Journal of The Korea Society of Computer and Information
Vol. 23 No. 9, pp. 73-80, September 2018
www.ksci.re.kr
https://doi.org/10.9708/jksci.2018.23.09.073

A Design of Client BBS System for Secure HVA

Jae-Kyung Park*, Young-Ja Kim**

Abstract

In this paper, we propose a new type of client server environment to improve the architecture vulnerable to hacking in an existing client server environment. On the server side, move the existing Web server to the client side and This is a way for clients to communicate only the data they need and suggests a structure that completely blocks the web attack itself to the server. This can completely prevent a server from being hacked, spreading malicious code and hacking data on a server. It also presents a new paradigm that will not affect servers even if malware is infected with client PCs. This paper validates the proposed environment through BBS (Big Bad Stick) hardware in the form of USB on the client side. This study proof that secure services are provided through encryption communication with server-side security equipment, indicating that this study is a system with new security.

▸Keyword: High Value Asset, Context Centric Network, Big Bad Stick, Profile, Raspberry Pi

I. Introduction

현재까지의 인터넷을 통한 서비스 환경은 전통적으로 클라이언트-서버 환경이 대부분을 차지하고 있으며 클라이언트는 대부분 웹브라우저를 통해 서버의 웹서버에 접근하여 서비스를 받는 환경을 사용해왔다. 하지만 이러한 서버에서의 서비스 방식으로 인해 해커는 서버의 취약점을 기반으로 해킹을 수행하고 악성코를 심어 놓음으로 인해 해킹된 서버에 접속하는 클라이언트는 2차적으로 감염되어 좀비PC화 되는 악순환이 반복되고 있다.

현재까지는 이러한 문제를 근본적으로 해결하기 위해서는 기본적으로 서버 앞단에 보안장비를 설치하여 해킹을 막는 방법이 유일한 방법이었다. 하지만 이러한 방어조치 또한 새로운 공격 앞에서는 무용지물이 되는 것을 실제 운영환경에서 겪고 있는 것이 현실이다. 최근까지 개발된 악성코드를 방어하기 위한 다양한 시스템도 APT(Advanced Persistent Threat)공격 앞에서는 무력화는 되는 것을 경험하였고 보안장비의 설치만이 방어를 위한 최선의 방법이라고는 단정할 수 없게 되었다[1].

이러한 근본적인 문제를 해결하기 위해 블록체인 기반의 새로운 네트워크를 제안하기도 하며 별도의 하드웨어 장치를 통해 문제를 해결하기 위한 시도도 있으나 가장 실제 서비스에 근접한 형태는 차세대네트워크인 CCN(Context Centric Network)을 적용한 시스템을 활용하여 기존의 TCP/IP의 취약성을 이용한 공격을 막고자 하는 시도가 주목할 만하다[1]. 하지만 이를 실제 서비스에 활용할 수 있는 방안에 대해서는 구체적인 연구가 부족하였으며 본 논문에서는 이러한 형태의 차세대 네트워크를 통한 새로운 형태의 시스템을 개발하여 제시하고자 한다.

본 논문에서는 앞서 언급한 기존의 서비스 모델의 취약점을 구조적으로 해결하기 위해 서비스를 제공해주는 서버(웹서버)를 클라이언트에 위치시키는 구조적인 변경을 제안하고자 한다. Fig.1과 같이 기존의 방식과는 달리 클라이언트 측에 별도의 클라이언트 하드웨어를 설치하여 해당 하드웨어에 웹서비스를 올린 후 클라이언트가 접속하는 방식으로 운영되는 모델을 제안하고자 한다. 이러한 클라이언트 하드웨어를 본 논문에서는 BBS(Big Bad Stick)이라고 한다. 이 BBS는 기존의 아두이노(Arduino)나 라즈베리파이(Raspberry Pi), 오렌지 파이(Orange Pi)와 같은 미니컴퓨터 형태로 본 논문에서 사용된 BBS에는 Linux 운영체제와 아파치 웹서버를 탑재하였다.

이처럼 서버에는 웹서비스가 존재하지 않으며 클라이언트에 웹서비스가 존재하며 데이터를 처리한 후 서버에 필요한 데이터 즉, 클라이언트가 필요로 하는 데이터만을 암호화하여 서버에

• First Author: Jae-Kyung Park, Corresponding Author: Young-Ja Kim
*Jae-Kyung Park (jakypark@kopo.ac.kr), Dept. of Information Security, Seoul Gangseo Campus, Korea Polytechnics.
**Young-Ja Kim (tiny89@kopo.ac.kr), Dept. of Data Analysis, Seoul Gangseo Campus, Korea Polytechnics.
• Received: 2018. 08. 21, Revised: 2018. 09. 06, Accepted: 2018. 09. 10.

전달하고 서버 앞단에 보안장비가 이를 복호화하여 뒷단에 데이터베이스 서버로부터 데이터를 받아 전달하는 구조를 갖는다.

본 논문에서는 기존 네트워크 서비스의 단점으로 나타난 보안의 문제를 어떻게 근본적으로 해결할 것인가에 대한 대안으로 CCN과 같은 새로운 네트워크를 활용하여 현재 서비스 모델의 단점을 극복하고자 한다[2]. 현재 인터넷의 근간을 이루고 있는 TCP/IP는 보안을 고려하지 않고 설계된 프로토콜로 40여 년간 많은 강점을 통해 현재의 인터넷을 이끌어 냈지만 최근 10여 년 동안 보안의 문제는 날로 심각해져 가고 있다. 이러한 차세대 프로토콜을 활용하여 클라이언트의 하드웨어 인증시스템을 제안하고 이를 서비스 모델로 구현하여 해킹을 통한 실험으로 증명하고자 한다. 본 시스템에서 제안하는 프로토콜은 내부적으로 CCN 프로토콜을 사용하므로 TCP/IP 공격 자체가 의미 없는 것으로 서로 다른 통신을 사용함으로 TCP/IP의 문제를 근본적으로 해결하고자 한다. 또한 제안시스템은 기존의 TCP/IP 네트워크와 호환을 해야 현재의 네트워크에 활용이 가능하므로 TCP/IP와의 호환도 지원한다[3].

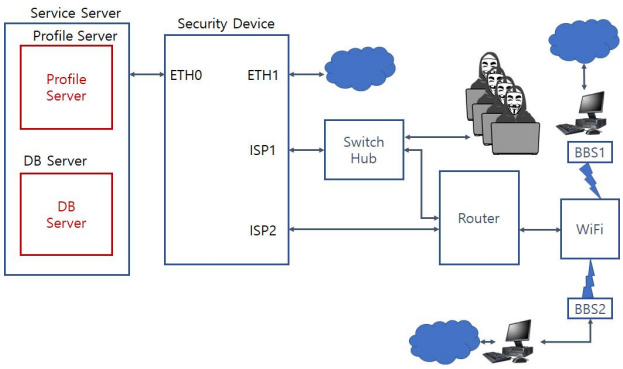

Fig. 1. Logical System Diagram

Fig. 1은 본 논문에서 제안하는 전체 시스템 구성을 나타내고 있으며 서버 단에는 기존의 서비스처럼 웹 서버가 존재하지 않는 것이 특징이다. 기존 서비스 방식과 전혀 다른 형태의 구조적인 변경을 통해 보안상 많은 이득을 얻을 수 있는 것이 본 논문의 가장 큰 특징이다. 2장에서는 본 논문과 관련된 국내외 차세대 보안에 대한 연구를 언급하고 3장에서는 본 논문의 제안 시스템에 대해서 상세히 설명한다. 4장에서는 본 제안시스템에 대한 해킹 테스트 결과를 통해 객관성을 입증하도록 한다.

II. Preliminaries

1. Related works

1.1 Domestic Trends

현재 전 세계적으로 가상화폐에 대한 열풍이 불고 있으며 원천기술인 블록체인을 활용한 다양한 시도가 진행되고 있다. 최근 국내의 KT에서는 블록체인을 활용한 인터넷을 개발한다고 발표하였다[13]. 이번에 공개된 KT 네트워크 블록체인의 경우, 기존 TCP/IP의 한계점을 극복하여 전국에 위치한 초고속 네트워크에 블록체인을 결합한 노드를 구축해 운영하는 방식으로 설계하였다. 기존 공개 블록체인은 처리속도와 용량이 낮아 사업화에는 부적합하고, 사설 블록체인은 비공개 데이터 관리로 인해 투명성이 낮으며 소규모 구조로 인해 상대적으로 보안성이 낮은 한계가 있었다. KT는 전국에 위치한 초고속 네트워크에 블록체인을 결합한 노드를 구축해 운영하는 방식으로 성능과 신뢰라는 두 가지 장점을 동시에 갖게 됐다. 이로써 KT 블록체인은 2019년 말까지 최대 10만 TPS(Transactions Per Second, 초당 거래량)의 성능을 구현할 예정으로 알려졌다.

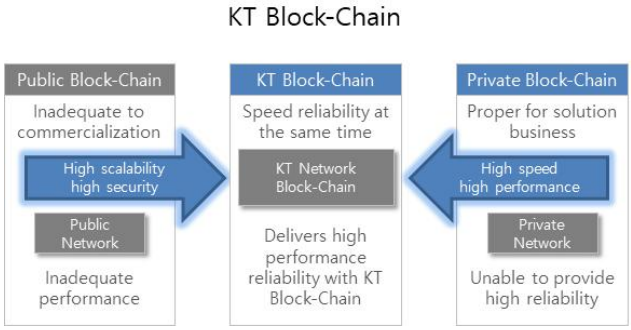

Fig. 2. Specification of KT Block Chain

KT는 기존 수직적 블록 검증 방식에서 벗어나 동시다발적으로 검증 가능한 병렬 방식을 사용하는 차별화된 알고리즘을 KT 네트워크와 결합했다. 아울러 이 블록체인 기술을 기존 인터넷 서비스에도 적용, IP가 아닌 고유 ID기반의 네트워킹을 통해 연결과 동시에 바로 본인인증이 가능한 블록체인 기반 인터넷 기술을 사용했다[9][10]. 이를 사용하면 블록체인 고유 ID가 모든 연결에 대한 인증을 대신 제공할 수 있고, IP를 네트워크 단에서부터 숨길 수 있기 때문에 기존 IP 인터넷에서의 해킹과 개인정보 도용, 분산서비스공격과 같은 공격을 원천적으로 차단할 수 있다[11][12].

특히, 최근 IP기반 웹캠 해킹으로 원격에서 집안을 훔쳐보고 동영상 거래 사이트에 해당 영상을 유통시키는 등 IoT 해킹 범죄가 증가하고 있지만, KT 블록체인 기반 인터넷 이용자는 보안걱정 없이 안심하고 IoT 제품을 사용할 수 있다는 장점을 가진다[14].

1.2 Foreign Trends

구글이 강력한 보안 수단이 필요하다는 점을 계속 강조해온 가운데 계정 보안을 극대화한 특별한 키(Key)가 출시됐다. 바로 'USB 보안키'(USB Security Key)다. 이미 구글은 2014년도부터 보안키를 통한 이중인증을 활용하여 피싱 공격에 따른 개인 정보 유출이나 악성코드를 통한 인증 공격으로부터 원천 차단시켜 왔다. 이를 활용하여 구글 직원들이 모두 사용한 결과 2018년 이전 1년 동안 해킹 피해를 단 한 번도 보지 않았다. 구글의 보안 비결은 '보안키를 이용한 이중 인증'이었다. 구글은 보안키 덕분에 지난해부터 현재까지 직원 8만5000명 가운

데 단 한 명도 계정 해킹 피해를 보지 않았다. 구글은 자체 보안키 '타이탄키(Titan Key)'를 기존 버전에 추가 개발·시판한다[15]. 구글이 보안키를 이용해 업무 계정에 접속하는 정책을 시행, 피싱 방어에 성공했다고 보도했다. 구글 대변인은 "2017년 USB포트에 끼우는 물리 보안키를 의무화한 후 업무 계정 손상이 발생하지 않았다"고 한다. 구글은 직원이 업무 계정에 접속할 때 반드시 실물 보안키를 이용, 이중 인증을 하게 했다. ID와 비밀번호를 넣은 후 다시 실물 보안키를 이용해 인증한다. 두 단계 인증을 거친다. 해커가 가짜 사이트를 만들어 구글 계정 ID와 비밀번호를 탈취해도 보안키가 없으면 접속할 수 없다. 보안키를 PC에 삽입하고 단추를 눌러야 로그인된다. 해커는 호시탐탐 구글 직원을 노린다. 낮은 직급이라도 구글 직원 피싱 공격에 성공하면 회사 내 민감한 시스템에 접속하거나 권한이 있는 직원을 다시 공격할 수 있다. 구글 계정을 탈취하려는 시도가 끊이지 않았다.

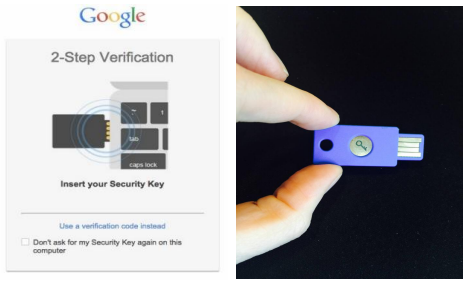

Fig. 3. Google Titan Key

보안키는 인증코드가 아닌 암호 기법을 사용한다. 키가 작동하도록 설정된 사이트에서만 유용하다. 피싱이나 파밍용으로 만든 가짜 구글 사이트에 접속하는 피해를 방지한다. 보안키는 특정 PC가 아닌 구글 계정에 등록된다. 크롬이 설치된 모든 PC에서 사용할 수 있다. 구글 계정이 여러 개 있어도 하나의 보안키를 이용할 수 있다. 반대로 여러 보안키를 하나의 구글 계정에도 등록할 수 있다. 보안키에는 계정과 관련된 어떤 기록도 저장되지 않는다는 장점을 가진다[16].

1.3 CCN(Content Centric Network)

CCN(Contents Centric Network)은 기존 위치(Where) 중심의 IP체계를 콘텐트(What) 중심의 네트워크 체계로 구현하여 콘텐트 전송능력을 향상시키고 강화된 보안체계를 제공하는 새로운 개념의 차세대 네트워크이다. CCN은 특정한 인증 이름 규칙을 콘텐트에 부여하여 IP가 없이도 콘텐트의 내용으로 데이터를 처리할 수 있는 메커니즘이다. CCN을 이용할 경우 요청자 또는 공격자는 콘텐트 서버에 접근자체가 불가하여 서버의 운영체제, 웹, 응용, 서비스 등을 전혀 알 수 없다. 공격자가 요청을 통해 콘텐트를 받을 수는 있으나 이는 콘텐트 저장소에 저장된 캐시 내용을 받는 것이며 이 또한 정상적인 인증을 해결해야만 받을 수 있는 개념이다[4][5].

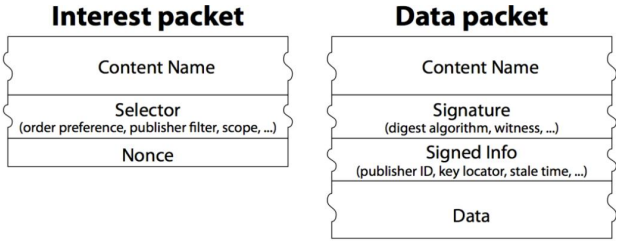

Fig. 4. CCN Interest Packet & Data Packet

Fig. 4에서와 같이 요청 패킷은 콘텐트 이름, 선택자, 임시 난수로 구성되고, 데이터 패킷은 콘텐트 네임, 서명(signature), 서명 정보(signed info), 데이터로 구성된다. 요청 패킷의 선택자와 데이터 패킷은 공개키 다이제스트를 포함한다. 공개키 다이제스트는 요청한 패킷에 대해 응답 데이터가 제대로 수신되었는지 확인하는 용도로 사용한다[6][7][8].

III. The Proposed Scheme

본 논문에서는 앞장에서 설명한 근본적인 문제점을 해결하기 위해 보다 다양한 형태의 시스템을 제안하고자 한다. 우선 시스템 구성을 기존의 방식과는 다른 형태의 구성을 통해 기존의 해킹을 완벽하게 무력화할 수 있도록 한다. 두 번째는 이러한 구성을 위해 별도의 하드웨어를 클라이언트에 도입한다. 마지막으로 각 개체 간의 통신은 새로운 네트워크 형태인 CCN을 활용하여 통신하도록 한다. 다음 Table 1은 본 논문에서 제안하는 새로운 형태의 기능 및 장비를 언급하고 있다.

Table 1. System Environment

Entity	Contents
Server Side	No Web Service No Web Server
Client Side	BBS(Big Bad Stick) BBS has Web Server
Security Device	CCN Communication No TCP/IP Routing

Table 1에서 언급한 형태로 클라이언트, 서버, 보안장비 등을 통한 전체적인 시스템 구성 및 특징은 다음 Fig. 5와 같다.

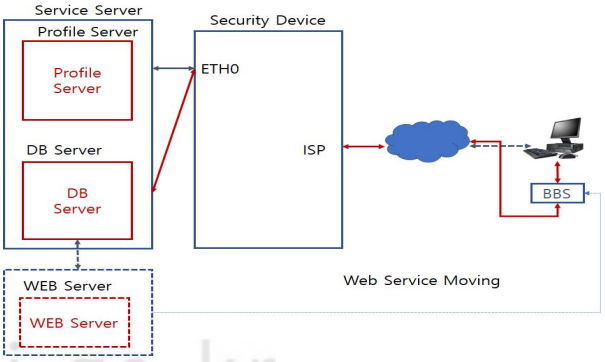

Fig. 5. Proposed System Diagram

본 시스템은 기존의 통신 흐름과는 다른 형태로 통신이 이루어지며 이때 해킹으로부터 원천적인 방어를 위해 각 개체별로 방어 전략을 도입한 형태의 시스템이다. 우선 기존의 서비스 시스템에서 서비스를 제공한 웹서버를 클라이언트로 모두 옮기도록 한다. 또한 PC에서 외부로의 직접적인 통신을 하는 대신 클라이언트 디바이스를 통해 서버에 접근하는 방식을 사용한다. 즉 기존의 서비스 흐름은 Fig. 5에서의 붉은색의 통신 흐름으로 변경하는 것을 제안한다. 본 논문에서 제안한 새로운 형태의 시스템을 통해 기존의 보안상의 많은 문제점을 해결할 수 있으며 이를 실험을 통해서 검증하고자 한다.

본 시스템의 서비스에 대한 전제조건은 다음과 같은 환경적 조건을 따르도록 한다.

① 서버에는 웹 서비스와 같이 외부 인터넷을 통해 직접적인 통신을 수행하는 서버가 존재하지 않으며 다만, 데이터베이스와 같은 서비스 주체에 대한 정보를 가진 서비스는 존재한다. 즉, 외부에서는 서버와 직접적으로 서비스를 수행하지는 않으며 특정한 디바이스만을 통해 서비스가 가능하다. 이때 서버에 저장된 중요한 정보를 본 논문에서는 HVA(High Value Asset)이라고 한다. 이는 고객의 중요한 정보 즉, 인증정보, 가상화폐 정보, 거래 정보 등을 의미하며 외부에서는 직접적으로 참조가 불가능한 정보를 의미한다.

② 클라이언트 PC는 일반적인 인터넷 서비스는 PC의 네트워크를 통해 인터넷 접근이 가능하지만 특정한 서비스를 위한 서버 접속 즉, HVA를 요청하는 서비스는 클라이언트의 디바이스인 BBS를 통해서만 통신이 가능하다.

③ 클라이언트 디바이스 BBS와 서버간의 통신은 CCN과 같은 별도의 프로토콜을 통해 접속하며 이러한 별도의 프로토콜을 해석할 수 있는 보안장비를 게이트웨이로 사용한다.

④ 서버단의 서비스를 제공해주는 서버는 보안장비를 통과하여 특정한 권한을 갖는 요청에만 응답하며 직접적인 요청에는 응답하지 않는다.

⑤ 서버 단에는 프로파일(Profile) 서버가 사용자의 인증정보 및 패스코드 및 CCN 접근 디렉터리 정보를 가지고 있으며 사용자는 미리 프로파일을 발급 받아야 서비스 이용이 가능하다.

1. Client Side

1.1 BBS(Big Bad Stick)

본 논문의 클라이언트에 사용하는 별도의 디바이스를 BBS라고 하며 이는 클라이언트 PC와 연결하여 클라이언트 통신의 일부를 대체하는 역할을 수행한다. BBS를 PC에 연결할 경우 RNDIS 드라이버가 설치되며 아래 그림 Fig. 6과 같이 CR-ROM 형태로 연결된다. 하지만, BBS는 자체적으로 운영체제 및 웹 서버를 탑재하고 있으므로 별도의 통신이 가능한 또 다른 PC와 동일하다. 이때 호스트 PC는 RNDIS로 연결된 BBS에 네트워크를 통해 접속하게 된다. 즉, 특정한 서버로 연결하기 위해서는 BBS를 통해서만 접속이 가능하고 일반적인 인터넷 서비스는 PC를 통해 통신이 진행되므로 서버 접근과 인터넷 접근이 완전히 분리된 형태의 망분리 효과를 가지게 된다.

다음 Fig. 7은 BBS의 내부 구성도를 나타내고 있다. 이 BBS는 라즈베리 파이를 활용하여 제작하였다[12]. 본 논문을 위해 제작한 BBS의 운영체제는 데비안 리눅스 4.14.50 버전을 사용하였으며 웹서버로는 아파치 2.4.25 버전을 탑재하였다. 또한 phython 2.7을 탑재하여 사용자 인증 및 통신 서비스를 phython 프로그래밍을 통해 구현하였다.

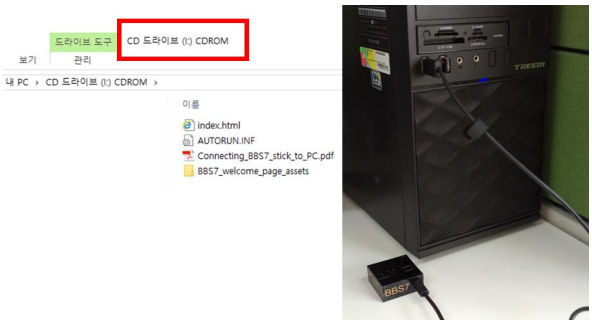

Fig. 6. Connect BBS for CD-ROM

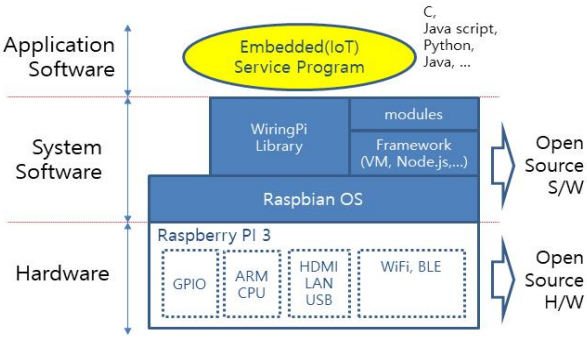

Fig. 7. Raspberry Pi Diagram

클라이언트 PC에서는 특정 서비스를 받기위해 CD-ROM으로 인식되는 BBS의 폴더에서 index.html을 클릭하여 서비스를 수행한다. 이때 웹 브라우저를 통해 BBS를 접근할 수 있는 BBS의 IP로 접근하게 되며 사용자 인증을 위해 인증을 수행하여야 한다. 사용자 인증 정보는 서버단의 프로파일 서버에 저장되어 인증을 위해 활용한다. 본 논문의 검증을 위해 제작한 서비스는 일종의 가상화폐 거래소를 모방한 형태의 서비스를 개발하였다. 4장에서 서비스의 구성 및 서비스를 자세하게 언급하도록 한다.

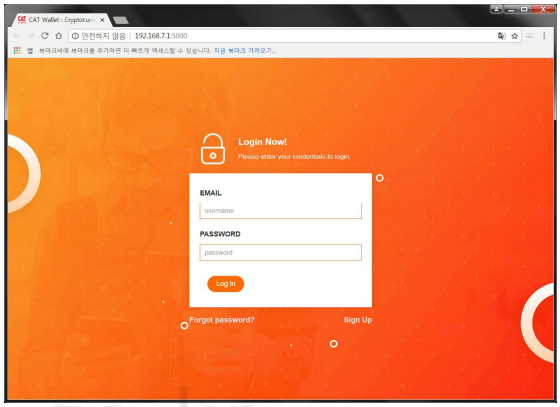

Fig. 8. Login for User Authentication

클라이언트 PC에서 BBS를 통해 접근하는 서버와의 통신은 기존의 TCP/IP 방식이 아닌 CCN 프로토콜을 활용하여 구형하였다. 즉, 외부에서 BBS를 통해 유출되는 패킷을 보호하기 위해 비밀성 및 무결성을 제공함으로 서버로의 통신 내용을 전혀 이해할 수 없는 방식을 채택하였다.

2. Security Device / Server Side

2.1 Security Device

본 논문에서 개발한 서버단의 보안장비는 기존의 방화벽이나 침입차단시스템과 같이 패킷을 필터링하거나 패턴을 검사하는 개념이 아니라 외부에서 유입되는 패킷을 구별하여 CCN통신인지 아닌지를 판단하고 CCN통신일 경우에만 이를 해석하여 뒷단의 서버로 전송하는 네트워크 변환 기능을 수행한다. 이러한 특징을 활용하여 기존의 TCP/IP 패킷이 직접적으로 유입이 되더라도 버려버림으로써 기존의 공격은 전혀 효과를 발휘하지 못하며 Fig. 9와 같이 패킷 해석을 위해 분석하더라도 암호화되어 전혀 해석이 불가능하다.

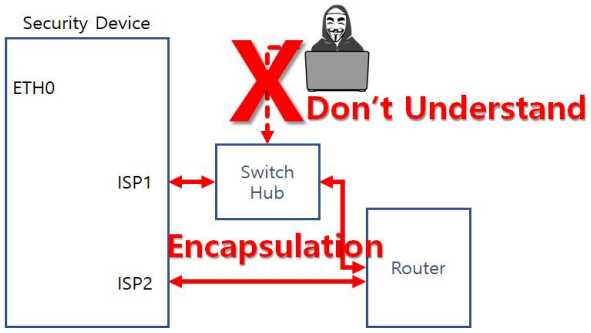

Fig. 9. Encapsulation Communication with CCN

또한 보안장비의 외부 인터페이스와 내부 인터페이스에는 어떠한 TCP/IP의 라우팅 정보가 포함되어 있지 않고 CCN 프로토콜에 의해서만 라우팅이 되므로 다음 Fig. 10과 같이 TCP/IP의 공격은 이 장비를 통과 할 수 없게 된다.

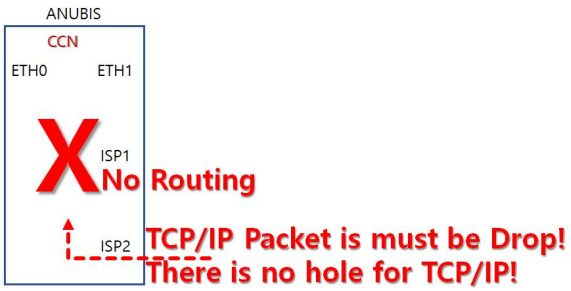

Fig. 10. Routing Policy in Security Device

2.2 Server Side

본 논문에서 개발한 형태의 시스템을 사용할 경우 서버 단에는 웹서버가 존재하지 않는다. 현재의 해킹 공격 중 90% 이상이 웹 서비스에 치중되고 있는 바 본 논문에서는 이러한 공격을 근본적으로 해결하기 위해 서버 단에서 웹 서버를 배제하여 클라이언트로 이동시켰다. 따라서 다음 Fig. 11과 같이 서버에 아예 웹 서버가 없으므로 악성코드와 같은 공격을 가할 여지가 전혀 없어지게 된다.

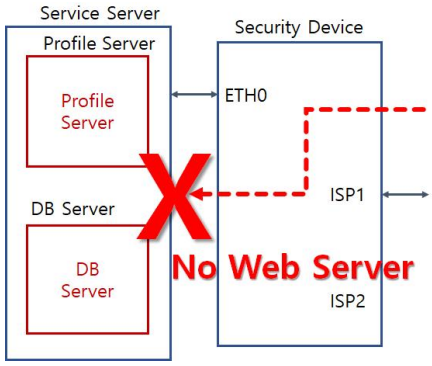

Fig. 11. Server Side Configuration

다만, 웹 서버를 제외하고 웹 서버에서 사용하는 콘텐트 서버는 기존의 방식과 동일하게 구성하면 되며 외부의 웹 서버를 통해 안전하게 데이터를 송수신하므로 별도의 구성을 갖출 필요는 없다. 앞서 언급한 것처럼 본 논문에서는 실제 시스템에 본 제안 시스템을 적용하기 위해 실제 서비스를 수행하고 있는 가상화폐 거래소와 같이 구성하여 테스트를 진행하였다. 신분 인증을 통해 인증 받은 사용자는 자신의 가상화폐를 팔거나 살 수 있는 거래를 하며 이때 기존의 TCP/IP 환경에서의 취약점이니 공격을 시도함으로 본 제안이 안전한지에 대한 검증을 수행하도록 한다.

IV. Test and Verification

본 논문에서 제안한 시스템의 서비스 절차는 Fig. 5와 같이 클라이언트, 보안장비, 서버 부분별로 진행하였다. 첫 번째로 클라이언트 PC에서의 웹 페이지는 BBS를 통해 클라이언트 PC로 전송되며 각각은 물리적으로 완전히 분리된 형태로 동작하여 망분리 효과를 갖게 된다. Fig. 8과 같이 등록된 사용자의 정보를 통해 로그인을 수행하게 되고 추가로 이중인증을 Fig. 12와 같이 수행하게 된다.

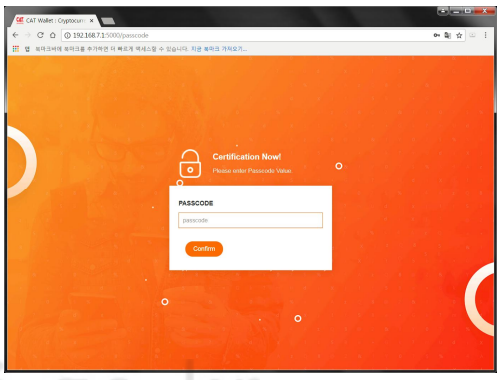

Fig. 12. 2nd Authentication with Passcode

로그인 이후 사용자 인증을 보다 강력하게 진행하기 위해서 2차 인증으로 사용자의 모바일 폰을 등록하여 아이디 인증이 완료된 이후에 OTP(One Time Password)와 같은 패스코드를 모바일 폰으로 전송하여 이 정보를 정확하게 입력하여야 최종 로그인이 가능하게 구현하였다. 향후 클라이언트의 BBS를 모바일 버전으로 개발할 경우 모바일의 휴대 인증을 극대화하기 위한 조치로 보다 강력한 형태의 인증 수단이 될 것이다. Fig. 12와 같이 패스코드를 입력한 후 사용자는 실제 서비스를 받기 위한 서비스 페이지로 로그인되어 Fig. 13과 같은 화면에 접근이 가능하게 된다. 본 논문에서는 가상화폐 거래소를 임의로 개발하여 적용하였으며 간단하게 가상화폐를 조회하고 거래할 수 있는 기능을 제공하며 Fig. 13은 초기 화면을 나타내고 있다.

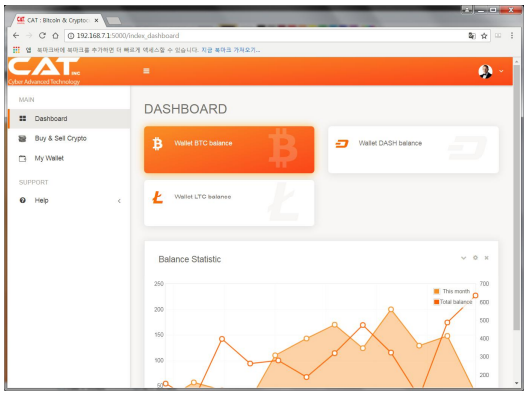

Fig. 13. Dashboard Display

Fig. 14는 로그인 한 사용자의 가상화폐를 거래할 수 있는 화면으로 현재 자신이 보유한 가상화폐 수량을 나타내고 있으며 이를 팔거나 추가로 가상화폐를 구매할 수 있다. 이러한 서비스가 수행될 때 서버에 HTTP 프로토콜로 요청하는 것이 아니라 BBS에서 웹 서비스를 진행 후 필요한 데이터만 서버에 전달하여 데이터 송수신만 진행한다. 즉, 클라이언트 PC에서 BBS간의 통신은 HTTP 통신을 수행하지만 BBS와 서버간의 통신은 CCN 프로토콜을 통해 데이터만 주고받으므로 기존의 웹 서버에 대한 해킹이 이루어질 수 없는 구조로 개발을 하였다.

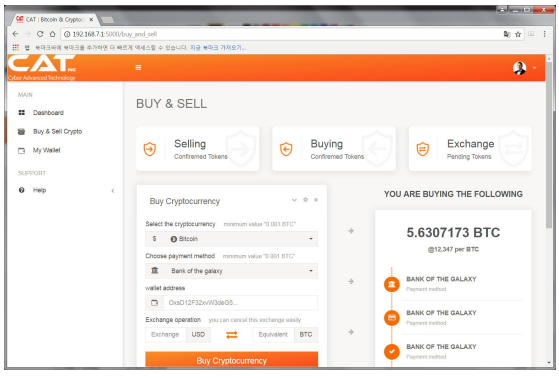

Fig. 14. Buy & Sell Crypto Currency

Fig. 15는 이러한 BBS와 서버간의 CCN 통신을 모니터링 한 것으로 두 개체 간에는 UDP 9696포트를 통해서만 통신이 되는 것을 확인할 수 있다. 즉, 외부에서 이 트래픽을 도청하더라도 기존의 프로토콜로는 해석이 불가능한 형태의 통신이 이루어지므로 비밀성을 확실히 유지할 수 있다. 또한 CCN 통신은 데이터 자체에 전자서명이 기본적으로 적용되므로 데이터에 대한 무결성도 충족할 수 있는 장점을 가진다.

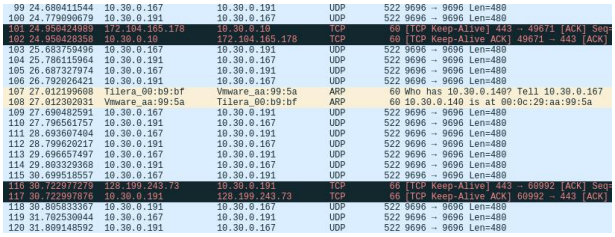

Fig. 15. CCN Traffic with UDP 9696 Port

Fig. 15에서 모니터링 된 패킷을 개별적으로 확인할 경우 Fig. 16과 같이 콘텐트 영역이 자체 암호화되어 해독이 불가능하다는 것을 확인할 수 있다. 이처럼 CCN의 특징을 활용할 경우 기존 TCP/IP에서의 보안상 문제점을 보다 강력하게 해결할 수 있음을 확인할 수 있다. 서버에서는 TCP/IP에 대한 트랙픽 자체를 해석하지 않고 UDP만을 해석함으로써 TCP 플러딩 공격과 같은 기본적인 DDoS 공격의 방어에 대해서도 많은 이점을 가질 수 있다는 것이 장점이다.

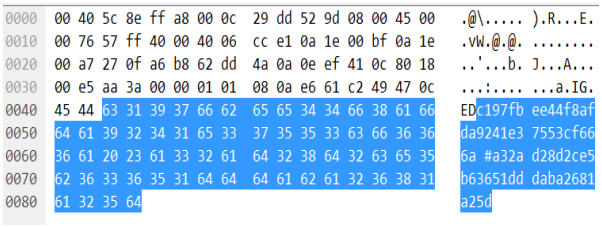

Fig. 16. Encapsulation Data

이와 같이 사용자의 로그인 정보 및 가상화폐에 대한 정보는 서버의 데이터베이스에 저장되어 있으며 Fig. 17과 같이 사용자의 로그인 정보 및 기타정보를 확인할 수 있다. 외부에서는 데이터베이스에 대한 직접적인 참조는 전혀 할 수 없으며 CCN 프로토콜을 통한 간접적인 참조만이 가능하다. 즉, 인터넷을 통해 직접적으로 서버에 침투할 수 있는 방법이 존재하지 않는다. 이처럼 서버 단에는 보안장비를 통해 CCN으로 유입된 프로토콜을 해석한 이후에 서버로 전송되는 서비스 요청에만 응답하므로 인해 외부만 뿐만 아니라 내부망에서의 직접적인 접근이 허용되지 않는다.

본 논문에서 제안한 시스템을 검증하기 위해 서버 단에 Fig. 18과 같이 다양한 형태의 동적코드를 활용하여 공격을 시도하였으나 기본적으로 TCP/IP 패킷은 처리하지 않으므로 Fig. 19와 같이 패킷이 버려지는 것을 확인하였다.

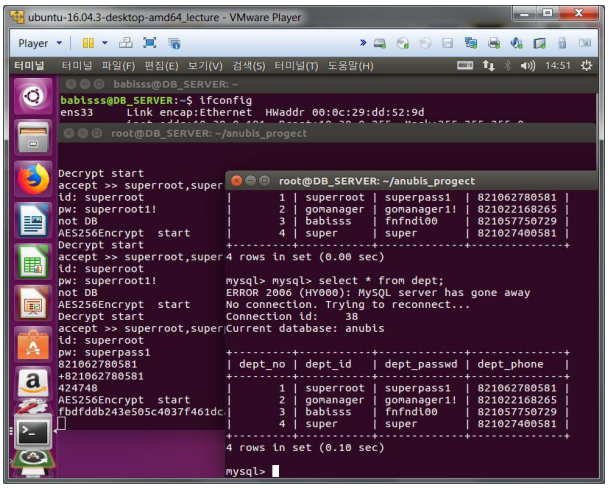

Fig. 17. Policy Server & DB Contents

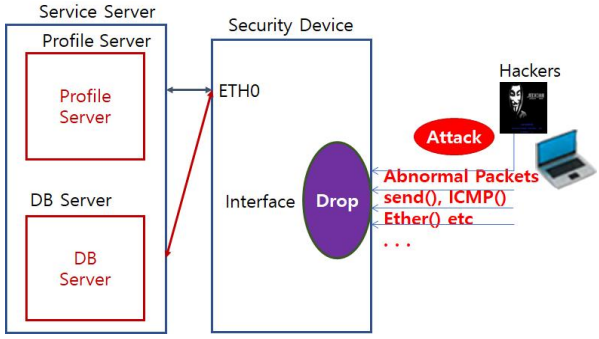

Fig. 18. Attack Test with Dynamic Code

Fig. 19와 같이 외부에서 유입되는 TCP/IP 공격에 대해서는 모든 결과가 패킷을 버리는 결과를 확인할 수 있었으며 이는 근본적인 TCP/IP의 문제점을 해결할 수 있는 강력한 방법이라고 할 수 있다. 이처럼 서버 단에 위협을 초래할 수 있는 웹 서버를 클라이언트 단으로 옮기므로 인해 얻을 수 있는 장점을 통해 가상화폐 거래소와 같이 사용자의 주요 정보를 처리해야 하는 금융시스템에는 본 논문에서 제안한 시스템을 활용할 경우 가장 적합하다고 할 수 있다.

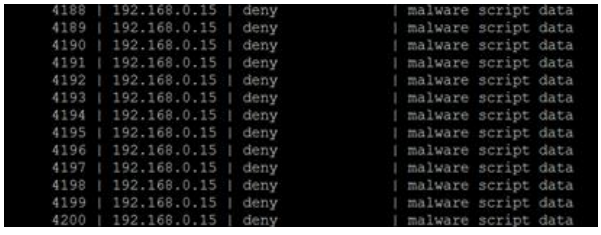

Fig. 19. Dropped Log Data

IV. Conclusions

본 논문에서 제안한 시스템은 기존의 서비스 방식이 아닌 클라이언트의 하드웨어 디바이스를 활용하여 서버 단에 가장 해킹으로부터 위험한 웹 서버를 제거하였다. 웹 서비스는 클라이언트 PC와 연결된 BBS를 통해서만 접근이 가능하므로 매우 안전한 형태의 서비스를 수행할 수 있다. 또한 클라이언트 PC와 연결된 BBS는 물리적으로 완전히 클라이언트 PC와 분리되어 있으므로 인해 악성코드의 감염을 통해서도 BBS에 공격이 이루어지지 않는 특징이자 장점을 제안하였다. 이러한 안전한 BBS를 통한 특정 데이터만 서버에 콘텐트 요청방식의 CCN을 활용함으로써 안전성 및 효율성을 모두 제공할 수 있는 새로운 방식의 서비스라고 할 수 있다.

이와 같이 기존 서비스 방식을 변경시킨 장점을 토대로 첫 번째 서버에 대한 공격의 원천적인 방어, 클라이언트 악성코드 무력화, 네트워크 도청에 대한 방어 등의 강력한 방어 시스템을 갖출 수 있게 되었다.

다만, 클라이언트 PC와 연결된 BBS에 서버의 웹서버를 모두 적재하여야 하는 부담 및 추가 개발은 개선해야 할 부분이라고 판단한다. BBS의 성능적인 문제 및 물리적인 한계가 분명 존재하므로 서버의 일부분을 적재함으로 인해 이러한 문제를 해결하고 또한 서버에 일부 웹서버가 운영되더라도 HTTP 프로토콜이 아닌 CCN 기반의 프로토콜로 통신하므로 인해 본 제안시스템의 장점은 그대로 유지할 수 있는 추가적인 연구가 필요하다고 판단한다.

REFERENCES

[1] Jae-Kyung Park, Won Joo Lee, Kang-Ho Lee, "A Study on the Isolated Cloud Security Using Next Generation Network" Journal of The Korea Society of Computer and Information Vol. 22 No. 11, pp. 41-48, November 2017.

[2] Sung-Jin Kim, Jae-Kyung Park, “Strengthening Authentication Through Content Centric Networking” Journal of The Korea Society of Computer and Information Vol. 22 No. 4, pp. 75-82, April 2017.

[3] Hyung-Su Lee, Jae-Pyo Park, Jae-Kyung Park, “A Network Transport System Using Next Generation CCN Technology” Journal of The Korea Society of Computer and Information Vol. 22 No. 10, pp. 93-100, October 2017.

[4] Jaehoon Kim, et al, “Content Centric Network-based Virtual Private Community,” IEEE ICCE, Las Vegas, January 2011.

[5] Jae-kyung Park, “A study of Secure Total Authentication System”, The Korea Society of Computer and Information Vol.23 No.2, pp. 283-284, 2015.

[6] Parc, A DESCRIPTION OF CONTENT-CENTRIC NETWORKING (CCN) based on a Special Invited Plenary

Short Course by Van Jacobson at the Future Internet Summer School, Bremen, Germany on July 22, 2009.
[7] Van Jacobson, D. K. Smetters, James D. Thornton, Michael Plass, Nick Briggs, and Rebecca Braynard. Networking Named Content. In CoNext, 2009.
[8] Van Jacobson, D. K. Smetters, James D. Thornton, Michael Plass, Nick Briggs, and Rebecca Braynard. Networking Named Content. In CoNext, 2009.
[9] Michael Meisel, Vasileios Pappas, and Lixia Zhang. Ad hoc networking via named data. In MobiArch'10. ACM, 2010.
[10] Van Jacobson, D. K. Smetters, Nick Briggs, Michael Plass, Paul Stewart, James D. Thornton, and Rebecca Braynard. VoCCN: Voice-over Content-Centric Networks. In ReArch, 2009.
[11] Q. Deng, Y. Luo, and J. Ge, "Dual threshold based unsupervised face image clustering," Proceedings of the 2nd International Conference on Industrial Mechatronics and Automation, pp. 436-439, 2010.
[12] SIMGRID Project, http://simgrid.gforge.inria.fr
[13] http://blog.kt.com/1139
[14] http://www.bikorea.net/news/articleView.html?idxno=20827
[15] http://m.etnews.com/amp/20180726000372
[16] https://en.wikipedia.org/wiki/Raspberry_Pi_Foundation

Authors

Jae-Kyung Park received the BS, Department of Computer Engineering, from Dongguk University 1994, MS and Ph.D. degrees in Department of Computer Science from Hongik University, in 1996, 2002, respectively.
Dr. Park joined the faculty of Department of Information Security at Seoul Gangseo Campus, Korea Polytechnics, in 2015. He is currently a Professor in Department of Information Security at Seoul Gangseo Campus, Korea Polytechnics. He is interested in network security and cyber security.

Young-Ja Kim received the BS, MS and Ph.D degrees in Department of Computer from Kunsan National University, in 1993, 1998, 2007, respectively.Dr. Kim joined the faculty of Computer Science at Korea Polytechnics, in 2000. She is currently a Professor in Department of Data Analysis at Seoul Gangseo Campus, Korea Polytechnics. She is interested in network security and cyber security.