for Prevent illegal data leakage by Internal users

서 대 희* 백 장 미** 이 민 경*** 윤 미 연**** 조 동 섭*****
Seo Dae Hee Baek Jang Mi Lee Min Kyung Yoon Mi Yeon Cho Dong Sub

요 약

인터넷의 급속한 발전은 사용자들의 정보 욕구를 증대시고 있으며, 이로 인해 정보의 홍수라 불리울 만큼 많은 정보들이 생성되고 사용되고 있다. 특히, 이윤을 추구하는 기업에서는 독자적인 기술력 확보를 위해 다양한 연구들을 수행하고 있다. 그러나 불법적인 외부 사용자 혹은 내부 사용자에 의한 정보의 불법적 유출로 인한 피해가 사회적 문제로 대두되고 있다. 따라서 본 논문에서는 내부 사용자에 의한 불법 데이터 유출 방지를 위한 안전한 지식 관리 시스템에 대해 제안하고자 한다. 제안된 방식은 내부 사용자들에 대한 명시적 인증을 수행하고 이를 기반해 데이터를 제공하고 2MAC을 이용해 악의적인 내부 사용자에 의한 불법적 데이터 유출을 방지하는 안전한 지식 관리 시스템이다.

ABSTRACT

Rapid development of Internet has increased users' desire for more information, and as a result, it created 'deluge of information', generating so much information. Especially, profit-pursuing corporations have done a lot of research to secure its own technological power. However, damages caused by illegal copy of information by illegal outside users or insiders are coming to the fore as social problem. Therefore, this paper is to propose secure knowledge management system to prevent illegal copy of data by insiders. The proposed scheme is a secure knowledge management system that carries out explicit authentication for internal users using 2MAC and provides data based on the authentication, thereby preventing illegal copy of data by insiders.

☞ KeyWords : Ubiquitous Computing, Knowledge Management System, Prevent illegal data leakage, Access Control, Authentication, 유비쿼터스 컴퓨팅, 지식관리시스템, 불법 데이터 유출 방지, 접근 제어, 인증

1. Introduction

유비쿼터스 컴퓨팅 환경을 기반으로 비즈니스 모델화가 활발하게 진행되고 있으며 이를 위한 다양한 연구들이 진행되고 있다. 특히, 다양한 정보들 가운데에서 산업화되어 활용되고 있는 시점에서 내부 사용자에 의한 불법적인 데이터 유출이 큰 문제로 대두되고 있다.

내부 사용자에 대한 문제점은 여러 가지 변수를 고려해야만 한다. 정당한 사용자임에도 불구하고 이를 이용해 불법적으로 데이터를 유출함으로써 발생하는 사회적, 시간적인 피해는 사회적 국

* 정 회 원 : 한국전자통신연구원 선임연구원
dhseo@etri.re.kr(교신저자)
** 정 회 원 : 순천향대학교 컴퓨터학부 강사
bjm1453@sch.ac.kr
*** 준 회 원 : 이화여자대학교 일반대학원 석사과정
mg0426@gmail.com
**** 정 회 원 : 한국인터넷진흥원 선임연구원 재직
myyoon@kisa.or.kr
***** 정 회 원 : 이화여자대학교 컴퓨터학과 교수
dscho@ewha.ac.kr
[2009/05/24 투고 - 2009/06/03 심사(2009/07/16 2차)
- 2009/08/26 심사완료]
☆ 본 연구는 2009년도 2단계 두뇌한국(BK) 21 사업에 의하여 지원 되었음

가적인 손실로 발생하고 있다. 대부분의 기존 연구는 외부 사용자에 의한 내부 데이터의 안전성 확보가 이루어지고 있는 반면 내부 공격자에 대한 연구는 미흡한 실정이다[1].

따라서 내부 공격자의 불법적인 데이터 유출을 방지하기 위해서는 내부 사용자들에 대한 안전성 확보를 위한 명시적인 인증과 더불어 정상적인 내부 사용자라 할지라도 불법적으로 데이터를 유출시키고자 할 경우 이를 방지하기 위한 연구가 시급히 요구된다[2].

이에 본 논문에서는 내부 공격자에 대한 안전성 확보를 위한 지식 관리 시스템을 제안하고자 하며, 2장에서는 지식 관리 시스템의 개요와 내부 공격자에 의한 데이터 유출의 문제점을 기술하고 제 3장에서는 보안 요구사항과 기존의 연구들에 대해서 분석하고자 한다. 4장에서는 3장에서 제시한 보안 요구사항을 만족하는 내부 공격자에 의한 불법적 데이터 유출 방지를 위한 지식 관리 시스템을 제안한 뒤 5장에서 이를 분석하고 6장에서 결론 및 향후 연구 방향을 제시하고자 한다.

2. 기술 개요

본 장에서는 지식관리 시스템과 내부 공격자에 불법적 데이터 유출의 문제점에 대해서 설명하고자 한다.

2.1 지식 관리 시스템의 개요

최근 인터넷과 유비쿼터스 컴퓨팅 환경의 구체화에 따라 기업들은 투자의 극대화를 위해 지식관리 시스템으로 정보를 통합하고 개인 용도에 맞게 분산함으로써 정보의 활용성을 높이기 위한 연구가 활발하게 진행되고 있다.

현재의 지식관리시스템은 데이터에 대한 저장, 검색 뿐만 아니라 원하는 데이터를 사용자와 연결 시켜주는 중계자적 역할까지 수행하고 있다. 따라서 기업 측면에서는 정보의 활용성 증대와 새로운 기술의 확충이 보다 발전적으로 가능하게 되었으며, 사용자 측면에서는 자동화된 형태의 지식관리가 가능하게 되었다. 특히, 보안적 측면에서는 기업의 중요 기술들이 인가되지 않은 제 3자에 의해 안전성을 유지할 수 있도록 네트워크 보안에 대해 많은 투자가 이루어지고 있다. 그러나 외부의 인가되지 않은 제 3자에 의한 취약성 뿐만 아니라 인가된 내부 사용자에 의한 불법적인 데이터 유출로 많은 문제점이 발생하고 있다[3][4].

이는 기존의 네트워크 보안적인 측면에서 연구와는 차별되며, 관리적인 측면에서 안전하고 효율적인 형태로의 전환이 절실히 요구되고 있다. 또한 내부 사용자에 의한 불법적인 데이터 유출시 이를 차단하고 사용자에 대한 별도의 추적 및 차단 서비스가 필수적으로 요구되고 있지만 현재의 연구들에서는 미흡한 실정이다. 따라서 지식관리 시스템의 능동적인 서비스와 더불어 내부 사용자들의 안전한 관리를 위한 별도의 보안 서비스 및 관리 체계가 반드시 요구된다.

2.2 내부 공격자에 의한 불법적 데이터 유출의 문제점

오늘날 정보통신 기술의 급격한 발전과 함께 '디지털화'가 가속화 되면서 비즈니스상의 거의 모든 문서가 전자화 되고 있다. 이렇게 생성된 각종 디지털 문서는 각종 정보 시스템 및 P2P 파일 전송 시스템 등 다양한 채널을 통해 다방면으로 유통되고 있으며 이는 최근 사회적으로 이슈가 되고 있는 내부 정보 유출이라는 심각한 부작용을 일으키게 되었다[5].

특히, 전자문서의 안전한 유통 환경을 위한 기존 정보보호 기술은 외부의 비인가자로부터 내부 시스템의 정보를 보호하는 것에 초첨을 두고 있으며 내부 인가자에 의한 비인가된 불법 유출에 대해서는 문제점을 인식하는 반면 이를 위한 별도의 연구에 대해서는 미흡한 실정이다[6].

내부 정보 유출을 방지하기 위해서는 내부 네트워크의 데이터를 위한 정보보호 관리 방식을 제공해야 하며, 정보기기별 신속한 대응을 통한

불법적인 외부 유출을 방지해야 한다. 따라서 정보 체계나 조직의 전체적인 정보 유통의 구조적 관점에서 정보보호 모델이 개발되고 분석이 가능한 체계적인 대책이 요구된다[2].

3. 기존 방식 분석

본 장에서는 내부 사용자의 불법 데이터 유출을 방지하기 위한 기존 연구들을 분석하고자 한다.

3.1 DLP(Data Loss Prevention) 방식

본 방식은 내부 인터넷 환경에서 데이터를 형식이나 내용 등을 기준으로 중요 정보에 대한 외부 불법 유출을 방지하는 방식이다. 제안된 방식은 에이전트 기반의 멀티캐스트 방식으로 사용자를 그룹화하고 이를 통해 효율적인 관리가 가능한 계층적인 구조를 갖는다. 특히, 사용자의 이동성을 고려하여 핸드오프가 가능하게 하였으며, 멀티캐스트 사용자의 안전한 인증을 통해 전체적인 네트워크의 안전성과 효율성을 갖도록 하였다[7]. 그러나 본 방식의 경우 다음과 같은 취약점을 내포하고 있다.

- 선택적인 권한 : 제안 방식은 계층적 구조를 통해 내부 사용자의 불법적인 정보 유출을 방지하고자 하였다. 그러나 멀티캐스트 사용자를 위한 데이터의 권한 설정이 이루어지지 않고 각각의 에이전트를 통해 상호 운용성만을 제공하였다. 따라서 내부 유출 방지가 요구되는 데이터에 대한 별도의 보안 서비스를 제공하지 못하고 있다.

- 통신의 안전성(ACIN) : 본 방식은 사용자에 대한 인증과 인가에 대한 서비스를 제공한다. 특히, 멀티캐스트 사용자의 인증을 위하여 사용되는 에이전트에 대한 별도의 보안 서비스를 제공하지 못하고 있다. 따라서 통신의 안전성 뿐만 아니라 안전한 관리를 위해 사용되는 개체에 대해서 별도의 보안 서비스가 요구된다.

- 안전한 관리 방식 : 제안된 방식은 사용자의 인증을 기반으로 데이터를 접근할 수 있는 사용자들을 위한 멀티캐스트 방식을 제시하였다. 그러나 이는 유동적으로 변화할 수 있는 사용자들에 대해서 적용성의 한계성을 갖고 있으며, 이로 인해 사용자들의 현실적인 데이터 접근을 어렵게 한다. 따라서 데이터 외부 유출 요소 및 사용자들의 관리를 위한 별도의 관리 체계가 요구된다.

- 내부 공격자에 대한 안전성 확보 : 제안 방식은 데이터가 외부 유출하고자 할 경우 이를 차단할 수 있는 서비스를 제공하지 못한다.

3.2 모니터링을 통한 통합 유출 경로 보안 방식

본 방식은 통합 보안 관리 시스템을 기반으로 데이터의 모니터링을 통해 내부 데이터에 대한 불법적인 외부 유출을 방지하기 위한 방식이다. 제안된 방식은 ESM(Enterprise Security Management)를 기반으로 기업 환경에서 문서 시스템의 보안, 사용자 관리 등의 방식을 제공한다[3][8]. 그러나 본 방식의 경우 개인 PC를 중심으로 접근하여 전체적인 네트워크 관리 측면에서 원천적인 정보 유출 방안에 이르지 못하고 있으며 효율성 측면과 정책적인 측면에서 적용의 한계성이 지적되고 있다. 따라서 이러한 문제점들을 보안적인 측면에서 분석할 경우 다음과 같다.

- 통신의 안전성(ACIN) : 제안 방식은 사용자의 개인 디바이스를 중심으로 데이터에 대한 안전성을 확보하고 이를 통해 내부 데이터의 외부 유출을 방지하고자 하였다. 그러나 사용자의 인증이 아닌 응용 프로그램의 제어를 통해 데이터 유출을 방지한다. 따라서 사용자의 개인 정보에 기반한 인증 뿐만 아니라 통신의

안전성 확보를 위한 추가적인 서비스를 제공해야 한다.

- 안전한 관리 방식 : 본 방식은 구조적인 신뢰성을 확보하기 위하여 통합 보안 관리 시스템을 기반으로 사용자 및 데이터의 외부 유출을 방지하고자 하였다. 그러나 내부적으로 많은 데이터가 사용되는 환경의 경우 모든 데이터에 대한 모니터링이 현실적으로 불가능하고 응용 프로그램의 모니터링을 통해 내부 데이터 유출의 취약성을 내포하고 있다. 따라서 신뢰적인 개체를 통해 안전한 사용자 및 데이터 관리 구조가 요구된다.

- 내부 공격자에 대한 안전성 확보 : 본 방식은 응용 프로그램의 모니터링을 통해 내부 데이터의 유출을 방지하고자 하였으나, 불법적인 데이터의 유출이 발생하거나 유출이 시도될 경우 이를 차단하거나 추적할 수 없어 이를 위한 별도의 보안 서비스가 요구된다.

- 사용자들의 안전한 정보 공유 : 제안 방식은 안전한 형태의 정보 공유를 위해서 모든 응용 프로그램들에 대한 모니터링을 실시한다. 따라서 사용자의 프라이버시 침해에 대한 문제점이 발생되고 있다. 이를 방지하기 위해서는 내부 사용자들에 대한 데이터가 공유되고 사용될 때 데이터에 대한 권한을 설정하고 사용자들의 데이터에 대한 사용 및 처리가 명시적으로 관리되고 있음을 확인할 수 있는 서비스가 요구된다.

3.3 보안 요구사항 분석

다음은 내부 사용자에 의한 불법 데이터 유출 방지를 위한 안전한 지식관리 시스템을 위한 보안 요구사항을 분석하고자 한다.

- 선택적인 권한 : 개인 정보보호를 위해서 모든 정보를 보호해야 할 것인지에 대한 정책적인 고려가 있어야 하며, 이를 위해서 각각의 데이터에 대한 권한 설정을 통해 데이터의 외부 유출을 방지할 수 있어야 한다.

- 통신의 안전성(ACIN) : 모든 데이터와 사용자에 대한 통신의 안전성을 보장해야 한다. 이는 중요 데이터에 대한 외부 유출 방지를 위해서 사용자 뿐만 아니라 데이터의 전송시 인가되지 않은 제 3의 공격자로부터의 안전성을 유지할 수 있어야 한다.

- 안전한 관리 방식 : 안전한 내부 데이터 유출 방지를 제공하기 위해서는 구조적으로 신뢰할 수 있는 방식이 요구된다. 즉, 데이터에 대한 권한 설정 뿐만 아니라 데이터의 외부 유출 요소 및 사용자의 관리에 대한 안전한 구조가 제시되어야 한다.

- 내부 공격자에 대한 안전성 확보 : 데이터가 외부 유출이 되고자 할 때 이를 차단하고 불법적으로 내부 데이터의 유출을 시도한 내부 사용자에 대한 추적과 이를 차단할 수 있는 방식이 요구된다.

- 사용자들의 안전한 정보 공유 : 내부 사용자들에 의해 데이터가 공유될 경우 해당 내용들이 공개되고 신뢰된 공간에서 이를 확인할 수 있어야하며, 이를 통해 데이터 사용, 처리가 명시적으로 처리되고 있음을 확인할 수 있는 방식이 요구된다.

4. 내부 사용자에 의한 불법 데이터 유출 방지를 위한 지식관리시스템

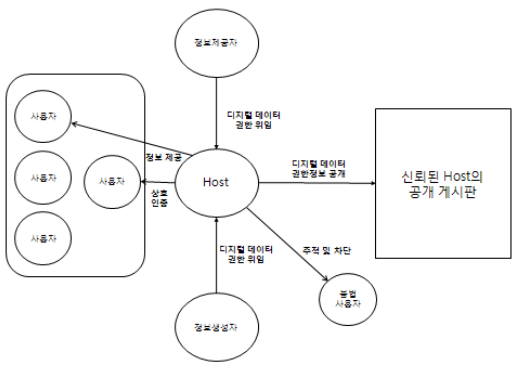
제안 방식은 내부 사용자에 의한 불법 데이터 유출 방지를 위한 안전한 지식관리 시스템을 제안하고 이를 기반으로 합법적으로 파일을 공유하기 위한 시스템을 제안하고자한다.

4.1 제안 방식 시나리오

기업 환경에서 각각의 사용자들은 다양한 디지털 데이터를 상호 공유하고 전송받는다. 이러한 정보의 상호 공유는 기업 내부의 기밀 정보를 불법적으로 외부로 유출시키는 사례가 빈번히 발생하고 있다. 따라서 본 논문에서는 정적인 신뢰기관을 기반으로 각 사용자들이 디지털 데이터에 대한 외부 유출 방지를 위해 디지털 데이터를 생성자 혹은 제공자로부터 권한 위임을 받고 이를 기반으로 디지털 데이터의 사용에 따른 명시적인 상호 인증과 세션키 설정을 통해 안전한 사용자 인증과 더불어 불법 내부 사용자에 의한 정보 유출이 발생할 경우 이를 추적하고 차단할 수 있는 방식을 제안하고자 한다. (그림 1 참조)

1) 가정 사항

내부 사용자에 의한 불법 데이터 유출 방지를 위한 안전한 지식관리 관리 방식을 위한 가정사항은 다음과 같다.



(그림 1) 내부 사용자에 의한 불법 데이터 유출 방지를 위한 안전한 지식관리 시스템 구조

① 제안 방식의 보안 구조는 신뢰할 수 있는 정적인 신뢰 개체인 Host와 공개 게시판을 기반으로 이루어진다.

② 각 사용자는 유선 통신이 가능한 디바이스(PC)에서 정보를 제공 받는다.

③ 디지털 데이터의 외부 통신은 반드시 Host를 통해서만 이루어진다.

2) 세부 프로토콜

내부 사용자에 의한 불법 데이터 유출 방지를 위한 안전한 관리 방식을 위한 세부 프로토콜은 다음과 같은 단계로 이루어진다.

(1) 내부 정보 데이터 생성자의 인증과 권한 위임

내부 정보 데이터 생성자가 자신이 생성한 디지털 데이터의 권한 위임을 위하여 Host와 상호 인증 과정을 수행하고 디지털 데이터에 대한 권한을 위임한다.

(2) 디지털 데이터의 사용을 위한 사용자 등록 및 상호 인증

정보 제공자가 제공한 디지털 데이터를 Host에서 제공할 경우 사용자 등록 및 상호 인증 과정이다.

(3) 디지털 데이터 배포 및 불법적인 데이터 유출에 따른 사용자 정보 제공

디지털 데이터를 요구하는 사용자에게 해당 데이터에 대한 권한을 규정하고 이에 대한 정보를 공개 게시판에 공개한 뒤 불법적인 데이터 유출이 발생할 경우 사용자 및 사용자의 단말기에 대한 추적이 이루어지며 다음과 같은 세부 단계로 구분된다.

① 세부단계 3-1 : 디지털 데이터 배포

디지털 데이터를 요구하는 사용자에게 해당 데이터를 제공하는 과정이다.

② 세부단계 3-2 : 불법적인 권한 이용에 따른 사용자 제한

불법적으로 권한을 이용하는 사용자에 대하여 Host에서 이를 제한하는 단계

4.2 시스템 계수

다음은 내부 사용자에 의한 불법 데이터 유출 방지를 위한 안전한 지식관리 시스템에 대한 시스템 계수를 기술하고자 한다.

* : 사용자 ($u \in U$), 호스트 (H), u_a (내부 공격자), cc (정보 생성자)
u_a : 정상적인 내부 사용자이지만 불법적인 데이터 유출을 위해 권한 설정을 변경하는 내부 공격자
e_* : 통신 이벤트 메시지
r_* : 의사난수 ($\in_R Z_p$)
$E()$: 안전한 암호 알고리즘
$H()$: 안전한 일방향성 해쉬 알고리즘
t_* : 타임 스탬프
$Content\ type$: 정보 생성자 혹은 제공자의 디지털 데이터 형태
$authorization$: 정보 생성자 혹은 제공자가 요구하는 디지털 데이터의 권한
Sig : 공개키 서명 알고리즘
ID_* : 개체의 Identity
$Authorization-information$: 디지털 데이터 권한 정보
$Digital-Contents_{list}$: Host에서 제공되는 디지털 데이터 목록
$seed$: 사용자와 Host의 상호 인증을 위한 초기값
u_{info} : 사용자의 개인정보
s: 함수 $f[]$로부터 $f_s[0,1] \rightarrow [0,1]$,

s는 $f_s(x) = \dfrac{1-2^{sx}}{1-2^s}$

$seed$: Host가 사용자와 안전한 통신을 위해 설정한 초기값
SR : 서비스 요청 메시지
p_*, q_* : 각 개체의 공개키, 개인키 쌍
t_{seed} : 사용자가 Host와 상호 인증 및 세션키 설정을 위한 시간 초기값

4.3 프로토콜

내부 사용자에 의한 불법 데이터 유출 방지를 위한 안전한 지식관리 시스템에 대한 프로토콜은 다음과 같은 과정으로 수행된다.

[단계 1] 내부 정보 데이터 생성자의 인증과 권한 위임

단계 1에서는 내부 정보 데이터 생성자가 자신이 생성한 디지털 데이터의 권한 위임을 위하여 Host와 상호 인증 과정을 수행하고 디지털 데이터에 대한 권한을 위임하는 단계이다.

① 정보 생성자는 자신이 생성한 디지털 데이터의 권한위임을 위하여 Host에 다음의 이벤트 정보 e_{cc}를 전송한다.

$Event$:
$e_{cc} = < ID, Content\ type, authorization, t >$

② Host는 정보 생성자의 이벤트 정보 e_{cc}를 수신하고 다음을 계산하여 정보 생성자의 디지털 데이터의 권한 정보 요청을 위한 C_H, V_H, SR, t_H를 전송한다.

$r_H \in_R Z_p$

$AID_H = (ID_H)^{r_H^{-1}}$

$C_H = H(AID_H, SR, t_H)^{r_H^{-1}}$

$V_H = E_{p_{cc}}(r_H || t_H)$

③ 정보 생성자는 C_H, V_H를 수신한 뒤 V_H를 개인키로 복호화한 뒤 r_H를 획득하고 이를 기반으로 AID_H를 계산한 뒤 C_H의 무결성을 검증한다.

[verify]

$\rightarrow AID_H' = (ID_H)^{r_H^{-1}\prime} \equiv AID_H$

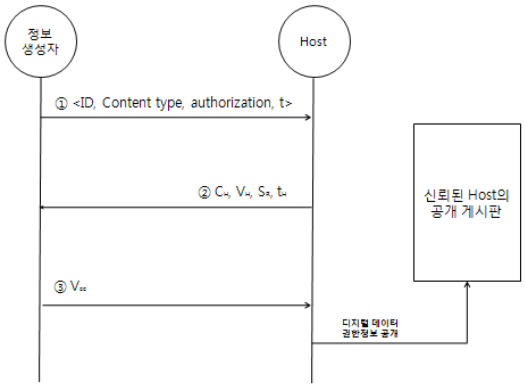
$\rightarrow C_H' = H(AID_H', SR, t_H)^{r_H^{-1}\prime} \equiv C_H$

검증이 올바른 경우 정보 생성자는 다음을 계산하여 Host에서 요구하는 디지털 데이터에 대한 권한을 설정하고 이를 전송한다.

$$V_{cc} = E_{p_H}(Digital-Contents_{list}, Authorization-information_{cc}, ID_{cc}, t_{cc})$$

④ Host는 정보 생성자로부터 전송된 V_{cc}를 개인키로 복호화한 뒤 정보 생성자가 요구하는 디지털 데이터에 대한 권한 정보를 획득하고 이를 기반으로 다음을 계산 한 뒤 그 결과를 공개 게시판에 게시한다.

$$S_H = Sig(Authorization-information_{cc}, ID_{cc})$$



(그림 2) 내부 정보 데이터 생성자의 인증과 권한 위임

[단계 2] 디지털 데이터의 사용을 위한 사용자 등록 및 상호 인증

다음은 정보 제공자가 제공한 디지털 데이터를 Host에서 제공할 경우 사용자 등록 및 상호 인증 과정을 수행한다.

① 사용자는 디지털 데이터를 제공 받기 위하여 Host에 사용자 등록 과정을 요구한다.

② Host는 사용자 등록 요청을 수신하고, 사용자가 디지털 데이터 요청을 보낸 시간을 $seed$ 로 하여 다음을 계산하여 사용자에 V_H, h_H전송한다.

$r_{H_1} \in_R Z_p$

$h_H = H(r_{H_1}, seed)$

$V_H = E_{p_u}(seed, r_{H_1}, t_{H_1})$

③ 사용자는 전송된 V_H, h_H를 수신한 뒤 V_H를 개인키로 복호화한 뒤 $seed$와 r_{H_1}을 획득하고 $r_{H_1} = r_{u_1}$를 만족하는 r_{u_1}을 선택하고 $r_{u_1}, seed$와 t_{u_1}을 계산한 후 V_u를 Host 서버에 전송한다.

$t_{u_1} = r_{u_1} * t_{H_1} - t_{seed}$

$V_{u_1} = E_{p_H}(r_{u_1}, u_{info}, t_{u_1})$

④ Host 서버는 V_{u_1}를 복호화하여 r_{u_1}, u_{info}, t_{u_1}을 획득하고 사용자의 u_{info}와 $seed$를 1:1 매칭하여 DB에 안전하게 저장하고 이를 등록한다.

이상의 과정을 수행한 후 Host와 사용자는 비밀 통신을 위한 세션키 sk_{H-u}를 다음과 같이 생성한다.

$$sk_{H-u_1} = H(seed, t_{u_1})$$

[단계 3] 디지털 데이터 배포 및 불법적인 데이터 유출에 따른 사용자 정보 제공

디지털 데이터를 요구하는 사용자에게 해당 데이터에 대한 권한을 규정하고 이에 대한 정보를 공개 게시판에 공개한 뒤 불법적인 데이터 유출이 발생할 경우 사용자 및 사용자의 단말기에 대

한 추적이 이루어진다.

<세부단계 3-1 : 디지털 데이터 제공>

다음은 디지털 데이터를 요구하는 사용자에게 해당 데이터를 제공하는 과정을 수행한다.

① 사용자 u_1은 디지털 데이터를 해당 Host에서 검색하고 2MAC을 생성한 뒤 이벤트 메시지 e_{u_1}을 생성하고 제공받고자 하는 데이터에 대한 요청 정보를 Host에 전송한다.

$$h_{u_1} = H(ID_{u_1} \| IP_{u_1})$$

$$e_{u_1} = < ID_{u_1}, Contents - Request, \; Contents \; type, h_{u_1} >$$

② 사용자 u_1으로부터 데이터 제공을 요청 받은 Host는 해당 데이터에 대한 정보 생성자의 권한 정보(S_H)를 공개 게시판에서 검색한 뒤 이를 기반으로 디지털 데이터에 대한 배포 권한을 설정하고 다음을 계산하여 사용자 u_1에 S_{H_1}, V_{H_1}을 전송한다.

$$e_H = < ID_{H_1}, Authorization - information, \; Contents - list >$$

$$S_{H_1} = Sig(e_H \| Contents - list)$$

$$V_{H_1} = E_{sk_{H-u_1}}(e_H, t_{seed})$$

③ 사용자 u_1은 S_{H_1}, V_{H_1}을 수신한 후 Host의 공개키로 서명값 S_{H_1}를 확인하여 e_H와 $Contents - list$를 획득하고 [단계 2]에서 설립한 세션키 sk_{H-u_1}으로 V_{H_1}을 복호화한 뒤 e_H와 t_{seed}를 추출하여 이를 검증한다. 검증이 올바른 경우 사용자는 Host에 h_{u_1}, V_{u_1}을 계산하여 전송한다.

$$f_{u_1}(x) = \frac{1 - 2^{s * seed}}{1 - 2^s}$$

$$h_{u_1} = H(Media\,Access\,Control_{u_1} \| t_{seed})$$

$$V_{u_1} = E_{sk_{H-u_1}}(f_H(x), t_{seed})$$

④ Host는 [단계 2]에서 공유한 세션키 sk_{H-u_1}과 $seed$값에 기반해 V_{u_1}을 복호화한 뒤 $f_{u_1}(x)$, t_{seed}를 획득하고 초기 공유한 $seed$를 이용해 데이터 배포에 따른 사용자 등록값인 $f_{u_1}(x)$를 사용자 정보와 1:1 매칭하여 안전하게 저장하고 해당 사용자의 2MAC 값을 생성하여 Host의 공개키로 암호화한 뒤 공개 게시판에 사용자의 ID, 제공되는 디지털 데이터와 1:1 매칭하여 공고한 뒤 사용자 u_1이 요구하는 디지털 데이터를 제공한다.

$$2MAC_{u_1} = H(Media\,Access\,Control \| t_{seed}) \oplus H(ID_{u_1} \| IP_{u_1} \| seed)$$

$$V_H = E_{p_H}(2MAC \| Media\,Access\,Control_{u_1} \| ID_{u_1} \| IP_{u_1} \| t_{seed})$$

$$ID_{u_1} \| Digital\,Data \| E_{sk_{H-u_1}}(f_{u_1}(x) \| Authorization - information_{\alpha})$$

Definition 1 : 2MAC : 2MAC은 사용자 NIC(Network Interface Card)의 하드웨어 고유 주소값인 Media Access Control과 해쉬 함수를 이용한 Message Authentication Code를 이용한 값이다.

2MAC은

$$2MAC \rightarrow H(Media\,Access\,Control) \oplus H(Message\,Authentication\,Code)$$

으로 정의한다. $H()$는 해쉬 함수(SHA-1), Media Access Control은 48bit, Message Authentication Code는 $H()$를 이용해 사용자 인증을 위한 해쉬 값이다.

Definition 2 : 함수 $f[]$로부터 $f_s[0,1] \rightarrow [0,1]$로 정의하며, s는 $f_s(x) = \frac{1 - 2^{sx}}{1 - 2^s}$로 정의한다.

(단 $s \neq 0$, $s \to 0; f_0(x) = x$) 따라서 s의 모든 값에 대하여 f_s는 연속적인 증가값이 된다[9].

<세부단계 3-2 : 불법적인 권한 이용에 따른 사용자 제한>

본 세부 단계에서는 불법적으로 권한을 이용하는 사용자에 대하여 Host에서 이를 제한하는 단계이다.

① 내부 공격자 u_a는 <세부 단계 3-1>에서 제공받은 디지털 데이터에 대한 불법적인 권한 변경하고 이를 기반으로 외부로 디지털 데이터를 유출하고자 할 경우 다음의 과정을 수행하고 Host에 외부 통신을 위한 연결 요청 메시지와 디지털 데이터 정보를 전송한다.

$ID_{u_a} \| Digital\ Data \| E_{sk_{H-a}}$
$(f_{u_a}(x) \| Authorization - information_{cc})'$
$Connection - Request$

② 연결 요청을 받은 Host는 ID_a를 기반으로 sk_{H-a}를 추출하여 암호화된 값을 복호화한 뒤 제공된 $Digital\ Data$의 권한 정보 $Authorization - information_{cc}$를 공개 게시판에서 이를 확인한다. 만약 $Digital\ Data$의 $Authorization - information_{cc}$의 정보가 외부 유출이 금지된 경우 공개 게시판에 공개된 V_H를 Host의 개인키로 복호화하여 $2MAC \| Media\ Access\ Control_{u_a} \| ID_{u_a} \| IP_{u_a} \| t_{seed}$를 획득하고, t_{seed}와 $seed$를 초기한 뒤 $2MAC$정보를 공격자 차단 리스트에 등록한다.

이상의 과정을 통해 불법적인 내부 사용자의 데이터 유출을 방지하기 위한 안전한 지식 관리 시스템을 제공한다.

5. 제안 방식 분석

본 장에서는 제안방식을 3장에서 제시한 보안 요구사항을 기준으로 기존 방식과 비교 분석하고자 한다.

- 선택적인 권한 : 제안 방식은 DLP 방식에서 사용하는 에이전트를 이용하지 않고 제 3의 신뢰 기관을 중심으로 데이터의 권한을 설정하고 이를 기반으로 전체적인 사용자의 관리를 위해 각각의 사용자별로 세션키 sk_{H-u}를 설정하였다. 또한 이벤트 메시지 e_u에 저장된 사용자의 데이터 권한 정보 메시지, 디지털 데이터의 정보, 사용자의 ID를 기반으로 $(e_H = < ID_{H_1}, Authorization - information, Contents - list >)$ 각각의 디지털 데이터에 대한 권한 정보를 설정하여 선택적인 권한 관리가 가능하도록 하였다.

- 통신의 안전성(ACIN) : 제안 방식의 모든 통신은 안전한 암호화 알고리즘과 일방향성 해쉬 알고리즘을 기반으로 각각의 사용자와 Host간의 상호 인증을 통해 세션키 sk_{H-u}를 설정하고 이를 이용해 안전한 암호 통신이 가능하도록 하였다. 특히, 각각의 사용자들의 정보를 이용해 내부 불법 사용자에 대한 추적이 가능하도록 2MAC 정보를 Host에 제공함으로써 내부 데이터 유출이 발생할 경우 해당 사용자에 대한 개인 정보($H(ID_{u_1} \| IP_{u_1} \| seed)$) 뿐만 아니라 사용 디바이스에 대한 정보 ($H(Media\ Access\ Control \| t_{seed})$)를 기반으로 이를 방지하고 차단할 수 있다.

- 안전한 관리 방식 : 제안 방식은 디지털 데이터에 대한 권한을 별도로 설정하고 이를 제공자 혹은 생성자와의 안전한 통신을 통해 공개 게시판에 공개키 서명(Sig)을 통해 이를 게시

한다. 따라서 공개키 서명을 통해 모든 사용자들이 제공자 혹은 생성자가 제공한 디지털 데이터에 대한 권한 정보를 열람할 수 있을 뿐만 아니라 자신이 제공 받고 있는 디지털 데이터에 대한 권한 정보를 검증할 수 있는 데이터로 활용할 수 있다. 또한 모니터링 방식과는 달리 사용되는 데이터에 대한 권한 설정을 통해 내부 데이터의 불법적인 유출을 방지하므로 복잡한 형태의 통합 보안 관리 시스템 방식을 이용하지 않더라도 안전하게 내부 데이터에 대한 안전성을 유지할 수 있다.

- 내부 공격자에 대한 안전성 확보 : 내부 데이터가 불법적인 유출이 시도될 경우 Host에서는 $ID_{u_a} \| Digital\ Data \| E_{sk_{H-a}}(f_{u_a}(x) \| Authorization - information_{cc})$ 를 공개 게시판에 있는 $Authorization - information_{cc}$과 비교하여 정상적인 외부 통신이 아닌 불법 유출로 판단될 경우 해당 사용자의 $2MAC$ 정보를 기반으로 사용자를 차단함으로써 불법적인 데이터 유출이 방지되도록 하였다.

- 사용자들의 안전한 정보 공유 : 제안 방식에서는 내부 사용자들이 신뢰할 수 있는 제 3의 신뢰 기관에서 서명한 디지털 데이터에 대한 정보를 공개 게시판에 게시함으로써 모든 사용자들이 해당 디지털 데이터에 대한 정보 획득이 가능하도록 하였으며, 이를 기반으로 정보 제공자는 현재 자신의 데이터가 어떠한 형태로 사용되고 있는지 확인할 수 있을 뿐만 아니라 데이터를 사용하는 사용자들에 대한 명시적인 상호 인증을 통해 생성된 세션키를 통해 안전한 정보 공유가 가능하도록 하였다.

이상의 내용을 기존 방식과 비교하여 볼 때 표 1과 같이 정리할 수 있다.

(표 1) 제안 방식 분석

방식 / 보안 요구사항	DLP 방식	모니터링 방식	제안 방식
선택적 권한	에이전트를 위한 상호 운용성만을 고려(취약)	통합 관리 시스템으로 권한 방식 제공	신뢰 기관을 통한 데이터의 권한 설정
통신의 안전성	사용자 인증 방식 (취약)	디바이스 인증 방식 (취약)	세션키와 상호 인증을 통한 안전성 확보
안전한 관리 방식	적용의 한계성(취약)	모니터링의 비현실성 (취약)	공개키 서명과 데이터에 대한 권한 설정을 통한 안전한 관리 방식 제공
내부 공격자에 대한 안전성 확보	제공하지 않음	제공하지 않음	2MAC 정보에 기반한 불법적인 사용자 차단
사용자들의 안전한 정보 공유	멀티캐스트 방식	중앙 집중형 방식	중앙 집중형 방식

6. 결 론

최근 컨버전스화된 환경으로의 변화는 모든 데이터의 사용에 대한 공유 및 자동화가 가능하게 되었다. 특히, 기업에서는 가치 창출을 위해서 독자적인 기술력 확보와 더불어 이미 확보된 기술력을 보호하기 위한 다양한 노력들이 이루어지고 있다. 따라서 외부적인 비인가된 공격자에 대한 안전성 확보를 위해서는 많은 투자와 연구가 이루어지고 있는 반면 내부 사용자에 대한 불법적인 정보 유출에 대한 연구는 미흡한 실정이며, 이로 인해 발생되는 취약성들은 사회적 문제로 대두되고 있어 이를 위한 연구는 매우 절실한 실정이다.

이에 본 논문에서는 기존의 연구들에서 제한적으로 정보 유출을 방지하는 방안의 문제점을 인식하고 내부 사용자에 대한 불법적인 정보 유출

을 방지하는 관점에서 제 3의 신뢰기관을 이용해 안전한 형태의 네트워크 관리 방식을 제안하였다. 제안된 방식은 각각의 데이터에 대한 권한 관리 뿐만 아니라 사용자에 대한 명시적 인증을 통해 사용자와 데이터의 안전한 관리가 가능하도록 하였고, 불법적인 데이터의 유출에 따른 불법 사용자와 사용 디바이스에 대한 추적이 가능하도록 하였다.

그러나 제안 방식에서는 기업내 다양한 컴퓨팅 환경에 적용의 한계성을 갖고 있으며, 사용자 및 관리자를 위한 보안 정책에 대해서는 고려하지 않았다. 또한 다양한 보안 툴과의 복합 모델이 아닌 단일한 형태의 관리 형태를 제공함으로써 대형화된 네트워크가 아닌 소형화되고 특수한 환경에서 요구되는 방식이다. 특히, Host를 통해서 모든 통신이 수행됨으로써 발생할 수 있는 효율성 부분에 대해서는 고려하지 않았다. 따라서 향후 연구 방향으로는 하나의 Host에 대한 통신의 비효율성을 보완하기 위하여 분산된 통신이 가능한 연구와 기업내 컴퓨팅 환경을 고려하여 제안방식을 확장시켜 블레이드피씨 모델에 적용하고 보다 다양한 보안 요구사항 및 성능 분석을 통해 효율적이고 안전한 형태의 내부 데이터 유출 방지 구조를 연구하고자 한다.

참 고 문 헌

[1] 송성근, 박지숙, 우재현, 임종인, “情報技術 유출 예방을 위한 기업內 컴퓨팅 환경 최적화 방안 연구,” 한국정보보호학회, 정보보호학회지 제18권 제6호, pp. 43-57, 2008.

[2] http://drm.insideitsolution.com/

[3] Seoksoo Kim, Soongohn Kim, Geuk Lee, ″Structure design and test of enterprise security management system with advanced internal security,″ Future Gener. Comput. Syst. Vol 25, 3, pp. 358-363, 2009.

[4] Todd Borandi, “Introduction to Secure Global Collaboration,” Information Security Journal: A Global Perspective, Vol 18, pp. 51-56, 2009.

[5] http://pdfserve.informaworld.com/880539_758492345_906858502.pdf

[6] 문진규, “내부 정보 유출 방지를 위한 DRM 적용 방법 설계,” 한국정보과학회 2007 논문집 제34권 제 1호, pp. 7-10, 2007.

[7] Hongju Yeom; Hwasung Kim, ″An efficient multicast mechanism for data loss prevention,″ Advanced Communication Technology, 2005, ICACT 2005. The 7th International Conference on , vol.1, pp. 497-502 Vol. 1, pp. 21-23 2005.

[8] 김동진, “기업환경의 내부보안을 위한 통합 보안 관리 시스템의 설계 및 구현,” 석사학위논문, 2008.

[9] Snader, R., Borisov, N., ″A tune-up for Tor: Improving security and performance in the Tor network,″ Network & Distributed System Security Symposium, Internet Society, 2008.

◐ 저 자 소 개 ◑

서 대 희

2003년 순천향대학교 전산학과 졸업(석사)
2006년 순천향대학교 대학원 전산학과 졸업(박사)
2006년~2007년 Howard University Post-Doc
2007년 5월~2007년 12월 한국정보보호진흥원
2008년 7월~2009년 9월 이화여자대학교 컴퓨터공학과 연구교수
2009년 10월~현재 한국전자통신연구원 선임연구원
관심분야 : 정보보호, 네트워크 보안, 소형 디바이스 보안, 오버레이 네트워크, 공격자 추적
E-mail : patima@sch.ac.kr

백 장 미

2003년 순천향대학교 전산학과 졸업(석사)
2006년 순천향대학교 대학원 전산학과 졸업(박사)
2006년~2007년 Howard University Post-Doc
2007~현재 순천향대학교 컴퓨터학부 강사
관심분야 : 임베디드 시스템, 모바일 헬스케어, 지능형 소프트웨어, 지식관리 시스템
E-mail : bjm1453@sch.ac.kr

이 민 경

2007년 세종대학교 컴퓨터소프트웨어학과 졸업(학사)
2009년~현재 이화여자대학교 일반대학원 석사과정
관심분야 : 유비쿼터스 네트워크, 실시간 분산 시스템, 상황인지 시스템, 멀티미디어 서비스
E-mail : mg0426@gmail.com

윤 미 연

2000.2~2002.2 : 숭실대학교 컴퓨터학과 공학석사
2002.3~2005.8 : 숭실대학교 컴퓨터학과 컴퓨터통신 공학박사
2005.6~2009.7 : 한국정보보호진흥원 선임연구원 재직
2009.7~현재 : 한국인터넷진흥원 선임연구원 재직
관심분야 : 정보보호, IPv6, IPTV, 다자간 통신, 멀티미디어보호
E-mail : myyoon@kisa.or.kr

조 동 섭

1981년 서울대학교 전기공학과 졸업(석사)
1986년 서울대학교 컴퓨터공학과 졸업(박사)
1985년- 현재 이화여자대학교 컴퓨터학과 교수
1996-1997년 미국 Univ.of California, Irvine Dept.of ECE Visiting Scholar
관심분야: 임베디드 보안, 웹서비스 아키텍쳐, 휴먼컴퓨팅, 웹서버 엔지니어링
E-mail:dscho@ewha.ac.kr