J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

STRIDE 위협 모델링 기반 가상 사설망 취약점 분석 및 보안 요구사항 도출☆

Analyze Virtual Private Network Vulnerabilities and Derive Security Guidelines Based on STRIDE Threat Modeling

김 다 현[1] 민 지 영[1] 안 준 호[1*]
Da-hyeon Kim Ji-young Min Jun-ho Ahn

요 약

디지털 통신 환경 기술이 다양화되고 네트워크 이용 접근성이 높아지고 있으며 보안이 중요한 방산업체, 국방 관련 기관 등 국가의 안보에 관련된 다양한 환경에서 가상 사설망 서비스를 사용한다. 하지만 기술에 발전에 따라 매년 가상 사설망의 취약점을 통한 공격이 증가하고 있다. 본 논문은 가상 사설망에서 발생 가능한 잠재적 취약점 및 신규 취약점에 대해 대비하기 위해 STRIDE 위협 모델링을 통해 보안 요구사항을 도출하였다. STRIDE 위협 모델링은 위협을 총 6가지 범주로 그룹화 위협을 체계적으로 식별한다. 이를 적용하기 위해 가상 사설망의 기능을 분석하고 가상 사설망 서비스가 이루어지는 동안의 자료 흐름도를 생성하였다. 그 후, 가상 사설망에서 발생 가능한 위협을 수집하고 이를 기반으로 STRIDE 위협 모델링을 분석했다. 생성한 가상 사설망의 자료 흐름도는 총 96개의 STRIDE 위협으로 분류되며, 실제 취약점 리스트와 비교 분석하여 분류 결과를 구체화했다. 그 후 위협들의 공격 루트를 파악하기 위해 위협 시나리오를 작성했다. 본 논문은 작성된 시나리오를 기반으로 가상 사설망의 구성요소에 따른 총 30개의 보안 요구사항을 도출했다. 본 논문을 통해 국방부와 같이 보안이 중요한 시설에서 사용하는 가상 사설망의 보안 안정성을 높일 수 있는 보안 요구사항을 제시한다.

☞ 주제어 : 가상 사설망, STRIDE 위협 모델링, 위협 분석, 위협 시나리오, 보안 요구사항

ABSTRACT

Virtual private network (VPN) services are used in various environments related to national security, such as defense companies and defense-related institutions where digital communication environment technologies are diversified and access to network use is increasing. However, the number of cyber attacks that target vulnerable points of the VPN has annually increased through technological advancement. Thus, this study identified security requirements by performing STRIDE threat modeling to prevent potential and new vulnerable points that can occur in the VPN. STRIDE threat modeling classifies threats into six categories to systematically identify threats. To apply the proposed security requirements, this study analyzed functions of the VPN and formed a data flow diagram in the VPN service process. Then, it collected threats that can take place in the VPN and analyzed the STRIDE threat model based on data of the collected threats. The data flow diagram in the VPN service process, which was established by this study, included 96 STRIDE threats. This study formed a threat scenario to analyze attack routes of the classified threats and derived 30 security requirements for each element of the VPN based on the formed scenario. This study has significance in that it presented a security guideline for enhancing security stability of the VPN used in facilities that require high-level security, such as the Ministry of National Defense (MND).

☞ keyword : Virtual Private Network, STRIDE threat modeling, Threat Analysis, Threat Scenario, Security Requirement

1. 서 론

오늘날 네트워크 장비나 휴대용 전자 기기의 보급과 같이 디지털 통신 환경 기술은 다양화되고 있으며 다양한 연결망으로 네트워크 이용 접근성이 높아지고 있다. 한편 무분별한 인터넷 연결은 사용자의 개인 정보나 구

1 Dept. of Software, Korea National University of Transportation, Chungju-si, 27469, Korea.
* Corresponding author (jhahn@ut.ac.kr)
[Received 29 August 2022, Reviewed 17 Septebmer 2022(R2 13 October 2022), Accepted 25 October 2022]
☆ This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (No. 2020R1I1A3068274). This research was supported by National Security Research Institute Established an Affiliated of ETRI (No. 202200600001).

동 환경의 노출 등 내부 보안상 위협이 존재하게 된다. 따라서 공공기관이나 기업의 경우, 자체 내부 인트라넷 환경을 조성하여 사내 기밀 누출의 위협을 줄이고 안전한 통신환경을 구축하게 된다. 우리나라의 국방은 국방부의 국한된 것이 아닌 한국의 안보를 위한 기술 자료, 고위 인사의 일정 자료, 방산 업체의 국방자료 등을 모든 것을 의미한다. 국방부가 발표한 보도자료[1]에 따르면 전투 효율성과 스마트 국방혁신의 필요성을 체감하여 스마트 기술을 통해 다양한 공격 양상에 대비하는 첨단전력을 증가하는 과제를 제안하였다. 또한, 국방부 산하의 방위사업청에서 제시한 방위산업기술 보호 종합계획에 따르면 사이버 위협 대응 역량 강화를 위해 가상 사설망 사용으로 인한 취약점을 점검한다[2]고 한다. 최근 가상 사설망의 취약점을 통해 한국항공우주산업 KAI에 공격자가 침입한 사건이 있다[3]. 이때, 대통령 참석 일정과 동선이 포함된 극비문서가 유출되었다. 이처럼 국방에서 가상 사설망의 취약점 식별 및 위협 대응에 중요도가 커지고 있다.

가상 사설망(Virtual Private Network, VPN)이란 공중망 상에 사설망을 구축하여 마치 사설 구내망 또는 전용망 같이 이용하는 통신망을 의미한다[4]. 가상 사설망 서비스를 이용하여 접속 반경의 범위를 넓히고 암호화된 사설망으로 안전한 데이터의 전송을 할 수 있다. 가상 사설망의 종류에는 개인 가상 사설망, 사이트 간의 가상 사설망, 원격 제어 가상 사설망, 모바일 가상 사설망 등 다양한 가상 사설망이 있다. 가상 사설망을 통해 내부망을 보안하고 있지만, 기술에 발전에 따라 해킹, 침투 공격 등의 위협도 증가하고 있다. 이에 따라, 가상 사설망의 취약점을 악용한 공격한 사례 역시 지속해서 발견되고 있다. 가상 사설망을 연결할 때, 내부망과 외부망을 제대로 분리하지 않아 가상 사설망과의 망 접점을 타고 기밀 정보를 탈취해간 사례[5]가 있다. 또 다른 사례로는 국내 가상 사설망의 취약점을 악용하여 기관과 기업의 내부망에 백도어를 설치하고 피해 기관에 소속된 직원의 이메일 주소와 계정정보를 탈취한 사례[6]가 있다. 가상 사설망을 공격할 경우 사용자의 개인 정보나 접속 이력, 기밀 파일, 사용자 권한 등 방대한 데이터와 네트워크가 공격자에게 그대로 노출되어 보안성을 침해할 수 있으므로 본 논문은 위협 모델링을 통해 가상 사설망의 보안 요구사항을 도출한다. 이를 위해 본 연구에서는 가상 사설망의 데이터 흐름도를 생성하고 STRIDE 위협 모델링을 통해 취약점을 식별 및 분석한다. 분석된 취약점을 통해 보안 요구사항을 도출하게 된다. 이와 같은 보안 요구사항을 통해 가상 사설망의 안정성과 보안성을 높이고 알려지지 않은 취약점들에 대해 보호 가능할 것이다.

본 논문은 2장에서 위협 모델링과 관련된 연구 및 가상 사설망의 취약점을 식별하는 연구들을 소개하며 3장에서 본 연구에서 제안하는 방법론의 전체 프로세스를 설명한다. 4장은 제안하는 방법론을 가상 사설망에 적용하여 취약점을 식별하고 보안 요구사항을 도출하는 과정을 구체적으로 서술하고 있다. 마지막 5장에서는 본 논문의 결론 및 도출된 보안 요구사항의 기대효과에 관해 서술한다.

2. 관련 연구

가상 사설망 장소의 제약 없이 넓은 공중망을 내부의 사설망처럼 이용한다는 이점이 있기 때문에 다양한 분야에서 사용된다. 이때, 가상 사설망의 취약점으로 인해 위협이 발생하면 이는 사설망의 위협으로 대규모의 피해가 발생할 수 있다. 따라서 이를 막기 위해 가상 사설망의 보안을 위해 취약점을 분석하는 다양한 연구[7-10]가 있다. 가상 사설망을 통해 차단된 콘텐츠를 사용하는 경우를 탐지하기 위해 Psiphone, OpenVPN 등 대표적인 가상 사설망 서비스를 분석한 연구[7]가 있다. 분석한 가상 사설망 서비스를 이용한 웹 서비스 중 웹 트래픽을 탐지 및 분류에 가장 적합한 가상 사설망 서비스를 도출했다. IoT 환경에서 엔드 포인트를 보호하기 위한 가상 사설망 보안을 제안하는 연구[8]가 있다. 해당 연구는 가상 사설망의 대표적인 보안 방법 중 IPsec/IPv6와 OpenSSL의 각각의 단점을 보완하고 장점을 조합하는 하이브리드 방식을 제안한다. COVID-19로 인해 가상 사설망을 사용하는 기업이 증가하고 있고 내부망을 보안하기 위해 실무자를 위한 가이드라인을 생성한 연구[9]가 있다. 해당 연구는 전문가와 비전 문자의 지식수준을 분석하고 가상 사설망을 사용하는 시점 등을 분석하여 실제 가상 사설망을 사용하는 실무자를 위한 가이드라인의 초안을 생성했다. 가상 사설망 내 암호화된 트래픽들 중 악성 트래픽을 식별하는 연구[10]가 있다. 해당 연구는 mRMR을 통해 암호화된 트래픽 중 중요한 트래픽을 추출하고 앙상블 모델을 통해 암호화된 악성 트래픽들을 식별한다. 본 연구는 다양한 기업 및 환경에서 사용되는 가상 사설망을 보안하기 위해 위협 모델링을 통해 취약점을 식별하고 보안 요구사항을 도출했다.

위협 모델링이란 보안 요구사항을 식별하여 위협 및 잠재적인 취약성을 도출하고 보안 지표를 목적으로 하는 구조화된 프로세스이다. 위협 모델링은 기존에 대상에

대한 취약점을 점검하기 위한 침투 테스트 및 코드 검토에서 사용되는 예산을 절감할 수 있고, 이와 같은 테스트에서 간과될 수 있는 취약점을 발견할 수 있다. 또한, 단일 모듈별 위협을 도출한 것이 아닌 각 모듈이 연결되어 공격자가 보낸 악성 메시지 등에 영향을 받는 모든 모듈을 도출할 수 있다. 위협 모델링에는 STRIDE[11], PASTA[12], LINDDUN[13], DREAD[14], OCTAVE[15], TVRA[16] 등이 있다. STRIDE 위협 모델링은 Microsoft 사가 SDL(Security Development Lifecycle)기반으로 개발한 컴퓨터 보안 위협 식별 모델링 방법론으로 총 6가지에 대해 위협을 범주화하여 체계적으로 분류한다. 제품뿐 아니라 제품을 개발하고 관리하는 모든 비즈니스 측면의 보안 위협을 분석하여 취약 상황을 단계별 프로세스로 제공하는 Versprite 사의 PASTA 방법론이 있다. 시스템 내 개인 정보 위협 완화를 위해 시스템 모델링, 위협 유도, 위협 관리 총 3단계 분석을 통해 LINDDUN의 7자기 위협 범주로 그룹화한 LINDDUN 방법론이 있다. Microsoft 사가 개발한 DREAD 별로 위협을 군집화하고 위협을 계산하여 위협 등급을 정의한 DREAD 방법론이 있다. Software Engineering Institute (SEI) 의 보안 전문가가 개발하여 3단계로 구성된 다양한 조직 내부의 사람들을 통해 조직의 보안 요구사항을 해결할 수 있는 OCTAVE 방법론이 있다. ETSI (European Telecommunications Standards Institute)에서 개발한 10가지 단계에 따라 주요 자산을 식별하고 그에 따른 시나리오 및 리스크를 평가하는 TVRA 방법론 등이 있다. 이때 본 논문에서는 다른 보안 위협 모델링과 비교했을 때 일반적인 상황에 사용이 가능하고, 비즈니스가 아닌 제품 및 시스템에 적용할 수 있으며, 공개된 자동화 분석 도구를 제공하고, 개발 단계가 아닌 완제품에도 적용이 가능한 STRIDE 위협 모델링 도구를 선정했다. STRIDE 위협 모델링은 총 6가지 범주로 위협을 범주화하여 보안 전문가뿐만 아니라 일반 사용자도 사용이 가능한 도구이다. STRIDE는 각 위협 범주별 의미와 보안 속성은 표 1과 같다.

STRIDE 위협 모델링을 통해 대상에 보안 요구사항을 도출하고 이를 기반으로 대상의 보안 가이드라인을 제시한 다양한 연구[17-19]가 있다. 보안 위협 모델링과 국제 공통평가 기준(CC 인증)을 통해 IP Camera의 보안 요구사항을 도출한 연구[17]가 있다. 해당 연구는 IP Camera의 정확하고 객관적인 보안 요구사항을 도출하기 위해 보안 위협 모델링을 활용했으며, 이를 통해 도출된 보안 요구사항은 IP Camera 만에 국한되는 것이 아닌 카메라를 사용하는 관리자와 카메라를 통해 저장되는 데이터의 흐름

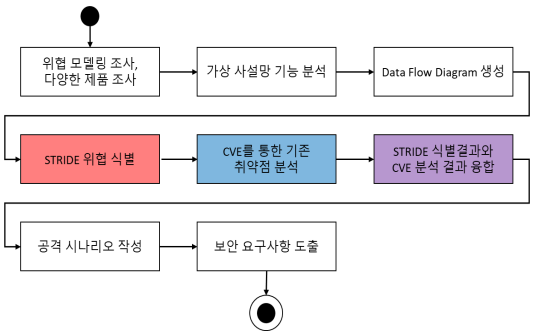
(표 1) STRIDE 각 범주별 정의와 보안 속성
(Table 1) STRIDE Definitions and Security Properties for Each Category

위협 범주	정의	보안 속성
Spoofing	공격자가 다른 사람으로 위장하여 데이터를 취득	Authentication (인증성)
Tampering	시스템이나 사용자가 전달하는 데이터 수정	Integrity (무결성)
Repudiation	시스템이 사용자의 작업을 적절하게 처리하지 않음	Non-repudiation (부인방지)
Information disclosure	시스템에서 전송 및 저장하는 중요 데이터를 열람	Confidentiality (기밀성)
Denial of service	시스템의 서비스를 거부하여 가용성 저하	Availability (가용성)
Elevation of privilege	공격자가 권한 상승을 통해 시스템 권한 획득 및 권한 외 정보에 접근	Authorization (권한 부여)

등 넓은 식별 범위를 가질 수 있게 된다. IP Camera처럼 스마트 도어락의 보안성 향상을 위해 위협 모델링을 적용한 연구[18]가 있다. 해당 연구는 STRIDE를 통해 식별된 위협에 대해 DREAD 분석 기법을 적용하여 위협에 대한 위험도를 제시하였다. 또 다른 연구[19]는 클라우드 컴퓨팅 환경의 보안을 위한 클라우드 보안 관제 시스템에 위협 모델링을 통해 분석된 보안 요구사항을 도출했다. 해당 연구는 클라우드 보안관제 시스템의 DFD를 그린 뒤, STRIDE 위협 모델링을 통해 클라우드 보안관제 시스템의 정보 보안 요소를 식별하였다. 그 후 공격 트리를 통해 공격 루트 및 시나리오를 구성하고 보안 요구사항을 도출한 연구이다. 선박 사이버 보안을 위해 위협 모델링을 적용한 연구[20]도 있다. 해당 연구에서는 선박 시스템에서 발생 가능한 보안 취약점과 사례를 통해 보안 요구사항을 도출하고 선박 시스템의 보안 대책을 제시하고 있다.

3. STRIDE 위협 모델링 적용 방법론

STRIDE 위협 모델링을 가상 사설망에 적용하기 위한 방법론은 그림 1과 같이 총 6가지 프로세스를 가진다. 다양한 위협 모델링을 중 취약점을 분석할 제품과 보호해야 할 정보자산에 가장 적합한 위협 모델링을 선정해야 한다. 예를 들어 일반적이고 다양한 제품에서 취약점을 식별하는 경우 STRIDE 위협 모델링이 가장 대표적이다. 하지만 보호해야 할 정보자산이 개인 정보일 때 개인 정보 취약점 식별을 위해 개발된 LINDDUN 위협 모델링을 통해 취약점을 식별하는 것이 더 적합하다. 가상 사설망



(그림 1) 위협 모델링 적용 프로세스
(Figure 1) Threat Modeling Application Process

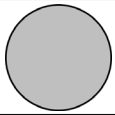
의 기능을 분석하고 기능에 따른 DFD를 생성한다. STRIDE 위협 모델링은 위협이 발생하고 영향을 받는 프로세스를 분석하기 위해 DFD 기반에서 취약점을 식별하게 된다. 생성된 DFD 기반으로 STRIDE의 위협을 식별하고 CVE 통해 실제 공개된 가상 사설망의 위협을 취약점을 식별 및 분류했다. STRIDE를 통한 취약점 식별 결과는 추상적일 수 있어 CVE와 융합하여 식별 결과를 구체화했다. STRIDE와 CVE를 융합한 결과를 바탕으로 공격 시나리오를 작성하여 공격루트 등을 파악하였다. 최종적으로 취약점이 발생 가능한 위치에 따른 보안 요구사항을 도출했다. 본 연구에서 취약점을 식별하고 분석하기 위한 프로세스 제안하고 있다. 이를 가상 사설망 서비스에 적용하여 가상 사설망의 취약점을 식별 및 분석하고 보안 안정성을 높이기 위한 보안 요구사항을 도출하였다.

4. 가상 사설망 위협 모델링

4.1 가상 사설망 기능 분석

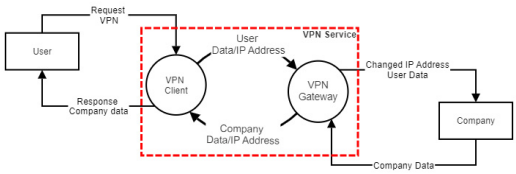
가설 사설망이 가지는 기능들을 분석한다. 본 연구에서는 인증 사무국에서 인증받은 가설 사설망 제품들의 인증 보고서[21-23]와 가설 사설망과 관련된 연구들[24-26]을 통해 기능을 분석했다. 가상 사설망은 네트워크 보안을 위해 인가된 사용자만 접근 가능하고 허용된 트래픽만 통과돼야 한다. 또한, 관리자가 설정한 규칙에 따라 내외부 네트워크 간의 인출 및 인입되는 데이터에 정보를 차단해야 한다. 가상 사설망 서비스는 사용자들과 연결 정보 등에 대한 감사데이터를 생성하고 이를 관리자에게 제공할 수 있어야 한다. 또한, 가상 사설망은 정확한 서비스를 보장하기 위해 시동 시, 주기적으로 자체시험을 실행하고 가상 사설망 구성의 설정값 및 서비스의 무결성을 검증해야 한다. 이와같이 도출된 기능을 통해 가상 사설망의 서비스 구성과 데이터 흐름을 분석하였다.

(표 2) DFD 구성요소
(Table 2) Elements of DFD

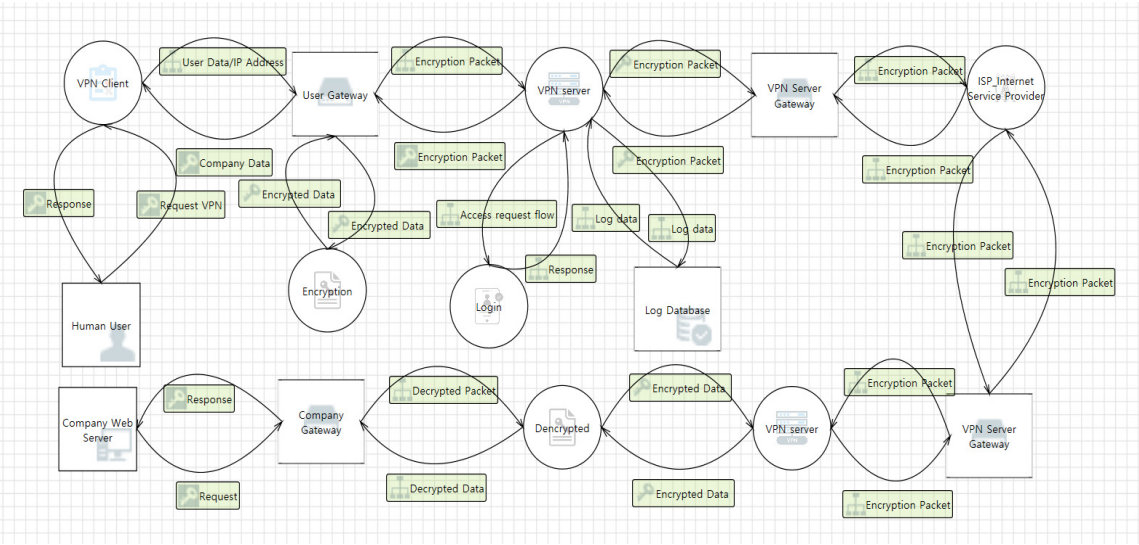
요소	상징	의미
외부 객체		데이터를 생성하고 소비하는 외부 객체로 직사각형으로 표현
프로세스		입력된 데이터가 처리되고 변환되어 출력되는 프로세스로 원으로 표현
데이터 저장소		데이터가 저장된 곳으로 평행선으로 표현
데이터 흐름선		각 구성요소 간의 관계 및 데이터 흐름을 나타내며 방향을 가진 화살표로 표현

4.2 Data Flow Diagram

가상 사설망의 기능을 바탕으로 본 논문에서는 Data Flow Diagram (DFD) 를 도출했다. DFD는 총 4가지의 구성요소와 3단계를 통해 대상의 데이터 흐름을 표현한다. 이때, DFD를 표기하기 위한 다양한 표기법 [27] 이 존재하며 본 연구에서는 표 2과 같은 DFD 상징을 사용하여 DFD를 표현했다. DFD는 하위 단계가 될수록 대상에 대한 데이터 흐름이 더욱 구체적으로 표현되는데, 0단계는 대상에 대한 간단한 상황도이다. 1단계는 상황도를 하위 프로세스로 나눠 시스템이 수행하는 주요 기능을 표현하며 2단계는 해당 주요 기능들에 대한 하위 프로세스를 통해 더욱 구체적이고 세부적으로 표현한 것이다. 그림 2는 가상 사설망의 0단계 DFD이다. 이때, 사용자가 가상 사설망 서비스를 통해 회사 내부망에 접속을 요청하고 있다. 가상 사설망은 사용자의 IP 주소를 회사 IP 주소로 변



(그림 2) 가상 사설망 0단계 DFD
(Figure 2) VPN Level 0 DFD



(그림 3) 가상 사설망 2단계 DFD
(Figure 3) VPN Level 2 DFD

경해 사용자의 환경과 회사 내부망을 연결해주는 Personal 가상 사설망 이용 상황이다. STRIDE를 적용하기 위해 Microsoft 사의 Threat Modeling Tool (TMT) [28] 를 사용하여 최종적으로 생성한 가상 사설망의 2단계 DFD는 그림 3과 같다. 사용자는 본인의 환경에서 가상 사설망의 클라이언트 프로그램을 통해 회사 내부망의 접속을 요청한다. 클라이언트 프로그램은 사용자 환경의 네트워크망을 지나가며 보내지는 데이터는 암호화가 되고 이는 가상 사설망의 서버가 있는 환경에 도달한다. 이때, 사용자는 로그인을 통해 본인을 인증해야 한다. 해당 서버에서는 접속된 사용자, 사용자의 이용 설정, 접속 시간, 접속 주소 등 다양한 로그 정보를 기록한다. 또한, 사용자에 따른 변환 주소나 사용자가 이용하는 클라이언트 프로그램을 관리한다. 그 후, 암호화된 정보는 가상 사설망의 게이트웨이를 통과하여 회사의 내부망 IP로 접속이 가능해진다. 데이터는 변조된 IP 주소와 연결되기 위해 IPS 백본을 통해 전송되어 최종적으로 회사 서버에 도달하게 된다. 사용자가 보내고자 한 데이터가 회사에 보내지게 되고 회사에서도 데이터를 사용자에게 보내기 때문에 모든 데이터 흐름 선은 양방향이다. DFD에 사용된 각 구성요소에 대한 설명은 표 3과 같다.

4.3 STRIDE 위협 도출

STRIDE를 통해 식별 및 분류한 결과는 표 4과 같다. 각 범주별 도출된 총 위협은 96가지이며 이때, 가상 사설망에서는 권한 상승에 대한 위협이 23개로 가장 많았다. STRIDE로 식별된 결과를 구체화하고 실제 취약점과 비교 분석하기 위해 공개된 취약점 리스트인 CVE [29] 를 통해 취약점을 분석했다. 이때, CVE 총 165개의 가상 사설망과 관련된 취약점과 STRIDE를 통해 식별된 결과를 비교 분석했다. 각각의 DFD를 통해 식별된 구성요소의 STRIDE 결과와 CVE를 시나리오로 분석한 것을 연결했다.

4.4 위협 시나리오

분석된 위협에 따라 공격 루트를 구체화하기 위해 본 연구는 위협 시나리오를 작성하였다. 위협 시나리오는 특정 위협들을 연결한 위협 이벤트 집합으로 위협으로 인해 발생하는 결과와 위협 방식, 행위자 등이 포함되어 나타나 진다. 표 5는 STRIDE로 식별하고 CVE 내용을 통해 구체화 시킨 취약점의 공격 시나리오를 나타낸다. 이때, 표 4에 표시한 CVE는 전체 중 최근에 발생한 최신 위협만 제시하기 위해 2020년 이후에 발견된 CVE 항목만 삽입하였다. STRIDE를 통해 식별된 취약점을 CVE와 비교 분석하여 STRIDE의 분류 결과를 구체화하며, 해당

(표 3) DFD 구성요소 설명
(Table 3) DFD Component Description

구성요소 타입	구성요소	설 명
외부 객체	Human User	가상 사설망 서비스를 이용하는 사용자
	Company Web Server	사용자가 접속하고자 하는 내부망의 서버
프로세스	VPN Client	가상 사설망의 사용자 전용 프로그램
	Encryption	사용자의 데이터를 암호화하기 위한 프로세스
	VPN Server	가상 사설망 서비스를 관리, 제어하는 서버
	Login	사용자 인증을 위한 로그인 모듈
	ISP_Internet Service Provider	인터넷망을 통해 원거리 연결을 위한 프로세스
	Dencrypted	암호화된 사용자의 데이터를 복호화하기 위한 프로세스
데이터 저장소	User Gateway	사용자 환경의 네트워크 장비
	Log Database	사용자의 접속, 데이터 인입/인출 등의 로그 데이터를 저장하는 저장소
	VPN Server Gateway	사용자의 IP를 회사 내부망 IP로 변경하기 위한 가상 사설망 장치
	Company Gateway	사용자가 접속하고자 하는 내부망 네트워크 장비
데이터 흐름선	Response	요청에 따른 응답을 나타내는 흐름선
	Request VPN	가상 사설망 연결을 요청하는 흐름선
	User Data/IP Address	사용자의 데이터와 IP 주소를 나타내는 흐름선
	Company Data	사용자가 얻고자 하는 회사 데이터
	Encrypted Data	암호화된 사용자 데이터
	Encryption Packet	IP 주소와 데이터를 암호화한 흐름선
	Access request flow	사용자 인증 요청을 위한 흐름선
	Log Data	사용자의 사용 기록 등을 나타내는 로그 데이터
	Decrypted Packet	복호화된 데이터와 IP 주소 데이터를 나타내는 흐름선

(표 4) STRIDE 위협 모델링 분석 결과
(Table 4) STRIDE Analysis Result

STRIDE	Value
Spoofing	12
Tampering	18
Repudiation	1
Information Disclosure	21
Denial of Service	21
Elevation of Privilege	23

STRIDE 식별 결과의 정당성을 증명한다. 또한, 시나리오를 통해 공격 루트, 시간, 대상 등을 구체화했다.

4.5 가상 사설망 보안 요구사항

공격 루트와 취약점에 대한 시나리오를 바탕으로 내용을 바탕으로 본 연구에서 표 6과 같은 가상 사설망 서비스가 이뤄야 하는 총 30개의 보안 요구사항을 도출하였다. 이때, 가상 사설망을 이루고 있는 각 구성요소에 따른 보안 안정성을 위해 구성요소별 보안 요구사항을 나타낸다. 기존 가상 사설망의 보안 요구사항을 도출하는 연구는 가상 사설망 전체의 서비스가 아닌 특정 상황, 특정 모듈에 한정되어 있었다. 하지만 본 연구는 기존의 취약점 도출 결과보다 좀 더 유연한 결과를 보여주며, 추상적일 수 있는 도출 결과를 CVE를 통해 구체화하고 있다. 이를 통해 최종적으로 도출한 보안 요구사항은 실제 취약점과 STRIDE 위협 모델링을 통한 잠재적 취약점이 모두 반영된 결과이다.

5. 결 론

국방을 위해 방위기술, 극비문서 등을 보호해야 하며 국방부 네트워크뿐 아니라 방산 업체, 국방과 관련된 정보를 가진 모든 기관의 네트워크를 보호해야 한다. 하지만 현대의 통신 기술은 발전하고 있으며 가상 사설망의 취약점을 악용하는 공격이 매년 발생하고 있다. 이때, 가상 사설망과 같은 보안 제품에서 발생하는 취약점은 제품이나 시스템 전체에 영향을 미칠 수 있기에 이를 예방하는 것이 중요하다. 이와 같은 보안 제품에 보안 요구사항을 도출하고 위협을 예방하기 위해 본 논문은 가상 사

(표 5) 위협 시나리오 결과
(Table 5) Threat Scenario Result

구성요소	STRIDE	누가	언제	무엇을	왜	CVE
VPN Client	S, T, I, I	공격자가	VPN Client의 권한 부여 취약점 존재 시	특수하게 조작된 요청을 제품에 전송할 수 있다.	권한이 상승하여 사용자의 민감한 정보 및 보호된 리소스를 취득하기 위해	CVE-2021-27857 CVE-2021-27858 CVE-2021-27860
	E	일반 사용자가	VPN Client를 재부팅 및 시작 시	서비스 경로에 임의의 파일을 삽입할 수 있다.	관리자 권한으로 VPN을 실행하기 위해	CVE-2022-26634
	S, I, E	공격자가	사용자가 VPN Client 사용 시	동적 라이브러리의 경로가 지정되지 않아 악성 동적 라이브러리를 실행 할 수 있다.	사용자의 시스템에서 사용자의 권한으로 악의적인 명령을 실행하고 사용자의 정보를 취득하기 위해	CVE-2020-5145 CVE-2021-20047 CVE-2021-20051
	E	공격자가	VPN Client가 VPN Server에 연결 시도 시	동적 라이브러리 구성 파일에 대한 점검 취약성으로 Client와 Server 간에 조작된 통신 메시지를 보낼 수 있다.	관리자 권한으로 악성 코드를 실행하기 위해	CVE-2021-20037
	E	공격자가	VPN Client를 사용 시	VPN의 구성파일에 대한 권한 취약성으로 구성파일을 수정할 수 있다.	사용자의 운영환경 내 악성 명령을 실행하기 위해	CVE-2020-26050 CVE-2021-1567
	T	공격자가	VPN Client 사용 시	사용자와 VPN Client 간의 데이터를 하이재킹하여 조작된 파일을 보낼 수 있다.	사용자 권한으로 권한 상승을 위해	CVE-2020-5144
	S, T, I, D, E	공격자가	VPN 관리 페이지에 입력 검사가 미흡한 경우	올바르지 않은 요청을 보내 수 있다.	공격자의 권한이 상승 되며, 사용자의 민감한 정보를 탈취하고 변조할 수 있다. 또한, 해당 관리 페이지와 연결된 VPN 장치가 다시 실행할 수 있으며	CVE-2021-1287 CVE-2021-27855 CVE-2021-1610 CVE-2020-3259 CVE-2021-34704 CVE-2021-1415 CVE-2021-1294 CVE-2020-25759
	E	공격자가	보안 제어가 약한 VPN Client를 사용하여	서버에 부적절한 명명된 파이프 메시지를 보낼 수 있다.	공격자의 권한을 관리자의 권한으로 상승시키기 위해	CVE-2022-23171
	T, I	공격자가	웹 페이지에 부적절한 유효성 검사를 하는 VPN Client를 사용 시	VPN Client에 악성 스크립트를 전송할 수 있다.	사용자의 민감한 정보를 탈취하고 변조하기 위해	CVE-2022-0734 CVE-2021-3824 CVE-2021-35027
	T	공격자가	입력에 대한 유효성 검사를 하지 않는 VPN Client를 사용 시	서비스 내 악의적인 메시지를 입력할 수 있다.	공격자가 원하는 임의의 악성 코드를 실행시키거나 서비스 내 중요 정보에 접근하기 위해	CVE-2020-3583
(중략)						
VPN Server Gateway	T	공격자가	VPN Server Gateway에서 암호화된 키 메시지가 전송될 시	암호화된 키 메시지를 가로채고 암호 분석 기술을 사용하여 암호화를 해제할 수 있다.	해독된 키 관련 메시지를 통해 전송되는 데이터를 해독, 읽기, 수정, 재암호화 하기 위해	CVE-2022-20742
	D	유효한 자격증명 키를 탈취한 공격자가	공격자가 소유한 자격 증명 키가 유효한 VPN Server Gateway 장치 사용 시	특수하게 조작된 악의적인 자격 증명 메시지를 전송할 수 있다.	장치를 다시 로드하여 사용에 대한 서비스 거부 상태를 유발하기 위해	CVE-2021-40125
Log Database	T	공격자는	VPN 서비스가 로그 데이터를 올바르게 분류하지 못하는 Database를 사용 시	조작된 로그 데이터를 전송할 수 있다.	시스템의 모든 파일에 대한 쓰기 권한을 취득하기 위해	CVE-2020-27569

(표 6) 가상 사설망의 보안 요구사항 도출 결과
(Table 6) Deriving Security Requirements for Virtual Private Networks

구성요소	보안 요구사항
VPN Client	VPN Client의 사용자의 개인 정보가 암호화 되어 전달되는지 점검해야 한다.
	VPN Client 실행파일의 함수의 조작 유무를 확인해야 한다.
	VPN Client에서 기존 서비스 구성 환경이 올바르게 정리되었는지 점검해야 한다.
	VPN Client를 관리자 권한으로 실행 시, 암호를 입력하는지 확인해야 한다.
	VPN Client의 실행 시 관리자 권한으로 실행하는 접근 범위에 대한 제한을 확인해야 한다.
	VPN Client의 HTTP/S 요청 및 응답이 유효성 검사 메커니즘을 통해 확인되는지 검증되야 한다
	VPN Client를 통한 연결 시 실행되는 동적 라이브러리, 외부 라이브러리 실행 파일과 구성 파일을 점검해야 한다.
	VPN Client 프로세스의 실행 시 스크립트를 점검해야 한다.
	VPN Client에서 사용자가 직접 실행함을 감지하는 메커니즘 유무를 확인해야 한다.
	VPN Client에 전송되는 문자열 값과 길이가 제한되는지를 확인해야 한다.
	VPN Client 내 사용된 트래픽 상태 확인 모듈의 설정을 점검해야 한다.
	VPN Client에 사용가능한 메모리 양을 제한하는지 확인해야한다
VPN Server	VPN Server프로세스의 명령 유효성 검사를 점검해야 한다.
	VPN Server 프로세스의 인증서 사용시 인증 방식을 점검해야 한다.
	VPN Server 프로세스 내 정책 파일 사용시 파일의 권한을 점검해야 한다.
	VPN Server 프로세스의 패킷 처리 코드 처리 방식을 점검해야 한다.
	VPN Server 프로세스의 VPN 세션 처리 방식을 점검해야 한다.
Log Database	Log Database에서 Log 데이터의 처리 방식을 점검해야 한다.
	Log Database에서 Database 관리 명령어 매개변수의 검증 방식을 점검해야 한다.
Company/ User Gateway	Company/User Gateway에서 옵션에서의 처리 방식을 점검해야 한다.
	Company/User Gateway에서 데이터 및 매개변수의 처리 방식을 점검해야 한다.
	Company/User Gateway에서 VPN 클라이언트에 사용한 ID의 처리 방식을 점검해야 한다.
	Company/User Gateway에서 전송 데이터의 처리 방식을 점검해야 한다
	Company/User Gateway에서 클라이언트의 연결에 대해 검증 방식을 점검해야 한다
VPN Server Gateway	Server VPN Gateway에서 메시지의 입력 및 출력에 대한 처리 방식을 점검해야 한다.
	Server VPN Gateway에서 트래픽 및 트래픽 처리의 검증 방식을 점검해야 한다.
	Server VPN Gateway에서 패킷에 대해 검증 방식을 점검해야 한다.
	Server VPN Gateway에서 시스템의 연결에 대해 검증 방식을 점검해야 한다.
	Server VPN Gateway에서 IKE패킷의 처리 방식을 점검해야 한다.
	Server VPN Gateway에서 인증된 Device 내부 서비스의 요청에 대한 처리 방식을 점검해야 한다.

설망의 보안 요구사항 도출하였다. 본 논문에서는 가상 사설망의 위협을 분석하기 위해 가상 사설망의 DFD를 생성하여 위협을 분석하였으며, STRIDE 각 범주별 총 96개의 식별했다. STRIDE 식별 결과를 증명하기 위해 CVE에서 실제 가상 사설망과 관련된 취약점 165개의 위협을 분석하여 STRIDE 결과와 비교 분석했다. 이때, STRIDE 결과의 공격 시나리오를 작성하여 실제 위협이 발생 가능한 방법을 보여준다. 위협 모델링을 통해 식별된 결과와 공격 시나리오를 바탕으로 총 30개의 보안 요구사항을 도출했다. 도출된 보안 요구사항을 통해 가상 사설망을 안전하게 보안할 수 있으며, 한국의 안보에 도움이 될 것이다. 향후 본 논문을 통해 가상 사설망과 같은 보안 제품의 기존 취약점과 잠재적인 취약점을 분석하고 보안 요구사항을 생성하여 발전하는 기술에 맞는 보안 체계를 수립하기를 기대한다.

참고문헌(Reference)

[1] Ministry of National Defense, “Ministry of National Defense, 2020 Defense Reform 2.0 and Smart Defense Innovation Promotion Inspection Meeting”, 2020. https://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=I_7650984&boardSeq=I_8449226&titleId=null&id=reform_020100000000&siteId=reform

[2] Defense Acquisition Program Administration, "Comprehensive Plan for Defense Industry Technology Protection," 2021. https://eiec.kdi.re.kr/policy/callDownload.do?num=221879&filenum=5&dtime=20211225083948

[3] SBS News, ""Presidential event data also leaked"... Certain VPNs have been drilled," 2021. https://news.sbs.co.kr/news/endPage.do?news_id=N1006376861

[4] Korea Information and Communication Technology Association Information and Communication Terminology, Virtual Private Network http://terms.tta.or.kr/dictionary/dictionaryView.do?subject=%EA%B0%80%EC%83%81+%EC%82%AC%EC%84%A4+%ED%86%B5%EC%8B%A0%EB%A7%9D

[5] Dong-A Ilbo, "KAI breached in North Korea did not properly 'network separation' to prevent hacking," 2021. https://www.donga.com/news/Politics/article/all/20210709/107867900/1

[6] KBS, "The Ministry of Defense PC was also hacked... "Possibility of North Korea," 2016. https://news.kbs.co.kr/news/view.do?ncd=3245302&ref=A

[7] Khaleque Md Aashiq Kamal and Sultan Almuhammadi, "Vulnerability of Virtual Private Networks to Web Fingerprinting Attack," Advances in Security, Networks, and Internet of Things, pp 147–165, 2021. https://doi.org/10.1007/978-3-030-71017-0_11

[8] Mazen Juma, Azza Abdel Monem and Khaled Shaalan, "Hybrid End-to-End VPN Security Approach for Smart IoT Objects," Journal of Network and Computer Applications, Vol. 158, pp. 102598, 2020. https://doi.org/10.1016/j.jnca.2020.102598

[9] Veroniek Binkhorst, Tobias Fiebig, Katharina Krombholz, Wolter Pieters and Katsiaryna Labunets, "Security at the End of the Tunnel: The Anatomy of VPN Mental Models Among Experts and Non-Experts in a Corporate Context," 31st USENIX Security Symposium, pp. 3433-3450, 2022. https://www.usenix.org/conference/usenixsecurity22/presentation/binkhorst

[10] C. Jie, Y. Xing-Liang, C. Ying, F. Jia-Cheng and C. Chin-Ling, "A VPN-Encrypted Traffic Identification Method Based on Ensemble Learning," Applied Sciences, Vol. 12, No. 13, pp. 6434, 2022. https://doi.org/10.3390/app12136434

[11] S. Hernan, S. Lambert, T. Ostwald and A Shostack, "Uncover Security Design Flaws Using The STRIDE Approach," MSDN Magazine, 2006. https://docs.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach

[12] Tony UcedaVelez, Marco M. Morana, "Risk Centric Threat Modeling: process for attack simulation and threat analysis", Wiley Publishing, 2015.

[13] Kim Wuyts, Wouter Joosen, "LINDDUN privacy threat modeling_ a tutorial", Department of Computer Science, KU Leuven; Leuven, Belgium, 2015.

[14] Mark Curphey, Joel Scambray, Erik Olson, "Improving Web Application Security", Springer, 2014.

[15] Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody, "Introduction to the OCTAVE Approach", Software Engineering Institute, 2003.

[16] ETSI, European Telecommunications Standard Institute: Telecommunications andf Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis, ETSI TS 165-1 V5.2.3, 2017.

[17] P. Jison and K. Seungjoo, "Security Requirements Analysis on IP Camera via Threat Modeling and Common Criteria," KIPS Transactions on Computer and Communication Systems, Vol. 6, No. 3, pp. 121–134, 2017. https://doi.org/10.3745/KTCCS.2017.6.3.121

[18] S. Shinwoo, I. Sun-young, R. Han-eul, J. Sung-goo and K. Taekyu, "Threat Analysis of the Smart Doorlock Systems Using Threat Modeling," The Journal of Korean Institute of Communications and Information Sciences(JKICS), Vol. 445, No. 11, pp. 1868-1877, 2020. http://doi.org/10.7840/kics.2020.45.11.1868

[19] H.Jang, "Derivation of Security Requirements for Cloud Managing Security Services System by Threat Modeling Analysis," IPS Transactions on Computer and Communication Systems, Vol. 10, No. 5, pp. 145-154, 2021.

https://doi.org/10.3745/KTCCS.2021.10.5.145

[20] Yong-Hyun Jo and Young-Kyun Cha, "A Study on Cyber Security Requirements of Ship Using Threat Modeling," Journal of The Korea Institute of Information Security & Cryptology, Vol. 29, No. 3, 2019. https://doi.org/10.13089/JKIISC.2019.29.3.657

[21] ITSCC, "AXGATE SSL V2.1 Certification Report," 2020. https://www.itscc.kr/certprod/view.do?product_id=1043&product_class=1

[22] ITSCC, "NetSpliter Certification Report", 2021. https://www.itscc.kr/certprod/view.do?product_id=1095&product_class=1

[23] ITSCC, "eWalker SSL VPN V10 Certification Report", 2022. https://www.itscc.kr/certprod/view.do?product_id=1168&product_class=1

[24] H. Sawalmeh, M. Malayshi, S. Ahmad and A. Awad, "VPN Remote Access OSPF-based VPN Security Vulnerabilities and Counter Measurements," International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), pp. 236-241, 2021. https://doi.org/10.1109/3ICT53449.2021.9581512.

[25] S. Rahimi and M. Zargham, "Security Analysis of VPN Configurations in Industrial Control Environments" International Conference on Critical Infrastructure Protection, Vol. 367, pp. 73-88, 2011. https://doi.org/10.1007/978-3-642-24864-1_6

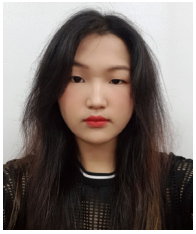
[26] S. Shunmuganathan, R. D. Saravanan and Y.Palanichamy, "Securing VPN from insider and outsider bandwidth flooding attack," Microprocessors and Microsystems, Vol. 79, pp. 103279, 2020. https://doi.org/10.1016/j.micpro.2020.103279.

[27] Visual Paradigm Online, "DFD Using Yourdon and DeMarco Notation," https://online.visual-paradigm.com/knowledge/software-design/dfd-using-yourdon-and-demarco

[28] Microsoft Documentation, "Microsoft Threat Modeling Tool," 2020. https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool#feedback

[29] CVE, https://cve.mitre.org/

◐ 저 자 소 개 ◑



김 다 현(Da-hyeon Kim)
2018년~2021년 현재 한국교통대학교 컴퓨터정보기술공학부 소프트웨어전공 졸업
2021년~현재 한국교통대 일반대학원 소프트웨어전공 석사과정
관심분야 : 딥러닝, 패턴인식
E-mail : 1826059@ut.ac.kr

민 지 영(Ji-young Min)
2020년 3월~현재 한국교통대학교 컴퓨터정보기술공학부 소프트웨어전공
관심분야 : 딥러닝, 컴퓨터 보안
E-mail : 2026025@a.ut.ac.kr

안 준 호(Jun-ho Ahn)
2009년~2013년 University of Colorado, Boulder, Computer science, Ph.D.
2013년~2017년 ETRI 국가보안기술연구소
2017년~현재 한국교통대학교 컴퓨터정보기술공학부 소프트웨어전공 교수
관심분야 : 인공지능, 사물인터넷
E-mail : jhahn@ut.ac.kr