과목명	시큐어코딩
담당교수	우사무엘 교수님
과제명	중간고사 대체 과제
학과	소프트웨어학과
학번	32151671
이름	박민혁
제출 일자	2021-04-18

목차

I. 과제 1 : C-ITS STRIDE 수행

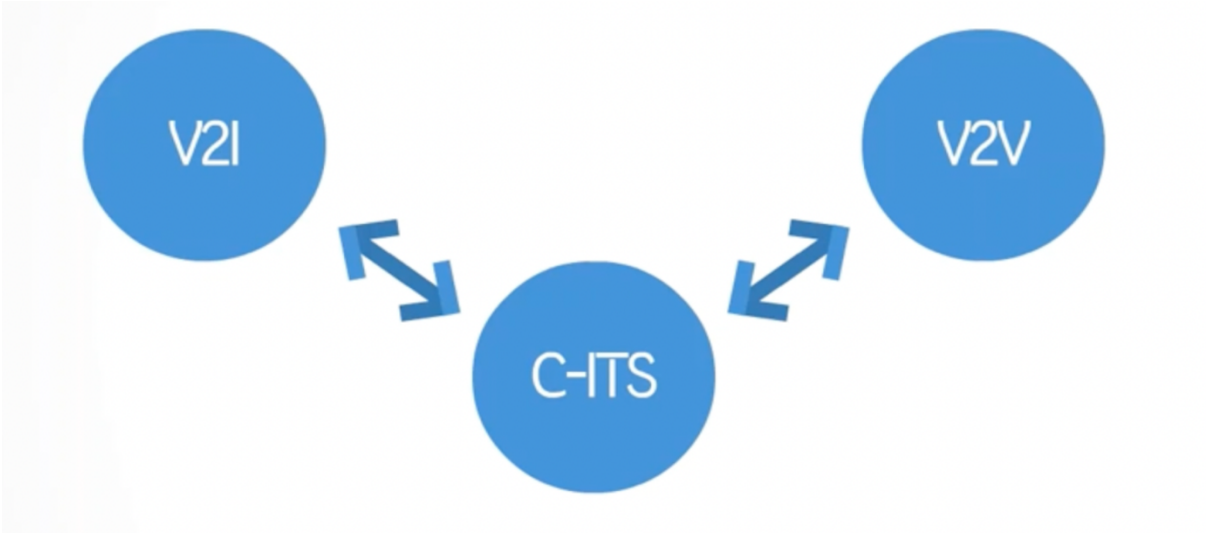
1. 기본 내용

(1) ITS 란?.

- Intelligent Transport Systems 의 약어로 교통, 전자, 통신, 제어 등 첨단기술을 도로, 차량, 화물 등 교통체계의 구성요소에 적용하여 실시간으로 교통정보를 수집, 관리, 제공하는 시스템

(2) CITS 란?

- Cooperative-Intelligent Transport System 의 약어로 차량이 주행 중 운전자에게 주변 교통상황과 급정거, 낙하물 등의 사고 위험 정보를 실시간으로 제공하는 시스템



- 도로의 상황 정보와 주변 차량정보를 공유하여 위험상황을 피할 수 있도록 사전에 경고하는 미래형 교통체계
- 자동차와 통신하는 객체에 유형에 따라 V2V, V2I, V2N, V2P 등 다양한 형태의 통신 환경이 존재한다

(3) V2X(Vehicle to Everything)

- 운전 중, 무선 통신을 이용하여 다른 차량, 도로 인프라 등 다양한 사물과 정보를 교환하는 차량 통신 기술
- 다양한 통신 객체를 모두 포함하는 Vehicle to Everything

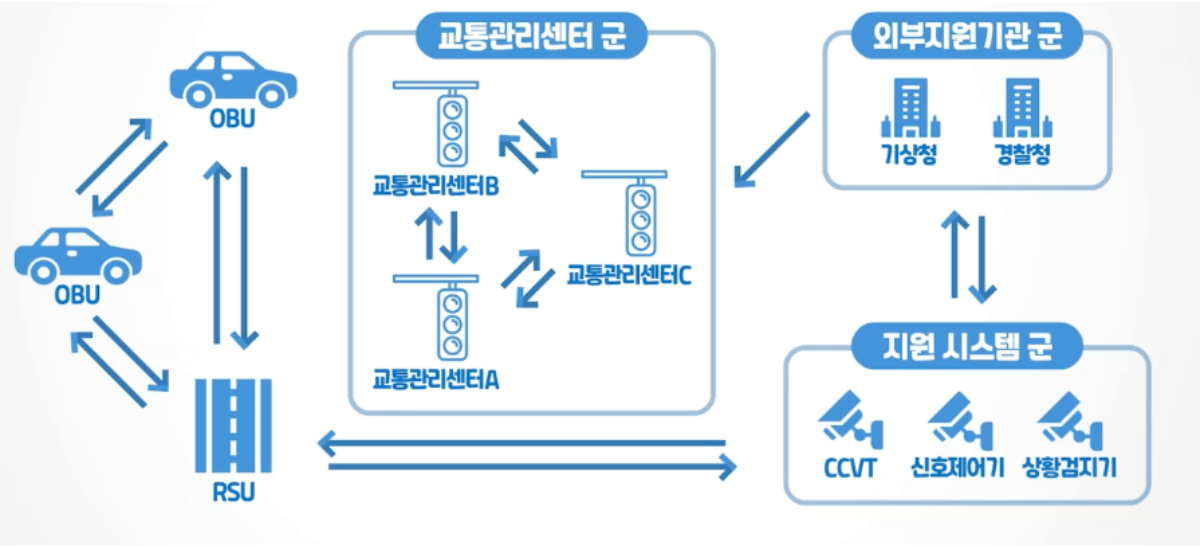
(4) V2V(Vehicle to Vehicle)

- 이동 중이거나 정차 중인 차량들 간의 데이터를 송수신하는 무선 통신 기술로서, 자동차들이 위치/속도, 교통상황 정보 등을 주고받으며 갑작스런 교통사고를 예방하는 시스템
- 도로를 달리는 차량들이 서로 대화를 주고받으며 충돌 위험성을 차단하기 위한 안전 시스템

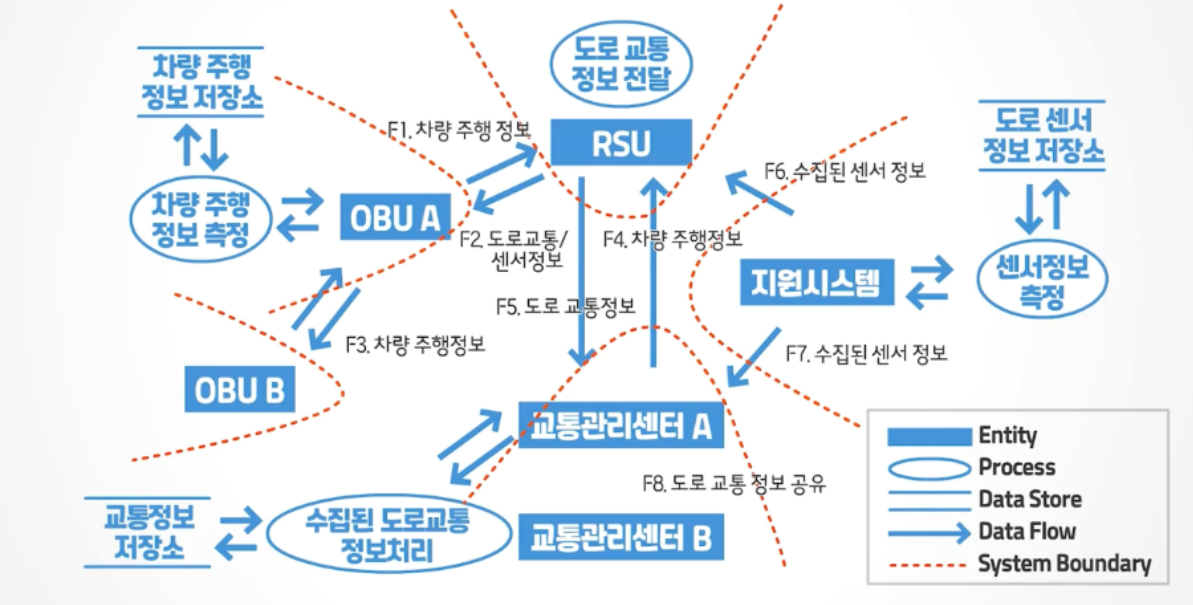
(5) V2I(Vehicle to Infrastructure)

- 차량 내에 설치된 통신 단말기와 정보를 교환할 수 있는 기지국을 도로에 설치하여 주행 정보를 수집하고, 이를 중앙 서버에서 분석하여 차량에게 제공하는 기술
- V2V 통신 기술과 결합하여 ITS/C-ITS 시스템에 활용, 실시간 교통상황 및 돌발 상황 파악이 가능

2. Data Flow



No.	Data Flow	정보제공 주체	
		송신	수신
F1	차량주행 정보	차량(OBU)	노변기기(RSU)
F2	도로교통/센서 정보	노변기기(RSU)	차량(OBU)
F3	차량주행 정보	차량(OBU)	차량(OBU)
F4	차량주행 정보	노변기기(RSU)	교통관리센터
F5	도로교통 정보	교통관리센터	노변기기(RSU)
F6	수집된 센서 정보	지원시스템	노변기기(RSU)
F7	수집된 센서 정보	지원시스템	교통관리센터
F8	도로교통 정보 공유	교통관리센터	교통관리센터



3. 수행

No.	위협
A1	다른 차량으로 위장
A2	차량 주행 정보 변경
A3	정보 전송 행위의 부인
A4	다른 노변 기기로 위장
A5	도로 교통 정보 변경
A6	다른 교통관리센터로 위장
A7	다른 지원 시스템으로 위장
A8	센서 정보 변경

No.	위협	STRIDE	방어 기법
F1	A1	Spoofing	인증
	A2	Tampering	인증, 전자서명
	A3	Repudiation	전자서명, 감사 로그

No.	위협	STRIDE	방어 기법
F2	A3. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A4. 다른 노변 기기로 위장	Spoofing	인증, 전자서명
	A5. 도로 교통 정보 변경	Tampering	해시, 전자서명

	A8. 센서 정보 변경	Tampering	해시, 전자서명
위협 선정 이유	(노변 기기 -> 차량) 노변 기기에서 차량에게 전송하는 정보는 센서 정보와 도로 교통정보이다. 그래서 이 두가지를 변경할 수 있어서 A5, A8 을 선정했고, 이러한 전송 정보들을 부인할 수 있는 A3 와 노변 기기 자체를 위장할 수 있는 A4 를 선정했다.		

No.	위협	STRIDE	방어 기법
F3	A1. 다른 차량으로 위장	Spoofing	인증, 전자서명
	A2. 차량 주행 정보 변경	Tampering	해시, 전자서명
	A3. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
위협 선정 이유	(차량 -> 차량) 차량에서 차량으로 주는 정보들은 차량 주행 정보이다. 따라서 자량 주행 정보를 변경할 수 있기 때문에 A2 를 선정 했고, 이러한 전송 정보들을 부인할 수 있는 A3 와 차량 자체를 위장할 수 있는 A1 을 선정했다.		

No.	위협	STRIDE	방어 기법
F4	A2. 차량 주행 정보 변경	Tampering	해시, 전자서명
	A3. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A4. 다른 노변 기기로 위장	Spoofing	인증, 전자서명
위협 선정 이유	(노변 기기 -> 교통관리센터) 노변 기기에서 교통관리센터로 주는 정보들은 차량 주행 정보이다. 따라서 차량 주행 정보를 변경할 수 있기 때문에 A2 를 선정 했고, 이러한 전송 정보들을 부인할 수 있는 A3 와 노변 기기 자체를 위장할 수 있는 A4 를 선정했다.		

No.	위협	STRIDE	방어 기법
F5	A3. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A5. 도로 교통 정보 변경	Tampering	해시, 전자서명
	A6. 다른 교통관리센터로 위장	Spoofing	인증, 전자서명
위협 선정 이유	(교통관리센터 -> 노변 기기) 교통관리센터에서 노변 기기로 주는 정보들은 도로 교통 정보이다. 따라서 도로 교통 정보를 변경할 수 있기 때문에 A5 를 선정 했고, 이러한 전송 정보들을 부인할 수 있는 A3 와 교통관리센터 자체를 위장할 수 있는 A6 를 선정했다.		

No.	위협	STRIDE	방어 기법
	A3. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그

F6	A7. 다른 지원 시스템으로 위장	Spoofing	인증, 전자서명
	A8. 센서 정보 변경	Tampering	해시, 전자서명
위협 선정 이유	(지원시스템 -> 노변 기기) 지원시스템에서 노변 기기로 주는 정보들은 수집된 센서 정보이다. 따라서 센서 정보를 변경할 수 있기 때문에 A8 을 선정 했고, 이러한 전송 정보들을 부인할 수 있는 A3 와 지원 시스템 자체를 위장할 수 있는 A7 를 선정했다.		

No.	위협	STRIDE	방어 기법
F7	A3. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A7. 다른 지원 시스템으로 위장	Spoofing	인증, 전자서명
	A8. 센서 정보 변경	Tampering	해시, 전자서명
위협 선정 이유	(지원시스템 -> 교통관리센터) 지원시스템에서 교통관리센터로 주는 정보들은 수집된 센서 정보이다. 따라서 센서 정보를 변경할 수 있기 때문에 A8 을 선정 했고, 이러한 전송 정보들을 부인할 수 있는 A3 와 지원시스템 자체를 위장할 수 있는 A7 를 선정했다.		

No.	위협	STRIDE	방어 기법
F8	A3. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A5. 도로 교통 정보 변경	Tampering	해시, 전자서명
	A6. 다른 교통관리센터로 위장	Spoofing	인증, 전자서명
위협 선정 이유	(교통관리센터 -> 교통관리센터) 교통관리센터 사이에는 도로 교통 정보를 공유한다. 따라서 도로 교통 정보를 변경할 수 있기 때문에 A5 를 선정 했고, 이러한 전송 정보들을 부인할 수 있는 A3 와 교통관리센터 자체를 위장할 수 있는 A6 를 선정했다.		

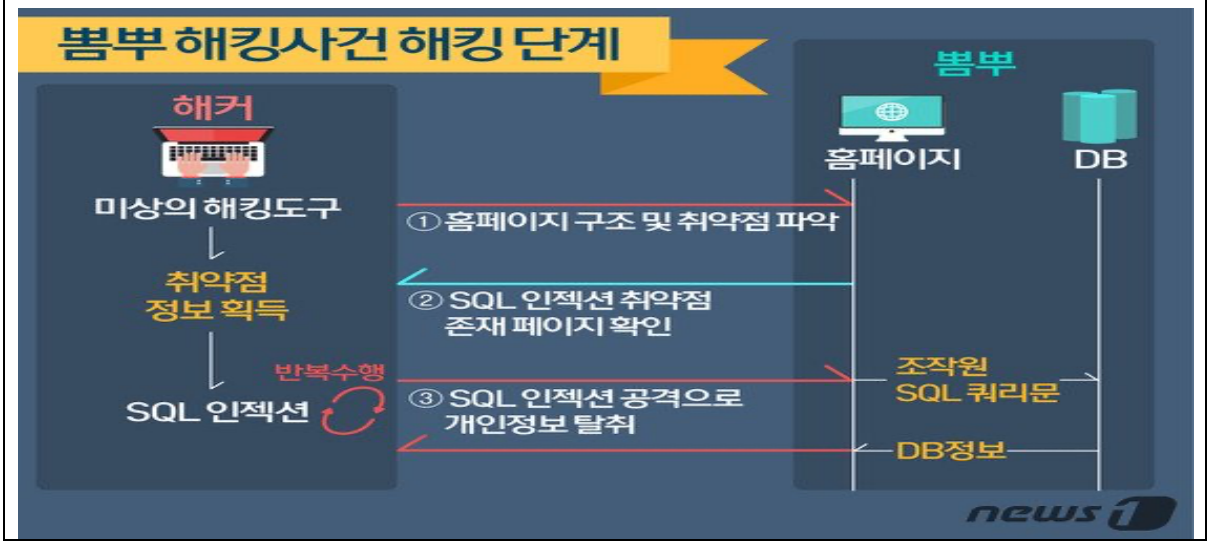
II. 과제 2 : STRIDE 설명

1. STRIDE 의 정의

종류	내용
Spoofing Identity (신분 위장)	거짓된 Identity 를 이용해 시스템 접근 권한을 획득한다.
Tampering with Data (데이터 변조)	불법적인 데이터를 수정한다.
Repudiation (부인)	사용자가 자신이 수행한 특정 액션이나 트랜잭션을 부인한다.
Information Disclosure (정보 유출)	유출되지 말아야 하는 개인정보가 유출된다.
Dos, Denial of Service (서비스 거부)	시스템 또는 애플리케이션이 정상적으로 수행되지 않도록 한다.
Elevation of Privilege (권한 상승)	제한된 권한을 가진 사용자가 권한 있는 사용자의 권한을 습득한다.

2. STRIDE 위협에 대한 실제 사례

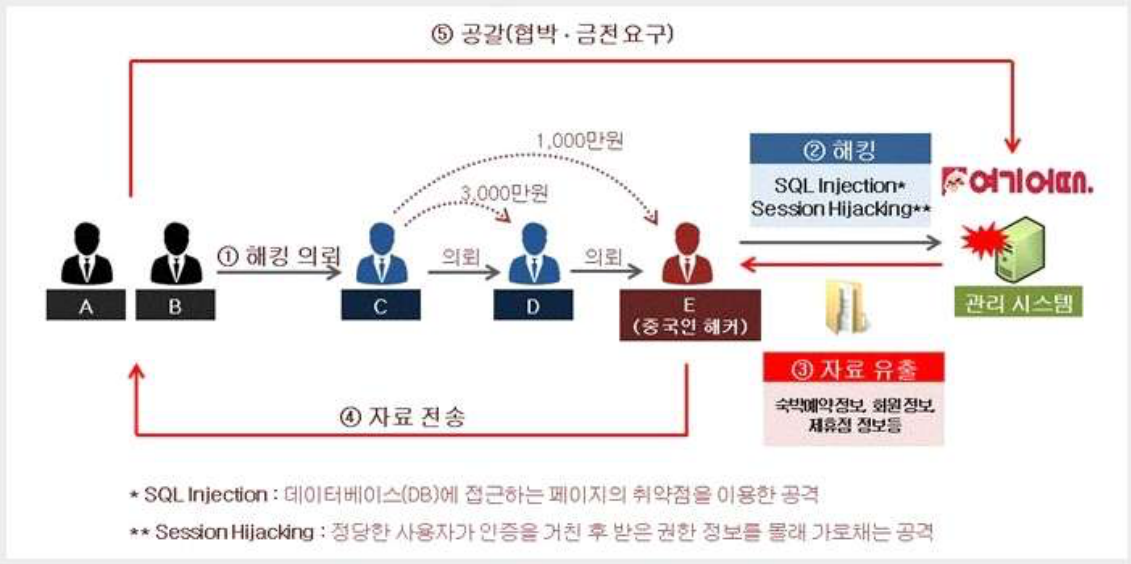
Spoofing Identity
2011 년 '뽐뿌' 해킹 사건이 발생했다. 해당 해킹 사건은 SQL 인젝션을 통해 취약점 존재 페이지를 확인하고 도메인을 IP 주소로 변환해주는 DNS 를 공격해 다른 사이트로 연결하는 'DNS 스푸핑'과 가짜페이지를 만들어 사용자를 속이는 '피싱'을 결합한 공격이다.



즉 위협 원은 미리 해당 사이트의 도메인을 바꾸기 위해 ID 와 패스워드를 탈취해 자신들이 만든 DNS 로 이동하게 하고, 이 DNS 는 다시 가짜 페이지로 연결하는 방식이다. 그래서 해당 공격은 해당 페이지가 진짜 페이지처럼 즉 'Spoofing'을 이용한 공격으로 판단된다.

Elevation of Privilege, Information Disclosure

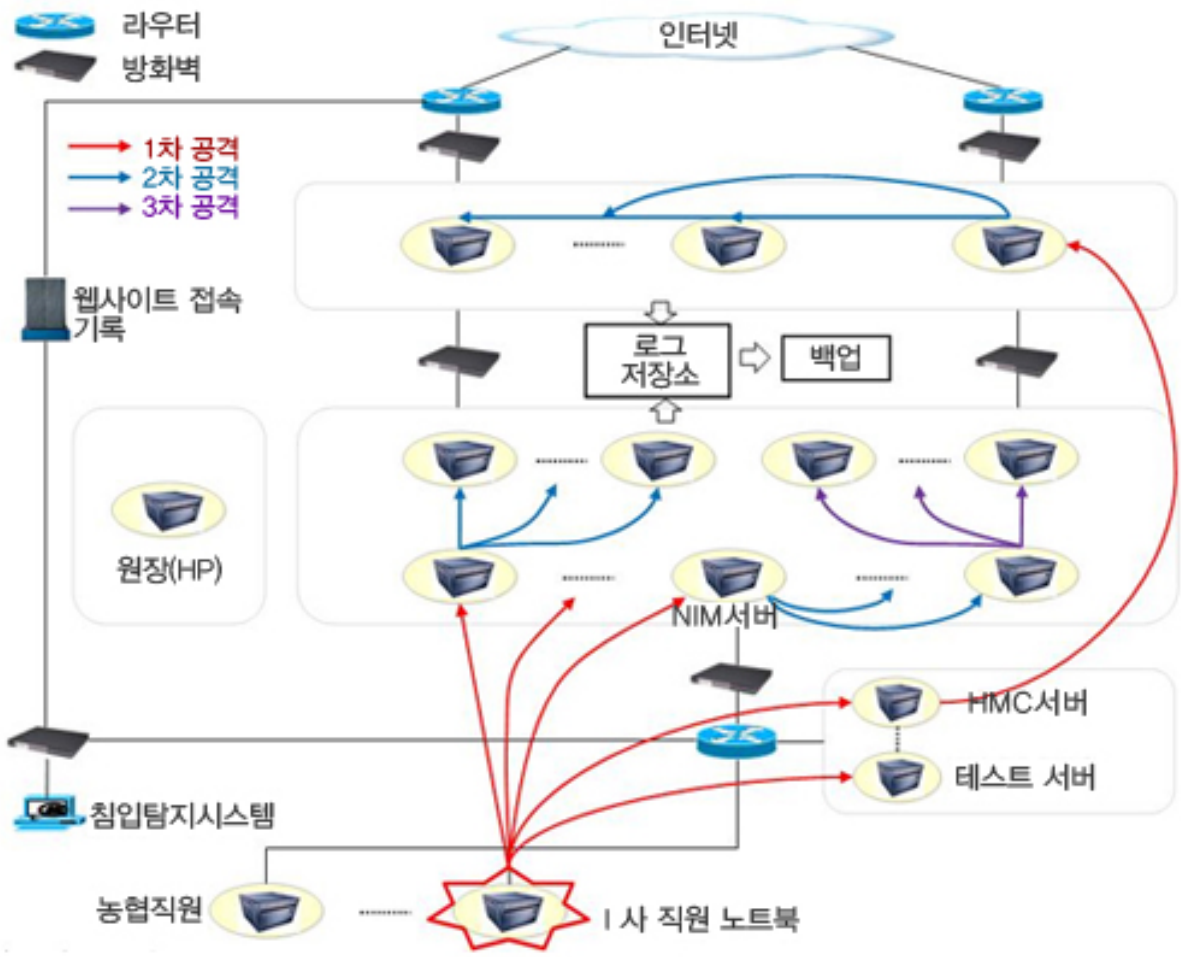
2017 년 '여기어때'가 SQL Injection 해킹에 의해 뚫린 사건이 발생했다. 해당 해킹 사건은 인증 과정의 취약점을 이용하여 공격하였다.



해당 취약점을 이용한 사건은 다음과 같다. 서버에 침입한 해커는 인젝션 방식을 통해 내부 직원의 아이디와 비밀번호를 탈취하고 나아가 문자메시지 인증과정까지 해킹해 내부 운영 서버에 침투했다. 이후 회원들의 개인정보를 빼돌려, 이를 무기로 가상화폐 비트코인 지급을 요구했다. 이러한 공격 형태를 분석해 보았을 때, 해당 공격은 중요한 정보가 유출 당하였고, 유출 당한 아이디로 권한을 가져 사용자의 정보까지 빼돌린 형태를 보아 Information Disclosure (정보 유출), Elevation of Privilege (권한 상승) 공격의 한 종류로 판단된다.

Dos, Denial of Service

2011 년 농협 전산망에 있는 자료가 대규모로 손상되어 수일에 걸쳐 전체 또는 일부 서비스 이용이 마비된 사건이 발생했다.

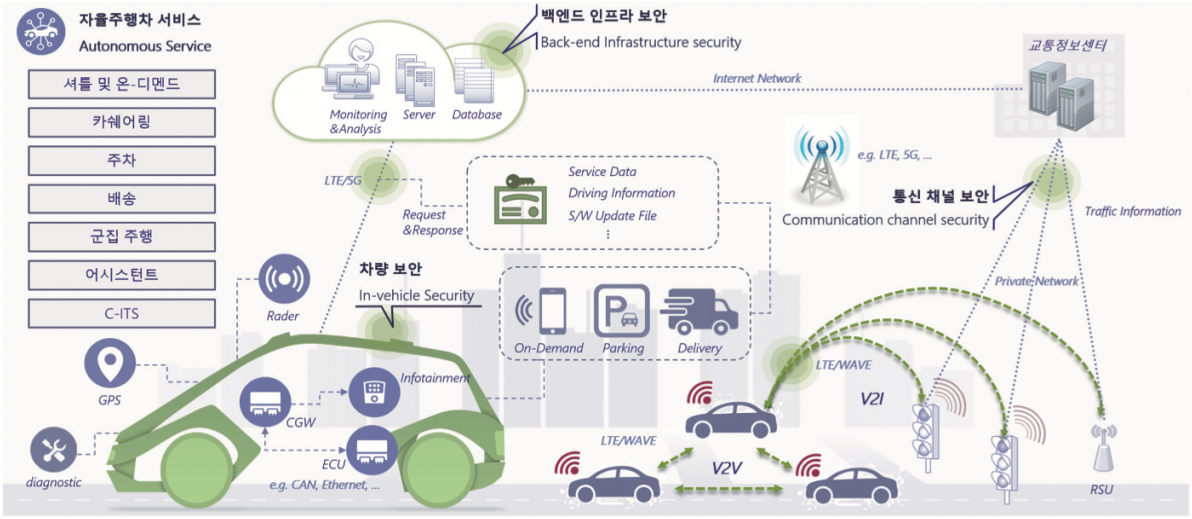


전체 서버	Web 서버	내부 서버	테스트 서버
전체 587대 피해 273대	전체 98대 피해 45대	전체 440대 피해 180대	전체 49대 피해 48대

해당 해킹 사건은 한 컴퓨터에 악성코드를 감염시켜 7 개월 이상 해당 노트북을 스크린 하며 필요한 정보를 획득한 후 원격조종방식으로 공격을 지시했다. 위협 원들은 악성코드를 삽입한 것 외에도 '백도어'라고 불리는 해킹프로그램을 설치해 노트북에 입력되는 모든 자료를 빼냈으며, 도청프로그램을 이용해 노트북 사용자의 일거수일투족을 치밀하게 감시했다. 이러한 취약점을 이용하여 공격명령파일을 노트북에 설치하고 인터넷을 이용한 원격제어로 명령을 실행했고 2 차, 3 차 공격이 이루어졌다. 실제 공격이 이루어졌을 때 농협 서비스 이용이 중지됐었다. 따라서 해당 공격은 Dos 공격의 한 종류로 판단된다.

III. 과제 3 위협 모델링 실습

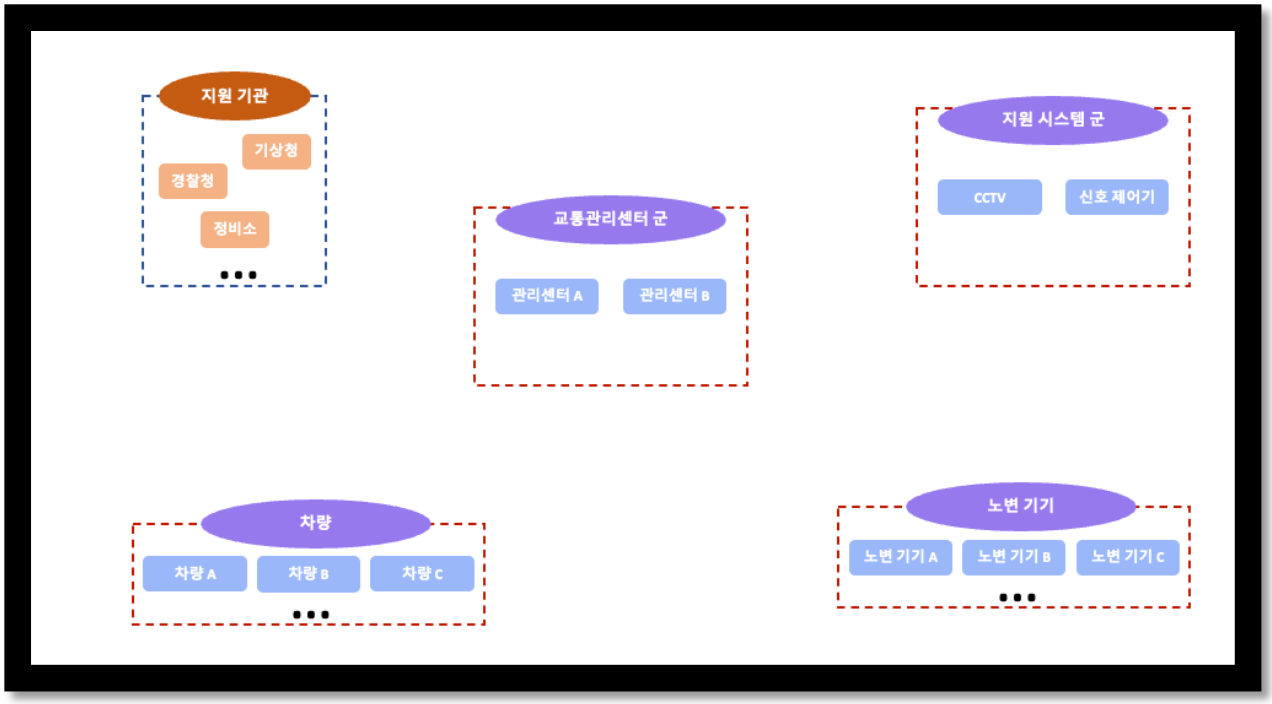
1. 서비스 대상 선정 및 설명

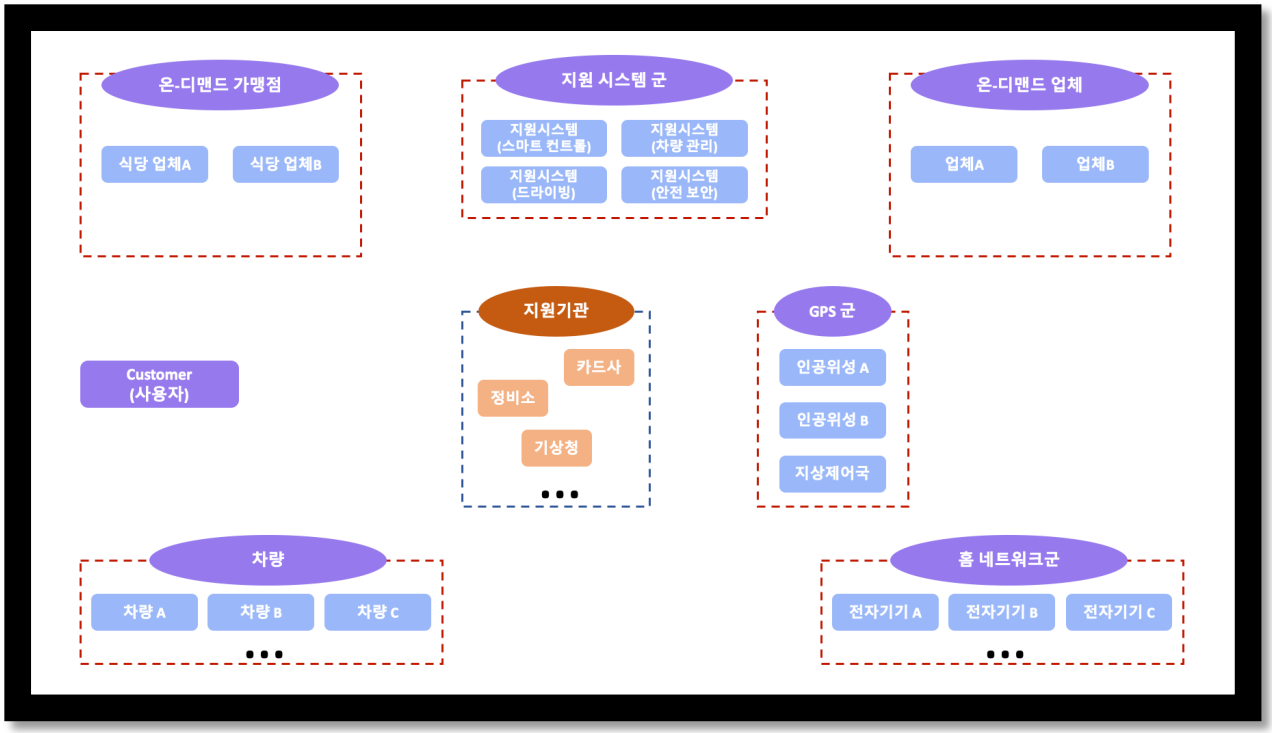


자율주행차는 커넥티비티 기술 및 센서 기술의 발전과 함께 급격하게 성장하고 있다. 자율주행차 서비스의 공통적인 구성요소들을 식별하였다. 사진과 같이 차량은 V2X 통신을 위하여 차량 간 셀룰러 통신(C-V2X), WAVE 통신을 한다. 그리고 이상 행위를 보고하기 위하여 차량은 RSU 를 통하여 인프라와 통신을 수행한다. 자율주행차 서비스는 차량을 기반으로 다양한 통신 채널을 통해 백엔드 인프라, 교통정보센터에 교통, 안전, 편의, 차량 관리 등 정보를 전달하고, 사용자는 해당 정보를 백엔드 인프라나 차량과의 통신을 통해 전달받아, 서비스를 이용할 수 있게 된다.

자율주행 서비스 7 가지 중에서 온-디멘드 서비스를 하려고 한다. 온-디멘드 서비스란 주문형 서비스이다. 아직 주문형 서비스에 자율주행 서비스를 주입하여 활용되고 있는지는 모르겠지만 코로나 시대가 길어져 온-디멘드 서비스가 최근 들어 급증하고 있다. 그래서 조만간 자율주행 서비스도 온-디멘드 서비스가 활성화가 될 것을 예측하여 주제를 선정했다. 온-디멘드 서비스를 단순하게 '내가 있는 곳으로 상품이나 서비스가 찾아온다.'라고 이해하면 쉬울 것 같다. 예를 들어 배달의 민족 앱을 통해 배달 주문을 하는 것과 같다. 배달 업체에 관한 온-디멘드 서비스를 조사했다. 우선 현재 서비스를 살펴보면 다음과 같다.

현재 서비스는 다음과 같이 고객이 배달 앱을 통해 주문한다. 주문을 받은 업체들은 해당 음식점에 정보를 전송하고 배달 대행업체를 통해서 배달하거나 직접 고용한 배달원을 통해 배달을 진행한다. 나는 이 마지막 시스템을 자율 주행으로 바꿔보려고 한다. 자율 주행의 기본은 C-ITS 기술을 기본으로 한다. C-ITS 기술이 도입된 차량이 대신해서 배달을 진행한다. 물론 이 시스템은 불편함도 분명 있을 것이다. 그것은 추후에 설명 하도록 하고 우선 객체들을 살펴보면 다음과 같다.



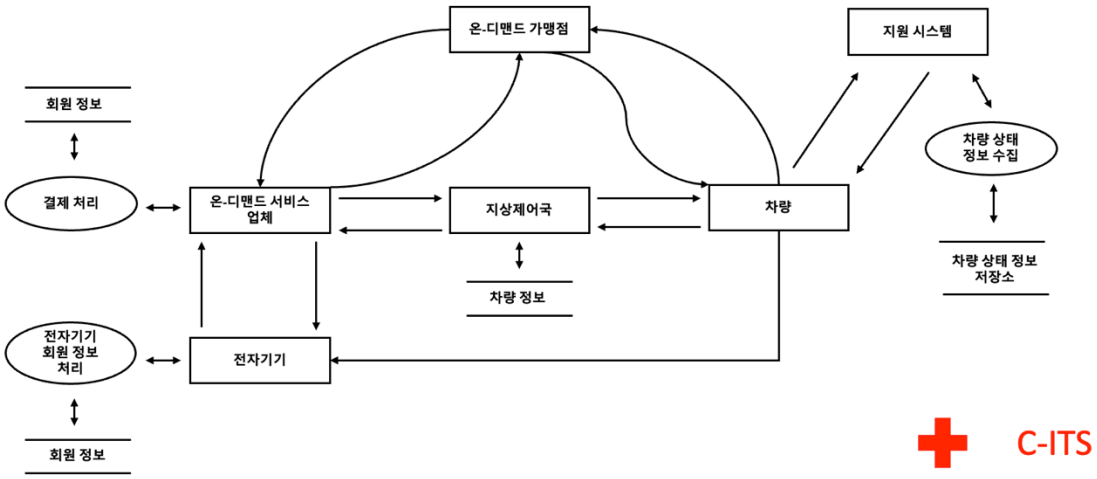


객체를 두 개 그린 이유는 다음과 같다. 우선 자율 주행의 기본은 C-ITS 서비스가 기본이다. 그래서 C-ITS 의 객체와 직접 상상한 자율주행 온-디맨드 서비스의 객체를 그려봤다. C-ITS 서비스는 강의와 위에 설명이 되어 있으니 생략하고, 온-디맨드 서비스의 객체들을 살펴보면 우선 Customer 가 이용하는 IoT 기반의 여러 전자기기가 홈 네트워크 군에 속해있다. 그리고 온-디맨드 업체가 존재하며 온-디맨드 업체 가맹점이 존재한다. 그리고 실시간 위치 정보를 받아야 하므로 GPS 군이 존재하고, 차량이 존재한다. 또한 차량 상태 정보를 위한 지원 시스템 군이 존재한다. 그리고 결제가 이루어지면 결제 카드사, 차량이 고장 나면 정비소, 현재 날씨 상태를 알려주는 곳들이 지원 기관에 속한다.

사실 이 시스템에 단점은 많을 것이다. 우선 배달 서비스의 형태가 바뀔 것이다. 배달 서비스는 배달원이 원래 문 앞까지 배달하는 시스템이었다. 하지만 이러한 시스템은 사용자가 직접 받으러 가야 할 것이고, 아파트 단지에 출입하기 위해 자신의 신분을 말해야 하는 아파트들 출입이 힘들어 질 수도 있다. 그러한 경우들을 제외한 나머지의 상황들을 봤을 때 괜찮은 시스템이라 생각하고 충분히 위에 단점들을 보완할 수 있는 대안이 나올 것이라 생각했다. 아직 지식수준이 얼마 되지 않아서 이 정도 상상으로만 해서 과제를 수행했다.

2. DFD 그리기

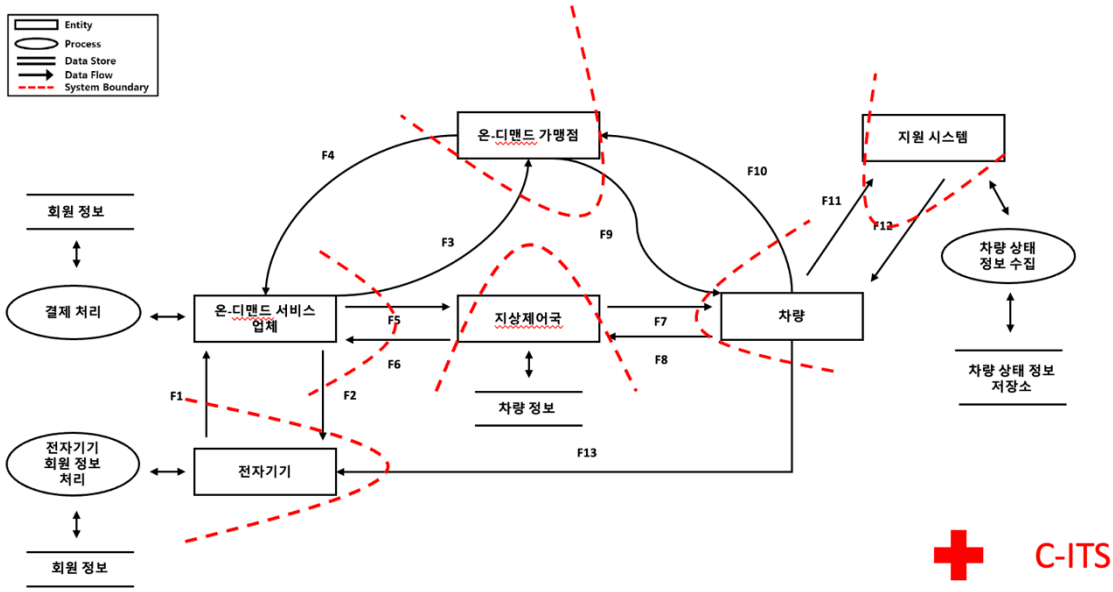
Level 0



Level 0 은 다음과 같이 그렸다. C-ITS 는 생략했다. 다음 그림을 살펴보면 소비자가 전자기기를 이용하여 온-디맨드 서비스 업체 애플리케이션을 통해 주문을 한다. 주문을 받은 온-디맨드

서비스 업체는 결제를 처리하고 가맹점에 결제 정보와 가맹점 위치를 전송한다. 그리고 가맹점은 소요 시간과, 수수료를 지불한다. 온-디맨드 서비스 업체는 가맹점 위치와 소비자 위치를 지상제어국에 전송하여 지상제어국은 배달이 가능한 차량들을 확인한 후 온-디맨드 서비스 업체에 전송한다. 또한 실시간 도로 정보도 같이 전달한다. (소비자에게 도착 예정시간을 알려주기 위하여) 가능한 차량이 있으면 차량에게 위치 정보들을 알려준다. 위치 정보를 받은 차량은 시간에 맞춰 가맹점으로 가 음식을 받고 자신의 위치를 실시간으로 소비자 전자기기에 전송한다. ,

Level 1



No.	Data Flow	송신	수신
F1	회원 정보/결제 요청 정보	전자기기	온-디맨드 서비스 업체
F2	결제 정보/소요 시간 정보/차량 정보	온-디맨드 서비스 업체	전자기기
F3	결제 정보	온-디맨드 서비스 업체	온-디맨드 가맹점
F4	대금 정보/소요 시간 정보	온-디맨드 가맹점	온-디맨드 서비스 업체
F5	가맹점 위치 정보/소비자 위치 정보	온-디맨드 서비스 업체	지상제어국
F6	차량 정보/실시간 도로 정보	지상제어국	온-디맨드 서비스 업체
F7	가맹점 위치 정보/소비자 위치 정보	지상제어국	차량
F8	실시간 차량 위치 정보/실시간 도로 정보	차량	지상제어국
F9	소요 시간 정보	온-디맨드 가맹점	차량
F10	차량 정보	차량	온-디맨드 가맹점
F11	차량 상태 정보	차량	지원 시스템

F12	차량 상태 정보	지원 시스템	차량
F13	실시간 차량 위치 정보	차량	전자기기

3. 위협 식별하기

No.	위협
A1	회원 정보 변경
A2	결제 요청 정보 변경
A3	결제 정보 변경
A4	대금 정보 변경
A5	소요시간 정보 변경
A6	차량 정보 변경
A7	가맹점 위치 정보 변경
A8	소비자 위치 정보 변경
A9	도로 정보 변경
A10	차량 상태 정보 변경
A11	차량 위치 정보 변경
A12	다른 전자기기로 위장
A13	다른 온-디맨드 서비스 업체로 위장
A14	다른 온-디맨드 가맹점으로 위장
A15	다른 차량으로 위장
A16	회원 정보 유출
A17	차량 정보 유출
A18	온-디맨드 서비스 업체 서비스 거부
A19	지상제어국 서비스 거부
A20	온-디맨드 서비스 업체 권한 탈취
A21	정보 전송 행위의 부인

4. 식별된 위협을 STRIDE 에 매칭 시키기

No.	위협	STRIDE	방어 기법
F1	A1. 회원 정보 변경	Tampering	해시, 전자서명
	A2. 결제 요청 정보 변경	Tampering	해시, 전자서명
	A12. 다른 전자기기로 위장	Spoofing	인증, 전자서명

	A16. 회원 정보 유출	Information Disclosure	암호화, ACLs
	A21. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
F2	A3. 결제 정보 변경	Tampering	해시, 전자서명
	A5. 소요시간 정보 변경	Tampering	해시, 전자서명
	A6. 차량 정보 변경	Tampering	해시, 전자서명
	A13. 다른 온-디맨드 서비스 업체로 위장	Spoofing	인증, 전자서명
	A17. 차량 정보 유출	Information Disclosure	암호화, ACLs
	A18. 온-디맨드 서비스 업체 서비스 거부	Dos, Denial of Service	필터링, ACLs
	A20. 온-디맨드 서비스 업체 권한 탈취	Elevation of Privilege	최소한의 권한으로 실행
	A21. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
F3	A3. 결제 정보 변경	Tampering	해시, 전자서명
	A13. 다른 온-디맨드 서비스 업체로 위장	Spoofing	인증, 전자서명
	A18. 온-디맨드 서비스 업체 서비스 거부	Dos, Denial of Service	필터링, ACLs
	A20. 온-디맨드 서비스 업체 권한 탈취	Elevation of Privilege	최소한의 권한으로 실행
	A21. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
F4	A4. 대금 정보 변경	Tampering	해시, 전자서명
	A5. 소요 시간 정보 변경	Tampering	해시, 전자서명
	A14. 다른 온-디맨드 가맹점으로 위장	Spoofing	인증, 전자서명
	A21. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
F5	A7. 가맹점 위치 정보 변경	Tampering	해시, 전자서명
	A8. 소비자 위치 정보 변경	Tampering	해시, 전자서명
	A13. 다른 온-디맨드 서비스 업체로 위장	Spoofing	인증, 전자서명
	A20. 온-디맨드 서비스 업체 권한 탈취	Elevation of Privilege	최소한의 권한으로 실행
	A21. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
F6	A6. 차량 정보 변경	Tampering	해시, 전자서명
	A9. 도로 정보 변경	Tampering	해시, 전자서명
	A17. 차량 정보 유출	Information Disclosure	암호화, ACLs

	A19. 지상제어국 서비스 거부	Dos, Denial of Serivce	필터링, ACLs
	A21. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
F7	A7. 가맹점 위치 정보 변경	Tampering	해시, 전자서명
	A8. 소비자 위치 정보 변경	Tampering	해시, 전자서명
	A18. 지상제어국 서비스 거부	Dos, Denial of Service	필터링, ACLs
	A21. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
F8	A9. 도로 정보 변경	Tampering	해시, 전자서명
	A12. 차량 위치 정보 변경	Tampering	해시, 전자서명
	A15. 다른 차량으로 위장	Spoofing	인증, 전자서명
	A21. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
F9	A5. 소요 시간 정보 변경	Tampering	해시, 전자서명
	A14. 다른 온-디맨드 가맹점으로 위장	Spoofing	인증, 전자서명
	A21. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
F10	A6. 차량 정보 변경	Tampering	해시, 전자서명
	A15. 다른 차량으로 위장	Spoofing	인증, 전자서명
	A17. 차량 정보 유출	Information Disclosure	암호화, ACLs
	A21. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
F11	A10. 차량 상태 정보 변경	Tampering	해시, 전자서명
	A15. 다른 차량으로 위장	Spoofing	인증, 전자서명
	A21. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
F12	A10. 차량 상태 정보 변경	Tampering	해시, 전자서명
	A21. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
F13	A11. 차량 위치 정보 변경	Tampering	해시, 전자서명
	A15. 다른 차량으로 위장	Spoofing	인증, 전자서명
	A21. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그

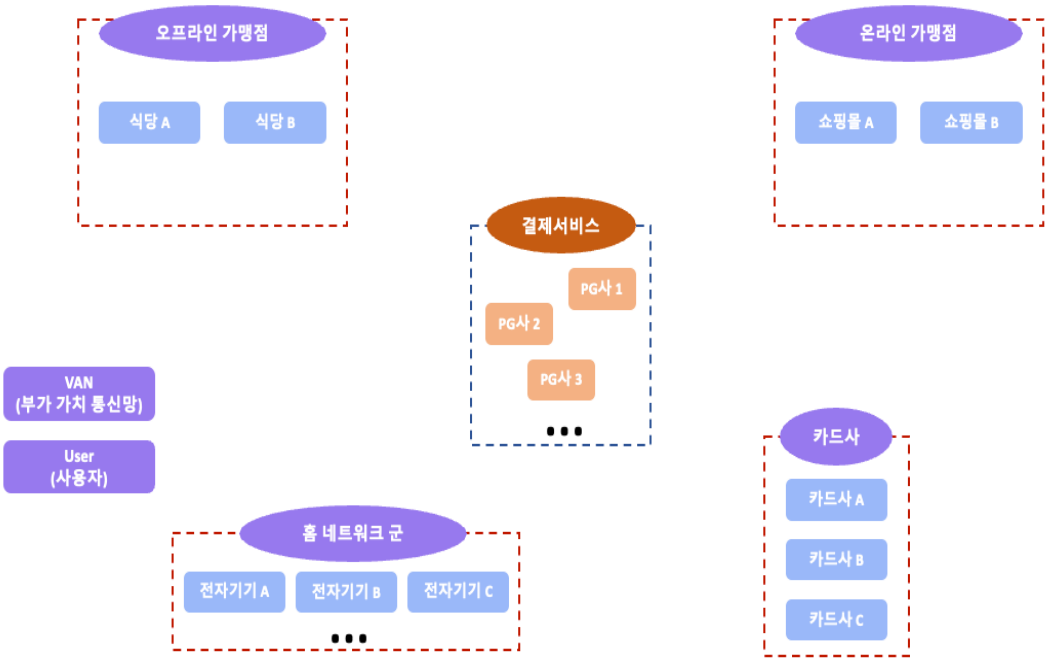
5. 고찰

이 과제를 수행하면서 가장 힘들었던 점은 당연히 3 번이었다. 1 번과 2 번은 자료 조사와 강의 시간 공부를 토대로 수행하면 되지만, 3 번은 자료 조사가 힘들었다. 우선 데이터 흐름표를 파악하는 것도 힘들었다. 아 우선 고찰 다음 페이지에 나오는 것들은 처음 주제 선정을 해서 했는데, 다시 보니 주제가 정해져 있어서 바꾸었다. 그래도 가장 관심 있는 시스템이어서 한 번 해보았던 내용을 첨부했다. 그리고 두 번째 과제 주제를 선정했던 가장 큰 이유는 간편 결제 시스템과 연관이 되어 있는 온-디맨드 서비스에 대해서 조사했다. 실제 온-디맨드 서비스가 뭔지 잘 몰랐었는데 이번에 자료 조사를 하면서 정확히 그 의미를 알게 되었다. 온-디맨드 서비스에 대한 자세한 데이터 흐름도가 없어 나와있는 자료를 토대로 데이터 흐름을 상상하고 과제를 수행했다. 그래서 두 번째 주제로 정한 게 과제로 제출하는 내용이다. 이 과제를 수행하면서 가장 힘들었던 점은 예를 들어 3-4 를 수행하다가 데이터 흐름에 뭔가가 추가되면 그림을 1 번부터 다시 수정작업 하는 것들이 힘들었다. 실제 완성되기 전까지 10 번 넘게 수정을 거쳤으며 이 과정에서 시간이 많이 지체되었다. 하지만 이 과정에서 어떤 정보들이 추가로 더 흘러 들어가는지 알게 되었고, 전반적인 중간고사 범위 전 내용을 파악할 수 있었다. 그리고 '간편 시스템' 같은 경우는 처음 했던 것인데 이 처음 한 것들이 두 번째(과제 제출 및 발표 자료) 과제물을 할 때 도움이 많이 되었다. 우선 객체와 다이어그램 그리는 법이 어느덧 익숙해져서 금방금방 해낼 수 있었다. 하지만 수정 작업은 마찬가지로 오래 걸렸다. 그리고 생각보다 취약점 형태가 많아서 시스템을 구성할 때 보안이 정말 중요한 것임을 알게 되었고 실제 백엔드 개발자 즉 서버 개발자를 희망하고 있는 상태인데 서버를 구축할 때 보안 사항도 생각하면서 해야겠다는 생각을 했다.

IV. 그 외

1. 서비스 대상 선정 및 설명

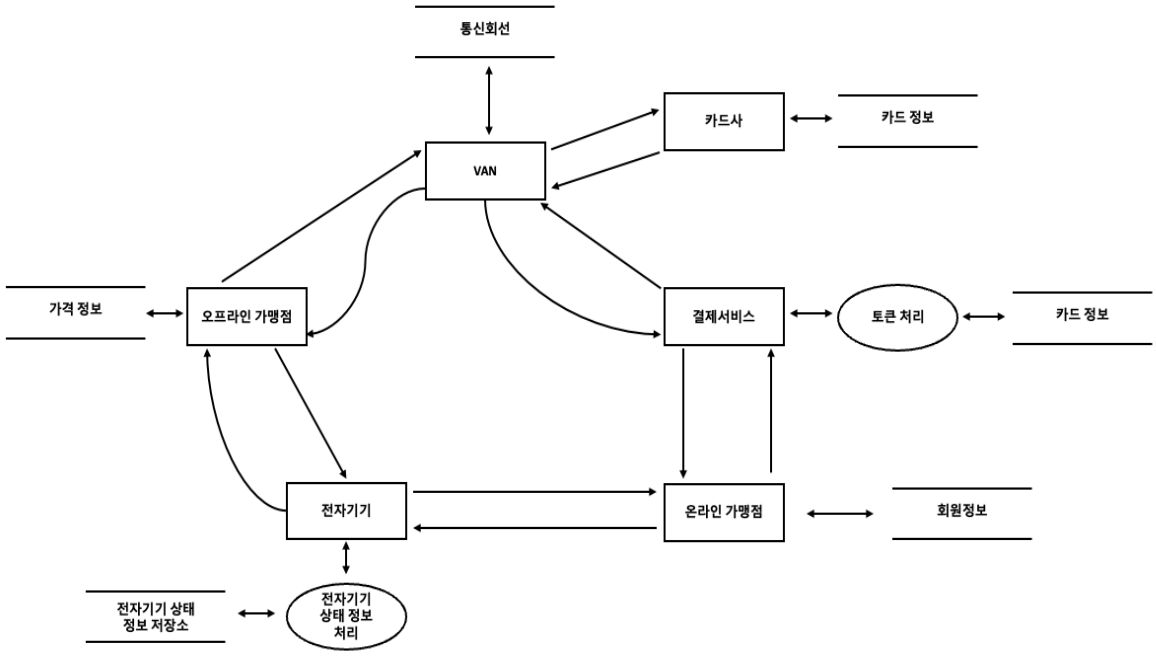
‘간편 결제 시스템’, ‘스마트 페이 시스템’
‘간편 결제 시스템’이란 간단한 방식으로 결제를 지원하는 시스템이다. 핀테크 기술의 일종이다. 일부 ‘스마트 페이’라는 표현을 사용하기도 한다. 공인인증서를 비롯하여 수많은 보안 프로그램을 통과해야만 결제가 가능한 시스템을 불필요한 과정을 생략하고 사전 인증 등을 통해 절차를 간소화해서 쉽게 결제할 수 있도록 내놓은 서비스다.



다음과 같이 객체를 나누었다. 간편 결제 시스템을 홈네트워크를 통해 이용하는 유저가 있다. 그리고 VAN(부가 가치 통신망)을 이용하는 결제서비스들이 있다. 간편 결제 시스템을 이용할 수 있는 기관으로는 온라인 가맹점과, 오프라인 가맹점으로 나누었다. 그리고 결제 정보를 처리하는 기관인 카드사가 있다.

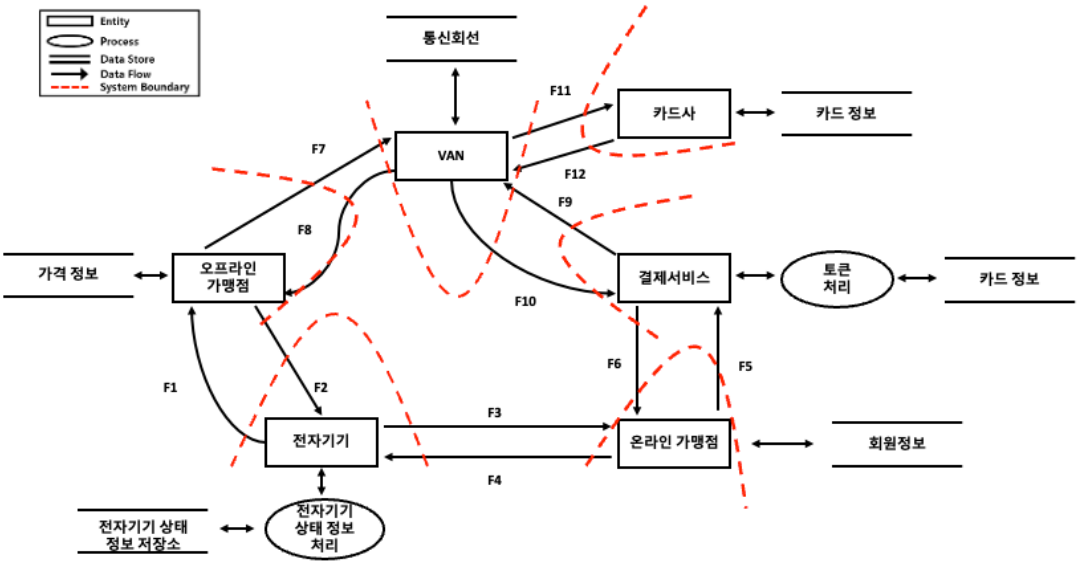
2. DFD 그리기

Level 0



전체적인 흐름도는 다음과 같다. 사용자가 전자기기를 통해 오프라인 가맹점과 온라인 가맹점을 통해 물품을 구입한다. 그럼 전자기기에 저장되어 있는 정보들이 가맹점을 통해 결제가 진행된다. 오프라인 가맹점 같은 경우는 바로 VAN 과 연결이 되어 있어 카드사와 연결하여 내장 되어있는 NFC/USIM 에 카드 정보와 카드사에 저장되어 있는 카드 정보가 일치한 지 확인하고 결제가 진행된다. 온라인 가맹점은 회원 정보와 NFC/USIM 에 저장되어 있는 정보들은 온라인 가맹점이 받은 후 저장 되어 있는 NFC/USIM 같은지 확인을 하고 결제 서비스를 통해 VAN 과 연결 된다. 결제 서비스는 회원 정보를 받아 토큰을 처리하고 토큰을 다시 받아 결제서비스 내부 서버에서 카드 정보를 가져온다. 카드 정보를 가져온 후 VAN 을 통해 카드사랑 연결이 되고 카드사에 연결되어 있는 카드 정보와 결제서비스에서 가져온 카드 정보가 같은지 확인을 하고 결제가 진행된다.

Level 1



No.	Data Flow	송신	수신
F1	NFC/USIM /카드 정보	전자기기	오프라인 가맹점
F2	결제 정보	오프라인 가맹점	전자기기
F3	회원 정보/ NFC/USIM	전자기기	온라인 가맹점
F4	결제 정보	온라인 가맹점	전자기기
F5	결제 정보	온라인 가맹점	결제서비스
F6	결제 정보	결제서비스	온라인 가맹점
F7	결제 정보/카드 정보	오프라인 가맹점	VAN
F8	결제 정보	VAN	오프라인 가맹점
F9	결제 정보/카드 정보	결제서비스	VAN
F10	결제 정보	VAN	결제서비스
F11	결제 정보/카드 정보	VAN	카드사
F12	결제 정보	카드사	VAN

Level1 은 Level0 에서 바운더리 구간과 실제 데이터 흐름에서 어떤 정보들이 전달되는지 표기했다. 또한 알아보기 쉽게 표를 통해 정리했다.

3. 위협 식별하기

No.	위협
A1	NFC/USIM 정보 변경
A2	결제 정보 변경
A3	회원 정보 변경
A4	카드 정보 변경
A5	다른 온라인 가맹점으로 위장
A6	다른 전자기기로 위장
A7	다른 결제서비스로 위장
A8	다른 VAN 으로 위장
A9	다른 카드사로 위장
A10	정보 전송 행위의 부인
A11	회원 정보 유출
A12	카드 정보 유출
A13	온라인 가맹점 권한 탈취
A14	결제서비스 권한 탈취
A15	VAN 권한 탈취
A16	카드사 권한 탈취
A17	VAN 서비스 거부
A18	결제서비스 서비스 거부
A19	온라인 가맹점 서비스 거부
A20	카드사 서비스 거부

4. 식별된 위협을 STRIDE 에 매칭 시키기

No.	위협	STRIDE	방어 기법
F1	A1. NFC/USIM 정보 변경	Tampering	해시, 전자서명
	A4. 카드 정보 변경	Tampering	해시, 전자서명
	A6. 다른 전자기기로 위장	Spoofing	인증, 전자서명
	A10. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A12. 카드 정보 유출	Information Disclosure	암호화, ACIS
F2	A2. 결제 정보 변경	Tampering	해시, 전자서명
	A10. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A1. NFC/USIM 정보 변경	Tampering	해시, 전자서명
	A3. 회원 정보 변경	Tampering	해시, 전자서명

F3	A6. 다른 전자기기로 위장	Spoofing	인증, 전자서명
	A10. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A11. 회원 정보 유출	Information Disclosure	해시, 인증
F4	A2. 결제 정보 변경	Tampering	해시, 전자서명
	A5. 다른 온라인 가맹점으로 위장	Spoofing	인증, 전자서명
	A10. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A13. 온라인 가맹점 권한 탈취	Elevation of Privilege	최소한의 권한으로 실행
	A19. 온라인 가맹점 서비스 거부	Dos	필터링, ACLs
F5	A2. 결제 정보 변경	Tampering	해시, 전자서명
	A5. 다른 온라인 가맹점으로 위장	Spoofing	인증, 전자서명
	A10. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A13. 온라인 가맹점 권한 탈취	Elevation of Privilege	최소한의 권한으로 실행
F6	A2. 결제 정보 변경	Tampering	해시, 전자서명
	A7. 다른 결제서비스로 위장	Spoofing	인증, 전자서명
	A10. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A14. 결제서비스 권한 탈취	Elevation of Privilege	최소한의 권한으로 실행
	A18. 결제서비스 서비스 거부	Dos	필터링, ACLs
F7	A2. 결제 정보 변경	Tampering	해시, 전자서명
	A4. 카드 정보 변경	Tampering	해시, 전자서명
	A10. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A12. 카드 정보 유출	Information Disclosure	암호화, ACIS
F8	A2. 결제 정보 변경	Tampering	해시, 전자서명
	A8. 다른 VAN 으로 위장	Spoofing	인증, 전자서명
	A10. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A15. VAN 권한 탈취	Elevation of Privilege	최소한의 권한으로 실행
	A17. VAN 서비스 거부	Dos	필터링, ACLs
F9	A2. 결제 정보 변경	Tampering	해시, 전자서명
	A4. 카드 정보 변경	Tampering	해시, 전자서명
	A7. 다른 결제서비스로 위장	Spoofing	인증, 전자서명
	A10. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A12. 카드 정보 유출	Information Disclosure	암호화, ACIS

	A14. 결제서비스 권한 탈취	Elevation of Privilege	최소한의 권한으로 실행
F10	A2. 결제 정보 변경	Tampering	해시, 전자서명
	A8. 다른 VAN 으로 위장	Spoofing	인증, 전자서명
	A10. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A15. VAN 권한 탈취	Elevation of Privilege	최소한의 권한으로 실행
	A17. VAN 서비스 거부	Dos	필터링, ACLs
F11	A2. 결제 정보 변경	Tampering	해시, 전자서명
	A4. 카드 정보 변경	Tampering	해시, 전자서명
	A8. 다른 VAN 으로 위장	Spoofing	인증, 전자서명
	A10. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A15. VAN 권한 탈취	Elevation of Privilege	최소한의 권한으로 실행
F12	A2. 결제 정보 변경	Tampering	해시, 전자서명
	A9. 다른 카드사로 위장	Spoofing	인증, 전자서명
	A10. 정보 전송 행위의 부인	Repudiation	전자서명, 감사 로그
	A16. 카드사 권한 탈취	Elevation of Privilege	최소한의 권한으로 실행
	A20. 카드사 서비스 거부	Dos	카드사 서비스 거부