**종단형PBL 팀 회의록**

**팀 이름: Aegis**

**멤버: 이경화(팀장), 손효림, 한별하, 한아림**

● 회의 내역

|  |  |  |  |
| --- | --- | --- | --- |
| **회차** | **일자** | **장소/시간** | **요약** |
| 2 | 2024.03.25 | 온라인 | (예정) |
| 1 | 2024.03.18 | 중앙도서관 세미나실/12:00~15:00 | 팀명 선정 및 프로젝트 주제 논의 |

**회 의 록**

|  |  |  |  |
| --- | --- | --- | --- |
| **회차** | 1회차 | **일시** | 2024.03.18 (월) |
| **참석자** | 한아림, 한별하, 손효림, 이경화 | **장소** | 서울여대 중앙도서관 세미나실5 |
| **제목** | 팀명 선정 및 프로젝트 주제 논의 | | |
| **회의내용** | * **팀명 후보**   + 일루미나티, 타임레스, 프리딜러, 렉틴스틴, 크린티센트, 호우대, 방우계, PNF, 운김, 안다미로, P.I.S., 퀘이사, F4, A4, fortess, Alcyone, Aegis, scutum, lustitia, geborgenheit * **팀명 선정**   + **Aegis(이지스):** 전쟁의 여신 아테나의 방패 이름에서 유래한 단어로, 현대에는 레이더로 미사일을 감지해 공중 요격하는 이지스 시스템을 탑재한 이지스함의 이름에 쓰이고 있음. 정보를 보호하는 완벽한 수호자가 되겠다는 의지를 담은 팀명. * **주제 제시**   + (아림)걸식 아동 복지 카드의 취약한 개인정보 관리 문제   + (아림)화기가 닿으면 자동으로 열리는 등의 도어락 보안 문제   + (아림)전동 스쿠터의 탑승인원을 감지하는 센서를 개발하여 초과탑승으로 인한 사고를 예방하는 프로젝트   + (아림)전동 스쿠터의 과속을 방지하는 기능을 구현하는 프로젝트   + (아림)특정 대상에 대한 독창적인 공격 모델 제안     - 사용자 기반 추천 알고리즘 등의 AI 머신러닝 모델을 대상으로 적대적 패치 등을 이용한 데이터 오염을 통해 입력층 혹은 은닉층을 손상시키는 공격 모델     - 사람의 입력값이 아닌 AI가 생성한 데이터를 AI에 재학습시킬 때 AI 모델의 성능이 저하되는 현상을 실제로 구현하는 공격 모델 제안 및 원인 규명     - 스마트 신호등을 대상으로 아두이노를 활용한 공격 모델     - http 프로토콜을 사용하는 홈페이지를 대상으로 하는 자동화 공격 모델     - 온라인 쇼핑몰, SNS, 동영상 플랫폼 등 특정 유형의 서비스를 대상으로 하는 공격 모델     - 가짜 url을 이용한 피싱 자동화 공격 모델 제안 및 방어책 제시     - 이 외의 공격 대상: 무선 LAN(Wi-Fi 공유기, 공공 Wi-Fi), 스마트 신호등(아두이노 활용) 등   + (효림)해킹에 취약한 것으로 알려진 CCTV 홈캠 해킹 방지   + (효림)불법 촬영 소형 카메라 탐지⑴   + (효림)security zone의 데이터를 외부로 끌어내서 공격하는 Fuzzer 사례와 같이 창의적인 IoT Fuzzer 개발   + (효림)IoT 기기를 대상으로 하는 랜섬웨어 연구 및 공격 방지 대책 제안   + (효림)가입한 사이트를 모아보고 계정을 일괄 관리할 수 있는 웹 또는 모바일 앱 개발(개인정보 포털 지우개)   + (효림)불법 웹툰, 영화, 음란물 사이트 등을 탐지하는 프로그램 개발   + (효림)딥페이크 탐지 프로그램 개발   + (경화)Matter의 통신 프로토콜 연구 및 개선 아이디어 제안⑵   + (경화)url의 위험성을 검증하는 절차를 통해 안전한 url만 변환해주는 QR코드 생성기   + (경화)개인정보 제공자가 개인정보 수집처에 제공한 개인정보를 라이프사이클에 따라 적절하게 관리되는지 모니터링할 수 있는 앱 개발   + (별하)IoT 기기의 과부하를 유도하여 화재를 일으키는 공격 모델 제안 및 방어책   + (별하)Fuzzing 방지 툴 개발   + (별하)리버싱 방지 기술 개발   + (별하)연쇄 공급망에서 이상행동을 탐지하고 백도어를 방지 혹은 무력화시키는 프로그램 개발   + (별하)키오스크 보안 취약점 연구 및 리눅스용 키오스크 프로그램 개발   + (별하)게임 핵 개발과 웹 사이트 리버싱   + (별하) 텔레그램 보안 취약점 연구 및 생성형 AI 딥페이크 음란물 생성 챗봇 문제에 대한 대응방안 제시   + **이외의 관심 주제**: 개인정보보호, 클라우드, 자동화, 공급망 보안, 차량 보안, IoT 보안, 랜섬웨어, 브라우저 취약점, 의료기기 보안⑶, 키오스크 보안과 리눅스, 게임 핵 개발, 웹사이트 리버싱   + **고려할 점**: 차별성, 혁신성, 유용성, 완성도 등 * **주제에 관한 의견**   + IoT 혹은 네트워크와 개인정보보호와 관련된 주제를 선정하면 좋겠음.   + 일반인은 시도하기 어려운, 전공자답게 적절한 수준의 전문성이 요구되는 주제여야 함.   + 프로젝트의 주제선정 시 윤리성이 고려되어야 함.   + Fuzzer 사용 경험이 채용 시 우대사항에 들어갈 만큼 Fuzzing 프로젝트는 유용한 스펙이 될 수 있으나, 발상의 전환을 시도하는 등 다른 Fuzzer와의 차별성이 필요함.   + 의료기기 보안은 실제로 연구하기에 현실적이 어려움이 있을 것으로 우려됨. * **주제 선정**   + **주제명**: 개인정보 라이프사이클 트래커(Privacy-Lifecycle Tracker)   + **주제 선정 이유**: 기업이나 기관이 아닌 학교 동아리 등의 소소한 모임에서는 회원이나 지원자 등의 개인정보를 수집하지만 적절하게 관리하지 못하는 경우가 많음. 따라서 특정 조직에 제공된 개인정보가 라이프사이클에 따른 관리표준에 따라 적절하게 관리되는지 모니터링할 수 있는 도구의 필요성을 느낌.   + **목적 및 기대효과:** 개인정보 전문가를 두기 어려운 모임에서 개인정보 관리를 적절하고 편리하게 할 수 있고, 개인정보 제공자는 본인이 제공한 개인정보가 안전하게 관리되고 있는지 모니터링할 수 있음.   + **개발 형태:** 웹 또는 모바일 어플리케이션   + **사용자 타겟:** 소모임 관리자 및 개인정보 제공자   + **구현 아이디어**     - 개인정보를 수집하려는 소모임 측에서 개인정보 제공자에게 초대토큰을 발급하여 클러스터 형성     - 개인정보 제공자는 자신이 제공한 개인정보가 항목별로 수집, 저장, 이용, 파기되는 라이프사이클에 따른 처리 현황을 실시간으로 모니터링 가능     - 보안문제를 고려하여 개인정보 자체를 앱에 저장하는 것이 아닌, 특정 항목의 개인정보가 제공되었는지 여부만을 저장함.   + **해결할 문제**     - 개인정보의 라이프사이클에 따른 관리 현황을 어떤 방법으로 추적하고 확인할 것인가?       * 개인정보가 네트워크를 통해 공유되는 경우 추적 방법은?       * 개인정보가 특정 파일에 저장된 경우 추적 방법은? | | |
| **향후계획** | * **회의 준비(멤버별)**   + (효림)다음주 회의 장소 예약   + (별하)팀&앱 로고 디자인 초안 제작(단톡방에 공유)   + (아림)PBL 팀장발표 PPT 제작   + (아림)GitHub Organization 생성 및 초대   + (경화)완성된 PPT LMS 제출(제출 후 카톡방 공지)   + (전체)선정주제와 유사한 연구 혹은 프로젝트 조사 * **다음 주 회의 안건**   + 주제 아이디어 구체화   + 유사 연구/프로젝트 점검 및 피드백 | | |
| **참고문헌** | ⑴[특허]드론 탐지기  <http://doi.org/10.8080/1020170172799>  ⑵Matter 핵심 명세서  <https://csa-iot.org/wp-content/uploads/2022/11/22-27349-001_Matter-1.0-Core-Specification.pdf>  ⑶SWING 인스타그램 보안뉴스 의료기기 보안  <https://www.instagram.com/p/Cmz7j_lrgY8/?utm_source=ig_web_copy_link> | | |