선박 사이버 보안 위협 모델링: VSAT 및 위성 통신 취약점 분석과 대응 전략

유예지1, 이정연1, 이지연2, 양소윤3 ,최현우4
1성신여자대학교 융합보안공학과 학부생
2성신여자대학교 컴퓨터공학과 학부생
3성신여자대학교 수리통계데이터사이언스학부생
4성신여자대학교 융합보안공학과 교수
20200936@sungshin.ac.kr, 20200948@sungshin.ac.kr, 20201006@sungshin.ac.kr,
20230875@sungshin.ac.kr, zemisolsol@sungshin.ac.kr

Ship Cyber Security Threat Modeling: VSAT and Satellite Communications Vulnerability Analysis and Response Strategies

Ye-Ji Yu1, Jung-Yeon Lee1, Ji-Yeon Lee2, So-Yun Yang3, Hyun-Woo Choi4
1Dept. of Convergence Security Engineering, Sungshin Women's University
2Dept. of Computer Engineering, Sungshin Women's University
3Dept. of Mathematical Statistics and Data Science, Sungshin Women's University
4Dept. of Convergence Security Engineering, Sungshin Women's University

요 약

본 연구는 해양·선박 산업의 디지털화에 따른 사이버 보안 위협, 특히 VSAT 및 위성 통신 시스템의 취약점을 분석한다. STRIDE 위협 모델링, 공격 트리 분석, 그리고 실제 위협 인텔리전스 데이터를 활용하여 체계적으로 위험 평가를 수행하였다. 분석 결과, 1,627개의 VSAT 관련 장치가 사이버 위협에 노출되어 있음을 확인하였으며, 주요 취약점으로 CVE-2022-22707, CVE-2019-11072, CVE-2018-19052 등이 발견되었다. STRIDE 및 DREAD 분석을 바탕으로 10개 항목의 강화된 보안 체크리스트를 개발하였으며, 각 항목의 중요도를 정량적으로 평가하였다. 본 연구는 선박 운영자들에게 실효성 있는 사이버 보안 가이드라인을 제공하며, 향후 글로벌 해운산업의 사이버 보안 향상에 기여할 것으로 기대된다.

1. 서론

해양·선박 산업의 디지털화로 인해 선박 대상 사이버 공격 위험이 증가하고 있다. 특히 위성 통신을 통해 연결된 해양·선박 시스템의 취약점이 주목받고 있다. 최근 사이버 위협 인텔리전스 Criminal IP에 수집된 자료에 따르면, 2023년 12월 3일부터 2024년 1월 3일의 한 달 사이에 약 1,627개의 선박 관련 장치가 사이버 위협에 노출된 것으로 나타났다.[1] 이러한 시스템 중 상당수가 위성 통신망을 사용하고 있어, 그 취약성이 더 크게 부각되고 있다. 이 중 VSAT(Very Small Aperture Terminal) 시스템은 심각한 취약점을 보유하고 있어, 한 선박 시스템의 IP 주소 위협보고서에서는 인바운드 위협 수치가 99% Critical로 나타났다. 본 연구는 VSAT 및 위성 통신 시스템의 취약점을 분석하고, 이에 대한 보안 체크리스트를 강화하여 선박 운영자들의 효과적인 사이버 보안 대응 방안을 제시하고자 한다.

2. 연구 방법

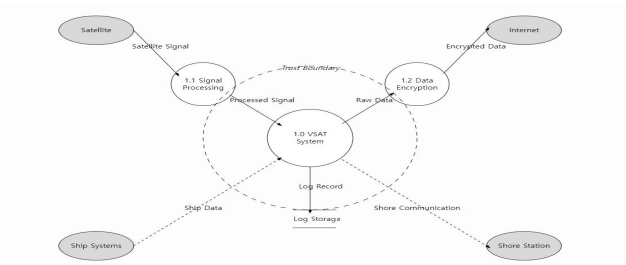
본 연구는 다음과 같은 체계적인 방법론을 통해 수행되었다:

①데이터 흐름도(DFD)분석 ②STRIDE 위협 모델링 ③공격 트리 분석 ④Criminal IP의 위협 인텔리전스 데이터 활용 ⑤STRIDE 및 DREAD 기반의 위험 평가

3. VSAT 및 위성 통신 시스템 취약점 분석

3.1 데이터 흐름도(DFD)분석

VSAT 시스템을 중심으로 한 선박의 데이터 흐름도를 다음과 같이 작성하였다:



(그림 1) VSAT 데이터 흐름도(DFD)

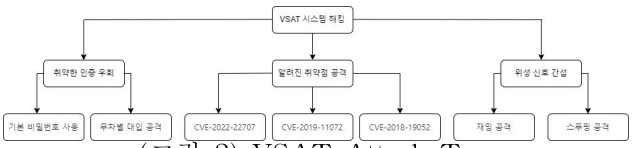
위 그림은 VSAT 시스템을 중심으로 위성, 선박 시스템, 인터넷, 육상 기지국 간 데이터 흐름을 보여주는 DFD(Data Flow Diagram) 이다. VSAT는 초소형 지구국이라는 뜻으로, 위성과 통신하며 선박 내부 시스템과 연결되어 있다. 또한 VSAT는 인터넷을 통해 외부와 통신하고, 육상 기지국과도 데이터를 주고받는 기능을 가진다.

3.2 STRIDE 위협 모델링

1. Spoofing: 위성 신호 스푸핑, GPS 스푸핑
2. Tampering: 통신 데이터 변조, 펌웨어 변조
3. Repudiation: 로그 삭제 또는 변조
4. Information disclosure: 민감한 선박 정보 유출
5. Denial of service: VSAT 시스템 과부하 공격
6. Elevation of privilege: VSAT 관리자 권한 탈취

3.3 VSAT 시스템 Attack Tree 분석

본 연구에서 VSAT 시스템 해킹을 위한 공격 트리를 다음과 같이 구성하였다:



(그림 2) VSAT Attack Tree

위의 도식도를 보면, VSAT 시스템은 Attack Tree에 적힌 다양한 방법으로 해킹 당할 수 있음을 알 수 있다. 주요 공격 vector로는 물리적 접근, 네트워크 공격, 소프트웨어 취약점 이용 등이 있다.

3.4 실제 취약점 분석 결과

Criminal IP의 위협 인텔리전스 분석 결과, 2023년 12월부터 2024년 1월까지 한 달간 1,627개의 VSAT 관련 장치가 인터넷에 노출된 것으로 확인되었다. 주목할 만한 것은 Cobham SAILOR VSAT Ku v.164B019에서 발견된 주요 취약점들이다. CVE-2023-44857는 원격 코드 실행 취약점으로 시스템의 무결성을 위협한다. 또한, CVE-2023-44856, CVE-2023-44855 등 여러 건의 크로스 사이트 스크립팅(XSS) 취약점이 발견되었다.

과거에 보고된 CVE-2022-22707, CVE-2019-11072, CVE-2018-19052 등의 취약점들은 여전히 유효한 위협으로, 웹 인터페이스를 통한 관리자 권한 탈취와 선박 위치 정보 및 장비 정보 노출 가능성을 내포하고 있어, VSAT 및 위성 통신 시스템에 대한 장기적인 보안 대책 마련이 반드시 필요하다.

4. 강화된 보안 체크리스트 및 위험 평가

STRIDE 및 DREAD 분석을 통해 각 보안 항목의 중요도를 평가하고, 이를 바탕으로 강화된 보안 체크리스트를 개발하였다. 평가 결과는 다음 표와 같다:

체크리스트 항목	STRIDE	DREAD 점수	총점
1. VSAT 시스템 펌웨어 및 소프트웨어 정기 업데이트	S, T, I, E	D:9, R:8, E:7, A:9, D:6	39
2. 강력한 인증 메커니즘 적용	S, R, E	D:8, R:9, E:8, A:9, D:7	41
3. VSAT 웹 인터페이스 접근 제한 및 모니터링	S, T, R, I, E	D:9, R:8, E:8, A:8, D:8	41
4. 위성 통신 데이터 암호화 적용	T, I	D:10, R:7, E:6, A:9, D:5	37
5. GPS 스푸핑 탐지 및 방어 시스템 구축	S, T	D:10, R:8, E:7, A:10, D:6	41
6. 네트워크 세그먼테이션을 통한 VSAT 시스템 격리	T, I, D, E	D:8, R:7, E:7, A:8, D:6	36
7. 보안 로그 모니터링 및 이상 징후 탐지 시스템 구축	S, T, R, I, D	D:7, R:9, E:8, A:8, D:9	41
8. 정기적인 취약점 스캔 및 침투 테스트 수행	S, T, I, D, E	D:8, R:8, E:9, A:8, D:9	42
9. VSAT 및 위성 통신 시스템 운영자 대상 보안 교육 강화	S, R, I	D:6, R:8, E:7, A:9, D:8	38
10. 사이버 보안 사고 대응 계획 수립 및 훈련	R, D	D:7, R:9, E:8, A:9, D:8	41

<표 1> STRIDE 결과

- STRIDE 범례: S(Spoofing), T(Tampering), R(Repudiation), I(Information Disclosure), D(Denial of Service), E(Elevation of Privilege)
- DREAD 범례: D(Damage Potential), R(Reproducibility), E(Exploitability), A(Affected Users), D(Discoverability)

분석 결과, 정기적인 취약점 스캔 및 침투 테스트 수행이 가장 높은 DREAD 점수(42점)를 받았으며, 강력한 인증 메커니즘 적용, VSAT 웹 인터페이스 접근 제한 및 모니터링, GPS 스푸핑 탐지 및 방어 시스템 구축, 보안 로그 모니터링 및 이상 징후 탐지 시스템 구축, 사이버 보안 사고 대응 계획 수립 및 훈련이 그 다음으로 높은 점수(41점)를 받았다.

5. 결론 및 향후 연구 방향

본 연구는 VSAT 및 위성 통신 시스템의 취약점을 중심으로 선박 사이버 보안 위협을 체계적으로 모델링하고 분석하였다. 특히 실제 위협 인텔리전스 데이터를 활용하여 현실적인 위험을 파악하고, STRIDE 및 DREAD 분석을 통해 각 보안 대책의 중요도를 정량적으로 평가하고 있다.

※ 본 논문은 해양수산부 실무형 해상물류 일자리 지원사업(스마트해상물류 x ICT멘토링)을 통해 수행한 ICT멘토링 프로젝트 결과물입니다.

참고문헌

[1] Kim, Y. (2024). Growing threat of ship hacking... Over 1,600 devices found exposed to attack surface. Boannews. https://m.boannews.com/html/detail.html?idx=126635

[2] Jo, Y.-H., & Cha, Y.-K. (2019). A Study on Cyber Security Requirements of Ship Using Threat Modeling. Journal of the Korea Institute of Information Security & Cryptology, 29(3), 657-673.