ISSN 1975-8359(Print) / ISSN 2287-4364(Online)
The Transactions of the Korean Institute of Electrical Engineers Vol. 63, No. 11, pp. 1571~1574, 2014
http://dx.doi.org/10.5370/KIEE.2014.63.11.1571

전원선의 전력분석을 이용한 주요정보 유출 가능성에 관한 연구

A Study on Leakage of Critical Information via the Power Analysis of Power Lines

한 경 호† · 이 성 호*
(Kyong-Ho Han · Seong-Ho Lee)

Abstract - In this paper, we propose a unidirectional transmission of critical information obtained by keyboard hacking or kernel and keyboard driver hacking even though the computer is not connected to the external network. We show the hacking can be attempted in the proposed method to show the way preventing such attempts in advance. Firewalls and other various methods are used to prevent the hacking from the external network but the hacking is also attempted in various ways to detour the firewall. One of the most effective way preventing from the hacking attack is physically disconnect the internal intranet systems from the external internet and most of the government systems, military systems and big corporate systems are using this way as on one of the protection method.
In this paper, we show the feasibility of transmission of security codes, etc via the short message to the external network on the assumption that a hacking program such as Trojan Horse is installed on the computer systems separated from the external network. Previous studies showed that the letters on the monitor can be hijacked by electromagnetic analysis on the computer to obtain the information even though the system is not connected ti the network. Other studies showed that the security code hint can obtained by analyzing the power consumption distribution of CPU.
In this paper, the power consumption distribution of externally accessible power line is analyzed to obtain the information and the information can be transmitted to the external network.
Software controlling the CPU and GPU usage is designed to control the power supply of computer. The sensors such as the Rogowski coils can be used on the external power line to collect the data of power consumption change rates. To transmit the user password by short message, due to the capacitive components and the obstacle from other power supply, A very slow protocol are used.

Key Words : Power Analysis, Hacking, one way send information, Rogowski coils, Network, Firewall

1. 서 론

해킹공격을 방어하기 위한 가장 최선의 방법은 보호할 컴퓨터를 외부 네트워크와 물리적으로 독립시키는 것으로 외부와의 통신가능성을 사전에 제거하는 것이다.

물리적으로 네트워크를 독립시켜 운영하는 대표적인 방법은 컴퓨터자체의 네트워크 연결을 모두 제거하는 방법과 내부 네트워크를 외부 네트워크와 분리시켜 독립적으로 운영하는 방법이 있다. 기밀 정보를 취급하는 국가망 또는 사내의 주요 네트워크는 사내 인트라넷으로 운영되어 외부로부터의 접근을 물리적으로 차단하고 있다.

물리적으로 외부 네트워크로부터 독립시키기 위해서는 경유지로 사용될 수 있는 외부 네트워크에서 접근이 가능한 웹서버나 어플리케이션 서버와 연결되지 않아야 하고 또한 스위치허브나 방화벽 같은 네트워크 장비도 독립적으로 사용되어야 한다. 하지만, 외부로부터 물리적으로 분리된 내부 네트워크를 사용하더라도 내부에서의 해킹 공격에는 취약할 수밖에 없다. 특히 경유지 역할을 하는 해킹 프로그램이 설치된 내부 컴퓨터, 공격 명령이 담긴 내부 네트워크에 연결된 컴퓨터 그리고 내부 네트워크 내에 장착된 유무선 네트워크 장치 등을 통해서 해킹 공격이 이루어 질 수 있다.

최상의 보안이 유지되어야 하는 상황에서 외부는 물론 내부의 네트워크 연결을 모두 제거하여 운영할 경우, 물리적으로 네트워크로부터 독립된 컴퓨터는 외부와의 통신이 원천적으로 차단됨으로써 외부의 공격으로부터 가장 안전하게 보호된다.

본 논문에서는 물리적으로 외부 또는 내부의 모든 네트워크로부터 완전하게 독립된 최상의 보안이 유지되는 컴퓨터로부터 정보 유출 가능성을 확인하였다. 네트워크로부터 물리적으로 독립된 컴퓨터에서 외부로 데이터를 단방향으로 전송하는 것을 목적으로 하며 사전에 트로이안 목마등을 사용하여 이미 비밀정보를 획득하였다고 가정하였다.

물리적으로 독립된 컴퓨터에서 외부로 데이터를 전송하기 위해 여러 가지 방법을 고려해 볼 수 있으나 여기에서는 전원케이블을 통하여 정보를 전달하는 것을 목표로 하였으며 전력사용의 의도적 제어에 의하여 의미 있는 정보를 외부로 전달할 수 있는지를 실험하여 시스템 보안에 도움이 되고자

† Corresponding Author : Dept. of Electrical and Electronic Engineering, Dankook University, Korea.
E-mail: ianlee@dankook.ac.kr, csharp1@gmail.com
* Dept. of Electrical and Electronic Engineering, Dankook University, Korea .
Received : August 27, 2014; Accepted : October 16, 2014

한다.

컴퓨터에 연결된 전원케이블 또는 서버실에 연결되어 있는 전원케이블에서 측정이 가능할 정도로 전력을 제어하기 위해서는 CPU 또는 GPU등 전력 소모가 큰 모듈을 제어하여야 한다. 두개 이상의 모듈을 동시 제어할 경우 보다 멀리까지 정보를 전송할 수 있을 것이다. 컴퓨터와 연결된 전원케이블에 전류센서를 연결하고 전류를 측정하여 신호를 전달받을 수 있다. 로그스키 코일(Rogowski coil)을 사용한다면 비접점으로 전류정보를 측정할 수 있어 전원케이블에 손상을 입히지 않고 원하는 정보를 수집할 수 있다.

2. Offline 상태에서의 데이터전송

네트워크가 연결되어 있지 않은 상태에서 데이터를 전송하기 위해 소프트웨어로 제어가 가능한 컴퓨터의 부품에 과부하를 주고 외부에서는 전력선의 전류를 측정하여 전송하고자 하는 정보를 수신하는 방법으로 진행하였다. 컴퓨터에서 외부로 단방향 전송되는 형태로 구성하였으며 실험장치의 구조적 제약상 저속통신으로 실험하였다.

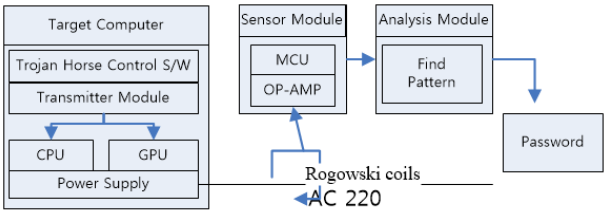

그림 1 Offline 상태에서 데이터를 전송하기 위한 구조도
Fig. 1 Structure chart to transmit data offline

데이터를 전송하기 위한 구성은 전송모듈(Transmitter Module), 센서모듈(Sensor Module), 분석 모듈(Analysis Module)로써 각각 독립적인 프로그램으로 개발한 후 실험하였다.

전송모듈은 트로이안 목마와 같은 소프트웨어 모듈로 대상 컴퓨터에 설치될 수 있는 순수한 소프트웨어로 구성되었으며 센서모듈은 컴퓨터 외부 또는 컴퓨터실 외부에서 전력을 측정할 수 있는 전류측정기를 사용하였다.

전류측정기는 전원선에 직접 연결하는 접점 방법과 로그스키 코일과 같이 무접점으로 전류를 검출할 수 있는 방법을 사용할 수 있다.

분석모듈은 수신부로부터 실시간으로 획득한 전류변화량 데이터를 분석하여 원래의 메시지를 복원하는 기능을 갖는 형태로 구현하였다.

2.1 전송모듈 (Transmitter Module)

전송모듈은 Software로 이루어져 있으며 CPU 또는 GPU의 사용을 의도적으로 제어하여 전류의 사용량을 변화시키는 방식이다. 데이터 전송을 위해 빠르게 CPU의 사용여부를 변화시켜야 하기 때문에 여러 개의 Thread를 동시 실행시키고 신호여부에 따라 동시에 CPU에 부하를 주는 방식을 사용하였다.

아래 그림2 의 구조도 같이 전송하고자 하는 문자를 프로토콜화한 후 BIT단위로 CPU의 사용을 제어하여 컴퓨터의 전원사용을 유도하였으며 추가로 CUDA와 같은 GPU연산을 의도적으로 유도할 수 있는 라이브러리를 사용할 경우 전원사용을 보다 효과적으로 유도할 수 있다.

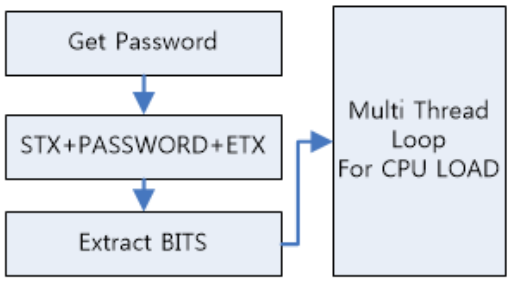

그림 2 Offline Transmitter 구조도
Fig. 2 Offline transmitter structure chart

2.2 센서모듈 (Sensor Module)

센서모듈은 전력선에 흐르는 전류의 변화량을 수집하는 기능을 갖고 있는 것으로 로그스키 코일이나 기타 전류량을 측정할 수 있는 센서를 사용할 수 있으며 센서를 통해 들어오는 값들을 증폭시키기 위하여 OP-AMP 사용하였다. 증폭되고 정류된 신호는 ARM Cortex M0 CPU를 사용하여 변화량을 데이터화하였다.

그림 3 오픈타입형 로그스키 코일
Fig. 3 Open type Rogowski coil

또한, 추가적으로 단순한 소프트웨어 방식의 필터를 사용하여 지속적으로 발생되는 노이즈를 제거하였다. 하지만 실험 목적이 아닌 실사용이나 목표 컴퓨터와 센서 모듈 간에 거리가 먼 경우에는 주변 전자기기에서 발생되는 전류사용량을 제거하기 위한 다양한 종류의 필터가 사용되어야만 할 것이다.

2.3 분석모듈 (Analysis Module)

수집된 자료에서 의미 있는 정보를 획득하는 모듈로써 전류의 사용량에서 PWM 데이터를 추출하는 방식으로 구현하였다. 이 실험에서는 1.5초당 하나의 Bit를 전송하는 방식으로 설계되었으며 High에서 Low로 Falling되는 시간에 따라 1 또는 0으로 결정되게 된다.

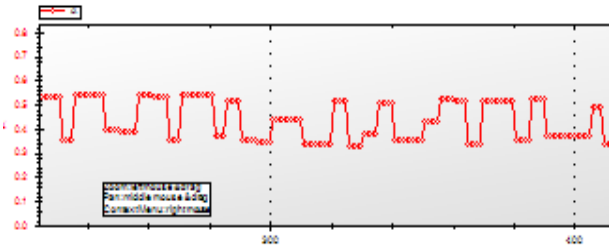

그림 4 센서로부터 수집된 데이터의 분석
Fig. 4 Analysis of received values

3. 실험 및 결과

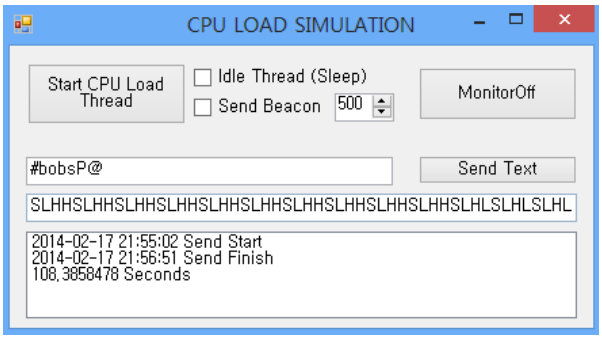

그림 5 송신모듈을 통한 데이터 전송
Fig. 5 Sending to test data

본 실험에서는 '#bobsP@'라는 사용자의 비밀번호를 사전에 설치해둔 트로이안 목마와 키로거 등과 같은 해킹 툴을 이용해서 이미 획득하였다고 가정한 후 전송 실험을 수행하였다. 송신 문자열의 구분을 위하여 전송하고자 하는 본문 앞과 뒤에 각각 1Byte씩의 STX, ETX를 붙였기 때문에 송신되는 데이터는 9Byte로 구성된다. 통신상의 노이즈를 고려하여 안정적으로 송신하기 위하여 1.5초 당 1Bit를 송신하였으며 9 Byte를 송신하는데 약 108초가 소요되었다.

표 1 전류량의 변화 측정
Table 1 Received values

SEQ	Source	Value		
125	AC	0.517	A	AUTO
126	AC	0.517	A	AUTO
127	AC	0.517	A	AUTO
128	AC	0.336	A	AUTO
129	AC	0.336	A	AUTO
130	AC	0.336	A	AUTO
131	AC	0.336	A	AUTO
132	AC	0.336	A	AUTO
133	AC	0.521	A	AUTO
134	AC	0.521	A	AUTO
135	AC	0.521	A	AUTO
136	AC	0.521	A	AUTO
137	AC	0.521	A	AUTO

표 1과 같이 CPU의 변화에 따른 전류사용의 변화량을 수신모듈을 통하여 수집할 수 있었다. 전송시에는 1.5 초당 1Bit를 송신한 반면 수신모듈에서는 0.1초 단위로 전류량을 측정하였기 때문에 대략 14~17개의 데이터가 하나의 Bit를 의미한다.

수집된 데이터는 Analysis Module을 통하여 Transmitter Module에서 보내고자 하는 원문 '#bobsP@'을 복원하였다.

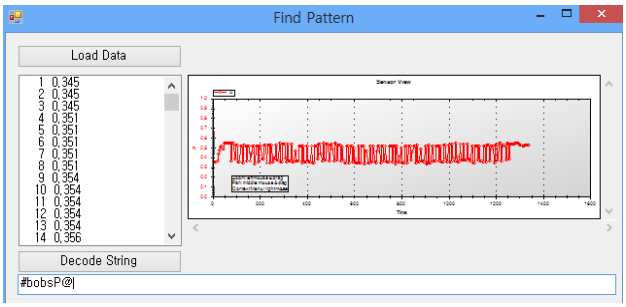

그림 6 분석 모듈
Fig. 6 Analysis module

그림 6은 수집된 데이터를 분석한 것으로 각각의 변화율 그래프는 아래의 그림7 과 같이 Bit에 따라 다른 형태를 갖게 된다.

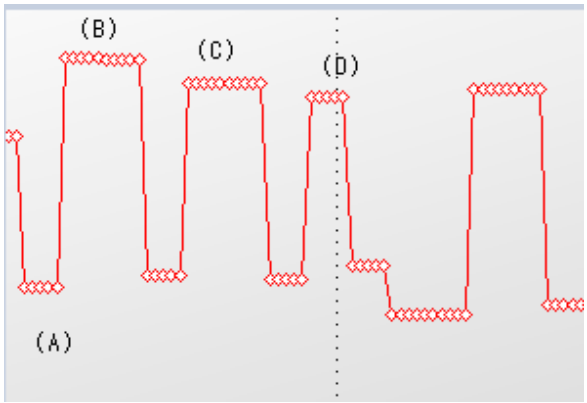

그림 7 전류 사용량 변화 패턴
Fig. 7 Finding Patterns on the Graph

그림7 의 (A) 지점과 같이 Rising되는 부분이 Bit의 시작을 뜻하며 이후 PWM방식으로 (B)와 (D) 지점과 같이 High Level의 Width로 1과 0으로 구분할 수 있다.

빠른 속도의 통신과 다양한 형태의 주변잡음 제거용 필터 등이 적용되지 않은 단순한 환경에서의 실험이었지만 물리적으로 독립시킨 컴퓨터에서 외부로 정보가 전달될 수 있는 가능성을 확인하였다. 특히 고성능의 CPU나 GPU가 더 큰

Power source를 필요로 하는 만큼 위의 방법이 보다 쉽게 사용될 수 있다.

실험한 속도이상으로 속도를 증가시킬 수 있지만 컴퓨터 하드웨어 자체의 Capacity 성분에 의하여 High와 Low의 Level 차이가 선명하지 않게 된다. High와 Low의 Level 차이가 선명하지 않은 경우 다양한 형태의 filter를 적용하여 노이즈를 제거하여야 하며, 노이즈를 제거하였다 하더라도 원거리 통신에는 어려움이 있을 것이다.

4. 결 론

주변 전자기기와 컴퓨터 내부의 부품 등에서 발생하는 다양한 노이즈 신호를 제거하기 위한 특별한 필터 없이 실험을 진행하였기 때문에 느린 속도로 실험을 수행하였다. 본 논문은 서버가 물리적으로 분리된 오프라인 상태에서 컴퓨터 내 비밀 정보의 유출 가능성 여부를 판단하기 위한 실험으로 결과는 느린 속도와 짧은 거리 일지라도 물리적으로 격리된 컴퓨터로부터 비밀 정보가 유출될 수 있음을 확인하였다. 특히, CPU와 GPU가 고성능 일수록 소모되는 전력이 크기 때문에 소프트웨어로 CPU 또는 GPU를 제어하여 전력 사용의 변화량을 보다 크게 할 수 있었다.

실사용에서는 다양한 형태의 알고리즘과 필터를 적용하여 통신 속도를 높인다고 하더라도 UPS 및 AVR 장비, 주변 변압기 등으로 인해 장거리 송신에는 어려움이 있을 것으로 예상된다. 하지만 이 실험을 통해 중요한 정보가 물리적으로 격리된 컴퓨터에서 외부로 유출될 가능성을 확인한 것과 같이 앞으로 이와 비슷한 다양한 공격방법이 출현될 수 있으므로 보안 시스템 설계자나 관리자는 향후 보안 시스템을 설계할 때 네트워크 보안을 고려하는 것과 같이 전력 시스템에 대한 보안 조치를 함께 고려할 경우 보다 안전한 보안 시스템을 구축할 수 있을 것이다.

References

[1] Kyong-Ho Han and Ha-Yoon Hwang, “Implementation of Dual Voltage Level DC Power Line Communication Driver for Multiple Access Serial Bidirectional Communication” Journal of the Korean Institute of IIluminating and Electrical Installation Engineers Vol. 23, No.10, pp. 29~35 October 2009.

[2] Kyong-Ho Han “Coding Method of Variable Threshold Dual Rate ADPCM Speech Considering the Background Noise” Journal of the korean institute of llluminating and Electrical installation Engineers Vol, 17.No 6,pp. 154~159 September 2003.

[3] Seong-hee Park, Kee-Joe Lim, Kil-Sou Kim and Seong-Hwa Kang, “Output Characteristics of Current Sensor and Voltage Sensor Built in Epoxy Spacer” Trans. KIEE Vol 56, No 2, FEB 2007

[4] Lennar Ljung, “Black box model from input output measurement.” 18Th IEEE Instrumentation and Measurement Technology Conference, Budapest, Hungary ,2001:21-23

[5] Nannan Yan, Zhengcai Fu, “The Impact of Current-carrying Bus Decentration and Inclination on Impulse Current Measurement by Large Size Rogowski Coils” 2012 International Conference on High Voltage Engineering and Application, Shanghai, China, September 17-20, 2012

[6] Qizhi Tian, Sorin A. Huss, “On the Attack of Misaligned Traces by Power Analysis Methods” ICCES Seventh Internation Conference on, Nov, 2012

[7] Microsoft MSDN Web Page: http://blogs.msdn.com/b/ie/archive/2011/03/28/browser-power-consumption-leading-the-industry-with-internet-explorer-9.aspx.

저 자 소 개

한 경 호(Kyong-Ho Han)

1984년 서울대학교 대학원 전자공학과 (석사). 1992년 미국 Texas A&M University, College Station (PhD). 1984~1985년 삼성휴렛팩커드 연구원. 1985~1987년 한국통신 전임연구원. 1989~1992년 Texas A&M University, Unix System Administrator & Network Analysist,
1992~1993년 한국전자통신연구원 이동통신 연구단 CDMA 개발 선임 연구원.
1993~현재 단국대학교 전자전기공학부 교수
관심분야 : 마이크로프로세서 및 Arm기반 Application, ITS, F/A System, 네트워크 통신

이 성 호(Seong-Ho Lee)

2012년 단국대학교 정보통신 학과 (공학석사), 2012~현재 단국대학교 전자전기공학과 박사과정
관심분야 : 소프트웨어 및 하드웨어 보안, Arm기반 Application, IoT Device 및 통신