2023/02/08

2022 개인정보보호 소학회

: SWUPI

2020110836 김수린 2020111646 이지은
2021111341 안현서 2022111354 한아림

개인정보보호 소학회 활동 발표

팀원 및 팀명 소개

01

팀원

2020110836 김수린

2020111646 이지은

2021111341 안현서

2022111354 한아림

팀명

SWUPI

: SWU(서울여대) + PERSONAL IMFORMATION(PI)

02

주별 계획 및 스터디 방식

진행 방식: 비대면 zoom + 대면(누리관)

1주-3주) 개인정보 위험대응 공모전 참여

- 1주 1,2회 : 개인정보보호법, 다크웹 및 딥웹 개념 조사
- 2주 1,2회 : 아이디어 도출
- 3주 1회 : 아이디어 마무리 및 제출

3주-5주) 개인정보보호에 대한 법적 및 기술적 관점에서의 접근

- 3주 2회 : 개인정보보호 논문 읽기 및 토론
- 4주 1,2회 : 논문을 활용한 개인정보 취약 기술 분석 및 조사
- 5주 1,2회 : 활동 마무리

2022 개인정보 위험대응 공모전 참여

03

다크웹 스캐너와 PDS를 이용한 개인정보 유출 탐지 및 통보

AI를 접목한 OCR(광학문자인식) 등 비정형 데이터 추적 기술과 웹 브라우저 렌더링을 활용한 컨테이너 기반 다크웹 스캐너를 융합해 정보 유출 여부 및 상황을 모니터링하고, 스캔된 유출 개인정보를 PDS 개인 데이터 저장소와 비교•대조하여 국가가 유출 당사자에게 통보한다. 유출 여부를 파악한 뒤에 암호화폐 추적 기술을 이용해 유출된 개인정보가 거래되었는지 확인하고 범죄자를 추적할 수 있도록 한다.

특강 참여

04

<개인정보보호 소학회 활동지 1 >

팀명	SWUPI	일시	2022 . 10 . 27
장소	50주년기념관 B106 소공연장	참석 인원	1 명
강사	제이앤시큐리티 김경하대표	주제	개인정보 침해사고 사례를 통해 본 개인정보 안전조치의 이해
특강 내용	본 특강에서는 개인정보 유출 유형과 주요 개인정보 침해사고 사례, 개인정보 안전조치 방안, 개인정보보호 프레임워크 등의 내용을 다뤘다. 특히 개인정보 침해사고에 대해서 자세히 다뤘는데 대표적인 개인정보보호 유출 사고들의 해킹 방법, 사고원인, 대응 방안에 대해 알 수 있었다. 옥션, sk 컴즈, KT, 인터파크, 카드 3사, 삼성플라우드 등의 주요 개인정보 유출 사고들을 통해 웹 해킹, APT 공격, 시스템 해킹, 크리덴셜 스터핑 공격 등 다양한 해킹 방식과 사고원인, 그에 따른 대응 방안으로 망 분리, 개발 보안 시큐어 코딩 및 정기적인 취약점 진단 조치, 영향분석 등을 통한 업무용 시스템상 비정상 행위 차단 기능 구현 등에 대해 배울 수 있었다. 또한 n번방 사건 관련 개인정보 유출 사고로 인한 공공분문 개인정보 유출 방지의 중요성과 대책, 개인정보 안전조치 관련 개인정보보호법 고시 등을 배울 수 있었다. 더 나아가 개인정보 보호 프레임워크로 1. 개인정보 Life Cycle 식별 관리 2. Compliance/Due Diligence 3. 보안대책(Risk Mgt./pbD) 4. 개인정보보호 관리체계(Plan-Do-Check-Act)에 대해 세부적으로 확인할 수 있었다. 마지막으로 개인정보보호를 위해서는 관련 법제도 및 표준, 관리 보안, 물리 융합 보안, 기술 보안, 개인정보보호 아키텍처 설계 구현, 관리체계 수립 운영, 거버넌스 구축 운영 등 많은 요소들에 대해 배워야 한다는 점을 알 수 있었다.		
추가적으로 스터디할 내용	개인정보보호 포털에서 지원하는 개인정보보호 온라인 강의 수강, 개인정보 조치 해설서 공부		

<개인정보보호 소학회 활동지 2 >

팀명	SWUPI	일시	2022 . 10 . 12
장소	50주년기념관 B102	참석 인원	2 명
강사	전진환(ph.D MIS)	주제	개인정보 침해사고 사례를 통해 본 개인정보 안전조치의 이해
특강 내용	**1. 개인정보의 이해** 1-1. 개인정보의 정의 - 우리나라 개인정보보호법 : PIPA (Personal Information Protection Act) - 각 필드가 모여 레코드 -> 레코드가 여러 개 모이면 데이터베이스 - 개인정보보호를 위해서 대상이 되는 목표가 누구인가: 특정 개인들의 정보를 데이터베이스에 넣어놓은 것을 보호해야 함 - 프라이버시는 개인정보 안에 중속된 것이므로 데이터베이스를 보호해야 함 - **개인정보**: 살아있는 개인에 관한 정보-'개인정보보호법 제2조(정의)' - **식별정보(개인정보 영역)**: 살아있는 개인에 관한 정보, 개인에 관한 정보, 개인을 알아볼 수 있는 정보, 쉽게 결합하여 알아볼 수 있는 정보, 정보의 내용, 형태 등은 제한 없음, 가명정보 - **비식별 정보(일반정보 영역)**: 익명정보 (아무리 복호화를 해도 알 수 없는 정보) -컨셉: 개인정보보호의 타겟이 주엇인지(특정 개인들의 정보를 DB안에 넣어둔 것을 보호해야 함) - 망자에 대한 정보는 보통 개인정보로 판단하지 않는다. => 사망자에 대한 법정 소송 때문에 발생하는 정보는 개인정보로 판단 - 식별성(식별정보)이 중요 1-2. 개인정보의 유형 - 일반정보 : 주민등록번호 - 정신적 정보 : 기호, 성향, 신념, 사상 - 통신-위치 정보 : 통화, IP 주소, GPS 좌표 등 - 신체적 정보 : 신체/의료/건강 정보 - 재산적 정보 : 개인금융/신용정보 - 사회적 정보 : 교육/근로/자격정보 - 비식별 처리 정보 : 가명정보 1-3. 개인정보의 법적 해석 -판례1. 이메일 주소는 개인정보에 해당할 수 있음 -판례2. 아이디, 비밀번호는 개인정보에 해당할 수 있음 -판례3. 휴대전화번호 뒷자리 4자리만으로도 개인정보에 해당할 수 있음 -판례4. 휴대전화의 IMEI(국제모바일기기 식별 코드)는 개인정보에 해당할 수 있음		

<개인정보보호 소학회 활동지 3 >

팀명	SWUPI	일시	2022 . 10 . 13
장소	50주년기념관 B106	참석 인원	2 명
강사	오내피플 조아영 대표님	주제	일상 속 개인정보보호
특강 내용	개인 정보의 정의와 정보 주체의 권리에 대한 설명으로 특강이 시작되었다. 이름이나 전화번호, 주민등록번호 등 이미 많은 사람들이 개인정보로 인식하고 있는 요소들은 물론, 휴대전화의 뒷자리 번호, SNS의 사진과 글 등 미처 개인정보라고 생각하지 못한 요소들도 포괄적으로 다루어주셨다. 또 개인정보보호법의 내용을 살펴보며 정보주체의 정의, 개인정보의 범위와 명확한 정의를 알 수 있었다. 더 나아가 정보주체의 권리에 대한 내용까지 접할 수 있었는데, 개인정보의 처리에 관한 동의 여부나 동의 범위 선택 등 이미 알고 있던 권리뿐만 아니라 다소 생소했던 개인정보의 처리에 관한 정보를 제공받을 권리 및 개인정보 처리 정지 권리까지 알아볼 수 있었다. 앞서 언급하셨던 정보보호와 관련하여 개인정보보호의 실제 사례와 개인정보보호 성공 사례를 설명해주셨는데, 많은 사례들을 접하며 개인정보보호에 대한 이해도를 높일 수 있었다. 마지막으로 회사나 국가 등 타인이나 타 기관에 의해 관리되는 정보보호 내용뿐만 아니라 내 스스로 관리해야 하는 개인정보의 중요성에 대해서도 배울 수 있었다. 내가 공개한 글이나 영상, 사진 등의 요소가 어떻게 내 개인정보를 침해할 수 있는지 사례를 접하며 경각심을 기를 수 있었다.		
추가적으로 스터디할 내용	개인정보 보호와 관련해서 개인정보를 탈취할 수 있는 기술들에 관한 스터디나, 그 기술을 구현할 수 있게 만드는 해킹 기법 등을 공부해보고 싶다. 개인적인 의견으로는 웹 본야, 시스템 본야를 가리지 않고 통합적으로 진행한다면 스터디의 완성도가 높아질 것 같다. 또 기존에 널리 알려진 기술이 아닌 아직 잘 알려지지 않은 기술들을 위주로 공부해보는 것도 괜찮을 것 같다. 더 나아가 스터디에서 다루었던 기술들이나 기법들을 팀원들끼리 적절히 융합하여 새로운 공격 가능성을 탐지해보는 것도 흥미로운 스터디 주제가 될 수 있을 것 같다.		

<개인정보보호 소학회 활동지 4 >

팀명	SWUPI	일시	2022 . 11 . 02
장소	50주년기념관 B106 소공연장	참석 인원	3 명
강사	SK쉴더스 성경원 그룹장	주제	개인정보 주요 동향 및 향후 고려사항
특강 내용	본 특강은 개인정보 주요 동향 및 향후 고려사항에 관한 내용이었다. 개인정보보호 동인, 개인정보보호 관련 주요 화두, 개인정보보호 핵심 영역 및 해결방향 등에 대해 다루었다. 확진자 동선 공개, 비대면 문화 확산 등 코로나 관련 개인정보보호 이슈와 n번방 사건, 공무원 개인정보 오남용, 다크웹 등 다양한 사회적 이슈들, 구글 및 메타 행태정보 처리 관련 제재, 법무부 안면인식 AI 시스템 사례 등 최근 개인정보보호 관련 이슈 및 사고가 증가한 원인들에 대한 다양한 사례들을 알 수 있었다. 또한 22년 상반기 개인정보 유출 사고 및 제재 현황과 개인정보 유출 주요 위반 사례 등 최신 동향 또한 알 수 있었다. 2022 개인정보보호 7대 이슈 전망으로 마이데이터, 가명정보 활용 확산, 개인영상정보보호, 과징금 기준 합리화, 온라인 플랫폼 이용 확대와 개인정보보호 등 최신 트렌드에 대해 자세히 다루었다. 또한 개인정보보호 핵심 영역 및 해결 방향에 대해서도 알 수 있었다. 개인정보보호 관리적, 기술적, 법적 현안 대응과 관리체계 고도화작업, 금융권 정보보호 상시 평가 등 체계 수립, 개인정보 life cycle 관리, 보호조치 구현, 개인정보 흐름분석 및 대책 수립 등 다양한 영역에서 앞으로 해결해 나가야 하는 부분들에 대해 짚어볼 수 있었다.		
추가적으로 스터디할 내용	법/제도 지식 공부(가이드라인, 해설서, GDPR 등 해외법령, 마이데이터, 가명정보 제도), 기술 지식 공부(개인정보보호 요소 기술, new ICT 기술)		

<개인정보보호 소학회 활동지 5 >

팀명	SWUPI	일시	2022 . 11 . 29
장소	50주년기념관 B106	참석 인원	1 명
강사	장은영	주제	개인정보의 시작과 끝
특강 내용	개인정보보호법에서 말하는 개인정보 : 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보 : 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보 : 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용 · 결합 없이는 특정 개인을 알아볼 수 없는 정보 개인정보 처리 시스템 : 서비스를 제공하기 위한 시스템, 주문 처리 관리 시스템, 배송 처리 관련 시스템, CS 시스템 등 개인정보보호 담당자가 하는 일: 개인정보보호 관련 정책/가이드 수립, 개인정보보호 교육, 인식 제고, 개인정보보호 관련 서비스, 시스템, 사업 등 검토, 개인정보 수집, 제공 등의서 작성/검토, 개인정보처리방침 작성/검토, 개인정보처리시스템 주기적 점검, 개인정보처리 위탁업체 주기적 점검 및 감독, 개인정보보호 관련 감사, 개인정보보호 관련 인증 획득, 개인정보보호 사고 대응, 개인정보보호 관련 보안 솔루션 정책 수립, 운영, 이외 개인정보와 관련된 모든 사항 개인정보보호 담당자 유형 1) 개인정보보호법 및 개인정보보호 관련 법률 이해 (법 전공자 및 변호사) 2) 서비스, 시스템 기획 (기획/개발) 3) 시스템, 클라우드 플랫폼 기술 가이드 및 설계(IT) 4) 개인정보보호 운영 (업무환경 보안, 보안솔루션 운영) 5) 개인정보보호 체계 관리 (정책, 보안인증) 6) 취약성 점검, 개발 가이드 (보안)		
추가적으로 스터디할 내용	개인정보 처리 시스템에 대해 자세히 알아보고 싶다. 또한 우리가 흔히 이용하는 쿠팡이라는 곳의 개인정보 처리라 하니 더욱 와닿았다.		

활동지

특강 내용

1-2. 개인정보의 유형
- 일반정보 : 주민등록번호
- 정신적 정보 : 기호, 성향, 신념, 사상
- 통신-위치 정보 : 통화, IP 주소, GPS 좌표 등
- 신체적 정보 : 신체/의료/건강 정보
- 재산적 정보 : 개인금융/신용정보
- 사회적 정보 : 교육/근로/자격정보
- 비식별 처리 정보 : 가명정보

1-3. 개인정보의 법적 해석
- 이메일 주소는 개인정보에 해당
- 아이디, 비밀번호는 개인정보에 해당
- 휴대전화 관련은 다 개인정보에 해당

1-4. 사생활 정보
- 민감 정보

1-5. 개인정보 보호의 보장
- 개인정보 자기결정권 : 국민의 기본권

1-6. 개인정보보호 관련 법률체계
- 본야 별 적용 기준 : 공공 본야, 민간 본야

2-2. 데이터3법 개정 주요 내용
- 개정목적 : 데이터 기반의 신산업 육성과 양질의 일자리 창출 기여, 감독기관의 독립성 확보 등
- 주요 내용 : 가명 정보 도입 등을 통한 데이터 활용 제고
- 데이터 3법 개정 전후 관계 : 금융회사의 경우 개정 후 개인정보는 신용정보법 우선, 신용정보법에 규정되지 않은 조항은 개인정보 보호법을 적용하도록 일원화
- 정보통신망법 내 개인정보보호에 관한 사항은 삭제 및 개인정보보호법으로 이관하고, 신용정보보호법은 개인정보 보호법과 유사 중복되는 조항을 정비하여 법률 체계 일원화

2. 개인정보 처리단계별 보호

3-1. 개인정보의 생명 주기
- 개인정보 수집, 이용, 제공, 보관, 파기
- 개인정보보호법은 10장까지 있음. (특례 - 개인정보 사업자들은 개인정보보호법의 6장을 적용받음)

추가적으로 스터디할 내용

데이터 3법 자세히 다루기

특강 내용

-개인정보의 유형과 분류: 일반정보, 통신 및 위치정보, 사회적 정보, 정신적 정보, 신체적 정보, 재산적 정보, 비식별 처리 정보(가명정보)
-차 번호도 개인정보가 될 수 있음(단, 법인차인 경우에는 개인에 대한 정보가 아님): 옥외주차장 운영자는 개인정보 처리자가 되므로 입출입하는 차에 대해 암호화하는 과정을 거쳐야 함 등
-개인정보자기결정권: 헌법 제 10조 및 제17조(사생활의 자유)에 근거한 국민의 기본권으로서 "개인정보 자기결정권"의 보장
-개인정보보호법 2차 개정 추진 경과
-데이터3법 개정 주요내용(개인정보보호법, 정보통신망법, 신용정보법)
->개보법이 많이 강화됨
-개인정보의 생명주기
-개인정보 처리단계별 의무사항

추가적으로 스터디할 내용

개인정보의 유출 및 보안 정도를 포괄적으로 알아보고 싶다. 개인정보 유출에 대해서 기술적인 측면에서도 접근하여 방어하는 법을 알아보고 싶다. 개인정보의 절대적 안전성은 없을지에 대해서도 궁금했다. 만약 없다면 이를 위해 어떤 기술을 적용시키면 좋을지 알아보고 싶다.

2-2. 데이터3법 개정 주요 내용
- 개정목적 : 데이터 기반의 신산업 육성과 양질의 일자리 창출 기여, 감독기관의 독립성 확보 등
- 주요 내용 : 가명 정보 도입 등을 통한 데이터 활용 제고
- 데이터 3법 개정 전후 관계 : 금융회사의 경우 개정 후 개인정보는 신용정보법 우선, 신용정보법에 규정되지 않은 조항은 개인정보 보호법을 적용하도록 일원화
- 정보통신망법 내 개인정보보호에 관한 사항은 삭제 및 개인정보보호법으로 이관하고, 신용정보보호법은 개인정보 보호법과 유사 중복되는 조항을 정비하여 법률 체계 일원화

2. 개인정보 처리단계별 보호

3-1. 개인정보의 생명 주기
- 개인정보 수집, 이용, 제공, 보관, 파기
- 개인정보보호법은 10장까지 있음. (특례 - 개인정보 사업자들은 개인정보보호법의 6장을 적용받음)

추가적으로 스터디할 내용

개인정보의 유출 및 보안 정도를 포괄적으로 알아보고 싶다. 개인정보 유출에 대해서 기술적인 측면에서도 접근하여 방어하는 법을 알아보고 싶다. 개인정보의 절대적 안전성은 없을지에 대해서도 궁금했다. 만약 없다면 이를 위해 어떤 기술을 적용시키면 좋을지 알아보고 싶다.

논문 스터디 후 토론

05

[가명정보 생명주기에 따른 개인정보보호 중심 설계 적용 원칙에 관한 연구]

Journal of The Korea Institute of Information Security & Cryptology
VOL.32, NO.2, Apr. 2022
ISSN 1598-3986(Print)
ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.2.329

가명정보 생명주기에 따른 개인정보보호 중심 설계 적용 원칙에 관한 연구

김 동 현†‡
한국인터넷진흥원 (책임연구원)

A Study on the Principle of Application of Privacy by Design According to the Life Cycle of Pseudonymization Information

Dong-hyun Kim†‡
KOREA INTERNET & SECURITY AGENCY (General Researcher)

요 약

최근 개인정보가 데이터로 활용되면서 다양한 신산업 등이 발굴되고 있지만 체계적인 관리체계 구축 미흡 등으로 개인정보 유출 및 오남용 사례가 연이어 발생되고 있다. 또한 지난 '20년 8월, 데이터 3법 시행 이후 개인정보를 가명·익명 처리하여 활용하는 서비스가 등장하고 있지만 불충분한 가명처리 및 가명정보 처리에 대한 안전성확보조치, 혐오표현 등의 민감정보의 처리 미흡으로 개인정보 이슈가 발생하고 있다. 이에 본 연구는 개인정보를 안전하게 활용하기 위하여 캐나다의 Ann Cavoukian[1]이 제시한 개인정보보호 중심 설계(Privacy by Design, 이하 PbD) 원칙을 기반으로 가명정보 생명주기에 적용할 수 있는 새로운 PbD원칙을 제안하였다. 또한, 제안한 방법에 대하여 개인정보보호 관련 전문가 30명을 대상으로 설문조사를 통하여 제안 방법의 유의미함을 확인할 수 있었다.

ABSTRACT

Recently, as personal information has been used as data, various new industries have been discovered, but cases of personal information leakage and misuse have occurred one after another due to insufficient systematic management system establishment. In addition, services that use personal information anonymously and anonymously have emerged since the enforcement of the Data 3 Act in August 2020, but personal information issues have arisen due to insufficient alias processing, safety measures for alias information processing, and insufficient hate expression. Therefore, this study proposed a new PbD principle that can be applied to the pseudonym information life cycle based on the Privacy by Design (PbD) principle proposed by Ann Cavoukian [1] of Canada to safely utilize personal information. In addition, the significance of the proposed method was confirmed through a survey of 30 experts related to personal information protection.

Keywords: Personal Information, Pseudonymization Privacy by Design, De-Identification Privacy by Design

I. 서 론

지난 '20년 8월, 이른바 데이터 3법의 개정과 함께 데이터 산업진흥 및 이용촉진에 관한 기본 법률도 '22년 4월 시행을 앞두고 있어 더욱 많은 산업에서 다양한 데이터가 활용될 예정이다. 또한, 디지털 뉴딜 등 우리나라를 비롯하여 전 세계적으로 데이터 경제를 강화하기 위한 다양한 개인정보 활용 정책들이 등장하고 있다[2]. 이 중 이종산업 간 가명정보의 결합 및 자율주행차, 스마트시티 등의 산업은 개인정보가 방대하게 활용되는 경우로 보다 안전한 개인정보에

Received(01. 26. 2022), Accepted(02. 21. 2022)
† 주저자, kdonghyun@kisa.or.kr
‡ 교신저자, kdonghyun@kisa.or.kr(Corresponding author)

개별 논문 스터디 보고서

06

[AI 서비스에서의 개인정보보호를 위한 책임과 원칙의 적용에 관한 연구]

1. AI 서비스에서의 개인정보보호를 위한 책임과 원칙의 적용에 관한 연구

나는 'AI 서비스에서의 개인정보보호를 위한 책임과 원칙의 적용에 관한 연구'를 읽었는데, 정말 흥미로운 내용이 많았다. 여러 흥미로웠던 점 중 가장 인상깊었던 부분들이 몇 있는데, 이 보고서에서 그 내용을 다뤄보고자 한다.

가장 먼저, EU나 미국, 호주 등의 나라들과 마찬가지로 우리나라 또한 AI의 기술적 수준이 상당히 발전한 상태임을 깨달을 수 있었다. 다만 다른 나라들과는 달리 개인정보보호에 관한 법령의 구체성이 부족한 상태인 것이 많이 아쉽다고 느꼈다. 한국도 데이터 3법, 지능정보화기본법 등 효율적이고 좋은 법률 체계를 십분 활용할 수 있게끔 법제의 구체화가 최대한 빨리 이루어졌으면 하는 바람이다.

두 번째로는 위 논문을 읽으며 AI와 개인정보의 보호가 굉장히 밀접하게 연관되어있다는 것을 다시금 깨달을 수 있었다. 이 논문을 접하기 전에는 AI와 개인정보보호가 정확이 어떤 연관성을 가지고 있는지, AI 서비스에서 개인정보들을 어떤 방식으로 보호할 수 있는지 명확히 인지하지 못한 상태였다. 하지만 이 논문을 보고 AI와 관련된 개인정보 침해사고가 정말 많이 일어나고 있다는 것과, 그와 연관된 몇몇 대응 방침들에 대한 정보를 접할 수 있었다.

마지막으로는 내가 알지 못했던 다양한 보안 위협의 사례들에 대해 배울 수 있었던 것이 정말 유익했다. 기존에 미리 알고 있었던 스피어 피싱이나 개인정보 유출 등에 대한 내용도 있었지만, 적대적 스티커 속성이나 정교 및 자동화된 스웜공격 등 내가 알지 못했던 보안 위협 속성들에 대한 내용도 접할 수 있었다.

[메타버스 이용자의 개인정보보호]

2. 메타버스 이용자의 개인정보보호

논문에서 밀했듯이, 메타버스는 데이터가 많은만큼 유출될 위험이 크고, 이미 유출 사례도 빌생하고 있다.

내가 메타버스에 회의적인 입장어서 그런지는 몰라도, 메타버스로 금융거래나 여러 활동이 이루어진다고 해서 실제로 사람들이 그것을 운영할까 의문이 든다. 이미 충분히 다른 앱들도 개빌되어 있는데, 메타버스가 빌달한다고 해서 사람들이 해당 서비스들을 많이 이용힐지는 질 모르겠다.

3. 메타버스 이용자의 개인정보보호

메타버스가 우리에게 친숙해지고 많은 서비스가 개빌됨에 따라 개인정보보호에 대해 막연하게 우려했던 부분들을 이 논문을 통해 어떤 지점에서 어떤 문제가 빌생힐 수 있는지에 대해 명확하게 짚어볼 수 있어서 유익했다. 특히, 메타버스에서 문제되는 개인정보 관련 쟁점 중 아동의 법정대리인 동의 절차가 메타버스의 몰입을 방해힐 수 있어 새로운 제도적 뒷받침이 필요하다는 부분이 생각해 보지 못했던 부분이라 인상적이었다.

[지능정보사회 개인정보자기결정권을 보완하는 데이터 활용과 개인정보보호]

4. 지능정보사회 개인정보자기결정권을 보완하는 데이터 활용과 개인정보보호

현재 우리는 지능정보사회를 실고 있고, 개인정보의 문제 또한 대두되고 있다. 이때, 자신의 개인정보에 대한 자기 결정권 문제가 중요시된다. 이는 헌법에서 보장해야 하는 기본권이며, 인격권의 성격도 갖고 있다는 점이 흥미로웠다. 또한 개인정보보호의 자기 결정권이 중요한 이유는, 개인정보 '보호' 라는 밀 때문에 활용을 금지하는 것처럼 보이나, 사실은 자기결정권을 통한 동의를 얻어 개인정보를 유통함으로써 이를 이용한 산업의 빌전을 촉진시킬 수 있는 점 또한 흥미로웠다. 이를 실현하기 위해서는 사이버 보안 또한 중요한데, 이 논문에서 기술적인 측면에 대해서는 자세히 다루고 있지 않아 이에 대해 더 조사해 보고 싶다고 생각했다.

개인정보보호 취약 기술 분석 및 조사

07

[개인정보보호 안드로이드 앱에 대한 취약점 분석]

Calculator - photo vault 앱 에 대한 역공학을 통해 접근제어 기능인 PIN을 알아내어 암호화 및 은닉이 적용된 사진, 문서 등의 파일에 대한 복호화 진행 논문을 참고했다.

- 처음 앱 실행 시 접근제어에 사용될 4~8자리의 PIN과 비밀번호 복구 질문, 이메일을 입력한다. 파일 암호화 시 접근제어에 사용한 암호화키와 암호화 알고리즘을 이용한다.
- 파일 복호화의 경우 암호화에 사용된 암호키와 알고리즘을 이용해 진행된다. 원본파일과 복호화된 파일의 Hex값 비교를 통해 확인한다.
- 그러나 암호화 및 은닉된 파일에 대한 로그가 저장된 데이터베이스 파일에 대해서도 복호화를 통해 값을 알아낼 수 있어 해당 앱의 취약점이 존재함을 알 수 있다.

[개인정보보호를 위한 익명 인증 기법 도입 방안 연구]

본 논문은 사용자 정보보호를 위한 새로운 접근방안으로 익명 인증 기반의 사용자 프라이버시 보호 방법을 체계적으로 제시한다. 특히 세밀한 익명성 제어를 위해 정량 및 정성적인 관점에서 요구되는 프라이버시 관련 고려사항들을 다룰 수 있는 프레임워크를 제안한다.

프라이버시 보호 방법에 이용되는 암호학적 기법

- **그룹서명(Group Signature)** : 키 발급자로부터 발급받은 키 값을 이용하여 영지식 증명을 통하여 서명자가 정당한 일원임을 증명하는 서명기법
- 환서명(Ring Signature) : 서명자가 자신을 포함한 환(ring)을 구성하여 자신의 비밀키와 다른 구성원들의 공개키를 이용하여 임의의 메시지에 대해 서명함
- 가명 기반 인증 시스템 : (1) i-PIN (2) TAC


THANK YOU!