https://kiisc.or.kr

2022년 한국정보보호학회 동계학술대회

CISC-W'22

Conference on Information Security and Cryptography-Winter 2022

2022년 11월 26일 (토) | 국민대학교

- 학술대회 등록대: 미래관 자율주행 스튜디오 (4층)
- 개회식/정기총회: 본부관 (1층)

Proceedings

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology

주관 KMU 국민대학교 KOOKMIN UNIVERSITY

후원 국가정보원 NATIONAL INTELLIGENCE SERVICE, 과학기술정보통신부, 행정안전부, KISA 한국인터넷진흥원, ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute, NSR 국가보안기술연구소 National Security Research Institute, KiSTi 한국과학기술정보연구원 Korea Institute of Science and Technology Information www.kisti.re.kr, 지란지교시큐리티, PILAB

한국정보보호학회
Korea Institute of Information Security & Cryptology

전력 패턴 유사성 기반 Geo-Location 인증 시스템 설계

정혜림*, 박기웅†

* 세종대학교 시스템보안연구실 대학원생 (지능형드론 융합전공)

† 세종대학교 정보보호학과

Design and implementation of Geo-Location authentication system based on power pattern similarity

HyeLim Jung*, Ki-Woong Park

* SysCore Lab. (Convergence Engineering for Intelligent Drone), Sejong University
† Department of Computer and Information Security, Sejong University

요 약

IT 기술 발전으로 다양한 IT 시스템을 구축한 기업들이 발전하였으며, 기업 내부에서 발생하는 산업기밀정보를 유출하는 사건들이 발생하였다. 이를 위한 보안체계는 이전부터 발전되어왔으며 보안 기술로 핵심기밀정보인 문서나 프로그램을 사용하는 데에 제한을 두는 방식이 존재한다. 문서 열람이나 프로그램 사용을 위해 인증을 요구하는 보안 프로그램들이 존재하며 본 논문에서는 이러한 보안체계의 인증값으로 기업 내에서 공급되는 전력망을 통해 인증을 수행한다. 기업 내 건물에 설비된 전력망에 연결된 PC는 공급되는 전력망이 가진 전력 패턴과 유사한 전력 패턴을 PC 내 하드웨어에서 측정하고 유사도를 통해 해당 PC가 기업 내 건물에서 지리적으로 사용되는 것을 인증할 수 있다. 전기적 패턴으로 발생할 수 있는 전력 패턴은 깜빡임이나 순간 전압 상승, 순간 정전 등이 있을 수 있다. 이러한 패턴은 인증값으로 사용하였을 때, 반복할 수 없는 유일성을 가지게 되며 지리적인 특징을 가지고 있기 때문에 위치를 특정할 수 있다.

I. 서론

최근 다양한 분야에서 IT 기술이 접목되면서 IT 서비스를 제공하는 기업들이 다양해졌다. 또한, 하나의 IT 서비스에도 다수의 기업들이 보다 발전된 IT 기술 제공을 위하여 기술 개발 연구를 수행해왔다. 이러한 핵심 기술 연구는 기업의 자산이 되며 산업기밀정보로 정의될 수 있다. 산업기밀정보는 IT 산업 활동에 있어 활용될 수 있는 모든 정보, 인력, 문서, 프로그램이 해당한다[1]. 이러한 산업기밀정보는 이를 노리는 많은 위협이 존재하며 이러한 위협들은 기업 외부 및 내부에서도 발생할 수 있다. 국내에서 발생한 기업 내부에서 해외로 산업기밀정보를 유출한 건수는 2016~2021년 사이에 총 111건으로 피해 예방액은 21조 원으로 예측하였다[2]. 이러한 위협으로부터 산업기밀정보를 보호하기 위한 보안 기술들도 발전되었다.

기업 내부 산업기밀정보를 유출하는 방법은 다양하였으며, 이에 따라 기업 내부 핵심정보 보호 기술들이 발전하였다[3]. 기업 내부에서 핵심정보 유출 방법으로는 기업 내부에서 수행한 프로젝트에서 필요한 자료를 메일 전송과 같은 네트워크를 통한 유출 또는 저장매체에 저장하여 외부로 전달하는 유출이 있었으며, 기업 내 주요 기능을 수행할 수 있는 노트북을 외부로 유출하여 기업 내 핵심정보를 유출하는 방법들이 존재하였다. 기업 내 주요 문서를 외부로 유출하거나 기업 외부에서 프로그램 사용을 막기 위한 방법으로 다음과 같은 방법을 수행해왔다. 기업 내 출입 시에 PC 및 저장매체 반입 제한을 위해 소지품을 확인하거나 기업 외부에서 문서 및 프로그램의 사용을 제한하기 위해 인증 및 사용처 분석을 수행하였다.

다양한 산업기밀정보 보호를 위한 기술들은 고도화되는 유출 기법을 막기 위해 보다 발전하고 있으며, 본 논문에서 제안하는 기술은 기업 외부에서 문서 및 프로그램 사용을 제한하기 위한 인증 기술을 제안한다. 본 논문에서 제안하는 기술은 기업의 건물 내에 구축된 IT 시스템에서 사용하는 전력을 측정하며 PC 내 부착된 하드웨어(스토리지 및 CPU)에서 사용된 전류 패턴을 측정한다. 해당 측정값을 통해 PC가 연결된 사내 망에 공급되는 전력원임을 패턴을 확인하여 해당 PC가 지리적으로 특정 영역에서 수행됨을 확인하여 기업 외부에서 사용되는 것을 방지할 수 있다. 해당 전력원에서 발생하는 미세한 전류 특징을 통해 유사도를 측정하며 미세한 전류 특징으로는 전력원에서 발생하는 전력 깜빡임이나 순간 전압 상승, 순간 정전과 같은 공급되는 전기적 특징을 통해 인증 패턴을 생성하는 것이다. 이러한 전력 패턴은 건물에서 발생하는 패턴을 측정하고 공급되는 전력에 연결된 PC에서 패턴을 측정하기 때문에 인증값이 유일성을 가진다. 기업 내부에서만 접근할 수 있도록 하는 것에 목적으로 두고 있으며, 전기적 특성과 지리적 특성을 이용하여 이를 인증 수단으로 사용한다.

본 논문의 구성은 다음과 같다. 2장에서 기존에 사용되는 사내 기술 유출 방지 기법들과 본 논문에서 제안하는 인증 시스템의 주요 핵심인 전력 분석을 통해 정보를 분석하는 부채널 기법에 관해 설명한다. 3장에서는 본 논문에서 제안하는 인증 시스템의 구동을 위한 환경 구성과 설계 및 구동에 관해 설명한다. 4장에서는 본 논문의 결론으로 인증 시스템의 적용 방안과 확장 방안에 관해 서술한다.

II. 관련 연구

본 논문에서 제안하는 인증 시스템은 기업 내부 핵심정보 유출로부터 보호하기 위해 제안한 인증 시스템으로 PC에서 사용하는 전력 패턴을 분석하여 정보를 취득하는 부채널 기술을 통해 PC의 지리적 위치를 특정하는 인증 시스템이다. 본 장에서는 이러한 관련 기술들에 관해 설명한다.

2.1 사내 정보 유출 방지 기법

기술 경쟁력이 강화되면서 사내 핵심정보 유출 문제가 심각해지고 있으며 기술이 유출된 중소기업의 피해를 막기 위해 2022년 국가에서 '중소기업 기술유출방지 시스템 구축사업'을 시작하였다[4]. 해당 시스템에서 제공하는 시스템으로는 네트워크 정보 유출 모니터링, PC 정보보안 기술, FACE aiDee가 있다. 네트워크 정보 유출 모니터링은 네트워크를 모니터링하여 인터넷에서 전송되는 문서를 기록하고 유출을 방지하는 기술이다. PC 보안 기술은 PC 내 저장된 파일을 모니터링하여 저장매체에 저장된 문서를 차단하는 기능이 포함되어있다. FACE aiDee는 인공지능 기반의 얼굴인식 서비스로 얼굴 확인으로 출입통제 본인확인을 수행한다. 그 외에 사내 정보 유출 방지 기술로 노트북 반·출입을 관리하는 시스템으로 노트북 내 파일 변화를 감지하거나 파일 유입/유출을 검사하는 시스템이 있다.

본 논문에서 제안하는 인증 시스템은 사내 정보 유출 방지 시스템의 하나로써 주요 문서 및 프로그램이 실행되는 PC가 사내 전력망에 연결되어 수행되는지를 검사하여 지리적으로 외부 반출을 금지한다. 또한, 이 기술은 문서 열람 시에도 지리적 위치를 확인할 수 있으며 인증값으로 적용되는 전력 패턴이 사내 전력망에서 생산된 전력임을 확인하기 때문에 복제 불가능한 인증값으로 유일성을 가질 수 있다.

2.2 부채널 기술

부채널 기술은 PC에 부착된 하드웨어들이 동작할 때 사용하는 전기 패턴이나 전자파, 타이밍 등에서 유추할 수 있는 신호들을 분석하여 정보를 취득하는 기술이다[5]. 부채널 기술로는 CPU가 연산을 수행하는데 걸린 시간을 측정하여 암호문을 유추하거나 하드웨어 장치가 매 순간 전력을 사용하는 것을 모니터링하여 전력 변화를 기반으로 분석하는 기법이 있다. 전자파를 분석하는 부채널 기술은 컴퓨터 화면에서 발생하는 전자파를 분석하여 정보를 유추하는 기술로 화면으로 출력되는 것을 유추하는 기술이다. 이 외

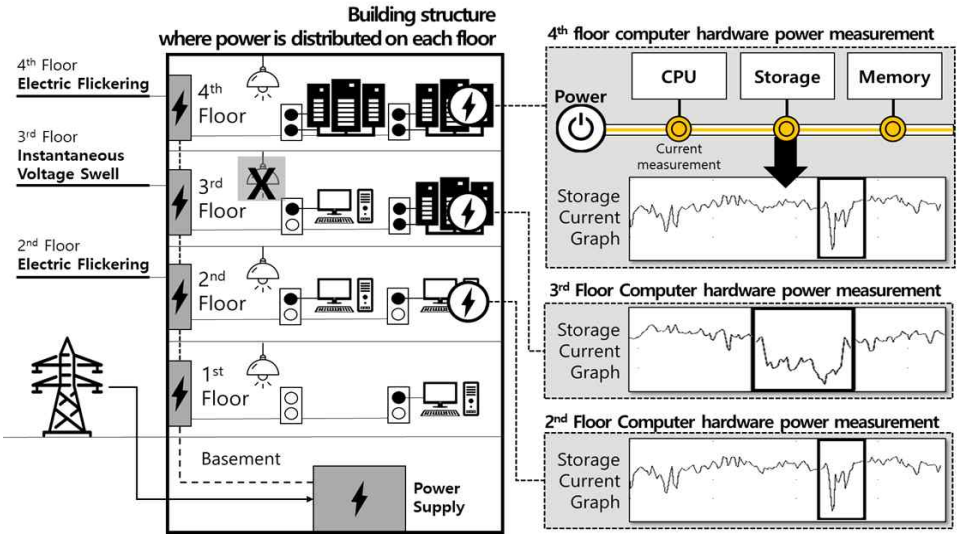

그림 1. 전력 패턴 유사성 기반 Geo-Location 인증 시스템 수행 환경 구성

에도 컴퓨터가 연산하는 과정에서 발생하는 소리나 빛을 통해 분석하여 정보를 유추하는 부채널 기술들도 존재한다. 이러한 부채널 기술을 통해서 컴퓨터가 수행하고 있는 행위 및 데이터를 유추할 수 있다. 본 논문에서 제안하는 시스템은 사내 전력망과 PC를 연결하고 해당 전력의 특정 패턴을 발생시켰을 때 이 PC에서도 발생하는지를 확인하여 인증하는 시스템이다.

III. 전력 패턴 유사성 기반 Geo-Location 인증 시스템

3.1 인증 시스템 환경 구성

본 논문에서 제안하는 인증 시스템은 사내망에 구성된 전력망을 대상으로 하며 그림 1과 같은 구성으로 인증 시스템 수행 환경을 제안하고 있다. 본 논문에서 제안하는 의 동작을 위해서는 그림 1과 같이 층마다 전력망을 배치하면 각 층에서 발생하는 전력 패턴이 다를 경우에 지역마다 발생하는 전력 패턴으로 지역을 구분할 수 있다. 그림 1에서와같이 2층과 4층에 발생하는 전력 패턴과 3층에서 발생한 전력 패턴이 다른 경우를 예를 들 수 있다. 전력이 다르게 발생할 수 있는 것으로는 전기적 플리커(깜빡임)이나 단시간 정전이나 순간 전압 상승/강하 등이 있을 수 있다.

CPU나 스토리지, 메모리에 공급되는 전력은 전력 품질 개선을 위한 기술들이 많이 연구되고 있다. 따라서 본 논문에서는 컴퓨터 내 하드웨어 소자들에서 측정하는 것을 제안하지만 하드웨어 성능에 따라서 컴퓨터 전력 공급원에서 측정해야 하는 상황도 고려하고 있다. 또한, 부채널 분석에 있어 특정 패턴을 탐지하는 데에도 있어 완전한 전력 패턴 일치보다 유사도를 측정하는 데에 초점을 맞추고 있다. 해당 컴퓨터에서 동작하는 연산에 따라서 전력 소모량이 변동되기 때문에 특정 시간에 발생하는 특정 전력 패턴을 함께 계산해야 한다. 이에 있어 기존의 부채널 기법은 전력 분석으로 정보를 취득하는 것에 목적을 두고 있지만 본 논문에서는 전력의 패턴 유사도를 측정하여 일부 구간이 일치함으로 인증값을 사용하고 있다. 하지만 인증값으로 사용하기에 있어 이는 전력 이벤트 발생 시간과 전력 이벤트에 의해 발생하는 전압 크기에 따라 미세하면서도 깊이 있는 분석이 필요로 한다.

3.2 인증 시스템 수행 과정

본 논문에서 제안한 환경에서 인증 시스템을 수행하기 위해서는 표본이 되는 각 층의 컴퓨터에서 전력 분석을 수행해야 한다. 그림 2에서와 같이 3층에서 발생한 전력 이벤트에 따른 전력 패턴을 비교할 수 있다. PC 3의 사용자가

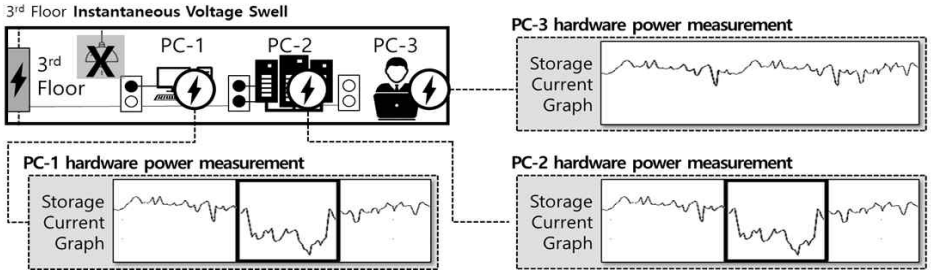

그림 2. 전력 패턴 유사성 기반 Geo-Location 인증 시스템의 인증 과정

본 건물에 전력원을 연결하지 않았을 때 발생하는 전력 패턴이 3층에 연결된 PC-1과 PC-2에서 발생한 전력 패턴이 다름을 통해서 지리적 인증을 수행할 수 없게 된다. 전력을 분석하기 위해서는 PC 내부 하드웨어로부터 전력을 측정하며 컴퓨터 하드웨어에서 제공하는 센서를 통해 값을 측정할 수 있다.

이 외에도 특정 PC가 기업 내 건물 전력망에 연결된다면 해당 PC가 어떤 층에 연결되었는지도 확인이 가능해진다. 또한, 인증 시스템 구동 환경을 건물이 아닌 물리적으로 거리가 있는 전력망에 구성한다고 하여도 표본 PC의 전력과 연결된 PC의 전력 패턴을 비교하여 해당 전력망이 배치된 지리적 위치 추정 및 인증을 수행할 수 있다.

IV. 결론

본 논문에서는 산업기밀정보 유출을 막기위한 인증 시스템을 제안하였으며, 해당 인증 시스템은 핵심기밀정보인 문서나 프로그램을 사용하는 데에 제한을 두는 방식을 제안한다. 문서 열람이나 프로그램 실행을 요청하는 PC가 인증값으로 기업 내에서 공급되는 전력망을 통해 인증을 수행한다. 기업 내 건물에 설비된 전력망에 연결된 PC는 공급되는 전력망이 가진 전력 패턴과 유사한 전력 패턴을 PC 내 하드웨어에서 측정하고 유사도를 통해 해당 PC가 기업 내 건물에서 지리적으로 사용되는 것을 인증할 수 있다. 전기적 패턴은 인증값으로 사용하였을 때, 반복할 수 없는 유일성을 가지게 되며 특정 전력원에서 발생하는 이벤트와 이벤트 발생 타이밍에 따라 전력원으로부터 전력을 공급받는 것으로 지리적으로 특정할 수 있다. 전력 분석을 수행하는 과정에서 기존의 부채널 기법이 정보를 유추하는 것과 같이 정밀한 분석이 필요하다. 컴퓨터 내에서 추가적으로 수행하는 연산이 있을 수 있으므로 정확한 패턴 일치보다 유사도를 인증값으로 사용한다. 또한, 본 논문에서 제안하는 인증 시스템은 기업 내 건물의 전력망을 대상으로 환경 구성을 하였지만 보다 넓은 지리적 위치도 특정 이벤트를 발생하는 전력원과 해당 망에 연결된 표본 PC의 전력 패턴을 분석하면 위치를 특정할 수 있을 것으로 기대한다.

Acknowledgement

본 연구는 2020년 국방과학연구소에서 주관하는 미래도전국방기술 연구개발사업(UD210029TD)의 지원을 받아 수행되었습니다.

[참고문헌]

[1] 장항배. 산업기밀 유출사고 사례분석을 통한 유형별 대응방안 연구. 융합보안논문지, 15.7: 39-45. 2015,

[2] 윤홍우, 국가 핵심 기술 유출만 35만건, 피해 규모 최소 21조 달해, 자료: 국가정보원, 서울경제, 2021.07.

[3] 차종환, 영업비밀 • 사내정보 PC 유출 “꼼짝마”, 정보통신신문, 2021.03.

[4] 중소벤터기업부장관, 2022년 기술유출방지시스템 구축사업, 2022.02.

[5] CHOE, Du-Ho; CHOE, Yong-Je. 보안 칩에서 중요 키의 공격 (부채널 공격 중심) 기술 동향. The Magazine of the IEIE, 43.7: 52-58. 2016,