**종단형PBL 팀 회의록**

**팀 이름: Aegis**

**멤버: 이경화(팀장), 손효림, 한별하, 한아림**

● 회의 내역

|  |  |  |  |
| --- | --- | --- | --- |
| **회차** | **일자** | **장소/시간** | **요약** |
| 12 | 2024.04.15 | 중앙도서관 세미나실/12:00~15:00 | 새 주제 정하기 |
| 11 | 2024.04.12 | 제2과학관 204호/18:00~19:00 | (박후린 교수님 면담)프로젝트 진행 관련 세부 피드백 |
| 10 | 2024.04.08 | 중앙도서관 세미나실/12:00~15:00 | 프로젝트의 필요성 및 정체성 확립, AI디지털교과서 관련 스터디 |
| 9 | 2024.04.05 | 제2과학관 610호/12:00~15:00 | 발표에 대한 박후린 교수님 피드백, AI 디지털교과서 개발 가이드 스터디 |
| 8 | 2024.04.03 | 제2과학관 505호/15:00~16:00 | (오준형 교수님 회의)프로젝트 주제 브리핑 및 지도사항 |
| 7 | 2024.04.01 | 제2과학관 505호/15:00~17:00 | (오준형 교수님 면담) **“AI 디지털 교과서 서비스에서의 개인정보보호 어시스턴트 모듈 개발”**로 주제 변경 |
| 6 | 2024.04.01 | 중앙도서관 세미나실/12:00~15:00 | 유사 프로젝트(공격 툴) 조사, 관련 논문 조사 |
| 5 | 2024.03.29 | 제2과학관 610호/12:00~15:00 | 팀로고 투명버전 선정, 공격대상 선정, 마일스톤 작성, 아이디어 구체화, 기능구현 우선순위, 교수님 피드백 |
| 4 | 2024.03.28 | 제2과학관 303호 /19:30~21:00 | **“MePreat:비대면 업무환경에서의 보안 위협 모델”** 주제 제안, 주제 변경 |
| 3 | 2024.03.27 | 50주년기념관 625호  /18:00~20:00 | (손종모 교수님 면담)**“개인정보 라이프사이클 트래커”** 주제에 관한 조언 |
| 2 | 2024.03.25 | 온라인/12:00~15:00 | 팀로고 확정, 유사 프로젝트 조사, 주제관련 연구자료조사 |
| 1 | 2024.03.18 | 중앙도서관 세미나실/12:00~15:00 | 팀명 선정 및 프로젝트 주제 논의 |

**회 의 록(12회차)**

|  |  |  |  |
| --- | --- | --- | --- |
| **회차** | 12회차 | **일시** | 2024.04.15 (월) |
| **참석자** | 손효림, 이경화, 한별하, 한아림 | **장소** | 중앙도서관 세미나실 |
| **제목** | 새 주제 정하기 | | |
| **회의내용** | * **주제 제시**   + (아림) 무인화 기기(키오스크) 취약점 분석 및 공격 모델 제안   + (아림) NFC 환경의 취약점 분석 및 공격 모델 제안   + (아림) (여성)노숙인을 위한 아이디어 제안   + (아림) 인공지능을 활용한 멀웨어 공격 모델 제안   + (경화) 스마트팩토리 보안솔루션 개발의 기반이 될 수 있는 연구 혹은 모델 개발   + (경화) 사회공학적 취약점 자동관리 앱 개발   + (경화) 자신의 RFID 카드가 취약한 암호화 기법을 사용하고 있는지 체크할 수 있는 툴 개발   + (별하) AI보이스   + (별하) 영상에서 특정 인물 등을 추출해서 그림을 만드는 AI   + (별하) 비밀번호가 설정되어 있지 않은 공공 네트워크 보안   + (별하) 투표장에서 무단 촬영을 제한하는 프로그램   + (별하) 공용PC 자동 로그아웃 프로그램   + (별하) 생체 인식 와이파이 보안 문제 연구   + (별하) 생체 인식 와이파이를 이용한 자세 교정 프로그램   + (효림) 다크웹 내 개인정보 탐지 및 삭제   + (효림) 생체 인식 네트워크를 이용한 방법 체계   + (효림) 와이파이 공유기를 이용한 랜섬웨어 유포   + (효림) 클라우드 보안 설정 자동화   + (효림) 취약점 분석 자동화 툴 개발   + (효림) 공급망 보안(SBOM, 제로 트러스트 등)   + (효림) ISMS-P 인증 자동화 시스템 * **주제 선정 투표**   + **(여성)노숙인을 위한 아이디어 제안(4표) →최종선정**   + 비밀번호가 설정되어 있지 않은 공공 네트워크 보안(1표)   + 공용PC 자동 로그아웃 프로그램(1표)   + 생체 인식 와이파이를 이용한 자세 교정 프로그램(1표)   + 와이파이 공유기를 이용한 랜섬웨어 유포(1표)   + 클라우드 보안 설정 자동화(2표) * **선정 주제: (여성)노숙인을 위한 아이디어 제안**   + **배경**: “노숙인(홈리스) 생활개선을 위한 SW개발”을 주제로 **2024년 ICT콤플렉스 제12회 피우다프로젝트**가 개최됨(4-7월). 해당 경진대회의 주제인 “노숙인 생활개선”을 PBL 주제로 삼아 대회에 참가하고 이후 남은 PBL 기간동안 프로젝트를 고도화할 예정임.   + **세부 주제 선정**     - **1주제: 위치 기반의 노숙인 안전 확인 및 관리 서비스**     - 2주제: 노숙 위기에 있는 사람들을 잘 찾거나 본인 스스로 신청하여 필요한 지원을 잘 받을 수 있도록 연계하는 서비스   + **대회 일정**     - 04.05 ~ 05.01 신청접수     - 04.17, 04.26 노숙인 시설 담당자 인터뷰     - 05.02 ~ 05.03 서류심사 및 참가팀 선정     - 05.03 ~ 06.28 개발진행 및 결과제출     - 07.04 발표평가 및 시상 | | |
| **향후계획** | * **회의 준비(멤버별)**   + (경화)15일 회의록 작성   + (전체)아이디어 구체화   + (전체)신청서 양식 중 개발물 설명, 배경 및 목적, 기대효과 작성해오기 * **다음 주 회의 안건** | | |
| **참고문헌** | [기사]헥톤프로젝트 EMR ‘닥터스’, ‘똑닥’ 연동∙키오스크 출시  <https://www.medifonews.com/news/article.html?no=165306>  [논문]김미선, 김현곤 , 이범기, & 서재현. (2013). *NFC 보안 기술 및 보안 취약점에 관한 연구* (pp. 54-61). 스마트미디어저널 v.2 no.3: 한국스마트미디어학회.  [블로그] SW마에스트로 프로젝트 기획안 콘셉트  <https://m.blog.naver.com/ndb796/221250325406>  [기사] "최근 20·30 여성 노숙인이 많이 늘어... 이유는"  <https://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0003016437>  [기사] 서울시 노숙인에게 중고스마트폰 지급  <http://www.sijung.co.kr/news/articleView.html?idxno=73674>  [공모전] [피우다프로젝트] 2024 제12회 SW개발 공모전(노숙인 생활개선을 위한 SW개발) 참가자 모집  <https://www.ictcoc.kr/04_com_n/com02_view.asp?idx=893&page=1&params>=  [블로그] 공유기 해킹 증상 진단법 및 조치방안 알아보기  <https://nordvpn.com/ko/blog/router-hacked-signs/>  [기사] 기업이 알아야 할 와이파이 취약점 5가지  <https://www.ciokorea.com/t/1663/How%20To/325758#csidx38774a43241de55b4af04b626d23ab1>  [기사] 1억 명 피해자 낳은 캐피탈원 침해 사고, 클라우드 보안 인식 바꿔  <https://www.boannews.com/media/view.asp?idx=107662>  [기사] 2025년까지 모든 행정·공공기관 정보시스템 클라우드로 전환한다  <https://m.boannews.com/html/detail.html?idx=99370>  [기사] AI 홈 보안이 뭐길래... 삼성전자도 혁신을 강조하나  <https://m.boannews.com/html/detail.html?tab_type=1&idx=128627>  [기사]인공지능 모델 공유 플랫폼 허깅페이스에서 위험한 취약점 발견돼  <https://m.boannews.com/html/detail.html?tab_type=1&idx=128693> | | |

**회 의 록(11회차)**

|  |  |  |  |
| --- | --- | --- | --- |
| **회차** | 11회차 | **일시** | 2024.04.12 (금) |
| **참석자** | 손효림, 이경화, 한별하, 한아림 | **장소** | 제2과학관 204호 |
| **제목** | (박후린 교수님 면담)프로젝트 진행 관련 세부 피드백 | | |
| **회의내용** | * **프로젝트 브리핑과 교수님 피드백**   + (우리의 프로젝트가 기존 가이드라인이 미흡하다는 전제에서 시작되는데) 기존 가이드라인을 신뢰할 수 없다는 것을 검증하는 것이 우선되어야 함.   + (미성년자의 개인정보 보호 문제라서 중요성이 강조된다는 설명에 대해) 관념적인 설명보다 구체적인 사항을 제시할 필요가 있음   + (전체적인 프로젝트 브리핑에서) 대상 서비스에 대한 설명과 우리가 하려고 하는 것을 명확하게 구분해야 함.   + (각자 개별적으로 조사한 부분이 어떤 식으로 통합되는 것인지 물어보심)   + 데이터셋의 종류에 따라 어떤 흐름으로 관리되며 세부 항목이 무엇인지 정의해보기   + 일반적으로 가이드라인에서는 어떤 법이 업데이트되면 다른 것도 업데이트 되도록 하기 위해 특정 법이나 지침을 참고하라는 식으로 설명하는 것이 보편적임. * **프로젝트 진행 관련 QnA**   1. **브리핑에 대한 전체적인 평**      + 모듈에 대한 설명 부족. 필요성 면에서 위협 시나리오를 만들면 좋겠음.   2. **창의성, 도전성, 적합성, 적정성 점수평가**      + 이전 발표평가: 창의성, 도전성: 공동 2등, 적합성: 3등, 적정성: 4등      + 무엇을 하겠다는 것인지 명확히 보이지 않았음      + 프로젝트 기간이 3학기 분량을 채우기에 부족해보였던 것은 금일 브리핑에서 보완되었는데 여전히 모듈의 기술적 구체성이 부족함.   3. **본 프로젝트에서 가장 우려되는 부분(기술적, 사회적, 현실적 측면)**      + 표준 작성 시 전문가의 시각이 많이 필요함. 학교 교수, 산업계 전문가들, 위원회 등 많은 전문가들의 검토 과정이 매우 고되기 때문에 우리가 만든 가이드라인이 공식 가이드라인으로 나올 수 있을 것이라는 기대는 내려놓는 것이 좋음. 기여를 했다는 정도로 생각하면 될 듯함.   4. **본 프로젝트를 진행하며 가장 신경써야할 점**      + 용어의 일관성. 개인정보보호법 상의 용어를 그대로 써야함.   5. **(과한 욕심은 내려놓으라고 하셨는데) 목표의 방향성을 어떻게 잡으면 좋을까요?**      + 목표는 완성본을 만드는 것. 데이터셋에서 어떤 것이 개인정보인지 정의하고 비식별화 처리를 어떻게 할지 신경써야함.   6. **공격 시나리오에 반드시 들어가야 할 요소**      + 실제로 구체적인 시나리오를 집필한다고 생각하면 됨. 인물에 대한 구체적인 페르소나를 설정하고 인물들 사이의 관계를 설정하고, 어떤 정보의 노출로 누가 어떤 손해를 입을 수 있는지 등을 고려해야 함. 또 페르소나를 다르게 잡았을 때 어떤 차이가 존재할 수 있을까도 고민해보면 좋음.   7. **최대한 다양한 시나리오 vs 소수의 시나리오에 대한 심도있는 구체화**      + 생각할 수 있는 모든 엔티티를 대상으로 가능한 시나리오들을 다양하게 써보는 것이 좋음.   8. **클라우드에서 클라우드로 데이터가 전달될 때 나올 수 있는 취약점**      + 데이터 센터 내에서 발생할 수 있는 보안허점은 도스 공격 혹은 클라우드 관리자의 비윤리적 행위 등이 있음.      + 주로 클라우드-클라우드의 데이터 전달 시 두 클라우드는 같은 데이터 센터에 속함. 서로 다른 데이터 센터에 있을 시 싱크 문제 및 데이터 이민 시 시간이 오래 걸리는 문제 등이 발생함.      + 데이터가 암호화되어있다면 전송 도중 패킷이 탈취되어도 키값이 노출되지 않는 이상 개인정보가 유출되지는 않음.      + 우리는 시스템적인 유출이 아닌 비식별화와 차등적 권한 부여 등에 초점을 두고 접근해야 함.   9. **아직 개발되지 않은 서비스에 대한 모듈 성능평가 방법**      + 특정 위협 시나리오에 대해 우리의 가이드라인을 따르면 막을 수 있다는 것을 증명하면 됨. 오버헤드 등의 성능 평가가 아님.      + 정형 기법[분석]을 활용하는 방법: 엔티티(어플리케이션, 클라우드, 라우터 등), 데이터 전달, 중요 정보, 화살표 등을 표기한 그림을 그려보는 것 권장. 흐름도를 통해 구체적으로 어떤 부분에서 우리의 가이드라인과 모듈이 필요한지 설명이 가능함.      + Symbolic Analysis Tools 추천: SCYTHER, TAMARIN      + 우리가 만들 것은 명확한 방어 기법보다는 어떤 위협에 대해 암호화와 비식별화를 어떻게 적용하면 안전한지에 대한 가이드   10. **본 프로젝트의 강점**       + 산출물이 확실히 나온다는 점.   11. **본 프로젝트의 약점**       + 특허 출원은 어려워보임.(공익을 목적으로 하는 경우 특허 출원 어려움)       + PBL4에서 보여줄 수 있는 산출물이 떠오르지 않음. | | |
| **향후계획** | * **회의 준비(멤버별)**   + (전체)새로운 주제 n개씩 생각해오기   + (경화)4월 12일 회의록 작성 * **다음 주 회의 안건**   + 프로젝트 주제 선정 | | |
| **참고문헌** | . | | |

**회 의 록(10회차)**

|  |  |  |  |
| --- | --- | --- | --- |
| **회차** | 10회차 | **일시** | 2024.04.08 (월) |
| **참석자** | 한아림, 한별하, 손효림, 이경화 | **장소** | 중앙도서관 세미나실 |
| **제목** | 프로젝트의 필요성 및 정체성 확립, AI디지털교과서 관련 스터디 | | |
| **회의내용** | * **프로젝트의 필요성**   + 현재 해결해야 할 과제 2025년에부터 활용될 예정인 AI디지털교과서와 관련하여 참고할 수 있는 **교육 환경의 특수성을 고려한 가이드라인 및 조력 기제의 부재**     - 교육 환경의 특수성       * 교육 데이터의 다양성 및 회귀성       * 해당 분야에서의 교육적 요구 충족의 필요성       * 미성년자를 포함한 사용자 보호의 필요성   + 해결해야 하는 이유(필요성)     - “어떤 데이터를 어떻게 수집하고, 기록에 남겨 어느 범위까지 부모에 알릴 것인지 등 **중요한 쟁점이 상당히 생략된 채 논의가 진행**되고 있다” (정현선 경인교대 국어교육과 교수)     - “민간 디지털교과서 발행사들이 학생들의 데이터를 자체 서비스 개발에 사용하지 않도록 권고했으나, **구체적인 관리·감독 가이드라인**이 안 보인다” (정현선 경인교대 국어교육과 교수) * **프로젝트의 정체성**   + 본 프로젝트에서는 교육계의 첫 대규모 인공지능 교육 서비스 **‘A.I 디지털 교과서’**에 대한 개인정보보호 가이드라인 및 조력 모듈을 개발하고자 함     - 기타 분야의 가이드라인을 참고하되, 교육 분야의 특성을 반영하기 위한 최적화 과정을 진행하여 구체적인 개인정보보호 가이드라인 제시를 목적으로 함     - A.I 디지털 교과서에서 활용되는 소프트웨어에 적용 가능한 개인정보 자동 비식별화 모듈 개발을 목적으로 함 * **프로젝트의 기대효과**   + 법규 준수를 통한 안정적인 서비스 운영   + 학생의 '안전하고 신뢰할 수 있는 환경에서 학습할 수 있는 권리' 보장   + 교육 분야에서의 대규모 A.I 기술 활용 시, 개인정보보호 표준 가이드라인 정립에 기여 * **AI디지털교과서 관련 스터디**   + **AI 디지털교과서의 서비스 플로우**     - 주요 서비스 항목       * AI 디지털 교과서 서비스   Untitled.png   * + - * AI 기반 맞춤형 학습   Untitled (1).png   * + - * 교육 디지털원패스 서비스   Untitled (2).png   * + - 사용자 UX-학생  1. 통합인증체제의 계정(ID, PW)을 통해 로그인 2. 대시보드에 접근 3. AI 튜터 활용    * + 사용자 UX-교사 4. 통합인증체제의 계정(ID, PW)을 통해 로그인 5. 대시보드에 접근 6. AI 보조교사 활용    * + 사용자 UX-학부모 7. 통합인증체제의 계정(ID, PW)을 통해 로그인 8. 대시보드에 접근 9. 학생 정보 열람    * **AI 디지털교과서의 데이터 처리 흐름**      + AI 학습 진단 시 데이터 흐름        - 성취평가 및 학습 현황 데이터 수집 → 성취 수준 진단 및 학습 현황 분석 (대시보드) → 개인별 분석 결과 제공 및 추천에 활용(AI보조교사 → 교사) → 맞춤 추천(학습 경로, 학습 콘텐츠 & 문항 등)      + 서비스 전체 데이터 흐름        - 학습진단 → 데이터허브에 저장 → AI튜터, 대시보드에서 사용 → AI보조교사등을 통해 학습 커리큘럼 생성 → 교사가 피드백 및 재정비 → 학생에게 전달 → 학생 학습 → 학습 데이터 데이터허브에 저장      + 기능별 활용 데이터와 데이터 타입  |  |  |  |  |  | | --- | --- | --- | --- | --- | | 기관 | 기능 | 1차 데이터 | 2차 데이터 | 데이터 타입 | | 공공 | 디지털교과서 인증 | 학교급, 학교명, 학년, 반, 번호, 학급 구성, 시간표, 교과서 채택 정보 | x | 정형 | | 공공 | 대시보드  (학생) | 개인정보, 학습참여도,  학습성취도, 비정형 : 학습이력, 학습분석 | x | 혼합 | | 공공 | 대시보드  (교사) | 학생정보, 학습참여도,  학습성취도, 비정형 : 학습이력, 학습분석 | x | 혼합 | | 공공 | 대시보드  (학부모) | 학생정보, 학습참여도,  학습성취도, 비정형 : 학습이력, 학습분석 | x | 혼합 | | 민간 | AI보조교사 | 교육과정 내용, 학생들의 성취기준 달성 정도, 학생들의 학습활동, 학생들의 평가 결과 | 맞춤화된 수업 설계, 콘텐츠 & 문항 추천, 피드백 문장, 담당 학생들의 평가 결과 | 혼합 (정형 데이터가 대부분) | | 민간 | AI튜터 | 학습활동 상태, 학습데이터, 학습 태도, 이해도, 관심사, 선호도 , 개별 학습과정,  학습과정과 결과에서 분석된 데이터, 풀어본 문제 | 학습 성취평가 정보, 추가 학습 방향 , 추가 학습자료, 학습 수행도, 학습 참여도, 학생의 강·약점,성취도, 학습 전략 제안, 피드백 & To do 리스트, 오답노트 | 혼합 (비정형데이터가 대부분) | | 공공 | 학습데이터  허브 | 학습 과정에서 발생하는 학습데이터 저장 | x | 혼합 |  * + - 대시보드 내 노출 정보   Untitled (3).png  Untitled (4).png Untitled (5).png   * + **클라우드에서의 개인정보 관리**     - 데이터 수집       * 수집한 학습데이터를 학습데이터 허브에서 필요한 형태로 가공하여 제공할 수 있어야 함(필수)       * 데이터 수집,저장 시 국제표준인 Caliper Analysis 또는 xAPI 활용 권장     - 데이터 관리 및 개인정보 보호       * 신뢰성 확보 : 오류나 왜곡 없는 데이터, 편향성 없는 데이터       * 데이터 활용 동의 : 데이터 수집 시점, 데이터 활용 목적, 범위, 기간 등에 대해 학생(학부모)의 동의       * 데이터 보안 : 학습데이터 보안을 위해 데이터 암호화, 접근 제어 등의 보안 기술과 절차를 적용할 수 있어야 하며, 데이터 유출 및 악용을 방지하기 위해 적절한 데이터 보안 정책을 마련       * 목적 외 활용 금지 : 자체 서비스를 위한 목적으로 사용해서는 안됨       * 데이터 제공 : 학생(학부모)의 데이터 전송요구 등의 요청에 적절히 대응       * 개인정보 비식별화 : <개인정보 비식별 조치 가이드라인>에 따라 비식별(익명화, 가명화) 조치       * 데이터 보존 및 파기 : 개인정보 활용 동의서에 따라 관리·보존     - 데이터 전송       * 개발사는 AI 디지털교과서 활용 과정에서 수집한 원천 학습데이터를 목적에 따라 가공하여 데이터셋을 생성하고 학습데이터 허브로 전송하여야 함       * 전송하는 데이터셋의 종류  1. 국가수준 학습 데이터셋 2. 통합 대시보드 데이터셋 3. 학습이력 데이터셋 4. AI 트레이닝용 데이터셋  * 데이터 전송 시 xAPI 표준으로 전송하며 전송된 데이터는 학습 데이터 허브 내 LRS(Learning Record Store)에 저장됨   + **가이드라인에서 언급된 법률, 조치 고시**     - 개인정보보호위원회의 인공지능(AI) 개인정보보호 자율점검표(개발자·운영자용)(2021. 5. 제정)의 항목 중 필수에 해당하는 사항을 준수하여야 함       * **개인정보 보호법** 제1조, 제2조, 제3조, 제4조, 제15조, 제16조, 제17조, 제18조, 제20조, 제22조, 제23 조, 제24조, 제26조, 제28조, 제29조, 제30조, 제31조, 제34조, 제35조, 제36조, 제37조, 제38조, 제39 조의3,4,6, 제58조의2, 제71조, 제75조       * **개인정보 보호법 시행령** 제14조의2, 제16조, 제17조 ~ 제19조, 제29조, 제30조, 제39조, 제40조, 제41 조~44조, 제48조의2,4,5       * **표준개인정보보호지침** 제6조, 제12조 ~ 제13조, 제15조, 제18조~제21조, 제25조~제29조, 제31조~제 34조, 제44조 등       * 「개인정보 처리 방법에 관한 고시」 제4조, 「개인정보의 안전성 확보조치 기준(고시)」 제4조 ~ 제12조, 「개인정보의 기술적·관리적 보호조치 기준(고시)」 제3조 ~ 제8조 | | |
| **향후계획** | * **회의 준비(멤버별)**   + (경화)회의록 작성   + (전체)비정형 데이터 가명처리 가이드라인 읽어오기   + (전체)AI 디지털교과서 기능 설명서 읽어오기 * **다음 주 회의 안건** | | |
| **참고문헌** | AI 디지털 교과서 개발 가이드  개인정보보호위원회의 인공지능(AI) 개인정보보호 자율 점검표(개발자·운영자용)(2021.5. 제정)  「개인정보의 기술적·관리적 보호조치 기준(2020.12.)」. 개인정보보호위원회  개인정보 보호 법령 및 지침·고시 해설(’20.12)  「개인정보 수집 최소화 가이드라인(2020. 12. )」, 개인정보보호위원회  「온라인 개인정보 처리 가이드라인(2020. 12. )」, 개인정보보호위원회  행정안전부 「개인정보 비식별 조치 가이드라인」  개인정보보호위원회 누리집 :정책·법령/법령정보/지침·가이드라인  개인정보 보호 포털 :자료마당/지침자료 | | |

**회 의 록(9회차)**

|  |  |  |  |
| --- | --- | --- | --- |
| **회차** | 9회차 | **일시** | 2024.04.05 (금) |
| **참석자** | 한아림, 한별하, 손효림, 이경화 | **장소** | 제2과학관 610호 |
| **제목** | 발표에 대한 박후린 교수님 피드백, AI 디지털교과서 개발 가이드 스터디 | | |
| **회의내용** | * **박후린 교수님 질문 및 피드백**   + **AI 디지털 교과서의 개인정보 관련 문제점을 명확히 설명해주세요.**     - AI디지털교과서는 학생의 학적 데이터와 학습 태도, 학습 수준 등의 학습 데이터를 수집합니다. 이러한 개인정보에 대한 관리가 미흡하여 개인정보가 유출될 경우 학생이 피해를 입을 수 있습니다.   + **AI 디지털 교과서의 개인정보 관리 정책이 미흡하다는 걸 어떻게 알았죠?**     - 금융, 의료 관련 개인정보 관리 가이드를 읽어보았는데, 해당 가이드와 비교해보았을 때 AI 디지털교과서에서 언급되는 개인정보 관리 가이드가 구체성이 부족함을 확인할 수 있었습니다.   + **이 프로젝트를 하면서 가장 오래 걸릴 것 같은 부분은 무엇인가요?**     - 비정형 데이터에 대한 개인정보 보호 정책 수립 부분이 어려울 것 같습니다. (정책 수립이 목적이라면 기존의 가이드를 참고하여 제시하면 되어서 그리 어렵지 않을 것 같아요.)   + **목표가 정책 수립으로 되어있는데, 기존에 사용하던 비식별화 방식이 안전하므로 같은 방법을 도입할 것인지 아니면 우리가 만든 가이드대로 진행해봤더니 안전하게 비식별화된다는 것을 주장할 것인지?**     - 기존의 비식별화 방법을 도입하는 쪽으로 갈 것 같습니다.   + **개발할 모듈의 기존 기술과의 차별점은 무엇인가요?**     - 기술적 차별점보다는 분야적 차별성을 이야기할 수 있을 것 같습니다. 기존에는 금융, 의료 분야에서 개인정보 보호 문제를 민감하게 다루었는데, 교육 분야에서는 이제 막 도입되는 단계라 기존과 차별점을 가질 수 있습니다.   + **민간에서 서비스하는 교육용 학습 툴과 AI 디지털교과서가 학생에게 맞춤형 교육 컨텐츠를 제공한다는 점에서 유사한 것 같은데 기존의 민간 툴에서와 다른 새로운 문제점이 있나요?**     - 민간에서 제공하는 학습 서비스와 달리 AI 디지털 교과서는 교육부가 주도하여 기존에 국가에서 진행하는 교육 관련 서비스들과 데이터가 연동되는 형식이기 때문에 민간 학습 서비스에서는 고려하지 않아도 되었던 부분을 신경 써야하는 부분이 있습니다. 예를 들면 연계 교육 기관 데이터 포털과 연계되어 학생의 학습 데이터를 평가 기관 등이 열람할 수도 있습니다. * **AI 디지털교과서 개발 가이드 스터디**   + 기능별 데이터 처리 상세     - AI 튜터, 통합 대시보드, 학습데이터 허브: 학생 학습시간, 학생 학습진도, 학습성취 수준     - 학생,교사,학부모 서비스: 학생 학습패턴, 학생 학습 관심사 및 선호도, 학생 학습시간, 학생 학습진도, 학습성취 수준     - 통합인증 체계, 연계: 학교급/명, 학년/반/번호, 교육디지털 원패스 + 나이스플러스 사용자 정보, 학급 구성 및 시간표, 교과서 채택 정보     - (내포) 교육디지털 원패스: 계정 ID, 패턴, PW, 지문, 사용자 얼굴(안면 인식용), 인증서   + 주요 페이지별 내용     - 7.2, 11.3: 보안 관련 내용     - P.15 개발 3원칙     - P.16 느린 학습자, 빠른 학습자     - P.23 서비스 흐름     - P.36 품질관리 및 환류 단계     - P.43 계정 및 보안 관리     - P.47 클라우드     - P.56~58 공통 기능 연계     - P.84 기술적인 부분에서 나올 수 있는 데이터     - P.86 학생/교사/학부모 대시보드 내 노출 정보     - P.93 AI 튜터     - P.96 AI 보조교사     - P.101 데이터 전송 관련 필수 준수 사항     - P.129 비정형 데이터 | | |
| **향후계획** | * **회의 준비(멤버별)** * (경화)회의록 작성 * (경화)평가지 양식 취합 후 제출 * (전체)프로젝트의 필요성 생각해오기 * (전체)프로젝트의 정체성 생각해오기 * (아림)서비스 플로우 공부해오기 * (별하)데이터 처리 흐름 공부해오기 * (경화)클라우드에서 개인정보 관리 공부해오기 * (효림)언급된 법률, 조치, 고시 등 조사해오기 * **다음 주 회의 안건**   + AI 디지털교과서 개발 가이드 읽고 각자 준비한 내용 공유 | | |
| **참고문헌** | AI 디지털 교과서 개발 가이드 | | |

**회 의 록(8회차)**

|  |  |  |  |
| --- | --- | --- | --- |
| **회차** | 8회차 | **일시** | 2024.04.03 (수) |
| **참석자** | 한아림, 한별하, 손효림, 이경화 | **장소** | 제2과학관 505호 |
| **제목** | (오준형 교수님 회의)프로젝트 주제 브리핑 및 지도사항 | | |
| **회의내용** | * **프로젝트 주제 브리핑**   + 주제: AI 디지털 교과서 서비스에서의 개인정보보호 어시스턴트 모듈 개발   + AI 디지털 교과서     - 지능정보기술을 활용하여 학습 지원 기능을 서비스하는 SW     - 개발 목적: 학생 개개인의 능력과 수준에 맞는 가양한 맞춤형 학습 기회 제공     - 주제 설명: AI 디지털 교과서 개발 과정 중 ‘학습데이터 수집, 관리, 전송’에서의 데이터 관리 정책 수립 및 개인정보보호 어시스턴트 모듈 개발   + 아이디어의 필요성과 중요성     - AI 디지털 교과서의 주요 기능       * AI에 의한 학습 진단과 분석       * 개인별 학습 수준과 속도를 반영한 맞춤형 학습       * 학생의 관점에서 설계된 학습 코스웨어     - AI 디지털 교과서의 기능 제공 과정에서 학생의 학업 성적, 성명, 학교 등 민감한 개인정보를 다수 활용하므로 해당 서비스에 대해 학습데이터 처리과정에서의 데이터 관리 조력이 필수적임   + 프로젝트 진행 계획 및 최종 목표 * **2024.04.01~05.31** : AI 디지털 교과서 개발 가이드라인 검토 및 업데이트 * **2024.06.01~08.31** : 학습데이터 처리 과정에서의 데이터 관리 정책 수립 * **2024.09.01~09.30** : 기타 서비스 정책과의 호환성 검토 * **2024.10.01~10.31** : 개인정보보호 어시스턴트 모듈화 진행 * **2024.11.01~12.31** : 모듈 정상화 및 안정화 작업 진행 * **2025.01.01~** : 서비스 최종 검토 후 정상 배포   + 예상 목표 산출물     - **논문** : 개인정보보호 관리 정책 수립     - **특허** : 개인정보보호 어시스턴트 모듈 * **지도사항**   + 가이드라인 작성: 배포되는 가이드라인은 현업 적용성을 생각해 실제 연구내용에 비해 모호한 편임. 따라서 우리는 먼저 구체적인 가이드라인을 만들어야 함.   + AI디지털교과서는 2025년 출시 예정. 사업이 급하게 진행된 편이라 출시 이후 개정이 필요함. 우리의 가이드라인과 모듈을 반영해서 개정하도록 하는 것이 목표.   + 프로젝트 진행 시 개발 가이드라인 검토 및 관리 정책 수립과 개발이 동시에 이루어져야 함.   + 자연어로 된 학습데이터가 많으므로 자연어 처리 관련 선행연구가 필요함.   + 다음주까지 AI디지털교과서 개발 가이드라인을 참고해서 기능을 꼼꼼히 파악 후 어떤 정보가 활용될 것이며, 그 중 위험성이 있는 개인정보가 무엇이며 어떤 형태인지 자세하게 정리해오   + 개인정보보호혁신인재양성사업단 연구 지원   + 특강 추천: 비정형 데이터 관련 개인정보보호 가이드라인 만드신 개인정보보호위원회 주문호 사무관님 특강(4월17일 15시, 제2과 B114호)   + 가이드에 학생 학적 데이터(일반데이터) 및 학습 데이터(비정형 데이터)에 대한 가이드가 모두 포함되어야 함. 학적 데이터의 경우 다른 가이드라인 참고해도 좋음. 비정형 데이터에 대해서는 특화된 가이드가 필요. 관련 스터디에 특별히 신경써야 함.   + 개인식별정보와 민감정보의 차이: 민감정보는 노출되면 개인에 대한 낙인이 찍힐 수 있는 정보로 종교, 정치, 성적지향 등의 정보가 해당됨.   + 가명화, 익명화 처리를 해도 데이터 결합 과정에서 보호조치가 무력화되는 경우도 있음. 이 문제 해결을 위해 테이블을 무분별하게 결합지 못하도록 각 테이블별 권한 설정을 달리 함.   + AI디지털교과서 개발하는 기업: 스마트앤와이즈 주식회사   + 주어진 가이드라인에서 개인정보 관리가 '자율점검'으로 가이드된 부분이 미흡함. 철저하고 편리한 관리를 위해 자동화를 제공하는 모듈 개발 필요. 가능하다면 개인정보 관리 모니터링도 구현해서 모듈이 아닌 온전한 SW 형태로 개발해도 좋음. | | |
| **향후계획** | * **회의 준비(멤버별)**   + (경화)회의록 작성   + (전체)AI 디지털교과서 개발 가이드 정독   + (전체)교수님 지도사항 숙지   + (별하,효림)회의 내용 요약 * **다음 주 회의 안건**   + AI디지털교과서 기능 상세 분석   + AI디지털교과서에 활용되는 정보 파악과 민감 정보 분별 | | |
| **참고문헌** | 교육부. AI 디지털교과서 개발 가이드라인(2023)  보건복지부, 개인정보보호위원회. 보건의료데이터 활용 가이드라인(2022)  금융위원회, 금융감독원. 금융분야 가명,익명처리 안내서\_개정(2022)  개인정보보호위원회. 비정형데이터 가명처리 기준 주요내용(2024) | | |

**회 의 록(7회차)**

|  |  |  |  |
| --- | --- | --- | --- |
| **회차** | 7회차 | **일시** | 2024.04.01 (월) |
| **참석자** | 한아림, 한별하, 손효림, 이경화 | **장소** | 제2과학관 505호 |
| **제목** | (오준형 교수님 면담) “AI 디지털 교과서 서비스에서의 개인정보보호 어시스턴트 모듈 개발”로 주제 변경 | | |
| **회의내용** | * **면담 내용 요약**   1. 주제 자체는 좋으나 보안 취약점을 발견하는 것이 어려워보임   2. 주제 정할 때 고려해볼만한 사항 : 깊이 있게 연구할 것이 있는지, 사람들에게 도움이 되고 니즈가 있는지   3. CVE를 한 개만 찾는 것으로는 논문을 쓰기에 부족함. 일반화할 수 있는 취약점이어야 함. 또한 공격 대상 중에 일반적으로 많이 쓰는 툴이 포함되어야 함.   4. 발전 방향성을 제시한다면 공격 시나리오를 다양화하여 모두 시도해보기.]   5. 특허는 새로운 공격 모델을 구상한 다음 그것을 정수화 시키면 가능   6. 취약점 분석 툴은 들은 바가 없음   7. 비대면 회의 툴의 개인정보 위협 요소: 참여 화면을 녹화하여 참여자 얼굴 유포, 사진이나 영상을 공개 플랫폼에 업로드하면 개인정보 위협이 될 수 있음   8. 이미 있는 것만 하는 것은 가치가 낮으므로 기존과 다른 새로운 것들을 창출해내는 것이 중요함.   9. 자동화 구현 경험 공유: C언어를 사용했었고, 홈페이지 크롤링은 셀레늄 활용.   10. 최근 자동화가 각광받는 이유: 인건비 절감   11. 개인정보 관련 서비스 추천: 내 개인정보를 관리해서 판매할 수 있는 서비스   12. 성공적인 프로젝트의 공통점: 매주 진척사항이 있음. 프로젝트는 대규모로 하는 것 추천. 많은 사람들이 재미있어하고 좋다고 생각하는 주제가 좋은 주제   13. 개인정보 관리 라이프사이클 주제에 대한 피드백: 소비자가 자신의 개인정보 관리에 신경을 쓰게 만드는 것이 선행되어야 함. 개인정보 관련 주제를 추천하자면 1차병원의 의사랑시스템 개인정보 관리 체계 개선, AI 디지털교과서에 대한 개인정보 관련 내용 보완 | | |
| **향후계획** | * **회의 준비(멤버별)**   + (전체)교수님이 주신 자료 개괄 파악 * **다음 주 회의 안건** | | |
| **참고문헌** | . | | |

**회 의 록(6회차)**

|  |  |  |  |
| --- | --- | --- | --- |
| **회차** | 6회차 | **일시** | 2024.04.01 (월) |
| **참석자** | 한아림, 한별하, 손효림, 이경화 | **장소** | 중앙도서관 세미나실 |
| **제목** | 유사 프로젝트(공격툴 및 공격기법) 조사, 관련 논문 조사 | | |
| **회의내용** | * **공격 툴과 공격기법**   + ZOOM을 대상으로 한 ‘줌바밍 공격’   + 짓시미트 취약점 CVE-2022-36736   + 짓시미트 취약점 CVE-2022-43550   + TechChip-CamPhish: 캠 피싱 툴   + EntySec-CamOver: 네트워크 카메라의 admin 패스워드 노출   + Metasploit-msfvenom: 악성코드 제작툴   + 줌 사칭 도메인에 악성 파일을 등록해 멀웨어 유포, 2020.4.   + 줌 ECB 모드에서 AES-256보다 보안상 취약한 AES-128 키 암호화 사용   + 줌바밍 (=줌 폭격), 회의 ID 유출로 침입하여 수업을 망침   + 줌 취약점 CVE-2022-22784 (부적절한 XML 검사)   + 줌 취약점 CVE-2022-22786 (업데이트 패키지의 다운그레이드),   + 줌 취약점 CVE-2022-22787 (부적절한 호스트 이름 검사),   + 줌 취약점 CVE-2022-22785 (부적절한 세션 쿠키 검사)   + 줌 마이크로 수집한 키보드 소리를 이용하여 내용의 93% 탈취 * **비대면 업무 툴 대상 공격모델을 다룬 논문 스터디**   + 줌의 보안 취약점 분석과 보안 업데이트 결과 비교(2020)   + 이메일 클라우드 보안 서비스(E-mail SecaaS)의 기술적 보안위협 연구 - 위협모델링 기법을 중심으로 -(2017)   + 위협 모델링 기법을 이용한 펨토셀 취약점 분석에 대한 연구(2016)   + 원격 약복용 모니터링 시스템의 보안 위협 모델링(2019)   + Zoombombing: causes and preventions (2023)   + 정적 분석 도구 성능 비교 및 분석: 오픈소스의 보안 취약점을 기반으로(2022)   + 오픈소스의 보안 취약점에 관한 연구   + 난독화된 오픈소스 안드로이드 앱을 탐지하는 기법 구현(2019)   + 소스코드의 취약점 이력 학습을 이용한 소프트웨어 보안 취약점 분석 시스템(2017)   + 오픈 소스 기반 5G 액세스 네트워크 보안 취약점 자동 검증 프레임워크(2023)   + 오픈 소스의 소프트웨어 보안 문제 및 시큐어 코딩 적용방안(2017)   + 오픈소스 보안취약점 관리를 통한 안전한 오픈소스 사용 방안   + 설계단계에서 발생하는 보안약점에 대한 연구 : 소프트웨어 개발보안 관점(2020) | | |
| **향후계획** | * **회의 준비(멤버별)**   + (전체)ZOOM의 하위호환 툴 조사   + (전체)비대면 업무 툴 대상 공격 모델을 다룬 논문 브리핑 준비   + (전체)서비스 가치 자료조사(연령, 용도, 사용자수 등) * **다음 주 회의 안건**   + 공격 대상 툴 선정   + 비대면 업무 툴 대상 공격모델 스터디   + 서비스 가치 문서화 | | |
| **참고문헌** | (이글루코퍼레이션)비대면 근무체계로 인한 보안이슈 및 대응방안(2020),  <https://www.igloo.co.kr/security-information/%EB%B9%84%EB%8C%80%EB%A9%B4-%EA%B7%BC%EB%AC%B4%EC%B2%B4%EA%B3%84%EB%A1%9C-%EC%9D%B8%ED%95%9C-%EB%B3%B4%EC%95%88%EC%9D%B4%EC%8A%88-%EB%B0%8F-%EB%8C%80%EC%9D%91%EB%B0%A9%EC%95%88/>  (Exploit Database CVE details)Jitsi : Secutiry vulnerabilities, CVEs  <https://www.cvedetails.com/vulnerability-list/vendor_id-16088/Jitsi.html> | | |

**회 의 록(5회차)**

|  |  |  |  |
| --- | --- | --- | --- |
| **회차** | 5회차 | **일시** | 2024.03.29 (금) |
| **참석자** | 한아림, 한별하, 손효림, 이경화 | **장소** | 제2과학관 610호 |
| **제목** | 팀로고 투명버전 선정, 공격대상 선정, 마일스톤 작성, 아이디어 구체화, 기능구현 우선순위, 지도교수님 피드백 | | |
| **회의내용** | * **팀로고 수정**   + 팀로고 투명버전 후보(순서대로 1,2,3)   **Green Logo 투명배경.pngOrange Logo 투명배경 1.pngOrange Logo 투명배경 2.png**   * + 선정 로고: 3 * **공격 대상 선정**   + 비대면 회의 플랫폼 조사     - Webex     - Microsoft Teams     - Skype     - Google Meet     - BlueJeans     - Boardmix     - 네이버 웨일온     - Jitsi Meet     - 버터(Butter.us)     - 웨어바이(whereby.com)     - 어라운드(Around.co)     - 팝(pop.com)     - 코시오피스(kosyoffice.com)   + 공격 대상 선정: **Jitsi Meet**     - 선정 이유: 오픈소스, 다수의 사용자 보유 * **마일스톤 작성**   + 공격대상 후보 조사   + 공격대상 선정   + 공격 툴 존재 유무 조사   + 유사 아이디어 혹은 논문 조사(보안 위협 모델 개발 방식 참고)   + 오픈소스 코드 분석   + 취약점 탐색   + 취약점 선정(선정기준: 익스플로잇 가능성)   + 취약점 분석   + 익스플로잇   + CVE 제보   + 취약점을 이용한 공격 툴 구현(로컬백신 우회방법 탐색 필요)   + 툴 삽입 후 시연 영상 제작 * **아이디어 구체화** * 공격 시나리오   + - Jitsi Meet 코드 분석하여 취약점 발굴 및 CVE 제보     - 찾은 취약점을 통해 공격자가 사용할 툴 삽입(기존에 있는 툴 사용 가능)     - 사용자의 회의 진행 중 실시간으로 정보 유출되는 과정 시연     - 공격자는 얻은 데이터로 2,3차 공격 수행 * 위협 모델링   1. 위협 모델링이란? 소프트웨어 개발 생명주기(SDLC) 과정 중에 구현 전 단계에서 시스템 구성도, 네트워크 구성도, UI/UX 문서 등 소프트웨어 관련 문서를 분석하고 이를 토대로 발생 가능한 잠재적인 취약점을 찾아 미리 대응할 수 있도록 하는 분석방법   2. Microsoft사의 Microsoft Threat Modeling Tool 등 활용 가능한 위협 모델링 툴이 있음 * **기능구현 우선순위**   + 마이크, 비디오 정보 획득   + 채팅 정보 획득   + 다른 공격대상에 적용 * **지도교수님 피드백** * 유사한 공격 툴은 아마 없을 것임. * ‘공격 툴 존재 유무 조사’와 ‘유사 아이디어 혹은 논문 조사’는 비슷한 내용이므로 동시에 진행해도 됨. * 직접 코드를 보고 취약점을 탐색하는 것은 CVE를 많이 알아야 가능하므로 난이도가 높음. 공개된 공격 툴 등이 있으면 활용 가능한지 테스트해보는 것을 추천함. * 로컬 백신을 우회하는 방식은 논문 참고 * 취약점에 대한 패치를 제시하는 것이 아닌 공격 탐지 기법을 제안하는 것이 좋음. 예를 들면 데이터 트래픽이 특정 포트에서 증가하면 공격이 들어오는 것으로 탐지하는 식. * 자동으로 취약점을 탐지하는 툴을 만드는 것을 목표로 하는 것이 아니라 취약점은 우리가 발견하고 해당 취약점을 뚫는 것을 툴로 시연. 만약 기존에 있던 툴이 없으면 우리가 제작. * 취약점을 긁어오는 툴은 제작 불가능. * 게임 등의 상용 프로그램에서는 해당 프로그램 실행 중에 비정상적인 메모리 접근이 탐지되면 프로그램을 종료하는 기능이 있는 경우가 있음. 따라서 먼저 로컬에 비대면 회의 플랫폼을 구축해서 데이터를 긁어오는 걸 시연해보고 실제 프로그램을 대상으로도 가능한지 시도해보기. * 도청 시 다양한 데이터를 모두 가져오는 것도 좋지만 일부라도 가능한 만큼만 가져오는 식으로 유연하게 구현 * 공격 툴 개발과 CVE 제보는 방향성이 조금 다름. ZOOM 실행 시 공격 툴을 실행하는 것이 ZOOM 자체의 취약점은 아닐 수 있음. 병행이 될지는 모르겠지만 CVE 제보도 괜찮아 보임. * (선정 주제의 적절성에 대해)효용이 있어 보임. 비대면이 없어질 순 없을 것임. * (프로젝트 방향성이나 추구미)기존 연구에서 백신 우회 방법을 조사해 적용하는 것이 중요할 듯함. 다양한 데이터를 훔치는 마이크, 페이스캠 등이 하나씩 보면 간단한 도청인데 공격에 성공하려면 모두가 백신을 우회해야 함. 기존 백신 중 어떤 것을 가정하고 외부에서 어떻게 우회할지를 제시하는 것이 쟁점. 백신이 잡지 못하는 것도 있음. | | |
| **향후계획** | * **회의 준비(멤버별)**   + (별하)오준형 교수님께 자료전송   + (경화)회의록 업데이트   + (전체)비대면 업무 툴을 대상으로 한 공격모델을 다룬 논문 조사 및 브리핑 준비   + (전체)우리와 유사한 공격 툴 조사 * **다음 주 회의 안건**   + 조사한 논문 브리핑   + 아이디어 구체화   + 교수님 상담을 통한 피드백과 반영 | | |
| **참고문헌** | 김규형; 최윤성. (2020). 줌의 보안 취약점 분석과 보안 업데이트 결과 비교. 디지털산업정보학회논문지, 16(4), 55-65김혜원; 유호준; 이재우. (2017). 이메일 클라우드 보안 서비스(E-mail SecaaS)의 기술적 보안위협 연구 - 위협모델링 기법을 중심으로 -. 情報保護學會誌, 27(6), 57-64김재기; 신정훈; 김승주. (2016). 위협 모델링 기법을 이용한 펨토셀 취약점 분석에 대한 연구. 정보처리학회논문지, 5(8), 197-210허승원; 최진영. (2019). 원격 약복용 모니터링 시스템의 보안 위협 모델링. 정보과학회. 컴퓨팅의 실제 논문지, 25(12), 622-627 최화연; 유성진; 박영호. (2021). 5G 네트워크 환경에서 화상 회의에 적용가능한 인증 및 그룹 키 합의 방식의 보안 취약점 분석 및 대응 방안. 한국통신학회 학술대회논문집, 2021(6), 850-851  한국인터넷진흥원-취약점 정보 공유> Zoom 제품 보안 업데이트 권고  <https://knvd.krcert.or.kr/detailSecNo.do?IDX=5699>  6년 최고의 무료 화상 회의 소프트웨어 플랫폼 2024개  <https://www.freeconference.com/ko/blog/best-video-conferencing-tools/> Kerentseva Nina; Volgograd State University; Trofimov Aleksandr; Galich Sergey; Volgograd State University; Volgograd State University. (2023). Analysis of VP9 Video Codec Used in Jitsi Multi-Protocol Platform. NBI Technologies, 2023(29), 29-34 [기사] “악용이 많아서…” 계정 인증 추가한 짓시미트  <https://techrecipe.co.kr/posts/57570>  Jitsi Meet 사용 매뉴얼  <https://www.jungnanglib.seoul.kr/sblib/index.php?g_page=community&m_page=community03&act=down&wd=93&bf_code=4045&bb_code=11463>  CVEdetails.com> Jitsi : Security Vulnerabilities, CVEs,  <https://www.cvedetails.com/vulnerability-list/vendor_id-16088/Jitsi.html>  CVE-2021-39205  <https://nvd.nist.gov/vuln/detail/CVE-2021-39205>  Robertas Maleckas; Kenneth G. Paterson; Martin R. Albrecht. (2023). Practically-exploitable Vulnerabilities in the Jitsi Video Conferencing System.  <https://eprint.iacr.org/2023/1118>  [공식문서]jitsi.org> Jitsi Meet Security & Privacy  <https://jitsi.org/security/>  허신욱, 인영진, 박창준, 김호원. (개최날짜). 오픈소스의 보안 취약점에 관한 연구. 한국정보과학회 학술발표논문집, 개최지.  임경환, 김병철, 조성제. (2019). 난독화된 오픈소스 안드로이드 앱을 탐지하는 기법 구현. 정보과학회 컴퓨팅의 실제 논문지, 25(2), 106-112, 10.5626/KTCP.2019.25.2.106  이광형, 박재표. (2017). 소스코드의 취약점 이력 학습을 이용한 소프트웨어 보안 취약점 분석 시스템. 한국산학기술학회 논문지, 18(11), 46-52.  정제원, 신재민, 이수기, 김유성. (2023). 오픈 소스 기반 5G 액세스 네트워크 보안 취약점 자동 검증 프레임워크. 정보과학회논문지, 50(6), 531-539, 10.5626/JOK.2023.50.6.531  정지인, 이재혁, 이경률. (2022). 정적 분석 도구 성능 비교 및 분석: 오픈소스의 보안 취약점을 기반으로. 한국통신학회논문지, 47(4), 679-689, 10.7840/kics.2022.47.4.679  김병국. (2017). 오픈 소스의 소프트웨어 보안 문제 및 시큐어 코딩 적용방안. 정보과학회 컴퓨팅의 실제 논문지, 23(8), 487-491, 10.5626/KTCP.2017.23.8.487  류원옥, 조수형, 이승윤. (개최날짜). 오픈소스 보안취약점 관리를 통한 안전한 오픈소스 사용 방안. 한국통신학회 학술대회논문집, 개최지.  Jason Byrne; Mariko Furuyabu; Jeff Moore; Takehiko Ito. (2020). The Unexpected Problem of Classroom Video Conferencing: An Analysis and Solution for Google Hangouts and Jitsi Meet | | |

**회 의 록(4회차)**

|  |  |  |  |
| --- | --- | --- | --- |
| **회차** | 4회차 | **일시** | 2024.03.28 (목) |
| **참석자** | 한아림, 한별하, 손효림, 이경화 | **장소** | 제2과학관 303호 |
| **제목** | “MePreat:비대면 업무환경에서의 보안 위협 모델” 주제 제안, 주제 변경 | | |
| **회의내용** | * **주제 제시: “MePreat:비대면 업무환경에서의 보안 위협 모델”**   + **아이디어의 필요성**     - COVID-19로 인해 비대면 업무 환경이 급격하게 활성화되었고, 펜데믹이 지난 지금까지도 비대면 업무 환경 툴이 널리 쓰이고 있음     - 회사 업무뿐만 아니라 단순 일상 회의 등 다양한 용도로 ZOOM, 구글 미트 등의 비대면 툴들이 쓰이게 되었으며, 이에 따라 비대면 업무환경에서의 보안 위협 사례 또한 증가하고 있는 추세임     - 핵심적이고 개인적인 정보가 오가는 비대면 회의의 특성상, 사이버 위협 발생 시 사고 규모가 커지는 문제 또한 존재함     - 이에 따라 우리는 비대면 업무환경에서의 보안 위협의 심각성을 촉구하고자 자체 제작 보안 위협 모델을 제안하는 바임   + **아이디어 개요**     - MePReat은 비대면 미팅 플랫폼을 뜻하는 Meeting Platform 과 위협을 뜻하는 Treat의 합성어입니다.     - 본 프로젝트에서는 비대면 업무환경에 심각한 위협을 줄 수 있는 모델을 제안하고자 합니다. MePReat은 사용자의 IoT기기에 도청 및 중간자 공격을 위한 환경을 조성하여, 실제 비대면 업무가 진행될 때 정보를 도청 및 탈취하는 공격을 수행하는 모델입니다.   + **공격 모델 작동 과정**  1. 사회공학적 기법으로 사용자의 PC에 접근 2. 정보 도청 및 누출을 위한 프로그램 or 툴 설치 3. 사용자가 ZOOM에 접속하여 회의 진행 → 이때 사용자는 본인PC가 감염되었다는 것을 모르는 상태 4. 회의 속 데이터들이 공격자에게 실시간으로 유출됨 5. 공격자는 얻은 정보를 토대로 2,3차 공격 수행    * **우리가 개발해야할 부분**  * ②번 과정에서 사용자 PC에 심을 수 있는 요소: Spyware, Malware, Keylogger, Adware, Phishing 등 * 형식에 상관없이 데이터 가로채기 및 도청을 수행할 수 있게 해야 함. * 여러 요소들을 혼합한 프로그램을 개발하는 것도 좋을 듯 * 다양한 종류의 데이터를 대상으로 하는 이유: 비대면 화상회의 툴은 회의할 때 여러 가지 개인정보 관련 데이터가 혼합되어 진행됨. 다양한 종류의 데이터를 확보할수록 완성도 있는 공격이 될 것으로 생각함. * 비대면 업무 중 통신되는 데이터 종류: 소리(음성):마이크, 비디오: 페이스캠, 글자(텍스트):채팅, 이미지:채팅, 파일:채팅   + **다른 유사 모델과의 차별성**     - 유사 아이디어 조사 예정     - 유사 아이디어가 있다면, 그 아이디어의 한계는 무엇인가?     - 아이디어의 한계를 우리의 수준에서 더 발전시킬 수 있는가?     - 첨언) 논문 등에서 한계를 밝히는 부분에서 아이디어를 얻을 수 있음   + **아이디어의 강/장점 및 기대효과**     - 새로운 공격 시나리오 제안을 통해 비대면 업무 환경에 대한 보안적 경각심 촉구     - 개인정보 대상 공격의 방어 기법까지 고안함으로써 개인정보보안 분야에 기여     - 공격 수행을 위한 새로운 IoT웨어 개발을 통한 사이버 보안 기술 분야에 기여   + **To-Do List**     - 유사 아이디어 조사     - 어떠한 툴을 개발할 것인가 논의 및 결정     - 상세한 공격 시나리오 작성     - 교수님들과 상담 진행 후 인사이트 얻기 * **주제에 관한 의견**   + ‘보안 위협 모델 제안’이라는 주제로 프로젝트하는 것이 흥미로울 것 같다.(해보고 싶은 주제였다!!)   + 시의 적절하며 ZOOM 등의 화상회의 플랫폼에 대한 취약점이 보고된 사례가 적지 않아 충분히 해볼만한 주제인 것 같다.   + 무엇보다 아이디어 구체화가 중요하다.   + 우리 수준에서 할 수 있는 것인지 ‘실현 가능성’을 잘 따져봐야 한다.   + 통계청 및 공공데이터를 사용할 수 있는 아이디어면 좋다.   + 소규모 집단보다는 대규모 집단들을 대상으로 하는 프로젝트가 좋다.   + 보안뉴스와 논문을 매일 보면서 지속적으로 인사이트를 얻는 것이 중요하다.   + **결론)“MePreat:비대면 업무환경에서의 보안 위협 모델”로 주제 변경** | | |
| **향후계획** | * **회의 준비(멤버별)**   + (별하)팀 로고 투명버전 제작 * **다음 주 회의 안건**   + 우선순위 정하기   + 아이디어 구체화 | | |
| **참고문헌** | . | | |

**회 의 록(3회차)**

|  |  |  |  |
| --- | --- | --- | --- |
| **회차** | 3회차 | **일시** | 2024.03.27 (수) |
| **참석자** | 한아림, 한별하, 손효림, 이경화 | **장소** | 50주년기념관 625호 |
| **제목** | (손종모 교수님 면담)“개인정보 라이프사이클 트래커” 주제에 관한 조언 | | |
| **회의내용** | * **면담 질문리스트**   + 저희의 아이디어에 대해서 어떻게 생각하시는지?   + 법적으로 우려되는 부분이 있으신지?   + 기술적으로 우려되는 부분이 있으신지?   + 아이디어의 구현 가능성(= 현실성)에 대해 어떻게 생각하시는지?   + 논문, 특허, 우수 프로젝트 수상 등의 성과 창출을 목표로 하기에 적절한 아이디어라고 보시는지?   + 유사 아이디어를 아시는 바가 있는지?   + 아이디어의 효용 측면에서는 어떻게 보시는지?   + 아이디어의 발전 방향성 및 추구미를 제시해주신다면?   + 더 말씀하고 싶으신 부분 & 짚고 싶으신 부분이 있으시다면?   + 아이디어의 장/강점이 무엇이라고 생각하시는지?   + 아이디어의 단점/한계는 무엇이라고 생각하시는지?   + 개인정보 보호와 관련해서 요즘 가장 중요하게 다루어지는 부분이 있다면?   + 소모임에서 수집하는 개인정보도 범죄의 표적이 될 수 있을까요? 이것을 보호하는 것이 경제성이 있는 프로젝트일지?   + 개인정보 관리에 있어서 개인정보 제공자의 역할이 관리자의 역할에 비해 거의 안 다루어지고 있는 것 같은데, 그런 이유가 있는지?   + 저희가 개인정보 라이프사이클 관련 스터디를 진행하고자 하는데, 추천해주시는 학습법이 있는지? * **답변 내용**  1. **저희의 아이디어에 대해서 어떻게 생각하시는지?**  * 취지 괜찮다. 특히 정보제공자 입장에서 괜찮은 아이디어이다. 구제척으로 정보와 어떤 상태로 수집, 저장, 파기 되어있는지 보여주는 형태로 접근 가능. 심플하게는 사용자가 가입한 웹, 앱 등에 일정기간 미사용시 알림 앱도 할 수 있다. * 시간, 재력 등 제한 사항이 있으므로 1차 목표, 2차 목표 선정이 중요하다.  1. **논문, 특허, 우수 프로젝트 수상 등의 성과 창출을 목표로 하기에 적절한 아이디어라고 보시는지?**  * 눈문주제로 삼기에는 범위가 명확하지 않다. 그저 개인정보 현황 파악으로는 실용성이 없으며 기존 앱과 차별성 등을 수치화하여 나타낼 수 있는 데이터가 있어야 의미가 있다. * 그렇기에 비교할 대상이 있는 것이 좋으며 해당 아이디어는 기술적으로 특별한게 없으니 다른 의미부여가 필요하다. * 만약 대상이 명확하다면 법적인 측면에서 미흡한 보안서, 현재 시행되고있는 서비스가 편의성은 좋으나 기타 다른 문제점은 없는지 등 제안 가능하다. * 기타 명확한 구상도의 필요성있음. * 또한 오내피플 타겟층이 우리와 비슷하니 참고하면 도움이 될거다.  1. **아이디어의 장/강점이 무엇이라고 생각하시는지?**  * 장점은 정보주체로서 보자면 내 정보가 어떻게 처리되고있는지 볼 수 잇다. 관리자적인 측면에서는 소규모라면 수집하는데 관심이 있는거지 그 다음 관리는 고민을 안 한다. 이걸 모니터링할 수 있다. 어떻게 앱을 만드는지에 따라 구체적인 장점이 달라지겠지만 파기를 예시로 하면 자동파기, 알림이 장점이 될 수 도 있다.  1. **개인정보 관리에 있어서 개인정보 제공자의 역할이 관리자의 역할에 비해 거의 안 다루어지고 있는 것 같은데, 그런 이유가 있는지?**  * 법에서 요구하지 않으며 비용적 문제도 있지만 제공자에게 데이터 접근권한을 주면 보안상 문제가 벌어질 수 있으며 관리가 어렵기에 안다뤄지고 있다. * 여담으로 마이데이터 사업 대상이 일반 기업까지 넓어질 수 있다. 그렇기에 여기서 관련 사업이 생길 수 있다. 그리고 전송요구법이 생겼으나 아직 데이터 처리기관이 없어 시행되고 있지 않다. 이는 2년내로 설립될 예정이다. * **그런 경우 마이데이터 풀이 중앙에 저장되는 형태인가요?** * 맞다! * 또한 범위를 확좁혀서 개인 신용정보로 주제를 삼아도 괜찮을 것 같다. * 일정을 빨리 잡을 수록 좋지만 아이디어를 구체화하고 다듬는 과정이 필요한거니 정확한 일정 정하는게 필요하다. * 개인정보라이프사이클은 법도 있고 정보제공자 측면에도 필요하나 어떤 관리를 할지, 서비스를 제공할지 포인트 잡는 게 필요하다.  1. **api 적용을 하나만 해도 의미가 있나요?**  * 하나를 했다는 것은 다른 것도 할 수 있다는 의미이므로 충분히 의미가 있다.  1. **저희가 개인정보 라이프사이클 관련 스터디를 진행하고자 하는데, 추천해주시는 학습법이 있는지?**  * 관련 자료 메일 발송 예정 효림에게 전달 예정 | | |
| **향후계획** | * **회의 준비(멤버별)**   + (전체)활용 가능한 API 조사   + (전체)서비스 구체화 * **다음 주 회의 안건**   + 프로젝트 주제 변경 여부 판단 | | |
| **참고문헌** | 손종모 교수님께 받은 개인정보 관련 스터디 자료 | | |

**회 의 록(2회차)**

|  |  |  |  |
| --- | --- | --- | --- |
| **회차** | 2회차 | **일시** | 2024.03.25 (월) |
| **참석자** | 한아림, 한별하, 손효림, 이경화 | **장소** | 온라인 |
| **제목** | 팀로고 확정, 유사 프로젝트 조사, 주제관련 연구자료조사 | | |
| **회의내용** | * **팀로고 선정**   + 팀로고 후보(순서대로 1,2,3,4)   **로고1.png로고2.png로고3.png로고4.png**   * + 선정 결과: 4로 확정 * **유사 프로젝트 조사**   + (효림)**데이티스바넷 – DataGenor PDS**     - 개인정보를 기준으로 엔터프라이즈 환경의 많은 정보들의 파기와 분리보관을 처리하기 위한 라이프사이클 관리 솔루션     - **강점**       * 개인(신용)정보 파이/분리보관의 어려움 해결       * 개인정보 파기/분리보관 자동화 솔루션       * 개인정보 compliance 준수와 ROI의 개선     - **우리 프로젝트와의 차이점**       * 기업용 개인정보 자동화 관리 데이터베이스 시스템이라는 점       * 개인정보가 라이프사이클대로 관리되고 있는지 모니터링하지는 않는다는 점   + (효림)**주식회사 오내피플 – 캐치시큐**     - 기업을 위한 컨설팅, 개인정보보호 규제 준수 자동화 솔루션     - **강점**       * 1000개 이상의 고객사 보유       * 2023 우수 정보보호 기술 선정       * 개인정보 수집 시에 AI가 개인정보 유형을 분류해서 맞춤형 동의서 만들어 제공       * 개인정보 관리자, 매니저, 외부 열람자 계정 만들어 처리 내역 관리       * 개인정보 분류해 광고 전송       * 정보 암호화, 마스킹, 워터마크 삽입       * 캐치폼 안에 보관되던 개인정보 파기일에 알아서 파기       * 본인 인증과 전사 서명       * 이메일로 정보 수집 알림 받기 가능     - **약점 및 우리 프로젝트와의 차이점**       * 타깃이 기업이라 우리 프로젝트와 공략층이 다른 점       * 개인정보 파기일 전에 알림 기능이 없는 점이 불편할 수 있음       * AI자동화에 대한 신뢰성 문제       * 라이프사이클에서 이용 및 제공 단계에 대한 기능이 약해보임   + (효림)**㈜이지서티 – 개인정보 오남용 상시모니터링 UBI SAFER-PSM Master**     - 개인정보취급자가 개인정보처리시스템에 접속해 업무를 수행하는 개인정보취급자의 계정, 접속일지, 접속지 정보, 처리한 정보주체 정보, 수행 업무 등의 전자기록을 생성하고 관리하는 솔루션     - **강점**       * Agent, Manager, Master 등 모듈별 GS인증 1등급을 획득       * 조달청에서 우수조달제품으로 지정돼 제품의 우수성을 인정받음       * 개인정보 오/남용 및 노출사고, 실시간 모니터링 가능       * 취약점 개선방안 제시 가능       * 개인정보 입출력 자료 관리 대장 자동화       * 통계 및 보고 기능       * 개인정보보호 수준 자가진단 서비스 기능       * 접속기록 수집/보관 및 위/변조 방지 기능     - **약점**       * 홈페이지 UI가 좋지 않음       * 개인정보 제공자의 관점이 고려되지 않음       * 서비스에 대한 가이드가 부족함   + (효림) **오피스키퍼 – 오피스키퍼**     - 통합 PC 보안 정보 유출 방지 솔루션 오피스키퍼의 기능 중 하나     - **강점**       * 서비스 소개가 부족하여 파악이 어려움       * 개인정보 실시간/예약 검사, 파일 암복호화/반출 제어     - **약점 및 우리 프로젝트와의 차이점**       * 기업 관리자 입장만 있고 개인정보 제공자 관점이 고려되지 않음       * 개인정보 라이프사이클에 따른 트래킹이 메인인 솔루션이 아니라는 점에서 우리의 프로젝트와 차이가 있음       * 관리자가 개인정보를 안전하게 보관하는데 모든 초점이 맞춰진 점에서 관리자의 개인정보 관리와 제공자의 모니터링에 초점을 둔 우리 프로젝트와 차이가 있음   + (경화)**엑소스피어 랩스-올인원 PC보안 상품 중 개인정보보호(DPL) 기능**     - 사내 PC에 보관된 개인정보를 탐지해서 암호화하여 보관하게 하는 프로그램으로, 사내 개인정보 보유현황과 처리자를 쉽게 파악할 수 있게 도와줌     - **강점**       * 개인정보 식별 기준 커스터마이징 가능       * 개인정보보호 전문가가 아니어도 사용 가능     - **약점**       * 올인원 상품으로만 이용 가능(단일 상품으로 제공되지 않음)   + (경화)**지란지교 데이터-개인정보보호 기술**     - 엔드포인트에 저장된 개인정보 탐지하고 암호화 및 완전삭제, 다양한 파일에서 개인정보 진단, 파일 공유, 외부 전송 시 개인정보 필터링, 출력물에서도 워터마크로 개인정보 가려줌     - **강점**       * 병렬 비식별 엔진과 빅데이터 기반의 In-Memory 처리기술을 적용하여 빠르게 비식별 처리       * 데이터 생명주기에 따른 이력 관리가 가능하여 투명하고 안전한 데이터 확보 가능       * 관리자 화면에서 대시보드를 제공하여 개인정보 관리 현황을 한 눈에 확인할 수 있음     - **약점**       * 소모임에서 쓰기에 불필요한 기능이 많음   + (경화)**IBM-IBM** **OpenPages Data Privacy Management**     - 개인정보 자산 실시간 모니터링. 각 개인정보 파일에 대한 메타데이터 제공. 보고서 작성     - **강점**       * 개인정보 관리를 통합적으로 관리할 수 있음       * 결산 보고서 작성 비용 절감     - **약점**       * 동아리 같은 소모임에서 사용하기에는 기능이 너무 많고 어려움   + (경화)**개인정보보호위원회-개인정보 종합지원시스템**     - 공공기관이 보유하고 있는 개인정보 파일 관리 목적. 개인정보보호 관련 업무 현황 파악. 개인정보보호 업무 프로세스 온라인화     - **강점**       * 국가기관에서 운영하는 것이므로 안정적이고 신뢰할 수 있음       * 무료 서비스     - **약점**       * 공공기관만 사용 가능   + (별하) **X-Log사의 X-LOG for ILM**     - DB를 이용한 데이터 수명주기 관리 시스템.데이터 생성과 저장, 소명까지 전체 프로세스를 효율적으로 관리하는 솔루션, 데이터 수명 주기에 따라 보관방식을 달리함 → 운영비 절감, 운영서버 성능 개선 X-LOG for CDC는 실시간 정보확인이 가능한데 이것도 가능한지는 모르겠음 (정보부족으로 정확한 기능은 파악할 수 없음)     - **강점**       * 데이터 수명 주기에 따라 보관방식을 달리해 운영비 절감, 성능개선     - **약점**       * 서버와 대상서버의 중간관리자 시스템이니 일종의 백도어 역할이 가능할 수도 있음       * 데이터 이관이 쉽다.       * 자동 이관도 가능하다.     - **목표 분석**       * 불필요하거나 관리 감시용 데이터를 운영서버에서 이관 혹은 제거하여 성능 향상       * 개인정보 법에 따른 관리가 주 목표보다는 외장하드와 같은 역할을 하는 듯   + (별하)**SAHI-SAHI ONE**     - SAHI의 채용 라이프사이클 관리를 위한 앱.     - **강점**       * 채용된 모든 사람들의 직무, 나이 등 기타 정보를 한 눈에 볼 수 있음 (게임 캐릭터 프로필 같은 느낌!)     - **약점**       * 프로필처럼 잘 정리되어있으나 개인정보를 앱 안에 저장하고 있어 보안상 위험할 수 있음 (정보 부족으로 정확한 장단점 파악어려움)     - **목표 분석**       * 채용 담당자가 채용관련 업무를 더 수월하게 할 수 있게 도와줌   + (별하)**Spiceware- 클라우드 내 개인정보 라이프사이클 관리 프로그램**     - AI를 이용해 분산된 클라우드와 시스템에서 자동으로 개인정보를 찾음 → 데이터 암호화 → 접속기록 관리 → 개인정보 이용내역 알림, 파기     - **강점**       * 클라우드와 시스템에서 자동으로 개인정보를 찾아줌.       * 클라우드 형태로 서비스를 제공하기에 설치가 간편.       * 개인정보 파기 규정에 맞게 이용내역 고객에게 알림, 자동 파기       * 유명한 기업들을 고객사로 두고 있음     - **약점**       * 개인정보를 추출하여 클라우드에 저장 → 보안상 취약할 수 있다.       * AI를 통해 자동으로 개인정보를 추출하기에 편리하지만 미처 추출하지못한 데이터가 남아있을 수 있음     - **목표 분석**       * 기업을 대상으로 개인정보 법을 준수하여 개인정보 관리를 수월하게 도와준다.   + (별하)**피앤피시큐어-인포세이퍼 V5.0**     - DB에 직접 접속시 DB서버 로그정보 분석, 모니터링, 파일 다운로드 탐지, 개인정보 데이터 유형에 대한 분석 기능 제공       1. DB스캐너를 통해 개인정보, 민감정보 추출       2. 접속기록 생성 → 암호화       3. 이상행위 탐지 (탐지 규칙 생성가능)       4. 소명처리 (이상징후 발견시 자동으로 위험 사용자에게 이메일 소명 요청, 요청받은 사용자는 업무, 사용시간, 개인정보 유형 등 확인가능)     - **강점**       * 개인정보 라이프 사이클에 따른 관리 설비가 잘되어있다.       * DB내 개인정보 생성, 파기 등 변화 감지, 주기적인 관리 감독에 용이       * 모든 경로의 접속기록 로깅 수행       * 다양한 데이터를 조합해 사용 환경에 맞는 개인 정보 위협 행위 자동 정의       * 위협 행위 발생 시 알림 기능       * 이상 징후 발생시 위험 사용자에게 이메일보냄       * 감사로그 통합 후 보고서로 재가공 지원     - **약점**       * 개인정보를 추출하여 DB에 저장 → 보안상 취약할 수 있다.       * 이상징후 발견시 바로 이메일로 내용이 보내지지만 취침시간 등 기타 사용자가 즉각 대응이 어려운 상황에는 큰 효용성이 없음       * DB스캐너를 통해 자동으로 개인정보를 추출하기에 편리하지만 미처 추출하지못한 데이터가 남아있을 수 있음     - **목표 분석**       * 기업에게 유출 사고 방지와 유출사고 발생 시 법정에서 유리한 증거를 남김   + (아림)**개인정보 포털-개인정보 기술지원 서비스**     - 개인정보의 안전성 확보에 필요한 기술적·관리적 및 물리적 조치에 어려움을 겪는 중소기업·소상공인을 대상으로 개인정보보호 기술상담 및 온라인 컨설팅, 현장방문 컨설팅 등을 지원     - **강점**       * 온/오프라인 상담 및 컨설팅까지 제공       * 국가 관련 기관에서 운영하는 서비스이다보니 체계가 있음. 우리도 어느 정도 체계성을 갖출 필요가 있어 보임.     - **약점**       * 문제가 생겼을 때 or 초기에 관리 어떻게 해야할 지 모를 때만 효용이 있음. 우리 아이디어처럼 어느 단계에서 어떻게 정보가 처리되고 있는지를 보지는 X       * 핸드폰에서 사용 못함, only PC       * 신청 및 이용 절차가 복잡함     - **기타**       * **서비스 이용 대상**: 소상공인 & 벤처기업 등 소기업(= 우리랑 타깃은 비슷)       * **특이사항:** 본인의 정보 관리에 대한 자가진단 서비스가 있음       * **출처:** 개인정보 포털   (<https://www.privacy.go.kr/front/per/tec/tecSupportReq.do>)  --> KISA 위탁운영 포털으로 신빙성 있음   * + (아림) **Google Android-개인정보 대시보드**     - 개인 정보 대시보드에서 데이터에 액세스하고 있는 앱, 앱에서 사용하는 권한, 해당 액세스가 발생한 시점을 확인하게 해주는 서비스     - **강점**       * App 형식이 아니어도 핸드폰에서 사용 가능한 서비스임       * 실시간으로 본인의 폰을 통해 앱별로 권한 변경 가능       * 사용 절차가 매우 단순하고 직관적     - **약점**       * 핸드폰 기종 & 사용하는 OS에 따른 서비스 이용 제약이 있음 (우리는 제약이 없는 앱이라는 것을 강조하면 좋을 듯)       * 데이터 저장 기한이 최대 7일으로 매우 짧음     - **기타**       * **서비스 대상**: 안드로이드 OS 휴대폰 사용자 전체       * **출처**: Google Android 고객센터   <https://support.google.com/android/answer/13530434?hl=ko>   * + (아림)**TOVEDATA-Privacy DAM**     - 개인정보 데이터의 접근을 제어하기 위한 관제 솔루션으로, 개인정보가 담겨있는 데이터베이스에 대한 접속을 등록/관리하고, 데이터 반출시에는 비식별화 처리를 통해 개인정보 활용의 안전성을 높여줌     - **강점**       * 거의 대부분의 작업이 실시간으로 이루어짐       * 제공하는 기능이 매우 다양함(가명처리 & API 통한 관리 등)     - **약점**       * 정보 공개가 너무 안되어있다는 것을 제외하면 없음     - **기타**       * **서비스 대상:** 중견 이상의 기업체를 대상으로 함       * **출처:**   <https://www.tovdata.com/>  <https://www.tovdata.com/privacydam>   * + - * **특이사항**         + 정보가 어느 단계까지 처리되었는지를 알리기보다는, 그냥 데이터 자체를 숨기려는 느낌         + API 생성 이력을 보고서 형태로 제공해줌. (우리는 이런 기능 굳이 필요 없을 듯)         + 기업이 2020년에 설립됨. 진짜 신생기업(카이스트 졸업생이 만든 듯)         + 기술적으로 DB 자체에 접근하기도 하는 중간자라고 하나 사전적인 중간자의 의미는 아닌 듯   + (아림)**TOVEDATA-Plip**     - 개인정보 라이프사이클에 필요한 문서 관리 도구     - **강점**       * AI 써서 거의 대부분 자동화, 특히 문서 자동생성이 서비스 강점인듯       * 제공하는 기능이 많음     - **약점**       * 이 서비스도 정보 제공자가 어느 단계까지 갔음을 실시간으로 확인하지는 못함     - **기타**       * **서비스 대상**: 기업의 개인정보담당자 (로그인 시 회사등록 필요)       * **출처**: 토브데이터 상품소개 페이지   <https://support.plip.kr/>  <https://www.plip.kr/>   * + - * **특이사항**         + 서비스가 제공하는 기능 중 ‘파기 관리대장’이 우리 아이디어와 가장 유사         + [파기 관리대장](https://support.plip.kr/6dda04f5-48e4-4a0e-8f66-1301894b8a94)         + 유일한 한계점은 개인정보 관리 담당자용 버전만 있다는 것         + 무료와 유료 서비스 모두 있음. 유료는 가격대 있음(80만원에서 180만원)         + 법무법인 디라이트와 파트너 관계 * **주제관련 연구조사**   + (효림)**개인정보 라이프사이클에 따른 프라이버시 보호 프레임워크**     - 정보위험사회의 도래로 사용자의 상황에 맞게 적응적, 적시적으로 개인정보보호 서비스 제공이 가능한 프레임워크 개발이 요구됨     - 기존 WASP 아키텍쳐와 IBM의 TPM 문제점 지적     - 라이프사이클 단계별로 침해 문제와 요구사항 정리     - 요구사항과 대책을 바탕으로 프라이버시 보호 모듈 구성     - 프라이버시 보호 프레임워크 모델 구성 (기존 WASP에서 고려하지 않았던 인증 모듈 추가, 시간이 지나면 폐기 + 시스템 정책과 별도로 정보 접근에 대한 정책 변경 가능 + 기밀성 유지하는 데이터 관리 모듈 + TPM 장점인 개인정보 실시간 모니터링 기능 가져옴)   + (효림)**개인정보의 법적, 기술적 특성을 고려한 라이프사이클 모델**     - 개인정보 라이프 사이클 모델 검토     - 국내 IT 기업에 적합한 개인정보 동의, 관리 기반 모델 제안 (기존 모델이 간과하고 있던 동의, 관리 요소 반영)     - 개인정보 활용 현황을 분석 및 보호 체계 마련에 기여 목적     - 4개의 라이프 사이클 모델을 비교, 분석한 후 개인정보 동의, 관리 기반 모델 제안 및 타당성 검증   + (효림)**개인정보 라이프사이클에 따른 개인정보보호 관리 실태 및 개선방안에 대한 연구: 장애인복지시설을 중심으로**     - 장애인 복지 시설의 개인정보 관리 현황 실태조사를 바탕으로 문제 및 개선방안을 제시하여 어플리케이션 개발   + (효림)**가명정보 생명주기에 따른 개인정보보호 중심 설계 적용 원칙에 관한 연구**     - 개인정보보호 중심 설계(Privacy by Design) 원칙을 기반으로 가명정보 생명주기에 적용할 수 있는 새로운 PbD 원칙을 제안     - 각국의 PbD 관련 법제도를 분석함     - 가명정보처리 가이드라인과 국제 표준 비식별 조치 생명주기 고려사항 비교     - 역시 우리의 선행 연구라기에는 생명주기 비중도 적고 연관도 떨어짐.   + (효림)**개인정보 생명주기에 따른 인공지능 개인정보보호**     - 인공지능 서비스를 개발하고 이용하는 과정의 데이터 활용에서 개인 식별 가능성이 높아지며 개인정보 침해가 우려되어, 개인정보 생명주기를 중심으로 인공지능에서 개인정보를 보호하기 위한 접근 방법을 제시     - 전체적으로 라이프사이클 5단계를 설명하는 글 같음   + (효림)**가명정보 Life-Cycle에 대한 위험 분석을 통한 관리적/기술적 보호조치 방안에 대한 연구**     - 위험 분석 및 관리 방안 제시   + (효림)**연구 데이터 관리를 위한 데이터 라이프 사이클 제안**     - 연구 데이터 관리에 대한 연구     - DCC, ICPSR, IWGDD, DataONE, USGS, UK Data Archive 등 해외 6개 기관의 데이터 라이프 사이클을 분석     - 공통적으로 도출된 구성 요소 ‘계획’, ‘생성 및 수집’, ‘프로세스’, ‘보존’, ‘이관 및 폐기’, ‘접근 및 이용’, ‘기술’, ‘보장’ 그리고 ‘백업 및 보안’ 등 9개 비교 분석     - 연구 데이터를 관리하기 위한 데이터 라이프 사이클을 제안   + (효림)**자동처리되는 개인정보 보호 가이드라인**   + (효림)**라이프로그 시스템(Life log system)의 개인정보 생명주기(Life cycle) 단계별 프라이버시 노출에 대한 위험성**   + (경화)**DLP(데이터 손실 방지) 솔루션**     - 중요한 데이터의 안전하지 않거나 부적절한 공유, 전송 또는 사용을 식별하고 방지하는 보안 솔루션   + (별하)**디지털 헬스케어 서비스의 데이터 컴플라이언스 방안에 관한 연구 - 개인정보 라이프사이클을 중심으로**     - 헬스케어 서비스 상에서 개인정보 포함 데이터 활용시 목적 분류 기준 여섯가지와 개인정보 보호법을 준수하기 위해 고려해야 하는 사항들을 라이프사이클 4단계에 따라 알아봄.     - 기업이 당초 수집한 목적 외에 개인정보를 사용하는 것은 금지되어있으나 사용자에게 적법한 동의를 받았다면 사용가능.     - 동아리 관리자를 대상으로 하는 탭에 주의사항, 권고사항 등을 삽입할 때 참고하면 좋을 듯   + (별하)**IoT 디바이스에서 GDPR에 부합하는 개인정보 관리 절차 설계**     - 생명 주기 단계별로 개인정보의 관리 절차 제안     - 암호화 방법에 대한 설명이 자세하여 암호화 알고리즘을 짜야할 일이 있을 때 참고하기 좋을 듯 * **기타 의견/아이디어**   + (효림)특허청에서 개인정보 라이프사이클, 개인정보 생명주기, 개인정보 LifeCycle이 제목에 포함된 검색 결과는 찾지 못함.   + (경화)DLP 솔루션에 대해 알아보고 프로젝트에 참고하면 좋을 것 같음.   + (아림)우리는 정보 제공자의 '실시간 조명 및 처리'에 강세를 두면 좋을 것 같음.   + (아림)데이터 저장 가능 기간이 길어야 함   + (아림)사용 절차가 복잡하지 않아야 함   + (아림)'개인정보 라이프사이클' 개념이 상상 이상으로 복잡함. 우리 아이디어의 핵심이니만큼 별도 스터디 진행하는게 어떨까?   + (아림)우리도 Google 처럼 앱 사용 가이드 만들면 좋을 듯   + (아림)불필요한 기능은 빼고 꼭 필요한 기능만 탑재하는 것도 하나의 강점이 될 수 있을 듯 -> 앱 가볍고 간단하게!   + (별하)토스 개인정보 담당자 선배님의 꿀팁: 개인정보보호법 해설서와 가이드부터 학습 시작하면 좋음!   + 기존에 명시된 목적을 벗어난 사용의 경우 제공자에게 별도 통지하는 기능이 있으면 좋을 듯 | | |
| **향후계획** | * **회의 준비(멤버별)**   + (별하, 효림)개인정보 전공 교수님께 상담 요청   + (전체)개발할 앱에 대한 아이디어 가져오기 * **다음 주 회의 안건**   + 프로젝트 주제 관련 아이디어 구체화 | | |
| **참고문헌** | 송유진, 이동혁. (2006). 개인정보 라이프사이클에 따른 프라이버시 보호 프레임워크. 정보보호학회지, 16(4), 77-86.  장재영, 박태환, 김범수. (2012). 개인정보의 법적·기술적 특성을 고려한 라이프 사이클(Life Cycle) 모델. 한국전자거래학회지, 17(3), 43-60.  장진원. (2014). 개인정보 라이프사이클에 따른 개인정보보호 관리 실태 및 개선방안에 대한 연구: 장애인복지시설을 중심으로. 동국대학교 대학원.  김동현. (2022). 가명정보 생명주기에 따른 개인정보보호 중심 설계 적용 원칙에 관한 연구. 정보보호학회논문지, 32(2), 329-339.  이아람. (2022). 개인정보 생명주기(Lifecycle)에 따른 인공지능(AI) 개인정보보호. 한국통신학회지(정보와통신), 39(12), 3-7.  차건상. “가명정보 Life-Cycle에 대한 위험 분석을 통한 관리적/기술적 보호조치 방안에 대한 연구.” 한국융합보안학회 융합보안논문지 제20권 제5호 (2020.12).  김주섭, 김선태 and 전예린. (2019). 연구 데이터 관리를 위한 데이터 라이프 사이클 제안. 한국문헌정보학회지, 53(4), 309-340.  자동처리되는 개인정보 보호 가이드라인(2020.12월), 개인정보보호위원회, 한국인터넷진흥원.  임혁,and 김태성. "라이프로그 시스템(Life log system)의 개인정보 생명주기(Life cycle) 단계별 프라이버시 노출에 대한 위험성." 한국경영정보학회 학술대회논문집 2014.1 (2014): 900-905.  정재은,and 양진홍 (2022). 디지털 헬스케어 서비스의 데이터 컴플라이언스 방안에 관한 연구 - 개인정보 라이프사이클을 중심으로. 한국정보전자통신기술학회 논문지, 제15권 제2호 (2022.04): 134-132(10page).  이용, 김화종, 이구연. (2020). IoT 디바이스에서 GDPR에 부합하는 개인정보 관리 절차 설계. 대한전자공학회, 전자공학회논문지 제57권 제10호(통권 제515호) (2020.10): 3-14(12page) | | |

**회 의 록(1회차)**

|  |  |  |  |
| --- | --- | --- | --- |
| **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> | | |