네트워크 계층에 강화된 보안 기능을 활용한 키 교환 암호 프로토콜 기반 데이터 시스템 및 암호화 방법

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

A DATA SYSTEM AND ENCRYPTION METHOD BASED ON KEY EXCHANGE CRYPTOGRAPHIC PROTOCOL USING ENHANCED SECURITY FUNCTION IN NETWORK LAYER

Jaekyung-ParkO
ODept. of Cyber Security, Korea Polytechics

● 요 약 ●

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 특징 으로 하는 네트워크 계층에 강화된 보안 기능을 활용한 키 교환 암호 프로토콜 기반 데이터 시스템 및 암호화 방법에 관한 것으로 개발된 프로토콜을 키 교환 프로토콜로 대체할 경우 보다 안전한 보안 프로토콜을 제공할 수 있다.

키워드: TCP/IP, 디피헬만(Diffie-Hellman), 시그니처(Signature), 키 생성(Key Generation), 인증(Authentication)

I. Introduction

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 것이다. 최근, 통신기술 및 IT기술이 발달하면서 보안에 대한 중요성이 커지고 있다. 특히 데이터 통신 네트워크에 기반하여 데이터를 전달, 교환, 수집, 저장하는 모든 시스템 및 디바이스는 데이터 전송 시 발생하는 해킹, 데이터 변조, 위변조 등의 보안 위협을 방지하기 위해, 다양한 암호 알고리즘을 적용한 데이터 암호화를 적용하고 있다. 이러한 암호화 알고리즘 중, 디피 헬만(Diffie-Hellman) 알고리즘은, 두 당사자 간에, 사전에 준비된 키가 없더라도, 일련의 패킷(데이터)를 교환해가며 대칭 키를 합의하는 키 교환 알고리즘이다. 디피 헬만 알고리즘은 대칭키를 사용하므로, 암복호화 속도가 빠르고, 사전에 준비된 키가 없어도 키 교환을 통해 비밀키를 만들 수 있으며, 이산 대수를 기반으로 하고 있으므로, 이산 대수 문제의 어려움으로 인해 안전성이 유지되는 장점이 있다. 그러나, 중간자가 개입하여 키 교환 단계에서의 데이터를 조작하면 MIM(Man In the Middle attack)에 취약한 문제점이 있다. 따라서, 상기 문제를 보완하여, 키 교환 과정에서의 안정성을 보장할 수 있는 보안 프로토콜을 적용하여 데이터 통신을 수행하는 시스템 및 방법이 필요할 것이다. 이를 통해 데이터 전송의 보안성과 효율성을 증대시킬 것으로 기대된다.

II. Preliminaries

1. Related works

1.1 국내 동향

암호화 알고리즘 중에서 디피 헬만(Diffie-Hellman) 알고리즘은 두 당사자 간에 미리 준비된 키가 없어도 일련의 패킷(데이터)를 교환하여 대칭 키를 합의하는 키 교환 알고리즘이다. 이 알고리즘은 대칭 키를 사용하여 암복호화 속도가 빠르고, 사전에 준비된 키가 없어도 키 교환을 통해 비밀키를 생성할 수 있으며, 이산 대수를 기반으로 하여 이산 대수 문제의 어려움으로 인해 안전성을 유지하는 장점이 있다.

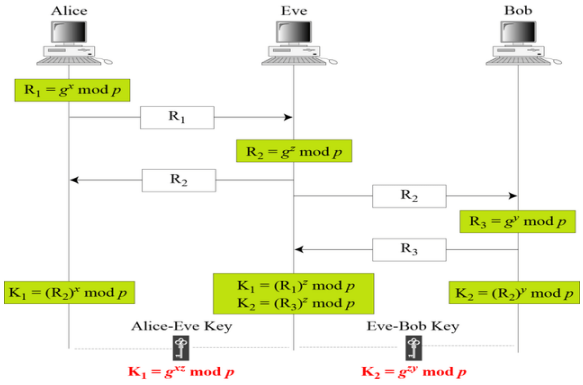

Fig. 1. Diffie-Helman System Architecture

III. The Proposed Scheme

본 논문은 기존 키 교환 및 암호 프로토콜의 현실적인 문제를 보완하고, 통신의 효율성과 안전성을 향상시키기 위해 표준 TCP/IP 네트워크 특성과 암호 프로토콜을 결합한 새로운 논문을 제안한다. 이로 인해 강력한 보안 프로토콜을 개발하고 효과적인 프로토콜을 기반으로 네트워크 계층에서 보안 기능을 강화하는 것을 목표로 한다.

본 논문의 일 실시예에 따른 네트워크 계층에 강화된 보안 기능을 활용한 키 교환 암호 프로토콜 기반 데이터 시스템은 클라이언트 장치와 보안 데이터 서버로 구성된다. 이 시스템은 시그니처 정보를 전달하여 장치 등록을 요청하고, 키 교환 암호 프로토콜을 사용하여 암호키를 교환한다. 클라이언트 장치는 암호키를 사용하여 데이터를 암복호화하며, 보안 데이터 서버는 클라이언트 장치의 시그니처 정보를 수신하여 등록하고, 상기 등록된 클라이언트 장치와 키 교환 암호 프로토콜을 사용하여 암호키를 교환한다. 이 때, 키 교환 암호 프로토콜은 시그니처 정보를 활용하여 키 교환을 수행하는 것이 특징이다.

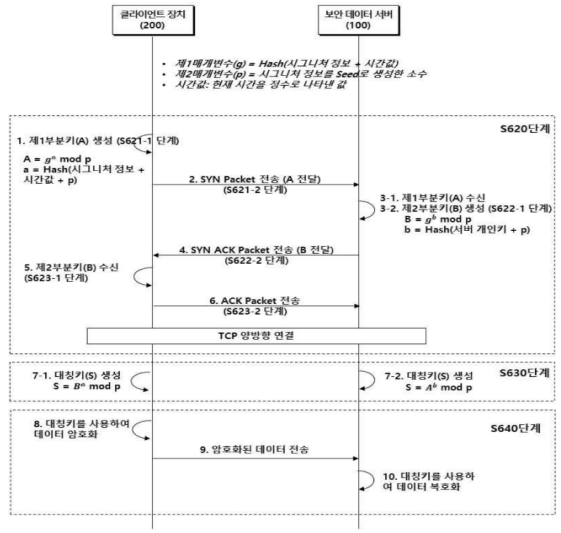

Fig. 2. Key Exchange Protocol

IV. Conclusions

본 연구에서는 표준 TCP/IP 네트워크 특성 및 암호 프로토콜의 결합을 통해 TCP Handshake 단계에서의 효율적인 암호 키 교환을 수행하며, 디바이스의 고유한 시그니처 정보를 활용하여 암호 키 생성 데이터로 사용하는 네트워크 계층 강화된 보안 기능을 도입한 키 교환 암호 프로토콜을 제안하였다. 이를 통해 데이터 시스템의 보안성을 강화하고 안전한 암호화 방법을 제시하였으며, 향후 네트워크 보안 분야에서의 활용 가능성을 모색할 수 있을 것으로 기대된다.

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