HVA를 이용한 안전한 클라이언트 시스템 연구

박재경[O], 김영자[*], 이형수[*]
[O*]한국폴리텍대학 서울강서캠퍼스 정보보안과
e-mail: {jakypark, tiny89, hslee01}@kopo.ac.kr[O*]

A Study of Secure Client System with HVA(High Value Asset)

Jae-kyung Park[O], Young-Ga Kim[*], Hyung-Su Lee[*]
[O*]Dept. of Information Security, Korea Polytechnics College

● 요 약 ●

본 논문에서는 기존의 클라이언트 서버 환경에서 해킹에 취약한 구조를 개선하고자 새로운 형태의 클라이언트 서버 환경을 제안한다. 서버 측에는 기존의 웹 서버를 클라이언트 측으로 내려서 클라이언트가 필요한 데이터 만을 전달하는 방식으로 서버에 웹 공격 자체가 이루어질 수 없는 구조를 제안한다. 이를 통해 기존의 서버가 해킹을 당해 악성코드를 유포하고 서버의 데이터를 해킹하는 문제를 완전히 차단할 수 있음은 물론 클라이언트 PC에 악성코드가 감염되어도 서버에는 여향을 미치지 않는 새로운 패러다임을 제시하고자 한다. 본 논문에서는 클라이언트 측에 USB형태의 BBS(Big Bad Stick) 하드웨어를 통하여 제안하는 환경을 검증하고 서버 측의 보안장비와의 암호화 통신을 통해 안전한 서비스가 제공됨을 증명하여 본 연구가 새로운 보안성을 갖춘 시스템임을 보인다.

키워드: 고가치자산(High Value Asset), CCN(Centext Centric Network), BBS(Big Bad Stick)

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.

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.

본 논문에서는 이러한 문제를 구조적으로 해결하기 위해 서비스를 제공해주는 서버(웹서버)를 클라이언트에 위치시키는 구조적인 변경을 제안하고자 한다. Fig.1과 같이 기존의 방식과는 달리 클라이언트 측에 하드웨어를 설치하여 해당 하드웨어에 웹서비스를 올린후 클라이언트가 접속하는 방식으로 운영된다. 이러한 클라이언트 하드웨어를 본 논문에서는 BBS(Big Bad Stick)이라고 한다. 이 BBS는 기존의 아두이노(Arduino)나 라즈베리파이(Raspberry Pi)와 같은 미니 컴퓨터 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 전달하고 서버 앞단에 보안장비가 이를 복호화하여 뒷단에 데이터베이스 서버로부터 데이터를 받아 전달하는 구조를 갖는다.

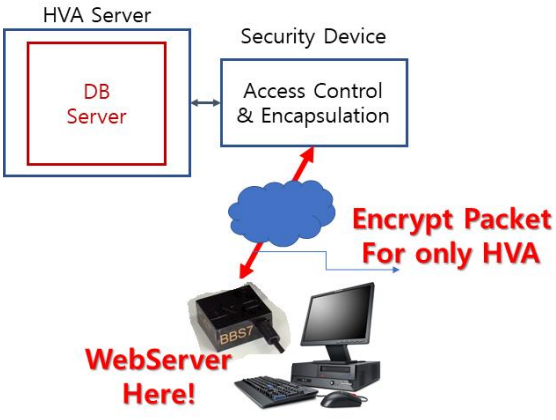

Fig. 1. Proposed New System Diagram

II. The Proposed Scheme

본 논문에서 제안하고자 하는 시스템은 기존의 전통적인 서비스 구성은 해킹을 근본적으로 피할 수 없는 구조를 가지고 있으므로 인해 아무리 많은 보안장비를 서버 앞에 설치를 하더라도 취약점이 발생하면 해킹을 당할 수 밖에 없는 구조이다. 따라서 근본적으로 해킹이 불가능한 구조를 만들어 해킹을 원천차단하고 하는 것이 본 논문의 목표이다. Fig.1과 같은 구조를 사용할 경우 크게 다음과 같은 장점을 가지게 된다.

1. 서버 해킹 불가능

서버에는 Fig.2와 같이 웹서버가 존재하지 않고 단순히 데이터만을 전달하는 서버 즉, HVA서버만 존재한다. 이 HVA서버로의 접근은 웹서버보다 훨씬 더 어렵기 때문에 직접적인 해킹이 거의 불가능하다.

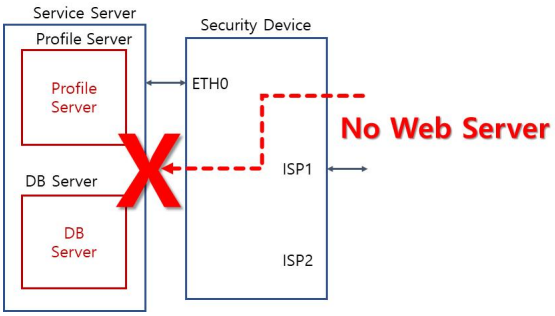

Fig. 2. Eliminate Web Server in Server Part

2. HVA와 외부 클라이언트 통신의 암호화

HVA서버는 외부에서 요구되는 데이터만 특정 키로 암호화하여 전달한다. Fig. 3과 같이 외부의 해커는 이 데이터의 내용을 해석할 수가 없다. 특히 CCN프로토콜을 사용하여 전달할 경우 기존의 TCP/IP 프로토콜이 아니므로 해석 자체가 불가능하다.

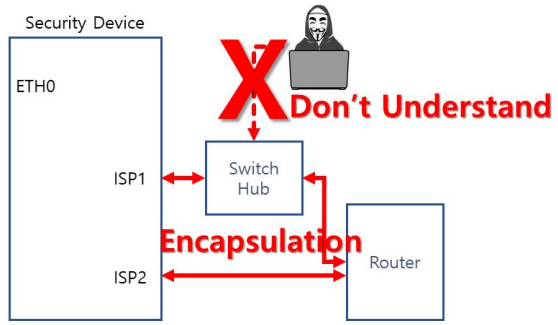

Fig. 3. Packet Encapsulation

III. Conclusions

위에서 설명한 바와 같이 기존의 서비스의 구조를 변경하고 특정 프로토콜을 통해 암호화 통신을 수행할 경우 기존의 해킹방법으로는 해킹자체가 이루어지지 않는 시스템을 제안하였다. 본 시스템을 통해 보다 안전한 형태의 서비스가 이루어질 것이라고 판단한다.

REFERENCES

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

[2] 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.

[3] Jay-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.

[4] 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.