AINA AI NETWORK ALLIANCE

AINA 산업융합위원회 정례회의(12월) 개최 결과

('25.12.17.(수), AINA 사무국)

Ⅰ. 회의 개요

○ **(일시/장소)** 2025.12.16.(화), 14:30~16:00/강남 토즈 컨퍼런스점 세미나 1번

○ **(논의내용)** AI 보안 관련 전문가세미나, 주요 이슈 및 현황 검토 등

○ **(참 석 자)** 산업융합위원장 및 부위원장, 위원, 사무국 등 13명

- 김태윤 책임(LG전자), 김동구 교수(연세대), 남기동 센터장, 강경순 책임, 최용훈 책임, 박경민 선임(이상 ETRI), 장준희 책임(NIA), 김요림 선임(IITP), 전형준 소장(유캐스트), 유동호 대표(넷큐브), 정상혁 본부장, 성창윤 프로(이상 이노와이어리스), 김현수 과장(KANI)

Ⅱ. 회의 결과

□ 산업융합위원회 소개 및 Kick-Off 결과 : 김태윤 책임(LG전자)

○ **스마트/자동화 공장(Dark Factory) 도입 현황 및 전략 논의**

- 스마트팩토리 미적용된 공장은 AI 자율운용 네트워크로 완전 자동화 전환에 약 7년 소요 예상(특정 구역 내 AI-RAN 도입 및 단계적 빠른 도입 시 일정 단축 가능하다는 의견)

- AI 장비 도입을 위해서는 데이터 확보 및 DB 구축이 중요, 데이터 확보만도 시간이 걸리기 때문에 빠르게 시작이 중요함

○ **위원회 운영 현황 및 향후 일정**

- Kick-Off 회의 진행 후 관련 발표내용(AMD) 연계해서 망고부스트 초청 전문가세미나 추진 검토 중

- 1월(퀄컴, 다산네트웍스), 2월(지엔텔, 뉴젠스, LG CNS 등 NIA 실증 참여기관) 정례회의는 계획한 사항에 따라 추진할 예정

AI NETWORK ALLIANCE

□ AI for Security 전문가 세미나

① **Self-Evolving 6G 네트워크에서의 AI for Security 기술 동향 : 박경민 박사(ETRI)** (발표자료 참고)

○ **기술 현황 및 한계**

- **(현황)** 기존 시그니처 기반(알려진 공격만 탐지)하는 IDS 한계를 넘기 위해 AI 기반 탐지기술 도입 중

- **(한계점)** 99% 이상이 정상 트래픽으로 공격 데이터 학습이 어려움, AI가 공격이라 판단해도 담당자가 진짜 공격인지 검증이 어려움, 탐지는 가능하나 대응은 어려움

○ **6G 네트워크 환경의 변화와 보안 위협**

- 네트워크 구조가 지능화, 개방화(Open RAN), 분산화되면서 장비 및 SW 확보가 비교적 쉬워져 취약점 분석 및 공격 가능성 증가

- 또한, 물리적 접근 포인트가 늘어나고 다양한 벤더의 SW가 섞이며 복잡성이 증가함에 따라 호환성 및 보안 홀 발생 가능성 증대

○ **차세대 보안 기술 제언 : Generative AI 활용**

- 단순 탐지를 넘어 생성형 AI를 활용한 능동적 기만(Network Deception)과 자동화 대응(AI Security Agent) 기술을 제안

- **(Network Deception)** 생성형 AI를 활용, 가짜 터미널 환경을 저비용으로 무수히 생성하여 해커를 유인하고 공격 패턴을 분석

- **(AI Security Agent)** 다양한 보안 도구에 접근 권한을 가진 AI 에이전트로 탐지부터 차단, 대응까지 수행함(AI CISO 역할)

② **AI-RAN 기반 제로트러스트 보안 적용 방안 : 유동호 대표(넷큐브)** (발표자료 참고)

○ **제로트러스트(Zero Trust) 보안의 개념 및 필요성**

- **(배경)** 미국 NIST(국립표준기술연구소) 가이드라인에 기반한 보안 철학이며, 클라우드, 모바일, 재택근무 등으로 물리적 위치와 논리적 보안 위치가 일치하지 않고 한 번 인증으로 신뢰하는 방식이 더 이상 안전하지 않은 이슈로 등장

- **(핵심원칙)** 모든 자원을 위치와 관계없이 보호 대상으로 간주하고 자원을 세션 단위로 쪼개어 최소 권한만 부여, 실시간 보안 상태를 평가하여 지속적 인증을 갱신

○ **제로트러스트 아키텍처 : NIST 모델 기반**

- 보안의 두뇌 역할하는 PDP(Policy Decision Point)와 실제 트래픽을 제어하는 장비인 PEP(Policy Enforcement Point)로 구성

○ **AI-RAN(O-RAN)과 보안의 융합**

- O-RAN 인터페이스(E2, O1, A1)를 통해 트래픽 처리량, 신호 세기, 채널 품질, 빔 정보 등 다양한 데이터를 수집

- 고성능 GPU가 아닌 CPU 기반에서 동작 가능한 경량형 모델 지향

- 시계열 데이터 처리에 적합한 TCNS, RNN, CNN 활용

○ **넷큐브 개발 현황**

- **(통합 보안 시스템)** 자체 AI 분석 외 모바일 전용 IDS 연동하여 로그 통합 분석하고 xApp 형태로 구현

- **(제어 및 대응 방식)** 아직은 O-RAN 인터페이스만으로 제어가 어려워 이상 징후 팀지 시 5G Core망을 통해 제어

□ 후속조치 계획

○ AINA 산업융합위원회 2026년 1월 정례회의

- 일시/장소 : 미정

Ⅲ. 회의 전경

<table>
<tr><td></td><td></td></tr>
<tr><td>(산업융합위원회 소개 및 Kick-Off 회의 결과)
김태윤 산업융합위원장(LG전자)</td><td>(전문가세미나1)
Self-Evolving 6G 네트워크에서의 AI for Security 기술 동향 : 박경민 박사(ETRI)</td></tr>
<tr><td></td><td></td></tr>
<tr><td>(전문가세미나2)
AI-RAN 기반 제로트러스트 보안 적용 방안
유동호 대표(넷큐브)</td><td>(임명장 수여식 : 산업융합위원회 부위원장)
장준희 책임(NIA)</td></tr>
</table>

끝.