



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0095704
(43) 공개일자 2017년08월23일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) G06F 21/60 (2013.01)
G06F 3/12 (2017.01)
(52) CPC특허분류
H04L 63/1433 (2013.01)
G06F 21/608 (2013.01)
(21) 출원번호 10-2016-0023048
(22) 출원일자 2016년02월26일
심사청구일자 2016년02월26일
(30) 우선권주장
1020160016899 2016년02월15일 대한민국(KR)

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
원유재
경기도 성남시 분당구 미금로 215, 813동 1901호
(금곡동, 청솔마을대원아파트)
김준희
대전광역시 유성구 유성대로821번길 14-17, 101호(장대동)
오재근
대전광역시 대덕구 계족로663번길 23, 5동 106호(법동, 유원아파트)
(74) 대리인
특허법인 공간

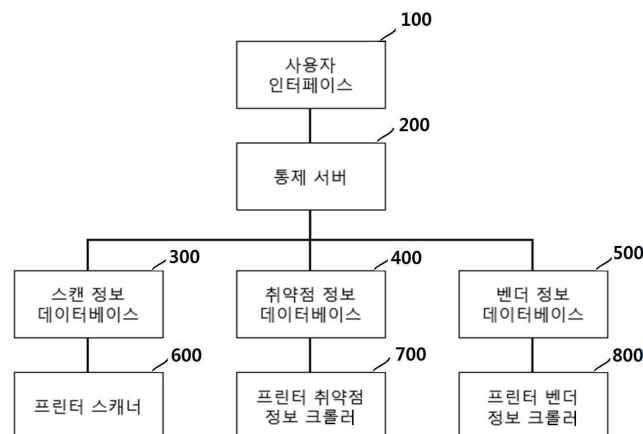
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 네트워크 프린터의 취약점 점검 방법 및 시스템

(57) 요약

본 발명은 네트워크 프린터의 포트 정보를 이용한 취약점 점검 방법 및 시스템에 관한 것으로서, 사용자인터페이스, 통제 서버, 스캔 정보 데이터베이스, 취약점 정보 데이터베이스, 벤더 정보 데이터베이스, 프린터 스캐너, 프린터 취약점 정보 크롤러, 프린터 벤더 정보 크롤러로 구성되며, 프린터의 열린 포트를 스캔하고 프린터의 취약점 정보와 벤더 정보를 수집하여 프린터에 대한 취약점과 패치 정보를 확인한다.

대표도 - 도1



(52) CPC특허분류

G06F 3/1222 (2013.01)

H04L 63/1441 (2013.01)

H04L 63/16 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 R2215-15-1001

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보통신기술인력양성

연구과제명 2015년 SW중심대학(ICT/SW창의연구과정)_충남대

기 여 율 1/1

주관기관 충남대학교

연구기간 2015.10.01 ~ 2016.02.29

명세서

청구범위

청구항 1

사용자의 입력을 받아 프린터에 대한 취약점 관련 정보를 보여주는 사용자인터페이스(100);

통제 서버(200);

스캔 정보 데이터베이스(300);

취약점 정보 데이터베이스(400);

벤더 정보 데이터베이스(500);

를 포함하고,

상기 통제 서버(200)는, 사용자 인터페이스(100)에서 사용자 입력을 전달 받아 필요한 스캔 정보를 스캔 정보 데이터베이스(300)에서 전송받고, 이와 관련된 취약점 정보와 벤더 정보를 취약점 정보 데이터베이스(400)와 벤더 정보 데이터베이스(500)에서 전송받아 취합한 후 사용자 인터페이스(100)로 전달하는 것을 특징으로 하는 네트워크 프린터의 취약점 점검 시스템.

청구항 2

청구항 1에 있어서,

프린터의 사용중인 포트 정보를 수집하고 수집한 정보를 스캔 정보 데이터베이스(300)에 전송하여 저장하도록 하는 프린터 스캐너(600)를 추가적으로 더 포함하는 것을 특징으로 하는 네트워크 프린터의 취약점 점검 시스템.

청구항 3

청구항 1에 있어서,

기존에 존재하는 프린터의 펌웨어, 프로토콜의 취약점 정보를 수집하여 취약점 정보 데이터베이스(400)에 전송하여 저장하도록 하는 프린터 취약점 정보 크롤러(700)를 추가적으로 더 포함하는 것을 특징으로 하는 네트워크 프린터의 취약점 점검 시스템.

청구항 4

청구항 1에 있어서,

제조사 별 프린터에 사용된 소프트웨어들의 패치 정보를 수집하여 벤더 정보 데이터베이스(500)에 전송하여 저장하도록 하는 프린터 벤더 정보 크롤러(800)를 추가적으로 더 포함하는 것을 특징으로 하는 네트워크 프린터의 취약점 점검 시스템.

청구항 5

사용자인터페이스(100), 통제 서버(200), 스캔 정보 데이터베이스(300), 취약점 정보 데이터베이스(400), 벤더 정보 데이터베이스(500), 프린터 스캐너(600), 프린터 취약점 정보 크롤러(700), 프린터 벤더 정보 크롤러(800)를 포함하는 취약점 점검 시스템을 이용한 네트워크 프린터의 취약점 점검 방법에 있어서,

프린터 스캐너(600)에서 수집한 정보를 스캔 정보 데이터베이스(400)에 저장하는 스캔 정보 데이터베이스 저장 단계;

프린터 취약점 정보 크롤러(700)에서 수집한 정보를 취약점 정보 데이터베이스(400)에 저장하는 취약점 정보 데이터베이스 저장 단계;

프린터 벤더 정보 크롤러(800)에서 수집한 정보를 벤더 정보 데이터베이스(500)에 저장하는 벤더 정보 데이터베이스

이스 저장 단계;

상기 통제 서버(200)가, 사용자 인터페이스(100)에서 사용자 입력을 전달 받아 필요한 스캔 정보를 스캔 정보 데이터베이스(300)에서 전송받고, 이와 관련된 취약점 정보와 벤더 정보를 취약점 정보 데이터베이스(400)와 벤더 정보 데이터베이스(500)에서 전송받아 취합한 후 사용자 인터페이스(100)로 전달하는 단계;를

포함하는 것을 특징으로 하는 네트워크 프린터의 취약점 점검 방법.

청구항 6

청구항 5에 있어서,

상기 스캔 정보 데이터베이스 저장 단계는,

호스트 스캔 단계, 호스트 존재 여부 판단 단계, 포트 스캔 단계, 호스트가 프린터인지 여부의 판단 단계, 펌웨어 및 프로토콜 버전 탐지 단계, 데이터베이스 저장 단계를 포함하는 것을 특징으로 하는 네트워크 프린터의 취약점 점검 방법.

청구항 7

청구항 5에 있어서,

상기 취약점 정보 데이터베이스 저장 단계는,

취약점 크롤링 단계, 프린터 관련 취약점 판별 단계, 취약점 정보 크롤링 단계, 취약점 번호, 원인, 영향 등 취약점 정보 탐지 단계, 데이터베이스 저장 단계를 포함하는 것을 특징으로 하는 네트워크 프린터의 취약점 점검 방법.

청구항 8

청구항 5에 있어서,

상기 벤더 정보 데이터베이스 저장 단계는,

패치 정보 리스트 확인 단계, 새로운 패치 존재 여부 판별 단계, 패치 정보 크롤링 단계, 취약한 펌웨어 버전, 패치 된 버전 등 패치 정보 탐지 단계, 데이터베이스 저장 단계를 포함하는 것을 특징으로 하는 네트워크 프린터의 취약점 점검 방법.

발명의 설명

기술 분야

[0001] 본 발명은 네트워크 프린터의 포트 정보를 이용한 취약점 점검 방법 및 시스템에 관한 것이다.

배경 기술

[0002] 기업, 공공기관, 가정에서는 효율적인 자원 관리와 편리한 이용을 위해 프린터를 인터넷에 연결하여 사용하고 있다. 하지만 인터넷에 연결된 네트워크 프린터는 사용자들이 인지하지 못하는 다양한 펌웨어와 프로토콜에 대한 보안 취약점들이 존재한다. 이러한 펌웨어와 프로토콜의 취약점을 이용하면 프린터의 환경을 통제할 수 있고 출력하는 문서를 가로챌 수도 있으며 프린터가 포함된 네트워크를 공격하기 위한 경유지로 프린터를 활용할 수도 있다. 즉, 프린터의 취약점으로 인해 기업과 공공기관의 기밀문서나 개인의 중요 정보가 외부로 유출되고, 최악의 경우 네트워크망 전체가 공격당할 수 있는 것이다. 사용자는 펌웨어와 프로토콜에 존재하는 취약점으로 인해 다양한 보안 위협에 노출되어 있음에도 불구하고 자신이 노출된 취약점에 대하여 인지하지 못하여 적절한 대응을 하기 어렵다.

[0003] 특허문헌 1(KR 10-1535622 B1)에서는 공용 프린터 보안 시스템 및 보안 방법을 개시하고 있지만, 이 기술만으로는 네트워크 프린터의 취약점과 패치 정보를 확인하기 어렵다.

선행기술문헌

특허문헌

[0004] (특허문헌 0001) 개인 인증과 암호화 및 복호화를 적용한 공용 프린터 보안 시스템, 그리고 이를 이용한 공용 프린터 보안 방법(등록번호: KR 10-1535622 B1, 등록일:2015. 7. 3.)

발명의 내용

해결하려는 과제

[0005] 본 발명은 사용자가 네트워크 프린터의 취약점과 패치 정보를 용이하게 확인하는 것을 목적으로 한다.

과제의 해결 수단

[0007] 본 발명에 의한 네트워크 프린터의 취약점 점검 시스템은, 사용자의 입력을 받아 프린터에 대한 취약점 관련 정보를 보여주는 사용자인터페이스(100); 통제 서버(200); 스캔 정보 데이터베이스(300); 취약점 정보 데이터베이스(400); 벤더 정보 데이터베이스(500);를 포함하고, 상기 통제 서버(200)는, 사용자 인터페이스(100)에서 사용자 입력을 전달 받아 필요한 스캔 정보를 스캔 정보 데이터베이스(300)에서 전송받고, 이와 관련된 취약점 정보와 벤더 정보를 취약점 정보 데이터베이스(400)와 벤더 정보 데이터베이스(500)에서 전송받아 취합한 후 사용자 인터페이스(100)로 전달하는 것을 특징으로 한다.

[0008] 상기 취약점 점검 시스템은, 프린터의 사용중인 포트 정보를 수집하고 수집한 정보를 스캔 정보 데이터베이스(300)에 전송하여 저장하도록 하는 프린터 스캐너(600)를 추가적으로 더 포함할 수 있다.

[0009] 상기 취약점 점검 시스템은, 기존에 존재하는 프린터의 펌웨어, 프로토콜의 취약점 정보를 수집하여 취약점 정보 데이터베이스(400)에 전송하여 저장하도록 하는 프린터 취약점 정보 크롤러(700)를 추가적으로 더 포함할 수 있다.

[0010] 상기 취약점 점검 시스템은, 제조사 별 프린터에 사용된 소프트웨어들의 패치 정보를 수집하여 벤더 정보 데이터베이스(800)에 전송하여 저장하도록 하는 프린터 벤더 정보 크롤러(800)를 추가적으로 더 포함할 수 있다.

[0011] 본 발명에 의한 네트워크 프린터의 취약점 점검 방법은, 사용자인터페이스(100), 통제 서버(200), 스캔 정보 데이터베이스(300), 취약점 정보 데이터베이스(400), 벤더 정보 데이터베이스(500), 프린터 스캐너(600), 프린터 취약점 정보 크롤러(700), 프린터 벤더 정보 크롤러(800)를 포함하는 취약점 점검 시스템을 이용한 네트워크 프린터의 취약점 점검 방법에 있어서, 프린터 스캐너(600)에서 수집한 정보를 스캔 정보 데이터베이스(400)에 저장하는 스캔 정보 데이터베이스 저장 단계; 프린터 취약점 정보 크롤러(700)에서 수집한 정보를 취약점 정보 데이터베이스(400)에 저장하는 취약점 정보 데이터베이스 저장 단계; 프린터 벤더 정보 크롤러(800)에서 수집한 정보를 벤더 정보 데이터베이스(500)에 저장하는 벤더 정보 데이터베이스 저장 단계; 상기 통제 서버(200)가, 사용자 인터페이스(100)에서 사용자 입력을 전달 받아 필요한 스캔 정보를 스캔 정보 데이터베이스(300)에서 전송받고, 이와 관련된 취약점 정보와 벤더 정보를 취약점 정보 데이터베이스(400)와 벤더 정보 데이터베이스(500)에서 전송받아 취합한 후 사용자 인터페이스(100)로 전달하는 단계;를 포함하는 것을 특징으로 한다.

[0012] 상기 스캔 정보 데이터베이스 저장 단계는, 호스트 스캔 단계, 호스트 존재 여부 판단 단계, 포트 스캔 단계, 호스트가 프린터인지 여부의 판단 단계, 펌웨어 및 프로토콜 버전 탐지 단계, 데이터베이스 저장 단계를 포함할 수 있다.

[0013] 상기 취약점 정보 데이터베이스 저장 단계는, 취약점 크롤링 단계, 프린터 관련 취약점 판별 단계, 취약점 정보 크롤링 단계, 취약점 번호, 원인, 영향 등 취약점 정보 탐지 단계, 데이터베이스 저장단계를 포함할 수 있다.

[0014] 상기 벤더 정보 데이터베이스 저장 단계는, 패치 정보 리스트 확인 단계, 새로운 패치 존재 여부 판별 단계, 패치 정보 크롤링 단계, 취약한 펌웨어 버전, 패치 된 버전 등 패치 정보 탐지 단계, 데이터베이스 저장 단계를 포함할 수 있다.

발명의 효과

[0015] 네트워크 프린터의 사용자는 보안 사고가 발생하기 이전에 자신이 사용하는 프린터의 취약점을 발견하고 취약한 부분에 대한 보완을 하여 보안을 강화 할 수 있다.

도면의 간단한 설명

- [0016] 도 1은 본 발명에 의한 시스템의 구성도
 도 2는 사용자 인터페이스의 블록도
 도 3은 통제 서버의 블록도
 도 4는 스캔 정보 데이터베이스의 블록도
 도 5는 취약점 정보 데이터베이스의 블록도
 도 6은 벤더 정보 데이터베이스의 블록도
 도 7은 프린터 스캐너의 블록도
 도 8은 프린터 취약점 정보 크롤러의 블록도
 도 9는 프린터 벤더 정보 크롤러의 블록도
 도 10은 프린터 스캐너 동작의 흐름도
 도 11은 프린터 취약점 정보 크롤러 동작의 흐름도
 도 12는 프린터 벤더 정보 크롤러 동작의 흐름도
 도 13은 프린터 취약점/패치 정보 검색 동작의 흐름도

발명을 실시하기 위한 구체적인 내용

- [0017] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변환, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.
- [0018] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다.
- [0020] 도 1은 본 발명에 의한 시스템의 구성도이다.
- [0021] 본 발명의 시스템은 사용자인터페이스(100), 통제 서버(200), 스캔 정보 데이터베이스(300), 취약점 정보 데이터베이스(400), 벤더 정보 데이터베이스(500), 프린터 스캐너(600), 프린터 취약점 정보 크롤러(700), 프린터 벤더 정보 크롤러(800)로 구성된다.
- [0023] 사용자 인터페이스(100)는, 사용자의 입력을 받아 프린터에 대한 취약점 관련 정보를 보여주는 장치이다.
- [0024] 통제 서버(200)는, 사용자 인터페이스(100)에서 사용자 입력을 전달 받아 필요한 스캔 정보를 스캔 정보 데이터베이스(300)에서 전송받고, 이와 관련된 취약점 정보와 벤더 정보를 취약점 정보 데이터베이스(400)와 벤더 정보 데이터베이스(500)에서 전송받아 취합한 후 사용자 인터페이스(100)로 전달하는 장치이다.
- [0025] 스캔 정보 데이터베이스(300)는, 프린터 스캐너(600)에서 주기적으로 스캔하여 얻은 정보를 저장/관리하며 통제 서버(200)로부터 정보 요청이 있을 경우 해당 정보를 전송해주는 장치이다.
- [0026] 취약점 정보 데이터베이스(400)는, 프린터 취약점 정보 크롤러(700)에서 기존에 존재하는 프린터의 펌웨어, 프로토콜의 취약점에 대해 수집한 정보를 저장/관리하며 통제서버로(200)부터 정보 요청이 있을 경우 해당 정보를 전송해주는 장치이다.
- [0027] 벤더 정보 데이터베이스(500)는, 프린터 벤더 정보 크롤러(800)에서 주기적으로 수집한 제조사 별 프린터에 사용된 소프트웨어들의 패치에 대해 정보를 저장/관리하며 통제서버(200)로부터 정보 요청이 있을 경우 해당 정보

를 전송해주는 장치이다.

- [0028] 프린터 스캐너(600)는, 주기적으로 IPv4 대역을 스캔하여 프린터의 사용중인 포트 정보를 수집하고 수집한 정보를 스캔 정보 데이터베이스(300)에 전송하여 저장하도록 하는 장치이다. 여기서의 포트는, 컴퓨터의 주변장치를 접속하기 위해 사용되는 연결 부분을 의미하는 것이 아니라, 통신을 위한 소프트웨어나 서비스의 논리적인 접속장소를 의미한다.
- [0029] 프린터 취약점 정보 크롤러(700)는, 주기적으로 기존에 존재하는 프린터의 펌웨어, 프로토콜의 취약점 정보를 수집하여 취약점 정보 데이터베이스(400)에 전송하여 저장하도록 하는 장치이다.
- [0030] 프린터 벤더 정보 크롤러(800)는, 주기적으로 제조사 별 프린터에 사용된 소프트웨어들의 패치 정보를 수집하여 벤더 정보 데이터베이스(800)에 전송하여 저장하도록 하는 장치이다.
- [0032] 도 2는 사용자 인터페이스의 블록도이다.
- [0033] 사용자 인터페이스(100)는 검색부(110), 출력부(120), 통신부(130)를 포함한다.
- [0034] 사용자 인터페이스(100)는, 모바일 애플리케이션, 웹 애플리케이션, PC 등 다양한 형태의 프로그램을 포함할 수 있고, 사용자로부터 검색어를 입력 받아 프린터의 취약점과 패치 정보를 출력하는 역할을 한다.
- [0035] 검색부(110)는, 사용자로부터 검색어를 입력 받는데, 검색어는 IP, IP대역, 제조사, 모델명, 특정 포트 등이 될 수 있다. 검색부(110)는 입력 받은 통신부(130)를 통하여 통제 서버(200)로 전달한다.
- [0036] 출력부(120)는, 통신부로부터 프린터의 취약점과 패치 정보를 전달 받아 화면을 통해 출력한다.
- [0037] 통신부(130)는, 검색부(110)를 통해 사용자로부터 입력 받은 검색어를 통제 서버(200)로 전송하는 역할과 통제 서버(200)로부터 전송 받은 프린터의 취약점과 패치 정보를 출력부(120)로 전달하는 역할을 한다.
- [0039] 도 3은 통제 서버의 블록도이다.
- [0040] 통제서버(200)는 통제부(210)과 통신부(220)를 포함한다.
- [0041] 통제부(210)는, 통신부(220)를 통해 사용자 인터페이스로부터 검색어를 전송 받고, 검색어를 이용하여 스캔 정보 데이터베이스(300)에 검색어에 해당하는 프린터 스캔 정보가 있는지 확인하기 위한 요청 메시지를 통신부(220)를 통해 스캔 정보 데이터베이스(220)에 전송한다. 스캔 정보 데이터베이스(300)로부터 스캔 정보를 전송 받으면 이와 관련된 취약점과 패치 정보를 요청하는 메시지를 통신부(220)를 통해 각각 취약점 정보 데이터베이스(400)와 벤더 정보 데이터베이스(500)에 전송한다. 그 후, 취약점 정보 데이터베이스(400)와 벤더 정보 데이터베이스(500)로부터 전송 받은 취약점과 패치 정보를 취합하여 통신부(220)를 통해 사용자 인터페이스(100)로 전송한다.
- [0042] 통신부(220)는, 통제부(210)에서 전달 받은 요청 메시지를 스캔 정보 데이터베이스(300), 취약점 정보 데이터베이스(400), 벤더 정보 데이터베이스(500)로 전송하고, 요청 메시지에 대한 응답을 전송 받아 통제부(210)로 전달한다.
- [0044] 도 4는 스캔 정보 데이터베이스의 블록도이다.
- [0045] 스캔 정보 데이터베이스(300)는 스캔 정보 관리부(310), 통신부(320)를 포함한다.
- [0046] 스캔 정보 관리부(310)는, 통신부(320)를 통해 프린터 스캐너(600)로부터 전송 받은 프린트 스캔 정보를 관리한다. 관리 정보는 프린터의 IP, 펌웨어, 열린 포트와 포트에 대한 서비스, 그리고 이에 대한 상세 버전 정보 등이 될 수 있다.
- [0047] 스캔 정보 관리부(310)는, 통신부(320)를 통해 통제 서버(200)의 스캔 정보 요청 메시지를 수신 받으면 해당 정보를 추출하여 통제 서버(200)로 전송한다.
- [0048] 통신부(320)는, 프린터 스캐너(600)로부터 전송 받은 스캔 정보를 스캔 정보 관리부(310)로 전달하는 역할과 통제 서버(200)로부터 스캔 정보 요청 메시지를 수신하여 스캔 정보 관리부(310)로 전달하고 이에 대한 응답 메

시지를 통제 서버(200)로 송신하는 역할을 한다.

- [0050] 도 5는 취약점 정보 데이터베이스의 블록도이다.
- [0051] 취약점 정보 데이터베이스(400)는 취약점 정보 관리부(410), 통신부(420)을 포함한다.
- [0052] 취약점 정보 관리부(410)는, 통신부(420)를 통해 프린터 취약점 정보 크롤러(700)로부터 전송 받은 취약점 정보를 관리한다. 관리 정보는 취약 대상, 취약 원인, 취약 내용, 공격 유형, 보완 방법 등이 될 수 있다.
- [0053] 취약점 정보 관리부(410)는, 통신부(420)로부터 통제 서버의 취약점 정보 요청 메시지를 수신 받으면 해당 정보를 추출하여 통제 서버(200)로 전송한다.
- [0054] 통신부(420)는, 프린터 취약점 정보 크롤러(700)로부터 전송 받은 취약점 정보를 취약점 정보 관리부(410)로 전달하는 역할과 통제 서버(200)로부터 취약점 정보 요청 메시지를 수신 받아 취약점 정보 관리부(410)로 전달하고 이에 대한 응답 메시지를 통제 서버(200)로 송신하는 역할을 한다.
- [0056] 도 6은 벤더 정보 데이터베이스의 블록도이다.
- [0057] 벤더 정보 데이터베이스(500)는 벤더 정보 관리부(510)과 통신부(520)을 포함한다.
- [0058] 벤더 정보 관리부(510)는, 프린터 벤더 정보 크롤러(800)로부터 수신 받은 벤더 정보를 관리한다. 즉, 벤더 별 펌웨어에 대한 정보, 프린터에서 사용하는 포트의 서비스들에 대한 정보 등을 관리한다.
- [0059] 벤더 정보 관리부(510)는, 통제 서버(200)의 패치 정보 요청 메시지를 수신 받으면 해당 정보를 추출하여 통제 서버(200)로 전송한다.
- [0061] 통신부(520)는, 프린터 벤더 정보 크롤러(800)로부터 전송 받은 벤더 정보를 벤더 정보 관리부(510)로 전달하는 역할과 통제 서버(200)로부터 벤더 정보 요청 메시지를 수신 받으면 벤더 정보 관리부(510)로 전달하고 이에 대한 응답 메시지를 통제 서버(200)로 송신하는 역할을 한다.
- [0063] 도 7은 프린터 스캐너의 블록도이다.
- [0064] 프린터 스캐너(600)는 스캔 정책 결정부(610), 패킷 생성부(620), 패킷 분석부(630), 통신부(640)을 포함한다.
- [0065] 프린터 스캐너(600)는 포트를 스캔하는 장치이므로, 프린터 포트 스캐너 또는 프린터 포트 수집기라고 부를 수도 있다.
- [0066] 스캔 정책 결정부(610)는, 스캔을 하기 위한 IP주소의 범위, 스캔 방식, 포트의 범위, 프로토콜 등을 결정한다. 이러한 결정은 관리자의 설정이나 수신된 응답 패킷을 통하여 이루어진다.
- [0067] 스캔 정책 결정부(610)는, 호스트 스캔 정책을 결정하여 패킷 생성부(620)에 전달한다. 호스트 스캔 정책은 호스트 스캔 시 IP 주소 범위와 IP 접근 방식(랜덤 혹은 순차), 스캔 방식(ARP, TCP, ICMP 등)을 결정한다. 패킷 분석부(630)에서 호스트 스캔의 응답 패킷을 확인하여 호스트 스캔 정보를 스캔 정책 결정부(610)에 전달하는 방식으로 포트 스캔이 수행된다.
- [0068] 스캔 정책 결정부(610)는, 포트 스캔 정책을 결정하여 패킷 생성부(620)에 전달한다. 포트 스캔 시 프린터에서 주로 사용하는 21(ftp), 80(http), 443(https), 515(printer), 9100(jetdirect), 427(svrloc), 631(ipp), 79(finger), 4000(remoteanything), 5000(upnp), 5001(complex-link), 9500(ismserver) 등의 포트 중 스캔할 포트와 스캔 방식(TCP SYN, TCP, UDP 등)을 결정한다. 포트 스캔에 관한 응답을 패킷 분석부(630)에서 분석하여 호스트가 프린터인 것을 확인하고 포트 스캔 정보를 스캔 정책 결정부(610)에 전달하면 펌웨어 및 프로토콜 버전 탐지를 수행한다.
- [0069] 스캔 정책 결정부(610)는, 펌웨어 및 프로토콜 버전 탐지 정책을 결정하여 패킷 생성부(620)에 전달한다. 펌웨어 및 프로토콜 버전을 탐지에서 각각의 프로토콜마다 어떤 과정을 통하여 상세 정보를 수집할지 결정한다.

- [0070] 프로토콜마다 정보를 수집하는 방법이 상이하다.
- [0071] 예를 들어, 443(https) 포트를 사용하는 ssl/tls의 경우 핸드셰이킹 과정에서 버전, 인증서, 암호 알고리즘 등의 정보를 수집할 수 있다.
- [0073] 패킷 생성부(620)는, 스캔 정책 결정부에서 전달된 정책을 기반으로 패킷을 생성 하여 통신부(640)로 전달한다.
- [0074] 패킷 분석부(630)는, 통신부(640)에서 수신한 호스트 스캔, 포트 스캔, 펌웨어 및 프로토콜 버전 탐지의 응답 패킷을 분석하고, 호스트 스캔의 응답 패킷일 경우 호스트 스캔 정보를 스캔 정책 결정부(610)로 전달하고, 포트 스캔의 응답 패킷일 경우 호스트가 프린터인지를 확인하여 프린터일 경우 포트 스캔 정보를 스캔 정책 결정부(610)로 전달한다. 515(printer), 9100(jetdirect), 631(ipp) 포트가 열려 있을 경우 호스트를 프린터로 식별할 수 있다.
- [0075] 펌웨어 및 프로토콜 버전 탐지의 응답 패킷일 경우 패킷의 상세 정보를 추출한 후 통신부를 통하여 스캔 정보 데이터베이스에 저장한다.
- [0077] 통신부(640)는, 패킷 생성부(620)에서 생성된 패킷들을 전송하고 이에 대한 응답 패킷을 수신하여 패킷 분석부(630)로 전달하는 역할과 패킷 분석부(630)에서 추출한 상세 정보를 전달받아 스캔 정보 데이터베이스(300)에 전송하는 역할을 한다.
- [0079] 도 8은 프린터 취약점 정보 크롤러의 블록도이다.
- [0080] 프린터 취약점 정보 크롤러(700)은 정보 수집부(710), 취약점 정보 비교부(720), 취약점 정보 탐지부(730), 통신부(740)을 포함한다.
- [0081] 정보 수집부(710)는 프린터 취약점 DB 사이트의 url을 관리하고, 취약점 DB 사이트의 url에 접근하여 페이지의 html 소스를 수집하여 취약점 정보 비교부(720)로 전달한다.
- [0082] 취약점 정보 비교부(720)는, 정보 수집부(710)로부터 전달받은 정보 중 'printer', hp, brother 등 프린터 제조사명 및 lpd, ipp 등 프린터 관련 프로토콜 등 프린터 관련 키워드를 포함하고 있는지를 비교한다. 프린터 관련 키워드를 포함하고 있을 경우 프린터 취약점으로 식별하여 취약점 상세 페이지 링크 url을 취약점 정보 탐지부(730)로 전달한다.
- [0083] 취약점 정보 탐지부(730)는, 벤더 정보 비교부로부터 전달받은 url에 접근하여 페이지의 html 소스를 수집하고, 수집한 정보를 html parser를 이용해 분석하여 취약점 이름, 위협, 영향 등 필요한 정보들을 식별하여 통신부(740)로 전달한다.
- [0084] 통신부(740)는, 취약점 정보 탐지부로부터 전달받은 식별된 취약점 정보를 취약점 정보 데이터베이스로 전송하는 역할을 한다.
- [0086] 도 9는 프린터 벤더 정보 크롤러의 블록도이다.
- [0087] 프린터 벤더 정보 크롤러(800)는 정보 수집부(810), 벤더 정보 비교부(820), 벤더 정보 탐지부(830), 통신부(840)을 포함한다.
- [0088] 정보 수집부(810)는, 프린터 벤더 패치 사이트 url을 관리하고, 벤더 패치 사이트의 url에 접근하여 페이지의 html 소스를 수집하여 벤더 정보 비교부(820)로 전달한다.
- [0089] 벤더는, 프린터의 기본이 되는 펌웨어나 소프트웨어의 정보를 가지고 있는 프린터 제조사나 프린터에서 사용되는 소프트웨어를 제작하는 제조사나 공급자를 의미한다.
- [0090] 벤더 벤더 정보 비교부(820)는, 통신부(840)를 통해 벤더 정보 데이터베이스(500)로부터 기존 패치 리스트를 전송 받고, 정보 수집부(810)로부터 전달받은 정보를 html parser를 이용해 분석하여 패치 리스트를 식별한다. 그

후에, 식별한 패치 리스트와 기존 패치 리스트를 비교하여 새로운 패치가 존재하는지 비교한다. 새로운 패치가 존재할 경우 새로운 패치의 태그를 확인하여 상세 페이지 링크 url을 벤더 정보 탐지부(830)로 전달하고, 식별한 패치 리스트는 통신부(840)으로 전달한다.

[0091] 벤더 정보 탐지부(830)는, 벤더 정보 비교부(820)로부터 전달받은 url에 접근하여 페이지의 html 소스를 수집하고, 수집한 정보를 html parser를 이용해 분석하여 패치 버전, 취약점 이름, 취약한 모델 등 필요한 정보들을 식별하여 통신부(840)로 전달한다.

[0092] 통신부(840)는, 벤더 정보 탐지부(830)로부터 전달받은 식별된 정보들과 벤더 정보 비교부(820)로부터 전달받은 패치 리스트를 벤더 정보 데이터베이스(500)로 전송한다.

[0094] 본 발명의 시스템은 크게 2가지 기능을 가진다.

[0095] 첫 번째 기능은, 스캐너와 크롤러가 각종 정보(스캔 정보, 취약점 정보, 벤더 별 패치 정보)를 수집하고 각각의 데이터베이스에 저장하는 기능이다.

[0096] 두 번째 기능은, 사용자에게 프린터의 취약점 정보와 패치 정보를 제공해주는 기능이다.

[0098] 각종 정보(스캔 정보, 취약점 정보, 벤더 별 패치 정보)를 수집하고 각각의 데이터베이스에 저장하는 기능을 달성하기 위해서는, 사용자에게 프린터의 취약점과 패치 정보를 제공하기 위하여 프린터 스캔 정보, 취약점 정보, 벤더 별 패치 정보를 수집하는 과정과 자동화된 프로그램을 사용하여 주기적으로 정보를 수집하여 데이터베이스에 저장하는 과정이 필요하다.

[0099] 프린터 스캐너에서 수집한 정보를 스캔 정보 데이터베이스에 저장하는 과정을 살펴보면 다음과 같다.

[0100] 도 10은 프린터 스캐너 동작의 흐름도이다.

[0101] 도 10에 표시된 바와 같이 프린터 스캐너 동작을 위해서는 다음의 단계를 거치게 된다.

[0102] 1) 호스트 스캔 단계(S110 단계)

[0103] 스캐너(600)는 IPv4 대역의 IP를 대상으로 랜덤 혹은 순차적으로 호스트가 존재하는지 여부를 확인한다. 호스트를 발견하기 위한 방법은 ARP 요청, TCP, ICMP 등 다양한 방법으로 진행할 수 있다.

[0105] 2) 호스트 존재 여부 판단 단계(S120 단계)

[0106] 호스트가 존재할 경우 다음 단계인 포트 스캔 단계(S130 단계)로 진행하고, 존재하지 않을 경우 종료한다.

[0108] 3) 포트 스캔 단계(S130 단계)

[0109] 발견된 호스트를 대상으로 포트 스캔을 진행하는 단계이다. 스캔 방식은 TCP SYN, TCP, UDP 등 다양한 방식으로 진행할 수 있다. 프린터에서 사용될 수 있는 21(ftp), 80(http), 443(https), 515(printer), 9100(jetdirect), 427(svrloc), 631(ipp), 79(finger), 4000(remoteanything), 5000(upnp) 등의 포트들을 스캔한다.

[0110] 4) 호스트가 프린터인지 여부의 판단 단계(S140 단계)

[0111] 프린터의 경우 위 포트 중 515, 631, 9100 포트가 열려있고, 이를 통해 호스트가 프린터인 것을 확인하면 다음 단계인 펌웨어 및 프로토콜 버전 탐지 단계(S150단계)로 진행하고, 프린터가 아닐 경우 종료한다.

[0113] 5) 펌웨어 및 프로토콜 버전 탐지 단계(S150 단계)

[0114] 열린 포트를 이용하여 프린터로 확인된 호스트에 대하여 사용중인 서비스의 버전을 자세히 조사하는 단계이다.

[0115] 버전 정보를 수집하기 위한 프로브 패킷은 프로토콜마다 다르다.

[0116] 예를 들어, 443(https) 포트를 사용하는 ssl/tls의 경우 핸드셰이킹 과정에서 버전 정보, 인증서, 암호 알고리

즘 등의 정보를 수집할 수 있다.

- [0117] 프로토콜마다 다양한 프로브 패킷을 생성하여 포트를 사용하는 서비스들의 자세한 정보를 수집한다.
- [0119] 6) 데이터베이스 저장 단계(S160 단계)
- [0120] 이전 단계에서 호스트 별로 어떤 서비스들을 사용하는지에 대하여 수집한 정보를 스캔 정보 데이터베이스에 저장한다.
- [0122] 프린터 취약점 정보 크롤러에서 수집한 정보를 취약점 정보 데이터베이스에 저장하는 과정을 살펴보면 다음과 같다.
- [0123] 도 11은 프린터 취약점 정보 크롤러 동작의 흐름도이다.
- [0124] 도 11에 표시된 바와 같이 프린터 취약점 정보 크롤러 동작을 위해서는 다음의 단계를 거치게 된다.
- [0125] 1) 취약점 크롤링 단계(S210 단계)
- [0126] 프린터 취약점 정보 크롤러(700)는 취약점 DB 사이트 url을 통해 취약점 리스트에 접근할 수 있다. 취약점 리스트의 취약점이름과 취약점 설명 요약을 python 스크립트를 통해 크롤링 할 수 있다.
- [0128] 2) 프린터 관련 취약점 판별 단계(S220 단계)
- [0129] 크롤링한 취약점 이름과 설명 요약 중 printer관련 키워드 검사를 통해 프린터 관련 취약점을 식별할 수 있다.
- [0130] 취약점 이름과 설명 요약 중 printer나 hp, brother와 같은 프린터 제조사, ipp, jetdirect등 프린터 관련 프로토콜 등의 키워드 포함 여부를 검사한다. 프린터 관련 키워드를 포함한 경우 프린터 관련 취약점으로 인식하여서 취약점 정보 크롤링 단계(S230 단계)로 넘어가고, 그렇지 않을 경우 종료한다.
- [0132] 3) 취약점 정보 크롤링 단계(S230 단계)
- [0133] 프린터 취약점으로 식별된 취약점의 상세 페이지에 url을 통해 접근할 수 있다. 취약점 상세 페이지의 모든 내용을 python 스크립트를 통해 크롤링할 수 있다.
- [0135] 4) 취약점 번호, 원인, 영향 등 취약점 정보 탐지 단계(S240 단계)
- [0136] 크롤링한 데이터에서 취약점 이름, 설명, 영향, 위협 등 취약점 정보에 html 태그를 통해 접근하여 식별할 수 있다.
- [0138] 5) 데이터베이스 저장단계(S250 단계)
- [0139] 식별된 취약점 정보를 데이터베이스에 저장하고 종료한다.
- [0141] 프린터 벤더 정보 크롤러(800)에서 수집한 정보를 벤더 정보 데이터베이스에 저장하는 과정을 살펴보면 다음과 같다.
- [0142] 도 12는 프린터 벤더 정보 크롤러 동작의 흐름도이다.
- [0143] 도 12에 표시된 바와 같이 프린터 벤더 정보 크롤러 동작을 위해서는 다음의 단계를 거치게 된다.
- [0145] 1) 패치 정보 리스트 확인 단계(S310 단계)

- [0146] 프린터 벤더 정보 크롤러(800)는 프린터 제조사 사이트 url을 통해 패치 정보 리스트에 접근할 수 있다. 따라서 패치 리스트를 python 스크립트를 통해 크롤링 할 수 있다.
- [0148] 2) 새로운 패치 존재 여부 판별 단계(S320 단계)
- [0149] 크롤링한 패치들을 기존 데이터베이스에 저장되어 있는 패치들과 비교하여 새로운 패치 존재 여부를 검사한다. 그 결과, 새로운 취약점이 있을 경우 패치 정보 크롤링 단계(S330 단계)를 수행하고, 그렇지 않을 경우 종료한다.
- [0151] 3) 패치 정보 크롤링 단계(S330 단계)
- [0152] 새로운 패치의 상세 페이지에 url을 통해 접근할 수 있고, 패치 상세 페이지의 모든 내용을 python 스크립트를 통해 크롤링 할 수 있다.
- [0154] 4) 취약한 펌웨어 버전, 패치 된 버전 등 패치 정보 탐지 단계(S340 단계)
- [0155] 크롤링한 데이터에서 패치된 취약점 내용, 취약한 버전, 패치된 버전, 패치 내용 등 패치 관련 정보에 html 태그를 통해 접근하여 식별할 수 있다.
- [0157] 5) 데이터베이스 저장 단계(S350 단계)
- [0158] 식별된 취약점 정보를 데이터베이스에 저장하고 종료한다.
- [0160] 프린터의 취약점 정보와 패치 정보를 사용자에게 제공하기 위해서는, 사용자가 프린터의 취약점과 패치 정보를 검색하여 결과를 확인하는 과정을 거치게 되는데, 프린터 검색과 결과 출력은 사용자 인터페이스(100)에서 수행되며, 스캔 정보 요청과 취약점/벤더 정보 요청은 통제 서버(200)에서 수행된다.
- [0162] 도 13은 프린터 취약점/패치 정보 검색 동작의 흐름도이다.
- [0164] 도 13에 표시된 바와 같이 취약점/패치 정보 검색 동작을 위해서는 다음의 단계를 거치게 된다.
- [0165] 1) 프린터 검색 단계(S410 단계)
- [0166] 사용자가 프린터의 취약점과 패치 정보를 확인하기 위하여 검색어를 입력하는 단계이다. 검색어는 IP, IP대역, 제조사, 모델명, 특정 포트 등이 될 수 있다.
- [0167] 검색어는 사용자 인터페이스(100)에서 입력 받으며, 사용자 인터페이스(100)는 웹 애플리케이션, 모바일 애플리케이션, PC 애플리케이션 등을 포함할 수 있다.
- [0168] 입력 받은 검색어는 통제 서버(200)로 전달된다.
- [0170] 2) 스캔 정보 요청(S420 단계)
- [0171] 입력 받은 검색어는 통제 서버(200)로 전달되며, 통제 서버(200)는 스캔 정보 데이터베이스(300)에 검색어에 대한 스캔 정보를 요청한다.
- [0173] 3) 요청 정보 존재 여부 확인 단계(S430 단계)
- [0174] 스캔 정보가 없을 경우, 사용자 인터페이스(100)에 이를 알리고 사용자 인터페이스(100)는 검색된 프린터가 없

음을 출력한다.

[0176] 4) 취약점 / 벤더 정보 요청(S440 단계)

[0177] 통제 서버(200)는 스캔 정보 데이터베이스(300)에 해당 스캔 정보가 있을 경우 취약점 정보 데이터베이스(400)와 패치 정보 데이터베이스(500)에 각각 취약점 정보와 패치 정보를 요청한다.

[0178] 통제 서버(200)는 요청에 대한 응답을 취합하여 사용자 인터페이스(100)에 취약점 정보와 패치 정보를 전달한다.

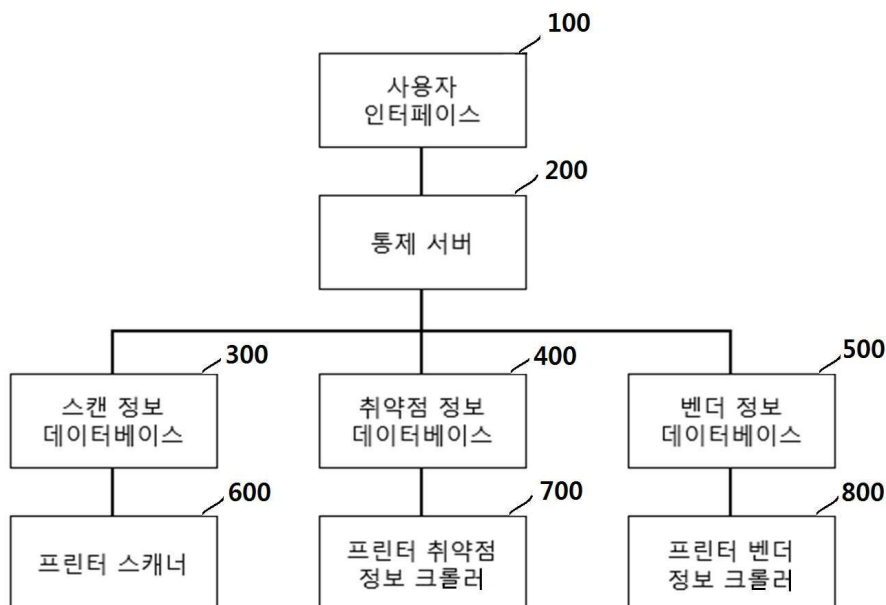
[0179] 4) 결과 출력 단계(S450 단계)

[0180] 사용자 인터페이스(100)는 검색한 프린터에 대한 취약점 정보와 패치 정보를 출력한다.

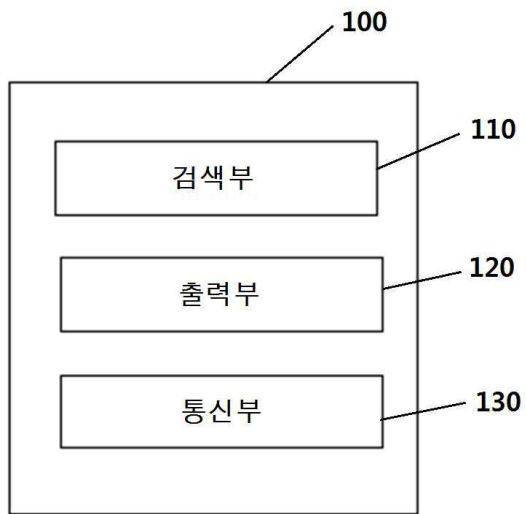
[0182] 그 결과, 본 발명에서는 네트워크 프린터의 열린 포트를 스캔한 후 포트를 사용하는 서비스의 상세 정보를 획득하고 프린터의 취약점과 벤더 정보를 수집하여 사용자에게 프린터의 취약점과 패치 정보를 제공하게 된다.

도면

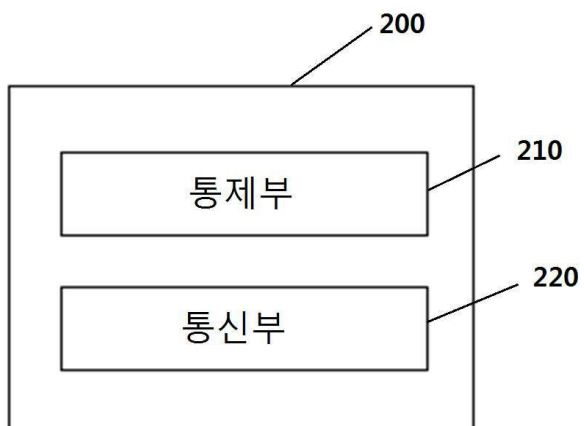
도면1



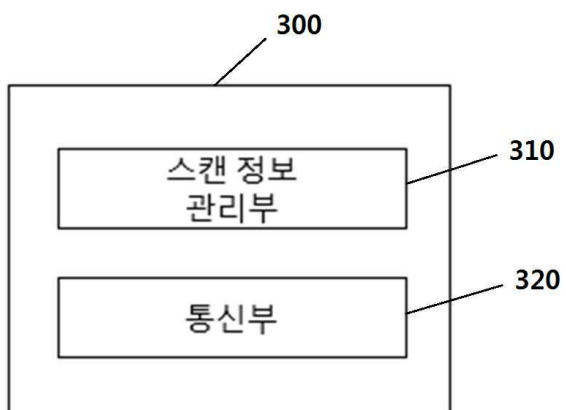
도면2



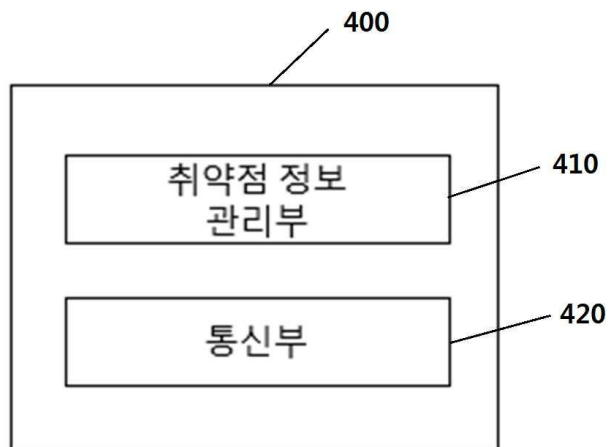
도면3



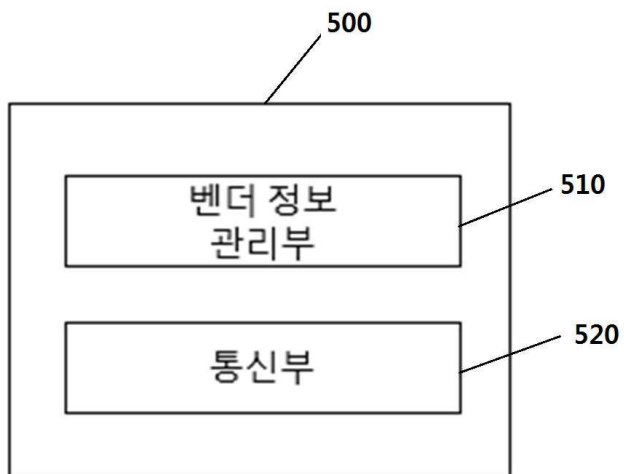
도면4



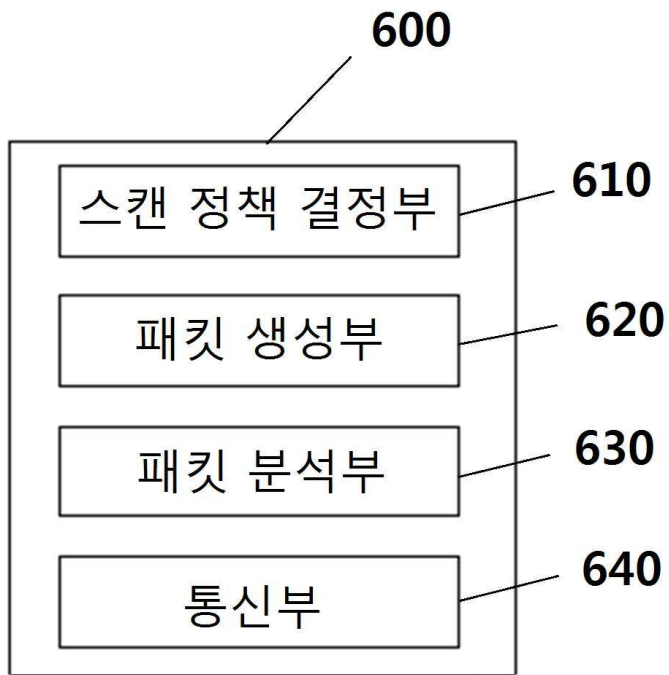
도면5



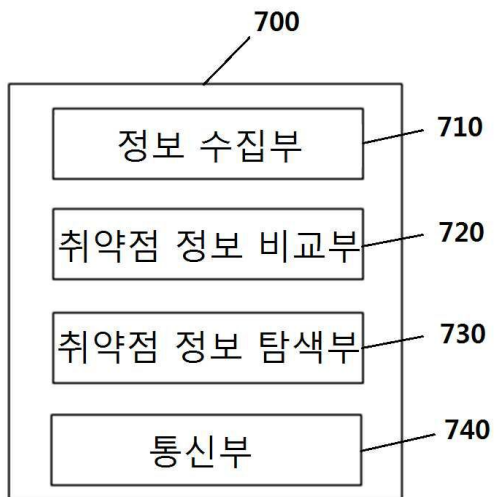
도면6



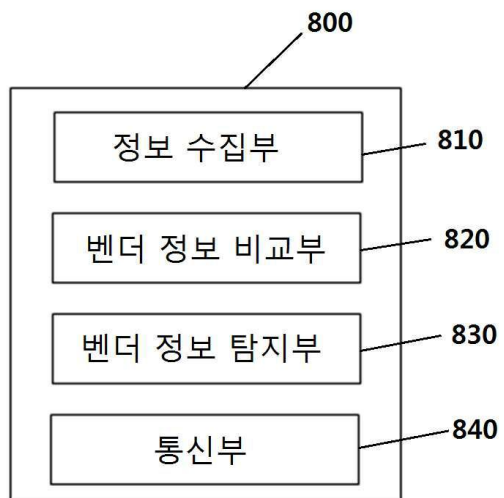
도면7



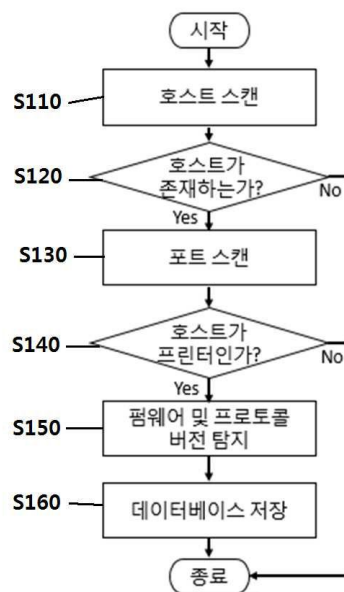
도면8



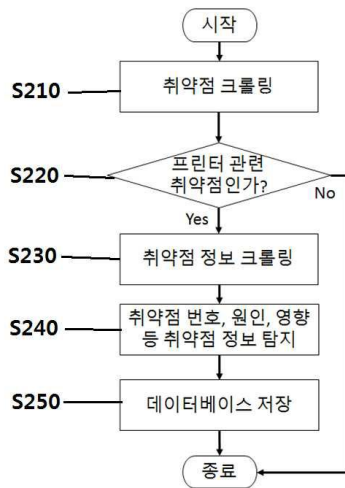
도면9



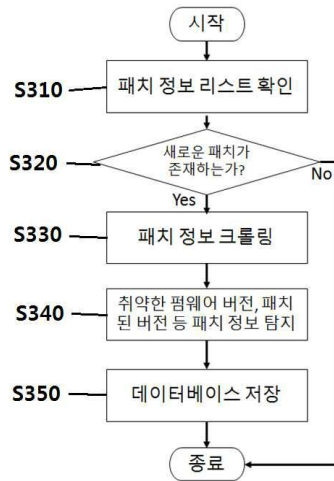
도면10



도면11



도면12



도면13

