한국컴퓨터정보학회 동계학술대회 논문집 제32권 제1호 (2024. 1)

키 교환 암호 프로토콜 기반 데이터 보안 전송 시스템 및 방법

박재경O
O한국폴리텍대학 서울강서캠퍼스 사이버보안학과
e-mail: jakypark@kopo.ac.krO

A data security transmission system and method based on key exchange encryption protocol

Jaekyung-ParkO
ODept. of Cyber Security, Korea Polytechics

● 요 약 ●

본 논문은 TCP/IP 네트워크 및 암호 프로토콜을 결합하여 CCTV 카메라 영상 데이터를 안전하게 전송하는 시스템에 관한 것이다. 특히, TCP Handshake에서 암호 키를 교환하고, 디바이스의 시그니처 정보를 활용하여 키를 생성하는 키 교환 암호 프로토콜을 도입한다. 이를 통해 CCTV 카메라의 영상 데이터를 암호화하여 전송하고, 수신 시 복호화하여 저장한다. 또한, 적어도 하나 이상의 CCTV 카메라에 대한 보안 인증과 네트워크 연결 상태를 제어하며, 중간자 공격을 방지하기 위한 안전한 키 교환을 수행한다. 이로써 안전성이 강화된 CCTV 카메라 시스템을 제공할 수 있다.

키워드: TCP/IP, 디피헬만(Diffie-Hellman), 시그니처(Signature), CCTV, 인증(Authentication)

I. Introduction

본 논문은 안전한 데이터 전송을 위해 표준 TCP/IP 네트워크와 암호 프로토콜의 특징을 융합한 획기적인 시스템에 대한 것이다. 주로 CCTV 카메라의 영상 데이터 보안 전송을 중점적으로 다룬다. 현대 사회에서 안전에 대한 관심이 높아지면서 CCTV 카메라의 보급이 증가하고 있으며, 이러한 카메라를 통해 얻은 영상 데이터는 다양한 목적으로 활용되고 원격지로 전송된다. 그러나 원격지 전송은 네트워크 보안 수준에 따라 해킹의 위험성이 존재한다. 이에 대응하여 데이터 전송 시 발생할 수 있는 해킹, 데이터 변조, 위조 등의 보안 위협을 방지하기 위해 다양한 암호 알고리즘을 활용한 데이터 암호화가 이뤄지고 있다.

종래 기술에서는 대칭키 방식을 주로 사용하며, 이를 안전하게 관리하고 공유하기 위한 과정이 필요하다. 대칭키 공유를 위해 RSA와 같은 비대칭키를 활용한 방법과 암호화 채널 없이 키 교환 알고리즘을 사용하는 방법이 있다.

특히, 디피 헬만 알고리즘은 미리 준비된 키 없이 안전한 키 교환을 가능케 하며, 이산 대수를 기반으로 하여 안전성이 유지되는 장점이 있다.

그러나 중간자 공격(MIM)에 취약한 측면이 있어 이를 보완하기 위한 안전한 키 교환 프로토콜이 필요하다.

본 논문은 이러한 문제점을 극복하기 위해 안정성을 보장할 수 있는 키 교환 과정과 함께 대칭키를 사용하여 영상 데이터를 암호화하는 보안 시스템을 제안한다. 이를 통해 CCTV 카메라 영상 데이터의 안전한 전송이 가능해지며, 최소한 하나의 CCTV 카메라에 대한 보안 인증과 네트워크 연결 상태를 효과적으로 관리할 수 있다. 따라서, 안전성이 강화된 CCTV 카메라 시스템을 제공함으로써 실시간 영상 데이터 전송의 보안성과 효율성을 증대시킬 것으로 기대된다.

II. Preliminaries

1. Related works

1.1 국내 동향

제로 트러스트는 네트워크 경계와 관계없이 아무도, 그리고 어떤 활동이든 기본적으로 신뢰하지 않는 것에 바탕을 둔 보안 개념이다[1].

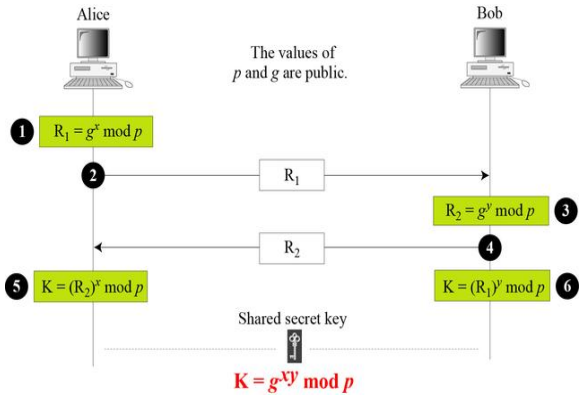

Fig. 1. System Architecture

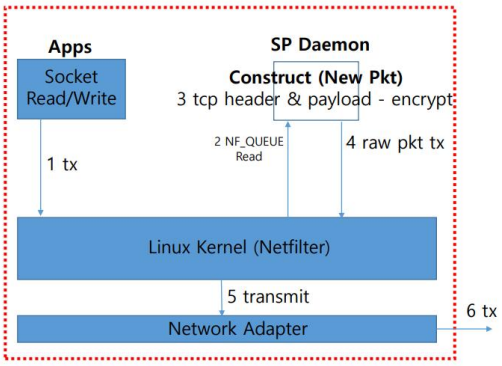

Fig. 3. Packet Transmission at Host

III. The Proposed Scheme

본 논문은 기존의 TCP/IP 네트워크와 암호 프로토콜의 결합으로 인한 문제점을 극복하고, 효과적이며 강력한 보안 프로토콜을 개발하기 위한 것이다. 기존 키 교환 및 암호 프로토콜의 현실적인 문제를 보완하고, 이를 효과적인 통신 프로토콜과 결합하여 네트워크 계층에 강화된 보안 기능을 제공하는 키 교환 암호 프로토콜 기반 데이터 시스템과 암호화 방법을 제공한다.

한 실시예에 따른 이 시스템은 클라이언트 장치와 보안 데이터 서버로 구성되며, 시그니처 정보를 통해 장치 등록을 요청하고 키 교환 암호 프로토콜을 사용하여 암호키를 교환한다. 클라이언트 장치는 해당 암호키를 사용하여 데이터를 암복호화하며, 보안 데이터 서버는 클라이언트 장치의 시그니처 정보를 수신하여 등록하고, 키 교환 암호 프로토콜을 사용하여 암호키를 교환한다. 이때, 키 교환 암호 프로토콜은 시그니처 정보를 활용하여 키 교환을 수행한다.

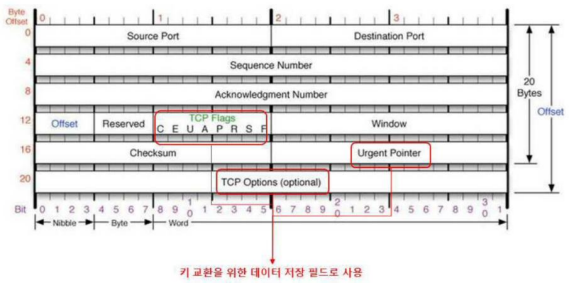

Fig. 2. TCP/IP Option

IV. Conclusions

본 논문은 표준 TCP/IP 네트워크의 특징 및 암호 프로토콜의 특징을 결합하여 TCP Handshake 단계에서 암호 키 교환을 수행하고, 디바이스의 고유한 시그니처 정보를 사용하여, 암호 키 생성 데이터로 사용하여, 보안성을 강화하는 것을 특징으로 하는 네트워크 계층에 강화된 보안 기능을 활용한 키 교환 암호 프로토콜 기반 데이터 시스템 및 암호화 방법에 관한 것으로 안전한 CCTV 개발에 적용할 경우 보다 안전한 CCTV 통신을 수행할 수 있을 것으로 기대한다.

REFERENCES

[1] 윤대균, “클라우드를 위한 제로 트러스트 보안”, 디지털서비스 이슈리포트, 2022.

[2] Department of Defense (DOD), “DOD Zero Trust Reference Architecture,”, 2021.

[3] Office of Management and Budget, “Moving the U.S. Government Towards Zero Trust Cybersecurity Principles”, 2021

[4] NSA, "Embracing a Zero Trust Security Model", 2021.