JANUS: 폐쇄망 환경을 위한 전략적 침투 허용 기반 보안 아키텍처 설계

안윤기*

*일반 (비전공자)

JANUS - A Strategic Intrusion Tolerance Architecture for Behavior-Based Security for Closed Networks

Yoon-Gi Ahn*

*General Participant(Non-major)

요 약

본 논문은 폐쇄망 기반 고위험 환경에서 침입 이후 상황에 대응하기 위한 전략적 보안 아키텍처 'JANUS'를 제안한다.
JANUS는 이상행동 탐지 후 설계자의 통제 아래 단계별 대응 절차를 구조화하며, Zero Trust[2] 및 NIST 프레임워크[1] 기반의 판단 체계, 신뢰 점수 분기 시스템, 샌드박스 기반 가상 격리 환경과 위조 DB(Fake DB), AI 기반 리포트 자동화를 통합하여 공격자의 행위 패턴을 정밀 추적·분석하고 원본 데이터를 보호한다.
JANUS는 APT 및 내부자 위협 대응을 위한 구조적 방어 모델로 설계되었으며, 공공기관, 군사기관, 국가기반시설의 폐쇄망 환경에 실질적 적용 가능성을 지닌다.

I. 서론

"보안은 자동화되었으나, 최종 판단은 여전히 인간의 몫이다."
고도화된 사이버 위협 환경에서 기존의 차단 중심 보안 체계는 한계를 드러내고 있다.
특히 폐쇄망 기반의 국가 기반 시설, 군사 및 정부 기관은 외부 침입뿐 아니라 내부자 위협에 더욱 취약하다.
완전한 차단은 현실적으로 불가능하며, 침입 이후를 고려한 설계가 보안의 핵심이 된다.
본 논문은 침입을 제거하기보다 설계자의 통제 하에 공격을 유도·분석·격리·복구하는 전략적 침투 허용형 보안 아키텍처 'JANUS'를 제안한다.
JANUS는 판단의 주체를 시스템이 아닌 인간, 즉 설계자에게 부여한다.
설계자는 침입 이후의 상황에 대해 구조적인 판단을 수행하는 내부 책임자이다.
이상행동 탐지는 사용자 반응 속도, 마우스 좌표 등 다크데이터를 기반으로 수행된다.
이 구조는 미국 사이버사령부(CNMF)의'억제-교란-격파'전략과 유사하며, APT 및 내부자 위협 대응에 효과적인 설계임을 시사한다.

II. JANUS 아키텍처 설계

JANUS는 침입 발생 시 신속한 차단보다는 통제된 상황에서의 심층 분석 및 대응에 초점을 맞춘다. Zero Trust와 NIST 프레임워크를 적용해 다층 보안 체계를 구축한다.

2.1 이상행동 탐지 시스템

JANUS는 클릭 반응 속도, 직접 URL 접근, 관리자 뷰 캡처 시도 등 사용자 행동 데이터를 수집하고, 기본 신뢰 점수를 기준으로 이상 여부를 평가한다. 점수가 임계값 이하로 하락하면 격리 대상자로 분류되며, 이때 다크데이터 기반 정량 분석이 함께 수행된다.
신뢰 점수는 자동 복구되지 않고 설계자에 의해 수동으로 조정된다.
설계자는 신뢰 점수가 충분하더라도 필요 시 직접 샌드박스 격리를 결정할 수 있다.

2.2 판단 로직 및 설계자 개입 흐름

설계자는 수집된 로그, 요약 리포트, 다크데이터를 바탕으로 격리, 복귀, 차단 등의 조치를 수동으로 수행한다. 상황에 따라 시스템 이상 여부와 무관하게 선조치가 가능하며,
이후 조치 내역은 중앙관리체계에 보고된다.
설계자 간 판단은 개별 기록되며, 향후 중앙사령부 또는 신뢰 관리자에 의한
교차 검증과 견제 구조가 추가될 수 있다.

2.3 샌드박스 및 Fake DB(허니팟) 구조

샌드박스는 실제 시스템과 동일하게 구성되며, 내부에 Fake DB를 배치하여 허니팟(Honeypot) 역할을 수행한다.
Fake DB는 실제와 유사하나 재식별이 불가능하도록 가공된 더미 데이터를 포함하며,
존재하지 않는 더미 계정이나, 실제 필드 구조를 변형한 가공 항목들이 삽입된다.
공격자는 이를 실제 환경으로 인식하고 자발적 조작을 수행하게 된다.
이 모든 행위는 내부자 식별 및 증거 확보를 위한 정밀 로그로 저장되며,
해당 환경은 설계자의 통제 하에 운영된다.

2.4 로그 저장 및 분석 리포트

이상행동 발생 시 로그는 DB, JSON 파일, 암호화 이메일로 동시 저장된다. 샌드박스에서는 다크데이터(예: 마우스 움직임, 클릭 속도 등)를 포함한 정밀 로그가 추가로 수집되며,
이 로그는 설계자의 판단 보조 자료로 활용된다.
AI는 마우스 좌표, 클릭 속도 등 다크데이터를 기반으로 LSTM 모델을 통해 이상행동 패턴을 분석하고, 이를 요약 리포트 형태로 자동 생성한다.

2.5 시스템 봉쇄 및 복구 전략

신뢰 관리자 계정 침해 또는 제로데이 공격 발생 시, 설계자는 전체 혹은 부분 시스템을 봉쇄할 수 있다. 복구는 정합성 검증 후 백업 시점으로 수행되며, Fake DB 변조 기록의 반영 여부는 설계자가 결정한다

2.6 윤리 및 AI 확장 구조

AI는 판단이 아닌 보조 역할만 수행한다. JANUS는 폐쇄망 환경 내에서 운영되므로, 접근자는 사전에 인증된 내부 인원에 한정되며, 이에 따른 기록·분석 행위는 정당한 보안 조치로 간주될 수 있다. 모든 로그는 비식별화된 상태로 암호화 저장되며, 판단 오류에 따른 격리 조치에는 추후 이의제기 및 복구 절차의 내재화 가능성 또한 고려되었다.

III. 시나리오

시나리오 A – 내부 관리자 스파이 탐지 사례

실제 운영 중, 한 관리자의 평소 언행과 반복적인 의심스러운 업무 처리 방식으로 인해
내부 보안팀은 해당 인물을 비공식 관찰 대상으로 분류하였다.
당시 시스템상 로그와 신뢰 점수 모두 정상 범위였으며,
AI 역시 별다른 이상을 감지하지 못했다.
그러나 설계자는 직관과 누적 정황을 근거로 해당 관리자를 샌드박스 환경으로 강제 격리시켰다.
이후 그는 Fake DB 내 존재하지 않는 더미 계정에 대한 정보 조작을 시도하였고,
이 모든 행위는 정밀 로그로 기록되어 내부자 위협으로 최종 판별되었다.
다만, 해당 격리는 설계자의 직관에 의한 판단으로, 오류 가능성 또한 존재한다.
※JANUS 구조흐름, 판단 분기, 용어정리, 시나리오는 GitHub 저장소[5]에 공개되어 있다.

IV. 결론

본 논문은 기존 폐쇄망 보안 시스템이 침입 자체를 차단하는 데만 집중해온 한계를 지적하고, 침입 이후를 설계하는 새로운 판단 중심 보안 아키텍처, JANUS를 제안한다.

다수의 보안 사고는 기술보다 인간의 판단 오류나 내부자의 행동에서 비롯된다 [3][4].
JANUS는 이에 대응하기 위해, 설계자의 판단을 구조화한 보안 모델을 제안한다.

JANUS는 판단의 주체를 시스템이 아닌 인간(설계자)에게 부여하며,
그 판단에 대한 책임과 검증을 위한 구조 역시 함께 설계되었다
또한, 이러한 인간의 판단 과정에서 발생할 수 있는 오류와 책임을 보완하기 위해 설계자 간의 교차검증 및 상호견제 시스템을 통해 시스템 전반의 신뢰도를 강화한다.

설계자의 위계는 시스템 구조에 따라 달라진다. 분산 모듈형에서는 부대급 판단자(예: 작전장교), 통합형에서는 장관급 통제권자가 판단 주체가 된다.
즉, 시스템의 형태가 설계자의 위상을 결정하게 된다.

이 설계는 단순한 침입 대응을 넘어, 공공기관 및 군사·국가기반시설과 같은 고위험 환경에서 보안 정책 수립 및 시뮬레이션형 보안 아키텍처로서 실질적인 활용 가능성을 지닌다.
JANUS는 향후, 판단개입 없는 행위 기반 정산 시스템 KARMA로의 확장을 목표로 한다.

[참고문헌][1] NIST. (2020). _Framework for Improving Critical Infrastructure Cybersecurity_, Version 1.1.[2] John Kindervag. (2010). _The Zero Trust Model_. Forrester Research.[3] Carnegie Mellon CERT. (2015). _Insider Threat Mitigation Guide_. Software Engineering Institute.[4] Eugene H. Spafford. (1991). _The Internet Worm Program: An Analysis_. Purdue University.[5] Yoon-Gi Ahn. (2025). _JANUS Security Architecture Initial Draft_, GitHub Repository. https://github.com/yoon0416/Security