한국산업정보학회논문지 제15권 제5호(2010. 12)

DHCP 절전시스템을 위한 보안 인증

(Security Certification for DHCP Power-Saving System)

오 임 걸*
(Im-Geol Oh)

요 약 DHCP 절전시스템은 전원 관리 서버가 IP 주소를 제한함으로써 사용자가 절전 소프트웨어 설치에 능동적으로 참여하도록 유도하는 장점이 있다. 그러나 이 방법에서의 문제점은 IP spoofing공격에 취약하여 절전의 효과보다는 전체 시스템이 마비되는 우를 범할 수 있을 것이다. 본 논문에서는 위와 같은 절전시스템을 기반으로 공공기관의 조직원 컴퓨터에 대한 높은 보안성을 제공함으로써 효율적인 절전을 구현할 수 있는 인증 시스템을 제안한다.

핵심주제어 : 인증, DHCP, IP 주소, 절전시스템

Abstract The DHCP power saving system provides advantage to driving active participation in which users installs the power saving software by restricting IP address through the power management server. However, the problem with this approach is the vulnerability to IP spoofing attacks, therefore we need to solve the mistake that disrupt the entire network system rather than saving electric power. In this paper, we propose the authentication system that can implement the efficiency saving power by providing high security for the members' computer system of the public institutions based on the saving power system.

Key Words : Authentication, DHCP, IP Address, Power-Saving System

1. 서 론

Forrester Research 보고서에 의하면 2008년 말 전 세계에서 사용되는 개인용 컴퓨터 대수는 10억대가 넘을 것으로 추정하고 있으며, 향후 5년 이내에 20억대의 컴퓨터가 보급되어 사용될 것이라고 추정하고 있다[1]. 또한 2007년 Gartner 보고서에 따르면, 정보통신분야 제품들은 전 세계 이산화탄소 배출량의 2%를 차지하고 있으며, 그 중 약 40%에 달하는 에너지가 PC와 모니터에 의해서 발생시키므로 전 세계의 에너지의 1%를 소모시키고 있는 셈이다. 그런데 1%의 에너지 소비 중 70%는 실제 사용하지 않는 대기상태로 컴퓨터 전력이 낭비되고 있다. 비효율적인 전원공급기 사용 및 대기전원 등으로 인한 전력낭비가 PC 전력 낭비의 주원인이다[2, 3].

특히, 우리나라의 연간 PC 대기전력 소모량은 85만 KW추산되며, 비용으로 환산하면 연간 5000억원 가량이 낭비되고 있는 실정이며, 이는 온실가스 배출량을 급증시켜 대기오염의 요인으로 무시할 수 없는 수준에 도달하고 있다[4].

이렇게 비효율적으로 낭비되는 PC 전력을 줄이기 위해 다양한 분야에서 그린 IT 기술 도입이 추진되고 으며, 그중에서도 가장 활발하게 적용되고 있는 분야는 데이터 센터, 개인용 컴퓨터, 인터넷 등이 대표적이다[5].

* 한서대학교 전자컴퓨터통신학부

데이터 센터와 인터넷 부분은 전기 분배·변환 등의 에너지 비효율성이 높아 전력 절감형 기종 채택 및 종합적인 그린 정책으로 개선 가능하다.

특히, 데이터 센터에서 소용되는 비용은 서버와 Storage등의 IT 장비 구매 비용과 전력 및 냉각에 필요한 비용으로 구분되는데, IDC(International Data Corporation)에 의하면, 전력 및 냉각에 필요한 비용이 전체 IT장비 구매비용을 초과하고 있으며, 또한 Gartner도 2008년까지 50% 정도의 데이터 센터가 필요로 하는 전력 및 냉각시스템을 충족시키지 못할 것이라고 전망하며, 에너지 사용증가에 대한 적극적이고 현실적인 대처방안이 필요하다고 지적하고 있다[6].

개인용 컴퓨터도 에너지 절감형으로 만들어진 제품을 구매 하거나, 대기전력 절감 등 개인용 컴퓨터 전력관리를 통한 전력 및 비용 절감이 가능하다. 이를 통해 연간 약 50%의 전력 소비와 이산화탄소 배출량을 줄일 수 있으며 전원 플러그 해제 시에는 약 22%의 추가 감축할 수 있다[7].

새로 전력 절감형 컴퓨터를 구매하지 않고 기존의 컴퓨터의 전원을 차단하는 습관 혹은 사용자가 운영체제상에서 컴퓨터의 대기모드와 최대절전 모드형태로 설정함으로써 절전의 효과를 거둘 수 있다.

HP사의 보고에 의하면, 절전관리 설정만 변경해도 컴퓨터 당 20-30W의 전력을 절약하며, 연간 60KW의 전력을 절감한다. 컴퓨터 한 대당 연간 7.2달러의 전기료가 감소되며, 14만대의 컴퓨터를 사용하는 HP사에서는 연간 47만 9700달러의 전기료를 절약하는 효과를 보았다[8].

기업 및 공공 기관의 컴퓨터에 대한 자발적인 절전 설정만으로도 큰 효과를 볼 수 있지만, 이러한 절전 설정을 위한 습관을 정착시키기 위해서는 상당한 시간과 교육이 필요하며 조직원들의 자발적인 참여가 수반되어야 하는 문제점을 내포하고 있다.

컴퓨터의 전원차단과 최대절전모드 설정을 조직원 교육과 자발적인 참여에 의존하지 않고, 소프트웨어 시스템을 이용하여 해결방법을 제안한 "DHCP를 이용한 절전시스템"방법은 사용자 컴퓨터의 절전 소프트웨어 설치를 감시한다. 절전 소프트웨어가 설치되지 않는 컴퓨터는 DHCP 서버가 IP 주소를 제한적으로 제공하는 환경을 제공함으로써 사용자가 절전 소프트웨어 설치에 능동적으로 참여하도록 유도하는 장점이 있다[5].

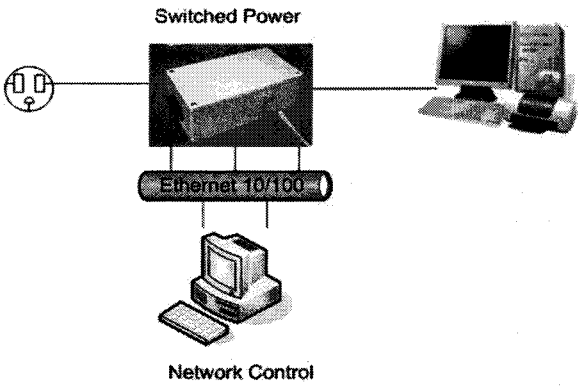
그러나 이 방법에서의 문제점은 DHCP서버가 IP주소를 제한적으로 제공하는 경우에 Attacker가 중간에 끼어드는 Connect hijacking과 같은 유형인 Non Blind IP spoofing공격에 매우 취약하여 절전의 효과보다는 전체 시스템이 마비되는 우를 범할 수 있을 것이다.

본 논문에서는 위와 같은 절전시스템을 기반으로 IP spoofing공격으로부터 안전하고 효율적인 절전 인증시스템을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 절전시스템에 관하여 설명하고, 3장에서는 DHCP를 이용한 절전시스템 방법에 대한 보안상 문제점을 기술하며, 4장에서는 해커들의 공격으로부터 안전한 절전시스템의 보안 인증 시스템을 제안하고, 5장에서는 안전성에 대해 분석한다. 마지막으로 6장에서는 결론을 맺는다.

2. 절전관리 시스템 종류

전력 소모량을 줄이기 위한 방안으로, 조직 내의 단말기가 일정 시간 동안 작동하지 않을 경우 일괄적으로 절전모드로 전환하는 컴퓨터 절전 관리 시스템을 사용한다.



<그림 1> 중앙 관리 절전 시스템의 예 [9]

2.1 중앙 관리 절전시스템

중앙 관리 절전 시스템은 조직원의 컴퓨터에 클라이언트용 절전 소프트웨어를 설치하고 관리 서버가

절전 프로그램을 실행한다. 클라이언트용 절전 소프트웨어는 업무용 소프트웨어와 함께 쉽게 설치할 수 있으며, 이 시스템은 조직원들의 근무상태에 관계없이 컴퓨터의 절전 관리가 가능하다. 또한 컴퓨터의 종료 현황을 중앙서버에서 관리할 수 있으므로 보안직원이 확인하는 수고를 덜 수 있다[5].

그러나 사용자의 컴퓨터가 업무용이 아닐 때는 중앙 관리 절전 시스템의 통제를 받지 않을 수 있다. 즉, 학교 혹은 연구소와 같은 기관의 컴퓨터 중 일부는 서버에 접속할 이유가 없고, 컴퓨터의 운영체제가 다양하므로 클라이언트용 절전 소프트웨어를 설치하고 관리하는데 어려움이 존재한다.

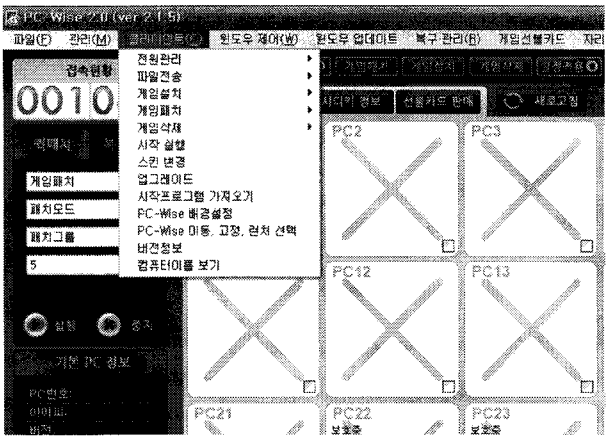
2.2 원격 관리 절전시스템

학교나 연구소와 같은 기관에서 운영하는 다양한 종류의 컴퓨터와 운영체제에서는 중앙 관리 절전 시스템을 통합적인 설치와 운영에 많은 기술적인 문제가 발생하므로 중앙 관리 절전 시스템은 적합하지 않다. 즉, 실습실 환경이 리눅스 등 다른 운영체제인 경우는 클라이언트용 절전소프트웨어 설치가 어려운 실정이며, 주기적으로 수업환경 구축을 위하여 교육용 소프트웨어를 재 설치하는 관계로 인하여 절전 관리 시스템을 구축하기란 쉽지 않다.

그러므로 원격 관리 절전시스템은 비교적 소규모로 사용하여야 하는 단점이 존재하지만, 구성원의 컴퓨터의 절전 관리와 보안 관리 업무등에 적합한 시스템이다

원격으로 컴퓨터의 전원을 켜고 끌 수 있는 기능을 구현하기 때문에 기본적인 자산 확인 및 보안 체크업무가 가능하고, 저렴한 비용으로 시스템의 업그레이드와 문제해결이 가능하므로 전력수요 축소 및 기타 부대비용을 절감할 수 있는 장점이 있다.

인텔사에서 개발한 v프로 솔루션을 도입한 미국의 통신업체 버라이존은 소프트웨어 문제 관련 방문 횟수를 최대 91%까지 줄일 수 있었으며, 미국 인디아나주는 사용하지 않는 PC 전원을 원격으로 차단하여 에너지 비용을 기존 대비 최대 70%까지 절감하였다[10].



<그림 2> 웹상에서 효율적으로 모니터링 하고 제어할 수 있는 원격 관리 절전시스템. [11]

2.3 프리웨어 절전시스템

다양한 운영체제에서 동작하는 프리웨어 소프트웨어는 다양한 특징의 기능들을 사용자 에게 제공한다. 즉 프리웨어 절전 소프트웨어는 사용자가 설정한 시간동안 컴퓨터를 사용하지 않으면 절전기능을 수행함으로써 큰 효과를 볼 수 있으며, 이러한 기능을 갖는 소프트웨어는 인터넷에서 쉽게 구할 수 있다.

또한 앞장에서 언급한바와 같이, 운영체제상에서 컴퓨터의 대기모드와 최대절전 모드형태로 설정함으로써 동일한 절전의 효과를 거둘 수 있으며, 이와 같은 형태의 프리웨어로서는 네이트온 환경 설정에서 절전기능을 설정하여 실행하면, 자리 비움 시마다 모니터가 자동으로 꺼져 에너지가 절약된다[12].

그 외에도 컴퓨터가 종료된 상태에서 다른 사용자가 컴퓨터를 사용하지 못하도록 해주는 보안기능, 자동 실행 설정 및 시스템 종료, 로그오프, 대기모드, 등등의 다양한 기능을 설정할 수 있다.

3. DHCP를 이용한 절전 관리 시스템

이 시스템은 전원 관리 서버와 클라이언트용 절전 소프트웨어 두 부분으로 나뉜다. 전원 관리 서버는 주기적으로 클라이언트용 절전 소프트웨어의 동작 여부를 묻는 요청을 하고, 클라이언트용 절전 소프트웨어는 그 응답을 하는 구조이다.

3.1 클라이언트용 절전 소프트웨어

클라이언트용 절전 기능 소프트웨어는 컴퓨터를 사용하지 않으면, 절전모드로 자동으로 전환되는 기능을 수행하면 된다.

윈도우즈 계열의 운영체제, 리눅스, Mac 운영체제들에서 동작하는 컴퓨터 절전용 프리웨어를 설치하여 사용할 수 있으며, 인터페이스 설치가 거의 필요 없으므로 절전기능은 쉽게 구현 할 수 있다.

프리웨어로 또는 간단하게 작성된 프로그램으로 절전 기능이 올바르게 동작하면 클라이언트용 절전 소프트웨어는 전원 관리 서버의 동작 여부를 묻는 요청에 응답한다.

3.2 전원 관리 시스템

일반적으로 전원관리 시스템은 그림과 같이 DHCP 서버, 전원 관리 서버, 클라이언트들의 3종류의 컴포넌트로 구성되며, 일반적인 전원 관리 시스템의 동작 원리는 다음과 같다.

DHCP의 주요동작은 DHCP 클라이언트가 DHCP_DISCOVER 메시지를 브로드캐스트하고, 메시지를 수신한 DHCP_OFFER 메시지의 제공여부를 결정하며 응답 시 yiaddr 필드에 가용한 IP주소를 담아서 브로드캐스트한다.

DHCP 클라이언트가 다수의 DHCP_OFFER 메시지를 수신하면 하나의 서버만 선택하고, 선택된 서버가 제공하는 IP 주소를 DHCP_REQUEST 메시지의 서버 identifier option 필드에 담아서 서버에게 브로드캐스트한다.

서버가 Server identifier option field를 검사하여 자신의 주소와 일치하면 DHCP_ACK 메시지를 수신한 클라이언트는 IP 주소를 할당하며, IP 임대기간, DNS, Default Gateway, WINS 등의 DHCP 옵션 값을 담은 DHCP_ACK 패킷을 만들어서 최종적으로 브로드캐스트로 보낸다.

DHCP_NACK 메시지를 받은 클라이언트는 IP 주소를 받을 수 없는 것으로 정의 한다[13].

클라이언트용 절전 소프트웨어가 설치되지 않은 컴퓨터에 제한적으로 IP 주소를 공급하기 위해서는 DHCP_NACK 메시지를 전송하도록 수정하여야 한다.

이러한 수정 작업을 쉽게 하기 위하여 전원 관리 서버를 DHCP 서버에 설치해야하며, Microsoft DHCP 서버의 Callout API는 DHCP 서버의 사용자 정의 확장 기능 및 통계 모니터 등의 개발을 가능하다[14].

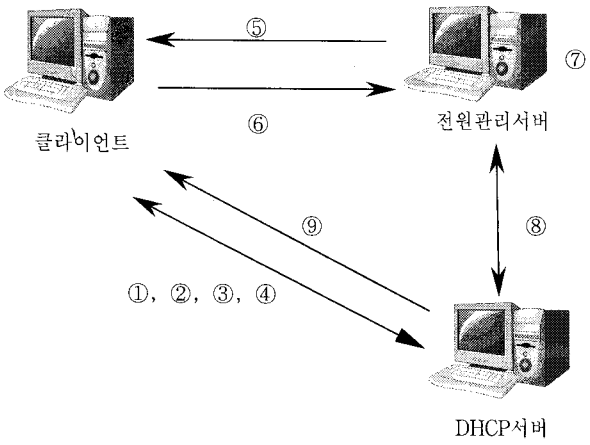
Callout API를 사용하기 위해서는 Callout DLL의 설치가 필요하며, 다음과 같은 콜백 함수는 msdn에서 제공된다[15].

DhcpAddressDelHook	DhcpAddressDelHook
DhcpControlHook	DhcpDeleteClientHook
DhcpHandleOptionsHook	DhcpNewPktHook
DhcpPktDropHook	DhcpPktSendHook

전원 관리 서버는 절전 소프트웨어가 설치되지 않은 클라이언트가 DHCP_Discover 메시지를 보내면 DHCP 서버가 DHCP_Offer 메시지 대신에 DHCP_Nack 메시지를 구성하고, DHCP_Offer 메시지 콜백 함수는 시급히 처리해야 하므로 클라이언트용 절전 소프트웨어의 동작 여부를 요청한다.

따라서 전원 관리 서버는 클라이언트용 절전 소프트웨어가 설치되지 않아서 IP 주소를 제한하는 MAC 주소 목록을 이용하여 DHCPAddressOfferHook 콜백 함수에서 DHCP_Offer 메시지와 DHCP_Nack를 선택적 전송한다. IP 주소를 제한하는 MAC 주소 목록을 작성하기위해서는 DHCP_Ack 패킷에서 구할 수 있으며, Callout API에서는 별도로 제공하지 않으며, 그 대신 DHCPPktSendHook 콜백 함수의 패킷이 DHCP_Ack 패킷일 경우 여기서 클라이언트의 IP 주소와 MAC 주소를 구하고, 이 IP 주소를 이용하여 클라이언트용 절전 소프트웨어 동작여부를 확인한다.

전원 관리 서버는 클라이언트 IP 주소로 절전 소프트웨어 동작 확인에 대한 3번의 요청에도 응답이 없을 때에는 절전 소프트웨어가 설치되지 않은 것으로 간주 IP 주소를 제한하는 MAC 주소 목록에 추가함으로써 클라이언트 컴퓨터는 IP 주소 제공에 제한을 받는다. 절전 소프트웨어 설치 이후에도 IP 주소를 제한하는 문제를 해결하기 위해서는 DHCP 클라이언트가 DHCP_Offer 메시지를 받지 못했다면 DHCP_Discover 메시지를 다시 브로드캐스트 한다.

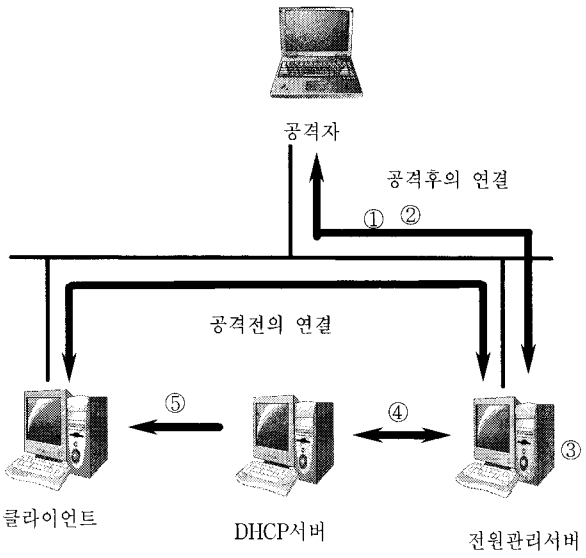


순서	From	TO	Operation
①	Client	DHCP 서버	DHCP_DISCOVER
②	DHCP 서버	Client	DHCP_OFFER
③	Client	DHCP 서버	DHCP_REQUEST
④	DHCP 서버	Client	DHCP_ACK
⑤	전원관리 서버	Client	절전 소프트웨어 동작여부 요청
⑥	Client	전원관리 서버	응답이 없을 시 절전 소프트웨어 미설치로 간주
⑦	전원관리 서버		절전 소프트웨어 미설치 클라이언트 MAC 주소 추가
⑧	DHCP 서버	전원관리 서버	절전 소프트웨어 미설치 클라이언트 MAC 주소 확인
⑨	DHCP 서버	Client	IP 주소 제한

<그림 3> DHCP를 이용한 절전 시스템과 작동 순서표

네 번째 요청 이후에도 받지 못했을 때 클라이언트는 5분마다 재 시도하며, MAC 주소가 15번 이상의 호출이 있으면 MAC 주소 목록에서 삭제하도록 하여 클라이언트용 절전 소프트웨어 설치 후에는 IP 주소를 재 할당 받도록 설계 하였다[5].

위 <그림 3>과 같이 DHCP 서버가 절전 소프트웨어가 설치되지 않는 컴퓨터에게 IP 주소를 제한적으로 제공하여 사용자가 불편을 느끼도록 환경을 제공함으로써, 절전 소프트웨어 설치에 능동적으로 참여하도록 유도한다.



순서	From	To	Operation
①	전원관리 서버	공격자	절전 소프트웨어 동작여부 요청
②	공격자	전원관리 서버	클라이언트로 가장하여 미 응답
③	전원관리 서버		절전 소프트웨어 미 설치 클라이언트 MAC주소 추가
④	DHCP 서버	전원관리 서버	절전 소프트웨어 미 설치 클라이언트 MAC주소 확인
⑤	DHCP 서버	Client	IP 주소 제한으로 인하여 해당 클라이언트 마비

<그림 4 > 절전 시스템의 공격모형 및 순서표

4. 제안한 전원 관리 시스템

4.1 DHCP를 이용한 절전 시스템의 문제점

앞장 <그림 3>의 작동순서표 ⑤번부터 ⑨번까지의 과정에서와 같이 전원관리 서버가 클라이언트에게 절전 소프트웨어 동작여부를 요청 시, 악의적인 공격자는 정당한 클라이언트로 위장하여 조직 내의 모든 클라이언트 컴퓨터가 절전 소프트웨어가 동작하지 않는 것으로 무응답 함으로써 전원관리 서버는 조직 내의 전체 클라이언트의 MAC주소를 저장한다.

그러므로 DHCP 서버는 CallBack 함수를 이용하여 절전소프트웨어가 작동하지 않는 클라이언트들의 MAC주소를 확인하여 IP 주소를 제한함으로써 절전의 효과보다는 전체 시스템이 마비되는 결과가 초래 될 것이다.

또한 <그림 4>와 같이 수동적 공격자가 과거에 전원관리서버와 클라이언트 사이에 절전소프트웨어 작동 여부에 관한 통신내용들을 도청한 후, 이를 재전송하여 합법적인 클라이언트 또는 전원 관리 서버로 인증 받으려는 공격으로부터 매우 취약하므로 안전하고 효율적인 절전 시스템을 제안한다.

이러한 방식으로 공격자는 네트워크안에 있는 모든 클라이언트들의 IP주소를 제한하도록 유도 할 수 있다.

4.2 제안한 전원관리 시스템

본 절에서는 안전한 전원관리시스템을 제안하며, <표 1>은 논문에서 사용되는 시스템 파라미터들을 정의한다.

<표 1> 시스템 파라미터

용어	정의
CID	Client에게 할당된 ID 정보(MAC주소)
k_{ct}	Client의 비밀키
$M_{k_{DB}}()$	k_{DB}를 이용한 메시지 인증코드(MAC)
Time	Client가 생성한 Time Stamp 값
Query	Client의 응답을 요청한 전원서버의 요청
C_{rand}	Client가 생성한 랜덤값
$h()$	일방향 hash function
$prng()$	의사난수 생성기
$\|$	연접연산(Concatenation)
$A \rightarrow B: X$	X가 A에서 B로 전송
$\oplus$	배타적 논리곱(XOR)

보안 서버 DB는 각 클라이언트에 대한 식별자(CID= MAC주소), 비밀키(k_{ct})와 MAC(Message Authentication Code)등 필요한 정보 집합을 관리하고 있으며, 전원 관리 서버와 보안 서버 DB간의 채널은 일반적으로 안전한 채널(Secure Channel)이며 전원 관리 서버와 클라이언트간의 채널은 안전하지 않은 채널(Insecure Channel)로 가정한다. 따라서 전원관리서버와 클라이언트 사이의 주고받는 모든 통신메시지들은 공격자에 의해 엿보기나 수정이 가능하다[19-21].

4.2.1 보안 서버 DB 정보 암호화

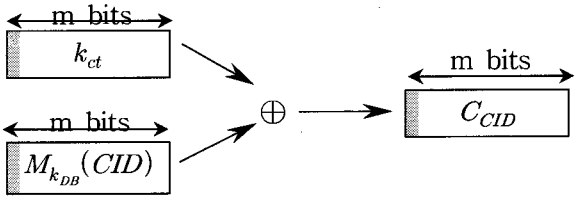
본 절에서는 보안 서버 DB의 환경에서 조직 및 기관내의 보안 서버 DB에 저장할 클라이언트에 대한 중요한 정보를 암호화하는 기법을 제안한다. 클라이언트에 관한 정보를 보안 서버 DB내에 저장 시에는 안전성뿐만 아니라 저장 효율성을 고려하여 저장 및 관리하여야 한다.

<그림 5>는 제안한 보안 서버 DB의 정보 암호화 방법을 보여주고 있다.

보안 서버 DB내의 클라이언트 비밀키 k_{ct}를 안전하게 암호화(Encryption)하여 저장하는 방법은 다음과 같이 동작한다.

(1) 보안 서버 DB는 클라이언트의 식별자인 CID (Client Identification)와 자신의 비밀키를 이용하여 고유한 메시지 인증 코드(MAC)값인 m비트열 길이의 $M_{k_{DB}}(CID)$값을 계산한다.

(2) 보안 서버 DB는 클라이언트의 비밀키 k_{ct}와 위에서 구한 메시지 인증 코드 $M_{k_{DB}}(CID)$와의 XOR연산 값 $C_{CID} = k_{ct} \oplus M_{k_{DB}}(CID)$계산하여 전원관리서버내의 해당 클라이언트의 비밀키 필드에 저장한다.



<그림 5> 보안 서버 DB내의 클라이언트 비밀키 암호화

4.2.2 클라이언트 인증

<그림 6>는 제안한 보안 서버 DB의 클라이언트 인증 프로토콜의 구성과 동작 과정을 보여주며, 다음의 4단계를 거쳐 인증과정이 이루어진다.

(1) 전원 관리 서버 → 클라이언트

$\{Query, Time\}$

전원관리서버는 타임스탬프 Time을 생성한 후, 클라이언트에게 Query와 함께 전송한다. 여기서 Tim은 시간동기화를 위한 것이 아니라 해당 클라이언트가

절전 소프트웨어 동작상태 컴퓨터인지를 빨리 검증하기 위해 사용된다.

(2) 클라이언트 → 전원 관리 서버 :

$\{H_{CID}, C_{rand}, Time\}$

클라이언트는 랜덤 값 C_{rand}를 $prng()$로부터 생성한 후, 전원관리서버로 부터 수신한 $Time$과 자신의 식별자인 CID 및 비밀 키 k_{ct}를 이용하여 해쉬 값 $H_{CID} = h(k_{ct} \| CID \| C_{rand} \| Time)$을 계산한 후, 전원관리서 서버에게 계산된 H_{CID}를 C_{rand}와 $Time$를 동시에 전송한다.

(3) 전원 관리 서버 → 보안 서버 DB :

$\{H_{CID}, C_{rand}, Time\}$

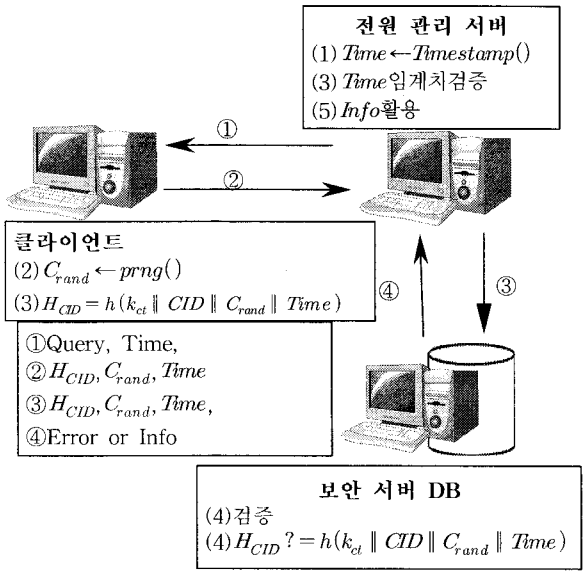
전원관리서버는 먼저 수신한 메시지가 자신이 정한 임계 시간(Threshold Time) 내에 도착하였는지 여부를 수신한 $Time$을 이용하여 검증한다. 검증을 통과한 클라이언트가 절전 소프트웨어 동작 상태의 컴퓨터임이 확인되면, 수신한 메시지들을 보안서버(DB)에게 전송한다.

(4) 보안 서버 DB → 전원 관리 서버 :

$\{Info\}$

보안 서버 DB는 전원 관리 서버로부터 전송받은 H_{CID}, C_{rand}, $Time$와 자신의 DB에 저장하고 있는 모든 CID와 k_{ct}를 이용하여 전원관리서버로부터 수신한 H_{CID}값과 일치하는 CID와 k_{ct}의 쌍을 검색한다. 만약 일치하는 값이 검색되지 않으면, 클라이언트가가 존재하지 않는다는 오류메시지를 전원관리서버에게 전송하고, 일치하는 값이 검색되면 해당 클라이언트를 인증하고 클라이언트에 대한 정보를 전원관리서버에게 전송한다.

(5) 전원 관리 서버는 보안 서버 DB로부터 수신한 값이 오류일 경우, 클라이언트와의 통신을 중단하고, 정상적인 인증이 되었을 경우에서는 보안 서버 DB로부터 수신한 전원관리 정보인 $Info$를 활용하여 해당 클라이언트에 대한 전원관리업무를 수행한다.



<그림 6> 제안한 보안 서버 DB에 기반한 인증프로토콜

5. 안전성 분석

본 장에서는 제안한 DHCP 절전 시스템을 위한 보안 인증에 대한 보안성 분석을 한다. 먼저, 제안한 인증 시스템의 안전성 분석을 위해 필요한 보안 항목을 다음과 같이 정의한다[20, 21].

[정의 1] 강력한 비밀 키(k_a와 k_{DB})는 높은 엔트로피(entropy)를 가지는 값으로써 다항식시간(polynomial time) 내에 계산되어 질 수 없다.

[정의 2] 일방향 해쉬함수(One-way hash function) $y = h(x)$와 메시지 인증코드 함수 $y = M(x)$에서 주어진 x에 대하여 y를 계산하는 것은 쉽지만, 주어진 y를 이용하여 x를 계산하는 것은 어렵다.

위의 정의들을 기반으로 DHCP 절전 시스템을 위한 보안 인증은 다음과 같이 재전송 공격, 스푸핑 공격, 위치 트래킹 공격, 클라이언트 키 유출 공격, 보안서버 DB 정보 유출 공격에 안전하며 클라이언트 익명성을 제공한다.

(1) 재전송 공격 : 공격자는 임의의 세션에서 전원관리 서버와 클라이언트사이에서 전송되는 정보를 도청한 후, 다음 세션에서 정당한 전원관리서버나 클라

이언트로 위장하여 재전송 공격을 수행할 수 있다. 그러나 제안한 보안 인증 시스템에서는 매 세션마다 전원 관리 서버가생성하는 새로운 타임스탬프 $Time$과 클라이언트가 생성하는 새로운 랜덤 값 C_{rand}를 이용하여 보안서버 DB에 의해 인증을 수행하기 때문에, 과거에 공격자에 의해 재전송된 랜덤 값들은 보안서버DB의 인증으로 검출됨으로 재전송 공격을 수행할 수 없다.

(2) 스푸핑 공격 : 공격자가 보안 서버 DB와 클라이언트 간에 공유된 비밀 키 k_{ct}를 얻을 수 있으면, 전원관리서버 또는 클라이언트로의 스푸핑 공격을 성공할 수 있다.

그러나 [정의 1]과 [정의 2]에 의해 제안한 보안 인증 시스템에서 공개 통신 채널 상으로 전송되는 정보들인 $\{H_{CID}, C_{rand}, Time\}$을 이용하더라도, 공격자는 보안 서버 DB와 클라이언트 내에 각각 저장하고 있는 비밀 키 k_{ct}를 직접적으로 구할 수 없으므로 스푸핑 공격을 수행할 수 없다.

(3) 위치 트래킹 공격 : 클라이언트에서 생성하는 랜덤 값 C_{rand}는 매번 다른 값으로 생성되므로, 계산된 H_{CID}는 역시 매번 변경된다. 그러므로 공격자는 현재 세션에서 클라이언트의 응답이 과거에 도청한 응답과 일치하는지를 쉽게 구별할 수 없다. 이로 인해, 공격자는 클라이언트를 추적을 할 수 없을 뿐만 아니라, 특정한 클라이언트를 식별할 수 없기에 위치 트래킹 공격을 수행할 수 없다.

(4) 보안 서버 DB정보 유출공격 : 모든 클라이언트의 비밀키 정보를 저장하고 있는 보안 서버 DB내의 클라이언트 관리 테이블이 유출되었다고 가정하자. 기존의 DHCP 절전시스템의 전원관리서버의 DB 유출로 인해 임의의 공격자는 암호화되어 있지 않는 MAC주소 테이블로 부터 모든 클라이언트의 MAC주소 값을 쉽게 얻을 수 있다.

그러나 제안한 보안 서버 DB의 프로토콜 상에서는 공격자가 클라이언트의 비밀 키 정보를 담고 있는 DB 테이블을 구하더라도 해당 클라이언트의 비밀 키 k_{ct}가 아닌 암호화된 $C_{CID} = k_{ct} \oplus M_{k_{DB}}(CID)$를 얻게 된다. C_{CID}는 보안 서버 DB의 비밀키 k_{DB}로 암호화되어 있으므로, C_{CID}로부터 클라이언트의 비밀키 k_{ct}를 복호화 할 수 없다. 결론적으로 제안한 보안 인증 프로토콜은 임의의 공격자에 의한 보안 서버 DB 유출 공격에 안전하다.

만약 합법적인 한 클라이언트의 비밀 키 k_{ct}를 알고 있는 공격자라도 $C_{CID} = k_{ct} \oplus M_{k_{DB}}(CID)$로부터 $C_{CID} \oplus k_{ct}$를 계산하여 $M_{k_{DB}}(CID)$를 얻을 수 있지만, [정의 1]과 [정의 2]에 의해 보안 서버 DB의 비밀키 k_{DB}는 얻을 수 없음으로, 나머지 클라이언트들의 비밀 키에 대한 안전성이 보장되므로 제안한 프로토콜은 합법적인 임의의 클라이언트에 의한 보안 서버 DB 유출 공격에 대해서도 안전하다.

(5) 클라이언트 익명성 : 전원관리서버는 타임스탬프 $Time$을 생성하여 클라이언트에게 전송하고, 클라이언트는 수신한 $Time$과 자신이 생성한 임의의 랜덤 값 C_{rand}, 식별자 CID, 비밀키 k_{ct}를 이용하여 일방향 해쉬 함수 $H_{CID} = h(k_{ct} \| CID \| C_{rand} \| Time)$을 계산한 후 전원 관리 서버에게 전송한다.

H_{CID}을 도청한 공격자는 클라이언트의 비밀 키 k_{ct}를 모르므로 클라이언트의 식별자 CID를 구할 수 없다. 또한 일방향 해쉬 함수의 성질에 의해 H_{CID} 로부터 클라이언트의 정보를 직접적으로 얻을 수 없으므로 클라이언트의 익명성이 제공된다.

그러므로 "DHCP를 이용한 절전시스템"의 문제점에서 지적한바와 같이 악의적인 공격자에 의한 스푸핑 공격, 재전송 공격, 위치트래킹 공격 등에 취약하여 절전의 효과보다는 전체시스템이 마비되는 결과를 초래될 것이다. 그러므로 본 논문에서는 기존의 시스템에서 보안상의 문제점을 해결하기위한 인증 기법을 제안함으로써 DHCP 서버가 절전소프트웨어가 설치되지 않은 컴퓨터에 대해 IP주소의 제한을 안전하게 실행할 수 있다.

6. 결 론

DHCP 서버가 클라이언트에 대한 IP주소를 제한하는 절전시스템은 사용자가 절전 소프트웨어 설치에 능동적으로 참여를 유도하는 장점이 있다.

그러나 이 시스템의 문제점은 악의적인 공격자에

의한 스푸핑 공격, 재전송 공격 등에 매우 취약하여 절전의 효과보다는 전체 시스템이 마비되는 결과가 초래될 수 있을 것이다.

이러한 문제를 해결하기 위하여 절전시스템에 대한 인증을 제안하였다. 제안한 인증 시스템은 안전하고 효율적으로 클라이언트의 정보를 보호할 수 있으며, 보다 높은 보안성을 제공함으로써 효율적인 절전시스템을 구현할 수 있을 것이다.

향후 연구로는 보안 공격으로부터 안전하고 효율적인 절전시스템을 개발을 통한 실용성 증명에 목표를 둔다.

참 고 문 헌

[1] 1 Billion PCs in use by end of 2008. http://www.news.com/8301-10784_3-9727337-7.html

[2] Gartner Estimates ICT Industry Accounts for 2 Percent of Global CO2 Estissions. http://www.gartner.com/it/page.jsp?id=503867.

[3] 이정일, "녹색 성장의 힘 '그린IT'가 뜬다," 아시아경제, 2009. 09. 17.

[4] 차종환, "루로아정보기술, 대기전력관리로 그린IT 선도," 한국정보통신신문 2009년 9월 14

[5] 김홍윤, "DHCP를 이용한 절전 시스템," 한국산업정보학회논문지 v.14, no.5, pp.75-82, 2009. 12

[6] 김태헌, "그린데이타 센타와 에너지 효율 평가 서비스," ITDaily 2008년 5월 2일

[7] 김윤겸, "그린 IT, 비용절감·효율성 증대 효과 기대," ITDaily, 2009. 11. 02.

[8] EDS, "Power Management Implemenation Case study EDS" http://www.climatesaverscomputing.org/docs/EDS_power%20management%20case%20study.pdf

[9] 중앙전원 관리시스템 http://www.aytechnology.com/products/pd_ctrl_epcon.aspx

[10] 윤상호, "원격 전원 ON/OFF…PC 관리 비용·시간 절감," 디지털 데일리 2008. 11. 26.

[11] 한지운, "메신저로 PC 전기절약을? 네이트온, 모니터 절전 캠페인," 경제투데이, 2009. 10. 4.

[12] 원격관리시스템 http://www.multiclick.co.kr/manual_pcwise/files2/manual_03.html

[13] 이종훈 외 4인, "Virtual LAN에서 DHCP NAK Loop 방지를 위한 유효 주소 인지 알고리즘," 한국정보과학회 가을 학술발표논문집, Vol. 29, No. 2, pp. 604-606, 2002.

[14] "DHCP Server Callout API usage," http://blogs.technet.com/teamdhcp/archive/2009/07/06/dhcp-server-callout-api-usage.aspx

[15] "DHCP Server Callout API Reference," http://msdn.microsoft.com/en-us/library/aa363373(VS.85).aspx

[16] F. Klaus, "RFID handbook," Second Edition, Jone Willey & Sons, 2003.

[17] S. A. Weis, "Security and privacy in radio-frequency identification devices," MS Thesis. MIT. May, 2003.

[18] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," Security in Pervasive Computing 2003, LNCS 2802, pp.201-212, Springer-Verlag Heidelberg, 2004.

[19] 윤은준, 유기영, "의료정보호를 위한 RFID를 이용한 환자인증 시스템," 한국통신학회논문지, Vol 35, NO 6. pp 962-969, 2010.

[20] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, "Handbook of applied cryptography," CRC Press, New York, 1997.

[21] B. Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C," 2nd edn. John Wiley, Chichester, 1995.

오 임 걸 (Im-Geol Oh)

- 정회원
- 1983년 2월: 인하대학교 수학과 (이학사)
- 1986년 2월: 인하대학교 수학과 응용수학전공(이학석사)
- 1993년 8월: 인하대학교 통계학과 (이학박사)
- 1995년 3월 ~ 현재 : 한서대학교 전자컴퓨터통신학부 교수
- 2010년 3월 ~ 현재 : 한서대학교 디지털 포렌직 연구소장
- 관심분야 : 암호학, 네트워크 보안, 디지털 포렌직