REPORT

제 목 : 중간고사대체과제 보고서

과 목 명 : 시큐어코딩
담당교수 : 우사무엘교수님
이 름 : 조 정 민
학 번 : 32164420

단국대학교
Dankook University

목차

과제1 [C-ITS STRIDE 수행]

1. F2 ~ F8에 대한 STRIDE를 수행하라

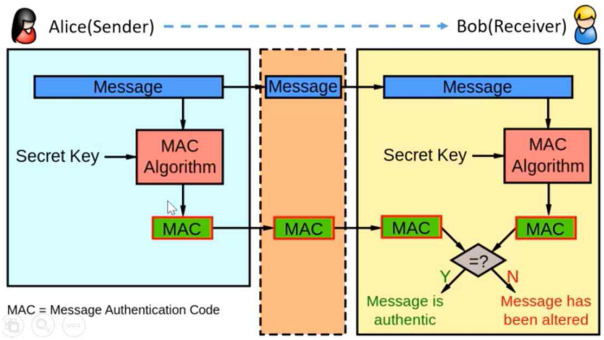
Data Flow	위협	STRIDE	방어 기법
F1	A1. 다른 차량으로 위장	Spoofing	인증, 전자서명
	A2. 차량 주행 정보 변경	Tampering	메시지 인증, 전자서명
	A3. 정보 전송 행위의 부인	Repudiation	전자서명
F2	A3. 정보 전송 행위의 부인	Repudiation	감사로그, 전자서명
	A4. 다른 노변기기로 위장	Spoofing	인증, 전자서명
	A5. 도로 교통 정보 변경	Tampering	메시지 인증, 해시, 전자서명
	A8. 센서 정보 변경	Tampering	메시지 인증, 해시, 전자서명
F3	A1. 다른 차량으로 위장	Spoofing	인증, 전자서명
	A2. 차량 주행 정보 변경	Tampering	메시지 인증, 해시, 전자서명
	A3. 정보 전송 행위의 부인	Repudiation	감사로그, 전자서명
F4	A2. 차량 주행 정보 변경	Tampering	메시지 인증, 해시, 전자서명
	A3. 정보 전송 행위의 부인	Repudiation	감사로그, 전자서명
	A4. 다른 노변기기로 위장	Spoofing	인증, 전자서명
F5	A3. 정보 전송 행위의 부인	Repudiation	감사로그, 전자서명
	A5. 도로 교통 정보 변경	Tampering	메시지 인증, 해시, 전자서명
	A6. 다른 교통관리센터로 위장	Spoofing	인증, 전자서명
F6	A3. 정보 전송 행위의 부인	Repudiation	감사로그, 전자서명
	A7. 다른 지원 시스템으로 위장	Spoofing	인증, 전자서명
	A8. 센서 정보 변경	Tampering	메시지 인증, 해시, 전자서명
F7	A3. 정보 전송 행위의 부인	Repudiation	감사로그, 전자서명
	A7. 다른 지원 시스템으로 위장	Spoofing	인증, 전자서명
	A8. 센서 정보 변경	Tampering	메시지 인증, 해시, 전자서명
F8	A3. 정보 전송 행위의 부인	Repudiation	감사로그, 전자서명
	A5. 도로 교통 정보 변경	Tampering	메시지 인증, 해시, 전자서명
	A6. 다른 교통관리센터로 위장	Spoofing	인증, 전자서명

2. F2 ~ F8에 해당하는 위협을 선정한 이유를 설명하라

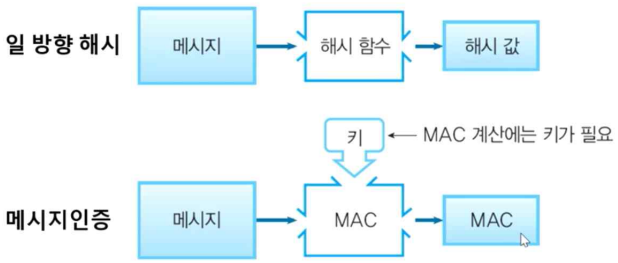
Data Flow	위협	선정 이유
F1	A1. 다른 차량으로 위장	/
	A2. 차량 주행 정보 변경	/
	A3. 정보 전송 행위의 부인	/
F2	A3. 정보 전송 행위의 부인	도로교통/센서정보 전송행위 자체를 부정할 수 있음
	A4. 다른 노변기기로 위장	정보를 주고 받는 주체로 위장할 수 있음
	A5. 도로 교통 정보 변경	송신자(RSU)에서 전송하는 도로교통정보를 변경하여 전송할 수 있음
	A8. 센서 정보 변경	송신자(RSU)에서 전송하는 센서정보를 변경하여 전송할 수 있음
F3	A1. 다른 차량으로 위장	정보를 주고 받는 주체로 위장할 수 있음
	A2. 차량 주행 정보 변경	송신자(차량)에서 전송하는 차량주행정보를 변경하여 전송할 수 있음
	A3. 정보 전송 행위의 부인	차량주행정보 전송행위 자체를 부정할 수 있음
F4	A2. 차량 주행 정보 변경	송신자(RSU)에서 수신자(교통관리센터)로 전송하는 차량주행정보를 변경하여 전송할 수 있음
	A3. 정보 전송 행위의 부인	차량주행정보 전송행위 자체를 부정할 수 있음
	A4. 다른 노변기기로 위장	정보를 주고 받는 주체로 위장할 수 있음
F5	A3. 정보 전송 행위의 부인	도로교통정보 전송행위 자체를 부정할 수 있음
	A5. 도로 교통 정보 변경	송신자(교통관리센터)에서 전송하는 도로교통정보를 변경하여 전송할 수 있음
	A6. 다른 교통관리센터로 위장	정보를 주고 받는 주체로 위장할 수 있음
F6	A3. 정보 전송 행위의 부인	센서정보 전송행위 자체를 부정할 수 있음
	A7. 다른 지원 시스템으로 위장	정보를 주고 받는 주체로 위장할 수 있음
	A8. 센서 정보 변경	송신자(지원시스템)에서 전송하는 센서정보를 변경하여 전송할 수 있음
F7	A3. 정보 전송 행위의 부인	센서정보 전송행위 자체를 부정할 수 있음
	A7. 다른 지원 시스템으로 위장	정보를 주고 받는 주체로 위장할 수 있음
	A8. 센서 정보 변경	송신자(지원시스템)에서 전송하는 센서정보를 변경하여 전송할 수 있음
F8	A3. 정보 전송 행위의 부인	도로교통정보 전송행위 자체를 부정할 수 있음
	A5. 도로 교통 정보 변경	송신자(RSU)에서 전송하는 센서정보를 변경하여 전송할 수 있음
	A6. 다른 교통관리센터로 위장	정보를 주고 받는 주체로 위장할 수 있음

3. Module 2-3 학습 내용을 활용해 방어 기법에 대해 간단히 논하라

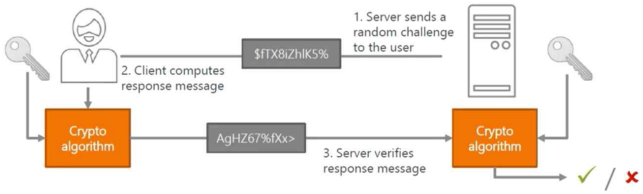
C-ITS에서 식별된 위협에 매칭된 STRIDE는 'Spoofing', 'Tampering', 'Repudiation'이었다. 이 요소들을 방어하기 위한 방어 기법으로는 '메시지 인증', '해시', '인증', '감사로그', '전자서명' 등으로 생각해보았다.



'메시지 인증'은 데이터 무결성을 보장하기 위한 메시지 인증 코드 생성에 사용된다. 송신자와 수신자가 서로 통신을 하려할 때, 송신자가 보내려는 정보를 능동적 공격자가 위조, 변조하는 행위를 방어할 수 있다. 송신자가 보내려는 원본 데이터와 MAC(Message Authentication Code)가 있다. MAC알고리즘과 비밀키를 통해서 MAC을 추출할 수 있다. 송신자는 원본 데이터를 MAC과 함께 전송을 해주면 수신자는 송신자와 함께 나누어 가진 대칭키를 통해서 MAC알고리즘을 수행하고 추출된 MAC을 송신자가 보낸 MAC과 비교하여 동일한지 아닌지 확인할 수 있다. 전송 과정에서 능동적 공격자가 데이터를 위조, 변조를 하였다면 수신자 측에서 수행한 MAC알고리즘을 통해 추출된 MAC과 송신자가 전송한 MAC이 일치하지 않을 것이다. 이를 통해, 데이터의 무결성을 보장하기 위한 행위를 할 수 있다.



'일방향해시'는 위 과정에서 MAC알고리즘을 통해 MAC을 추출하는 것이 아니다. '메시지 인증' 과정은 MAC알고리즘을 수행해야 하고 이에 필요한 비밀키도 있어야 하지만 '일방향해시'는 MAC알고리즘 수행을 할 필요가 없이 해시 함수를 가지고 해시 값을 추출하기 때문에 비밀키를 사용하지 않아도 된다.



'사용자인증'은 클라이언트가 서버에 자신임을 인증하고 싶을 때 클라이언트 측에서 서버 측으로 비밀키를 전송한다. 서버에는 이미 클라이언트의 비밀키가 존재하기 때문에 클라이언트에서 보낸 비밀키와 기존의 비밀키를 매칭시켜 인증을 할 수 있다. 하지만 이런 방식은

공격자가 통신회선을 도청해 키를 획득할 수 있고, 비밀키를 사용할 수 있기에 안전하지 않다. '안전한 사용자 인증'은 서버에서 랜덤한 값을 클라이언트에 전송한다. 클라이언트는 랜덤 값과 비밀키를 이용하여 응답 값을 만들고 이 응답값을 서버에 전송한다. 서버는 응답값을 풀어 검증을 할 수 있다. 이를 통해 보다 더욱 안전한 사용자 인증 방식을 사용할 수 있다.

'감사로그'는 송신자가 수신자 측에 액세스한 후 기록을 저장하여 일련의 기록을 조사하는 것이다. 감사 로그는 특정 서버의 로그 디렉터리에 존재한다. 보안을 위한 사용자(송신자)가 있을 경우, 감사 로그를 이용해 언제, 어떤 활동을 했는 지를 확인할 수 있다. 부인 방지를 위해 모든 기관은 로그를 기록하고 저장 및 검토해야 한다.

'전자서명'은 데이터와 데이터를 생성한 사람과의 인증을 의미하며 데이터(메시지)에 전자적인 서명을 하는 것을 의미한다. 이는 사용자(송신자)와 데이터(메시지)에 대한 인증 기능을 포함한다. 송신자는 서명 알고리즘을 이용하여 메시지에 서명을 하고 서명은 수신자의 검증 알고리즘에 의해서 검증된다. '전자서명'의 구조로는 RSA, EL:Gamal, Schnorr, DSS, ECDSA 등이 있다. '전자서명'을 통해서 데이터 위조, 변조 불가, 서명자 인증, 부인방지 등의 기능을 활용할 수 있다.

과제2 [STRIDE 설명]

1. MS-SDL에서 위협 모델링에 사용하는 STRIDE의 정의와 특징에 대해 보고서를 작성하라

STRIDE는 Microsoft사에서 개발한 보안 위협 모델링 방법이다. STRIDE는 인증(Authentication), 무결성(Integrity), 부인 방지(Non-repudiation), 기밀성(Confidentiality), 가용성(Availability), 권한 부여(Authorization)와 같은 보안 속성을 고려하고, DFD(Data Flow Diagram)의 개체, 프로세스 등에 존재하는 위협을 식별한다.

STRIDE 단계에서는 구성원, 개발자, 테스터, 분석가, 설계자 등 다양한 분야의 구성원들이 모여서 위협 모델링 모임을 구성해야 한다. 이 모임의 목표는 위협을 해결하기 위한 것이 아닌 최대한 많은 위협들을 사전에 도출하기 위함이다. 이 단계에서 시나리오에 대한 DFD (Data Flow Diagram)를 검토하여 신뢰경제, 진입점, 최종위치 사이의 데이터 흐름을 참조하여 위협을 도출할 수 있다.

STRIDE의 위협 분류와 정의는 다음 표와 같다.

STRIDE 위협	관련 보안 속성	위협 정의
위장 (Spoofing identity)	인증 (Authentication)	거짓된 identity를 이용해 시스템 접근 권한을 취득하는 행위
데이터 변조 (Tampering with data)	무결성 (Integrity)	불법적으로 보호 대상 데이터를 수정하는 행위
부인 (Repudiation)	부인 방지 (Non-repudiation)	사용자가 자신이 수행한 특정 액션이나 트랜잭션을 부인하는 행위
정보 유출 (Information disclosure)	기밀성 (Confidentiality)	유출되지 말아야하는 개인정보나 중요 데이터가 외부로 유출되는 위협
서비스 거부 (Dos, Denial of Service)	가용성 (Availability)	시스템 또는 애플리케이션이 정상적으로 수행되지 않도록 방해하는 행위
권한 상승 (Elevation of privilege)	권한 부여 (Authorization)	비정상적인 방법을 사용하여 더 많은 권한 획득

위 여섯 가지 위협 범주를 확인하면 시스템의 취약성 및 잠재적인 공격 가능성을 식별하는 데 도움이 된다.

Spoofing(위장)은 권한이 부여되지 않은 상태에서 사용자 또는 프로세스를 가장하는 것이다. 가장 단순한 위장 공격의 예로는 다른 사용자의 자격 증명을 입력하는 것이다. 일반적으로 엄격한 인증을 사용하면 위장 공격을 방해할 수 있다. 비공개 정보에 대해 액세스를 요청하는 사용자가 있다면 본인이 확실한지 항상 확인을 할 필요가 있다.

Tampering(데이터변조)란 권한이 부여되지 않은 상태에서 리소스를 변경하거나 삭제하는 상황을 말한다. 데이터변조의 예로는 악의적인 사용자가 사이트에 침입한 후 파일을 변경하

여 웹페이지를 훼손하는 행위가 될 수 있다. 데이터 훼손을 막을 수 있는 기본적인 방법은 응용프로그램을 가능한 최소한의 권한으로 실행하는 것이며, 윈도우 환경에서는 windows 보안을 사용하여 파일, 디렉토리 및 기타 윈도우 리소스를 잠그는 것이다.

Repudiation(부인)은 트랜잭션과 관련된 보안 주체가 증거가 남지 않도록 트랜잭션을 수행하는 것을 말한다. 간단히 말해서, 악의적인 활동 이후에 해당 활동에 대해 부인하는 것을 뜻한다. 엄격한 인증을 사용하면 부인 공격으로부터 보호할 수 있다. 또한 windows 로깅 기능을 사용하면 서버에서 발생하는 모든 활동에 감사내역을 추적할 수 있다.

Information disclosure(정보유출)은 개인정보를 도용하거나 노출시키는 행위, 또는 외부에 노출되면 안되는 중요 정보가 외부로 유출되는 위협을 뜻한다. 정보유출의 일반적인 예는 서버에 있는 임의의 파일 또는 리소스에 불법적으로 접근하여 데이터를 유출시키는 행위이다. 정보유출로부터 데이터를 보호하는 최상의 방법은 유출될 정보를 전혀 보관하지 않는 것이다. 예를 들어, 패스워드를 저장하지 않거나 패스워드의 해시 값만 저장하는 것이다.

Denial of service(서비스 거부)는 특정한 네트워크나 웹 리소스에 합법적인 유저가 접근하지 못하도록 방해하는 행위이다. 전형적인 공격방법으로는 막대한 양의 트래픽을 발생시켜 특정 대상에 과부하를 주거나 악의적인 요청을 보내 해당 리소스의 오작동을 유발시키는 공격 등이 있다. 악의적인 의도를 가진 것으로 판명된 사용자나 IP주소의 접근을 거부하여 이를 방어할 수 있다.

Elevation of privilege(권한 상승)은 비정상적인 방법을 사용하여 정상적으로 할당된 권한보다 더 많은 권한을 획득하는 것이다. 예를 들어, 악의적인 사용자가 권한 높이기 공격에 성공하는 경우, 웹서버에 대한 관리 권한을 얻어 서버 기능을 제어할 뿐 아니라 서버에 있는 모든 데이터에 대한 접근 권한을 가질 수 있을 것이다. 권한 상승으로부터 보호하려면 응용프로그램을 되도록 최소 권한으로 실행해야 한다.

다양한 위협을 식별하였다면 각 위협을 완화할 대응 방안을 마련해야 한다. 여섯 가지 위협에 대응되는 대표적인 대응방안은 다음과 같다. 위장은 인증, 데이터 변조는 무결성, 부인은 부인방지, 정보 유출은 기밀성, 서비스 거부는 가용성, 권한 상승은 인가 등 여섯 가지 기술로 대응할 수 있다. 이 여섯 가지 기술은 추상적이며 대응 기법의 분야만 나타내고 있다. 구체적인 대응 기술은 매우 다양할 수 있다.

2. STRIDE가 의미하는 위협의 실제 사례를 찾아 보고서를 작성하라

싱가포르 CCTV 해킹 사건	
위협	S(Spoofing identity) - 위장
설명	해당 사고사례는 CCTV가 네트워크에 연결되어 있고, 유무선 공유기 및 IP 카메라 접속만 한다면 CCTV 네트워크에 접속할 수 있다. 해당 IP주소로 위장만 한다면 해킹이 가능하다. 해당 사건에서는 저장된 CCTV 영상을 유출시킨 것 뿐만 아니라 실시간으로 CCTV 영상을 볼 수 있었다. 공격자가 해당 카메라의 IP주소로 위장하여 IP 카메라에 접속하는 과정을 통해 공격이 이루어졌다. 이러한 공격형태를 분석해 본다면, IP Spoofing 공격의 한 종류로 판단된다.

뽐뿌, 아시아나, KFC 개인정보 유출 사건	
위협	T(Tampering with data) - 데이터 변조
설명	웹 취약점을 이용하였고, sql 인젝션을 통해 개인정보가 유출되었다. DB 서버 중 일부 서버에서만 로그를 저장하는 등 데이터베이스의 데이터 변조를 통한 해킹 사례이다. 공격자가 보안상의 취약점을 이용하여 임의의 SQL 문을 주입하고 실행되게 하여 데이터베이스가 비정상적인 동작을 하도록 조작하는 과정을 통해 공격이 이루어졌다. 이는 Tampering with data(데이터변조) 공격의 한 종류로 판단된다.

여기어때 해킹 사건	
위협	I(Information disclosure) - 정보 유출
설명	여기어때 어플리케이션을 서비스하는 위드이노베이션의 해킹으로 회원 91만명의 숙박 정보 등이 유출되었다. 관리자 고유 식별값을 탈취하여 외부에 노출된 서비스 관리 웹페이지를 관리자 권한으로 우회 접속하여 DB에 접속해 SQL 인젝션을 통하여 각종 정보를 유출시켰다. 이러한 공격형태를 보았을 때, 이는 Information disclosure(정보 유출) 공격의 한 종류로 판단된다.

2013년 6월 25일 사이버 테러	
위협	D(Dos, Denial of Service) - 서비스 거부
설명	해당 공격은 2013년 6월 25일, DNS 증폭 DDoS 공격을 이용하여 청와대 홈페이지 및 정부 기관의 홈페이지를 공격한 사례이다. 기존에 알려져 있지 않은 악성파일과 보안취약점을 이용해 주요 웹사이트에 침투하여 공격으로 수행했다. 공격자는 내부 침투 이후, 장기간 분석으로 각 피해 기관의 내부 인프라를 이용한 공격을 수행했다. 이는 서버를 다운시키기 위한 시스템 부팅영역 파괴, 시스템의 주요 파일 삭제 등 홈페이지의 주요기능을 마비시키는 공격형태였으며, 이는 Dos 공격의 한 종류로 판단된다.

캐피탈 원 고객 정보 유출	
위협	E(Elavation of privilege) - 권한 상승
설명	2019년 캐피탈 원(금융지주회사)이 해킹을 당해 1억명에 이르는 고객정보가 유출됐다. 고객의 이름, 주소, 전화번호 등 신상 정보와 신용점수, 신용한도 등의 금융 정보까지 유출되었다. 캐피털 원에서 사용되는 고객 개인정보 데이터는 아마존 클라우드인 ASW에 저장된 것이었다. 공격자는 open-source WAF의 설정이 잘못된 것을 이용하여, AWS 상에 저장되어 있는 캐피털 원의 고객 데이터에 접근하였다. 공격자는 SSRF 취약점을 이용하여 메타데이터 서비스에 요청을 보내 데이터 저장소에 액세스할 수 있는 임시 자격증명을 획득한 후, 저장된 파일들을 이와 같은 공격 형태를 본다면, Elavation of privilege(권한 상승) 공격의 한 종류로 판단된다.

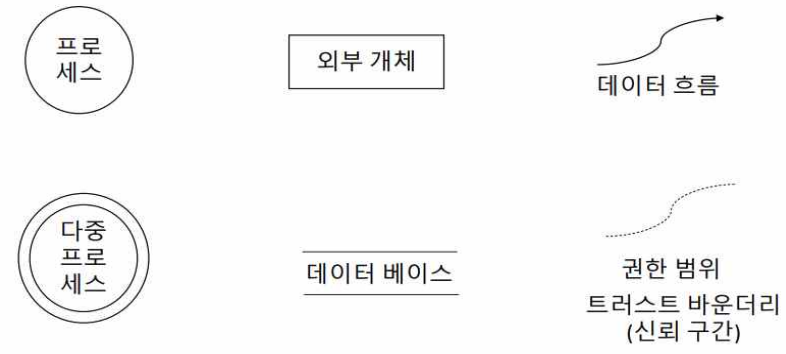
과제3 [위협 모델링 실습]

1. 서비스 대상 – 자율주행 버스

<출저 - 한국타이어 공식 블로그 Driving Emotion>

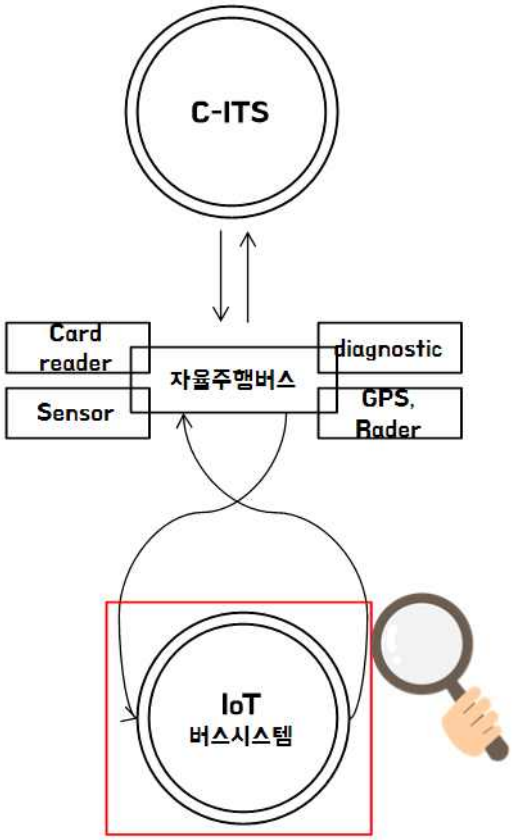
자율 주행은 향후 모빌리티 혁신에 있어 가장 핵심적인 기술 중 하나이다. 이미 우리가 일상에서 만나고 있는 차 중 상당 수는 어느 정도 스스로 주행할 수 있는 단계에 이르렀다. 이러한 흐름에 발맞춰 국내에서도 운전석이 없는 완전 자율 주행 버스를 시험 검토 중이다. 자율 주행 버스의 상용화는 시민들의 이동에 있어 큰 변화를 불러일으킬 것이다. 자율 주행 버스는 돌발 상황에서 사람과 달리 위험을 더 빨리 인지하고 대처하여, 사고를 막거나 줄여주는 데 큰 역할을 할 수 있다. 또한 시스템에 의해 움직이는 자율 주행 버스는 다른 차량 및 전체적인 도로 교통 시스템과 데이터를 주고 받으며 최적의 움직임을 구현하는 형태로 진화할 것이다. 이에 따라 안전한 이동이 가능해짐은 물론 전반적인 교통 체증도 줄어들어 더욱 쾌적한 환경에서 대중교통을 이용할 수 있는 시대가 올 것이다. 세종시에서는 올해 상반기가 지나기 전 일반 시민도 자율주행버스에 탈 수 있는 '간선급행버스체계(BRT)' 대중교통 서비스 실증에 나선다고 발표한 바가 있다. 이러한 상황에서 이번 대체과제의 위협 모델링 실습의 대상으로 자율주행버스를 선정하며 매우 흥미로울 것이라 생각했다.

DFD(Data Flow Diagram)의 표현 방법은 다음과 같다.



2. DFD(Data Flow Diagram)

Lv.0

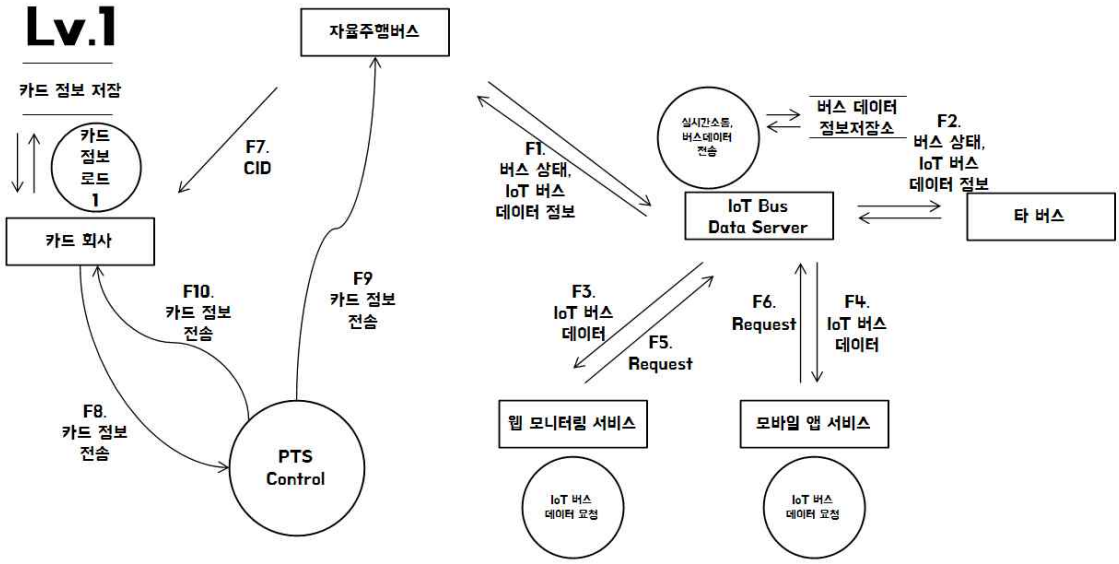


레벨 0의 Data Flow Diagram이다. 자율주행버스의 차량 내외부에 대한 DFD를 그리는 것보다는 자율주행버스 운행 서비스에 대한 DFD를 그려야겠다는 생각이 들었다. 자율주행버스는 자율주행이 제일 주가 되는 기본 기능이기에 C-ITS가 기본적으로 운영이 되어야 한다. 추가적으로 무인으로 운행되는 버스라는 특징이 제일 크다 보니 IoT와 관련된 버스시스템도 중요한 역할이라 생각을 했다. C-ITS에 대해서는 7주차 강의에서 다루었기 때문에 이번 과제를 하면서 C-ITS에 대한 분석을 다시 한 번 하는 것보다는 다른 다중 프로세스를 분석하는 것이 위협 모델링을 다방면에서 학습하는 데에 유익할 것이라 생각했다.

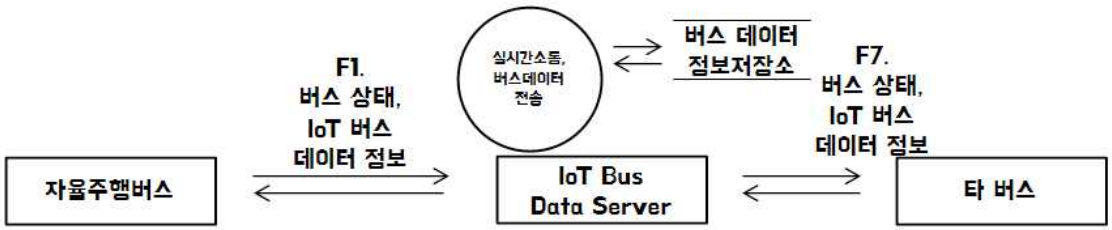
레벨 0에서 구상해본 큰 틀의 데이터 흐름은 다음과 같이 진행될 것이라 생각했다.

- 카드 리더기를 통한(결제) 데이터 흐름
- 차량 실내에 존재하는 센서에 관한 데이터 흐름
- 차량 자가 진단을 위한 diagnostic에 관한 데이터 흐름
- 차량 위치를 관리하기 위한 GPS와 Rader에 관한 데이터 흐름

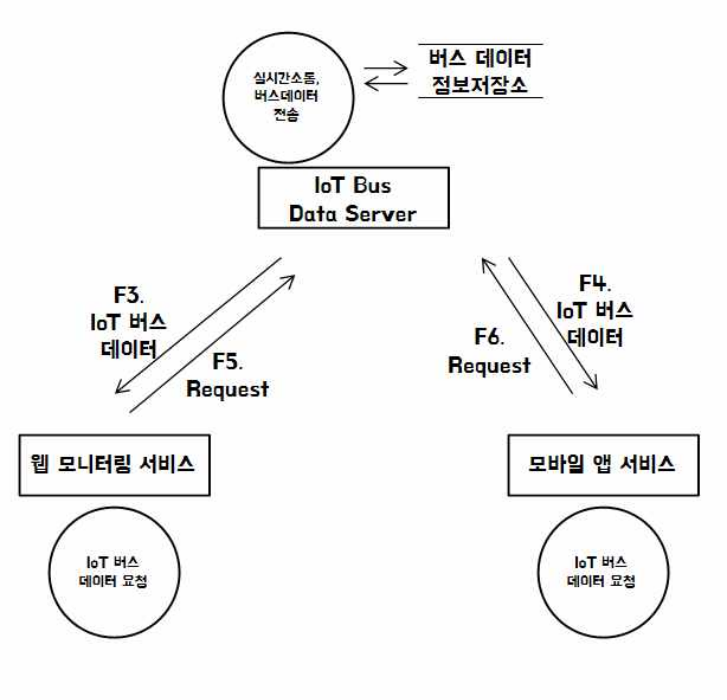
다음으로 알아볼 것은 IoT 버스시스템의 분석 내용이다.



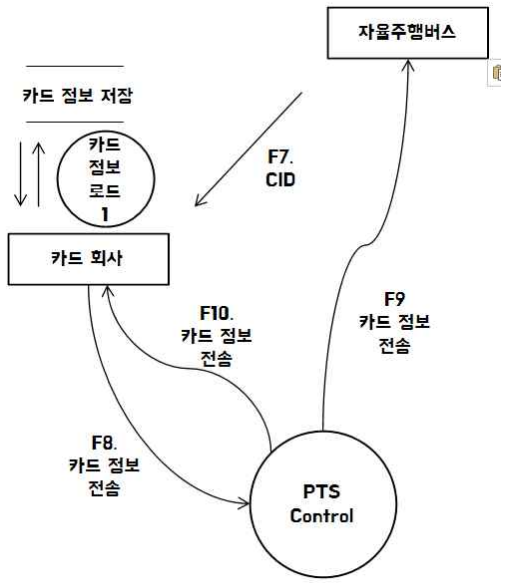
레벨 1의 Data Flow Diagram이다. IoT 버스시스템의 데이터 흐름을 위와 같이 표현해봤다. 이 부분을 크게 두 가지로 나눠볼 수 있는데 첫 번째는 자율주행버스와 IoT Bus Data Server와의 통신, 두 번째로는 카드 결제를 위한 프로세스이다.



우선 IoT Bus Data Server는 자율주행을 운행하고 있는 버스와 다른 버스와의 통신을 주로 한다. 이 통신에서는 버스의 상태나 버스 실내의 센서를 통해 수집된 데이터를 Request/Response한다. IoT Bus Dats에 들어온 이와 같은 데이터는 버스 데이터 저장소에 저장이 되고, 각 버스와의 실시간 소통으로 교류가 될 수 있다.



추가적으로 IoT Bus Data Server에서는 회사나 승객들의 웹/어플리케이션에 버스의 주행정보가 표시될 수 있도록 웹 모니터링 서비스, 모바일 앱 서비스가 데이터를 요청하면 응답으로 IoT 버스 데이터를 보낼 수 있다.



다음은, 카드 결제와 관련된 부분이다. 카드 리더기에 입력된 카드의 CID를 카드 회사에 전송한다. 카드 회사에서는 CIRD를 인덱싱하여 해당 카드의 잔액, 탑승 단말기, 승/하차, 태그 시간, 환승 상태 정보 등을 로드하여 카드 정보 저장소에 저장을 한다. PTS 컨트롤 프로세스에 이와 같은 카드 정보 데이터를 전송하여 결제를 한다. 업데이트 된 정보를 자율주행버스 측으로 전송하여 자율주행버스 측에서는 이를 기록 및 출력한다.

3. 위험 식별하기

레벨 1 Data Flow Diagram에서 식별된 위협은 다음과 같다.

No.	위협
A1	다른 버스로 위장
A2	IoT 버스 데이터 정보 변경
A3	정보 전송 행위의 부인
A4	다른 모바일 앱 서비스로 위장
A5	다른 웹 모니터링 서비스로 위장
A6	카드 정보 변경
A7	CID 정보 변경
A8	정보 요청 행위의 부인
A9	카드 정보 유출
A10	다른 카드 회사로 위장
A11	다른 IoT Bus Data Server로 위장
A12	악성 프로그램 배포 및 서비스 마비

각 개체로부터 발생할 수 있는 위협은 위장이다. 모든 개체가 다른 개체로 위장할 수 있다는 위협을 가질 수 있다. 개체 별로 정보를 주고 받는 과정에서도 위협은 존재한다. 주고 받는 정보를 요청하거나 전송하는 행위 자체를 부인할 수 있는 위협이다. 또한 저장된 정보를 변경하거나 전송하는 정보를 중간에 변경할 수 있는 위협도 존재하고, 카드 결제 부분에서는 카드 정보가 유출될 수 있는 위협이 존재한다.

4. 식별된 위협을 STRIDE에 매칭시키기

Data Flow	위협	STRIDE
F1	A1. 다른 버스로 위장	Spoofing
	A2. IoT 버스 데이터 정보 변경	Tampering
	A3. 정보 전송 행위의 부인	Repudiation
	A11. 다른 IoT Bus Data Server로 위장	Spoofing
F2	A1. 다른 버스로 위장	Spoofing
	A2. IoT 버스 데이터 정보 변경	Tampering
	A3. 정보 전송 행위의 부인	Repudiation
	A11. 다른 IoT Bus Data Server로 위장	Spoofing
F3	A2. IoT 버스 데이터 정보 변경	Tampering
	A3. 정보 전송 행위의 부인	Repudiation
	A11. 다른 IoT Bus Data Server로 위장	Spoofing
	A.12 악성 프로그램 배포 및 서비스 마비	Dos
F4	A2. IoT 버스 데이터 정보 변경	Tampering
	A3. 정보 전송 행위의 부인	Repudiation
	A11. 다른 IoT Bus Data Server로 위장	Spoofing
	A.12 악성 프로그램 배포 및 서비스 마비	Dos
F5	A5. 다른 웹 모니터링 서비스로 위장	Spoofing
	A8. 정보 요청 행위의 부인	Repudiation
F6	A5. 다른 웹 모니터링 서비스로 위장	Spoofing
	A8. 정보 요청 행위의 부인	Repudiation
F7	A1. 다른 버스로 위장	Spoofing
	A3. 정보 전송 행위의 부인	Repudiation
	A7. CID 정보 변경	Tampering
F8	A3. 정보 전송 행위의 부인	Repudiation
	A6. 카드 정보 변경	Tampering
	A9. 카드 정보 유출	Information disclosure
	A10. 다른 카드 회사로 위장	Spoofing

F9	A3. 정보 전송 행위의 부인	Repudiation
	A6. 카드 정보 변경	Tampering
	A9. 카드 정보 유출	Information disclosure
F10	A3. 정보 전송 행위의 부인	Repudiation
	A6. 카드 정보 변경	Tampering
	A9. 카드 정보 유출	Information disclosure

DFD에서 나타낸 데이터 흐름 F1 ~ F10까지의 위협을 각각 선정해주었다. 크게 위장, 부인, 정보변경, 정보유출의 위협이 있었고 그에 따른 STRIDE를 위의 표에서 매칭시켰다.