자동차공학회 추계학술대회

AUTOCRYPT

전기차 충전 환경의 사이버보안 이슈

2022.11.17

송종혁

AUTOCRYPT

TU-Automotive AWARDS
Best Auto Cybersecurity Product/Service 2019
The Automotive Tech Company of the Year Finalist 2020
Automotive Cybersecurity Product of the Year Finalist 2021

CYBER MOBILITY AWARDS
2020 Global Cyber Achievement Award

CTOTECH BREAKTHROUGH AWARDS
2020 & 2021 Automotive Cybersecurity Company of the Year

AIIA
Artificial Intelligence Industry Association
2020 Emerging AI+X Top 100 Company
Mobility Category

Forbes Asia
2021 100 to Watch

ISO 15118: Road Vehicles – Vehicle-to-Grid Communication Interface

EV와 EVSE 혹은 EVCC와 SECC 사이의 통신을 정의한 규격

Electric Vehicle(EV) ←→ Electric Vehicle Supply Equipment (EVSE)

Electric Vehicle Communication Controller (EVCC) ←→ Supply Equipment Communication Controller (SECC)

- ISO 15118-1
  - General information and use-case definition
- **ISO 15118-2**
  - **Network and application protocol requirements**
- ISO 15118-3
  - Physical and data link layer requirements

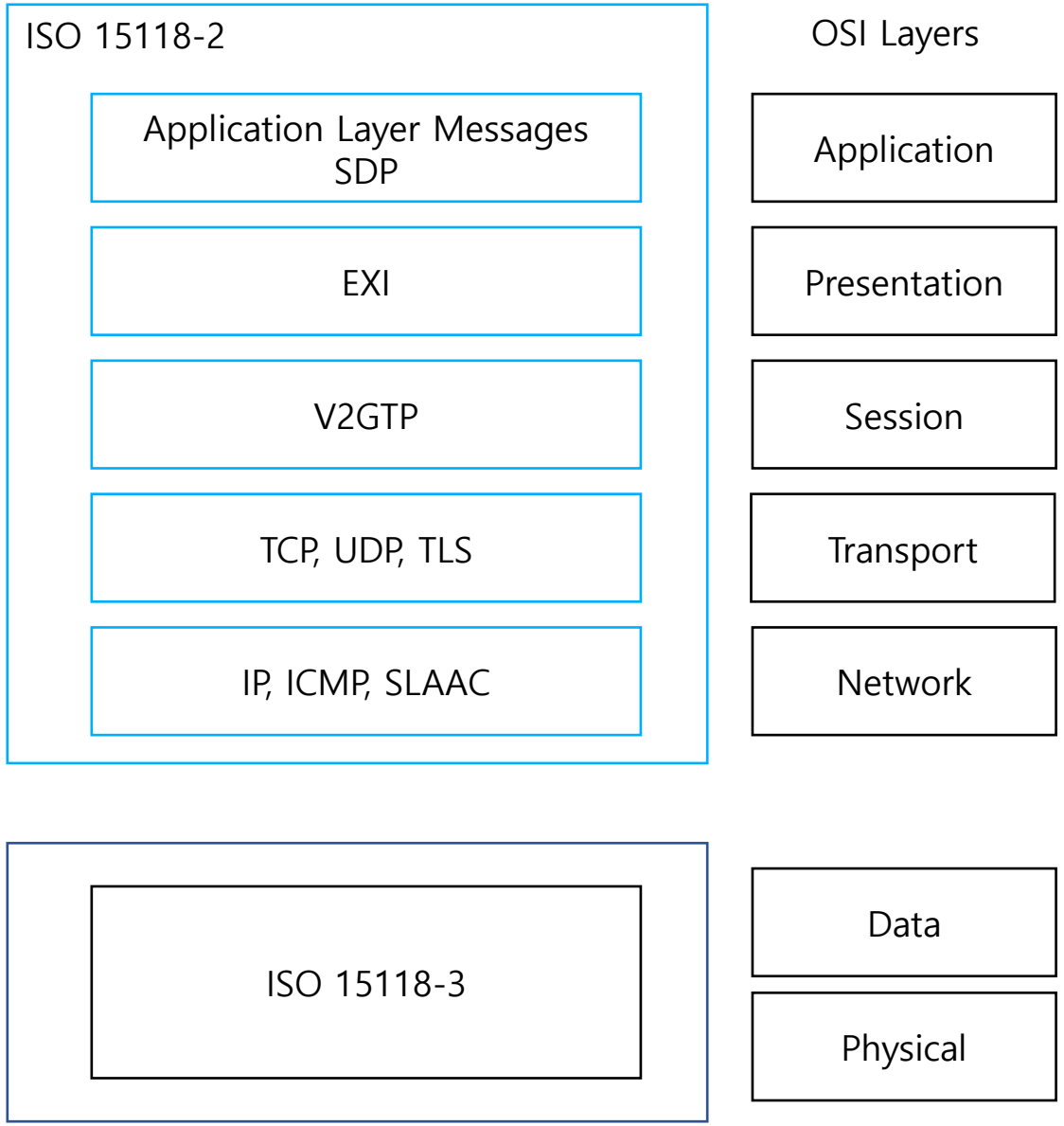
- ISO 15118-4 (under preparation)
  - Network and application protocol conformance test
- ISO 15118-5 (under preparation)
  - Physical layer and data link layer conformance test

V2G Communication Overview

SDP → SECC Discovery Protocol
EVCC가 SECC의 IP, port 등을 파악하기 위해 사용

EXI → Efficient XML Interchange
XML의 바이너리 포맷 (인코딩)

V2GTP → V2G Transfer Protocol
EVCC와 SECC사이의 전송 프로토콜

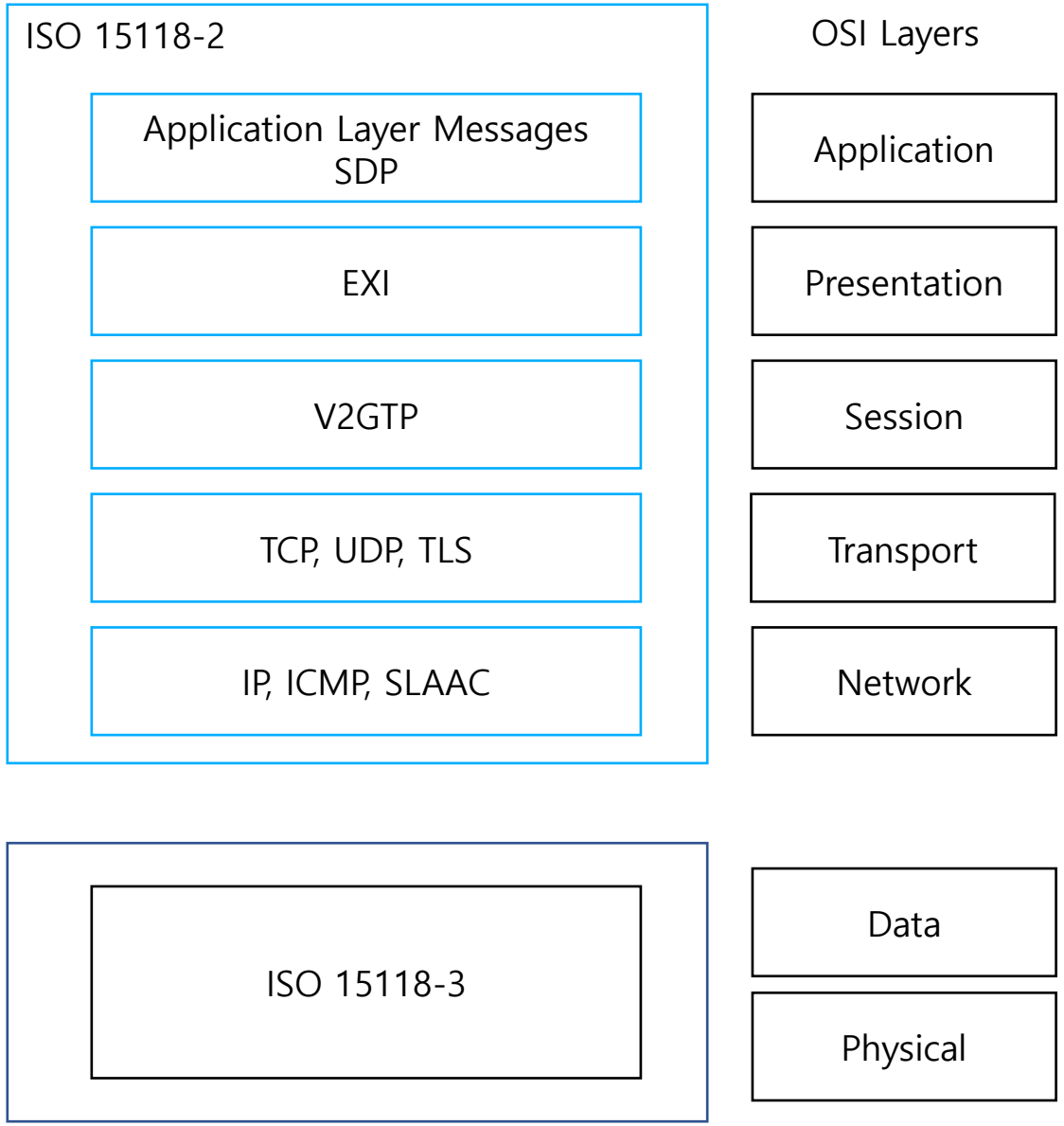


ISO 15118-2에서의 사이버보안 공격 가능성

기존 네트워크 환경 그대로 사용 (IP/TCP/UDP)
→ 이미 존재하는 네트워크 공격들에 똑같이 위험

XML 사용
→ XML을 활용한 공격, XML parser를 노리는 공격에 위험

새로운 프로토콜
→ 아직 충분히 보안성이 검증되지 않음



이번 발표에서는 ...

- ISO 15118-2에서 가능한 사이버보안 위협들과 그 대응책들을 알아본다.

ISO 15118-2 환경에서 발생 가능한 사이버보안 공격 - 1

- Eavesdropping (도청)
  - 충전시 자동차와 충전소가 주고 받는 데이터에는 개인정보 및 결제 관련 정보가 포함되어 있음
  - 이러한 정보들이 공격자에게 노출될 수 있음 (개인정보유출)
  - 유출된 정보들을 통해 다른 공격에 사용 가능(e.g., 위장)

- Masquerading (위장)
  - 충전시 주고 받는 변수들 중 운전자/자동차의 신원을 확인할 수 있는 변수 존재
  - 해당 변수들이 조작 가능하다면, 다른 운전자/자동차 행세를 하여 충전 비용을 다른 운전자에게 청구하는 공격 가능

Type	Name
Identification	EVCCID, EVSEID, SessionID
Charge	MeterInfo, EVMaxVoltage
Tariff	SalesTariffID

< ISO 15118-2에서 사용되는 parameter 예제>

ISO 15118-2 환경에서 발생 가능한 사이버보안 공격 - 2

- 충전 데이터 조작
  - 충전시 주고 받는 변수들 중 결제 관련 변수들 존재
  - 해당 변수들이 조작 가능하다면, 공짜 충전이나 결제한 금액보다 더 많은 양을 충전하는 등의 공격 가능

Type	Name
Identification	EVCCID, EVSEID, SessionID
Charge	MeterInfo, EVMaxVoltage
Tariff	SalesTariffID

< ISO 15118-2에서 사용되는 parameter 예제>

ISO 15118-2 환경에서 발생 가능한 사이버보안 공격 - 3

- Denial of Service(DoS) 공격
  - 기존 네트워크 DoS 공격 가능성
    e.g., SYN flooding
- XML Injection 공격
  - 기존 XML injection 공격 가능성
    e.g., XXE injection attack
- Invalid Data Attack
  - 악성 XML 데이터 전송으로 crash 유발

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns6:V2G_Message xmlns:ns6="urn:iso:15118:2:2013:MsgDef"
xmlns:ns5="http://www.w3.org/2000/09/xmldsig#"
xmlns:ns7="urn:iso:15118:2:2013:MsgBody"
xmlns:ns2="urn:iso:15118:2:2010:AppProtocol"
xmlns:ns4="urn:iso:15118:2:2013:MsgDataTypes"
xmlns:ns3="urn:iso:15118:2:2013:MsgHeader">
<ns6:Header>
    <ns3:SessionID>3CEFDB85233A321EF</ns3:SessionID>
</ns6:Header>
<ns6:Body>
    <ns7:ChargingStatusRes>
        <ns7:ResponseCode>OK</ns7:ResponseCode>
        <ns7:EVSEID>KR*V2G*K12345</ns7:EVSEID>
        <ns7:SAScheduleTupleID>1</ns7:SAScheduleTupleID>
        <ns7:MeterInfo>
            <ns4:MeterID>1</ns4:MeterID>
            <ns4:MeterReading>32000</ns4:MeterReading>
            <ns4:TMeter>1654232745</ns4:TMeter>
        </ns7:MeterInfo>
        <ns7:ReceiptRequired>false</ns7:ReceiptRequired>
            <ns7:AC_EVSEStatus>
                <ns4:NotificationMaxDelay>0</ns4:NotificationMaxDelay>
                <ns4:EVSENotification>None</ns4:EVSENotification>
                <ns4:RCD>false</ns4:RCD>
            </ns7:AC_EVSEStatus>
    </ns7:ChargingStatusRes>
</ns6:Body>
</ns6:V2G_Message>
```

< ISO 15118-2 XML 메시지 예제 >

대응책

1. TLS 적용
2. 충전 변수 검증
3. ID 변수 검증
4. DoS 공격 prevention 적용
5. XML injection 공격 prevention 적용
6. V2GTP data 검증

1. TLS 적용

- TLS를 제대로 적용한다면 많은 공격들을 예방할 수 있음
  - 암호화를 통해 eavesdropping(도청) 공격 방지 가능
  - 유효한 인증서가 없다면 통신을 할 수 없으므로 조작 및 injection 공격들도 불가능

- TLS 적용 확인 절차
  1. SECC/EVCC에 TLS가 enable되어있는지 확인

  2. 최신 버전 TLS를 사용하고 있는지 확인
     ▷ TLS v1.2/v1.3 사용 해야함

  3. 인증서가 유효한지 확인
     ▷ expired된 인증서인지 확인 필요

OpenSSL 명령어로 TLS 확인하기

```
jhsong@jhsong-macbook:~$ openssl s_client -connect fe80:0:0:0:485:2a30:b42e:5d20%en0:64872
CONNECTED(00000003)
depth=2 CN = CPOSubCA1, O = RISE V2G Project, C = DE, DC = V2G
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/CN=SECCCert/O=RISE V2G Project/C=DE/DC=CPO
   i:/CN=CPOSubCA2/O=RISE V2G Project/C=DE/DC=V2G
 1 s:/CN=CPOSubCA2/O=RISE V2G Project/C=DE/DC=V2G
   i:/CN=CPOSubCA1/O=RISE V2G Project/C=DE/DC=V2G
 2 s:/CN=CPOSubCA1/O=RISE V2G Project/C=DE/DC=V2G
   i:/CN=V2GRootCA/O=RISE V2G Project/C=DE/DC=V2G
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIBzjCCAXWgAwIBAgICMDkwCQYHKoZIzj0EATBRMRIwEAYDVQQDDAlDUE9TdWJD
QTIxGTAXBgNVBAoMEFJJU0UgVjJHIFByb2plY3QxCzAJBgNVBAYTAkRFMRMwEQYK
CZImiZPyLGQBGRYDVjJHMB4XDTIyMDYwMzA0Mzg1OFoXDTIyMDgwMjA0Mzg1OFow
UDERMA8GA1UEAwwIU0VDQ0NlcnQxGTAXBgNVBAoMEFJJU0UgVjJHIFByb2plY3Qx
CzAJBgNVBAYTAkRFMRMwEQYKCZImiZPyLGQBGRYDQ1BPMFkwEwYHKoZIzj0CAQYI
KoZIzj0DAQcDQgAE8mvUtuxAigGGdcP2mQYBEE45mhc8nCdmOfsWCRr1xsLlJ6rj
LIu/vZLXJR84eMhhuNwy5Wo0gRZfdT/3LzP6c6M/MD0wDAYDVR0TAQH/BAIwADAO
BgNVHQ8BAf8EBAMCA4gwHQYDVR0OBBYEFOvH2xrR3Yx0G4Z3whksJj40HGTQMAkG
ByqGSM49BAEDSAAwRQIgP2JWvR/4ZYmcfIR41y33LP834D2x8Sdxms2pWffGWzwC
IQDHOZk8YySvjN7x++s7iubEr36H2j/jbOyDm1YpUmQB3g==
-----END CERTIFICATE-----
subject=/CN=SECCCert/O=RISE V2G Project/C=DE/DC=CPO
issuer=/CN=CPOSubCA2/O=RISE V2G Project/C=DE/DC=V2G
---
No client certificate CA names sent
Server Temp Key: ECDH, X25519, 253 bits
---
SSL handshake has read 1738 bytes and written 329 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-ECDSA-AES128-SHA256
Server public key is 256 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-ECDSA-AES128-SHA256
    Session-ID: C814616477A434CA4CD6BCEB495066FD78EA5C152866EDE47ADC5F291EC1FAF8
    Session-ID-ctx:
    Master-Key: CA48BF83A3A40801FCE2C00FF52A2FB9B18A5F503AFEC998F2C62D35F23B06C26C7537EDEB92AA
    Start Time: 1654677366
    Timeout   : 7200 (sec)
    Verify return code: 20 (unable to get local issuer certificate)
```

인증서

TLS 버전 정보

$ openssl s_client -connect [IP]:[port]

```
jhsong@jhsong-macbook:~$ openssl s_client -connect fe80:0:0:0:485:2a30:b42e:5d20%en0:52979
CONNECTED(00000003)
```

TLS가 적용되어있지 않다면, 위와 같이 인증서 정보가 출력되지 않음

OpenSSL 명령어로 TLS 확인하기

```
jhsong@jhsong-macbook:~$ openssl x509 -enddate -noout -in cert.pem
notAfter=Aug  2 04:38:58 2022 GMT
```

Expiration date

- OpenSSL로 인증서 만료 날짜 확인 가능

2. 충전 변수 검증

충전 변수 조작 공격을 막기 위해 SECC/EVCC는 충전 변수 검증 수행 필요

→ ISO 15118-2에 정의된 충전 변수들의 type 및 restriction들을 활용하여 검증 가능

Parameter Name	Type (restriction)
VersionNumberMajor	unsignedInt
SchemaID	unsignedByte
ServiceScope	String (max length: 64)
SelectedPaymentOption	Enumeration (Contract, ExternalPayment)
RequestedEnergyTransferMode	Enumeration (AC_single_phase_core, AC_three_phase_core, DC_core, DC_combo_core, …)
ChargeProgress	Enumeration (Start, Stop, Renegotiate)

< ISO 15118-2에 정의된 충전 변수들의 type과 restriction >

3. ID 변수 검증

위장 공격 등 ID를 변조하는 공격을 막기 위해 SECC/EVCC는 ID 변수 검증 수행 필요

→ ISO 15118-2에 정의된 ID변수들의 type과 restriction을 참고하여 검증 가능

Parameter Name	Type (restriction)
SessionID	hexBinary (length <=8)
EVCCID	hexBinary (length <=6)
EVSEID	String (3 <= length<= 7)
ServiceID	unsignedShort

< ISO 15118-2에 정의된 ID 변수들의 type과 restriction >

악성 데이터 예제

(null), “A”*1024, 0, -1, 4294967296 (unsigned int max+1), 18,446,744,073,709,551,616 (unsigned long max+1), …

```
<ns0:V2G_Message xmlns:ns0="urn:iso:15118:2:2013:MsgDef"
xmlns:ns1="urn:iso:15118:2:2013:MsgHeader" xmlns:ns2="urn:iso:15118:2:2013:MsgBody">
<ns0:Header>
<ns1:SessionID>
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA
</ns1:SessionID>
</ns0:Header>
<ns0:Body>
<ns2:SessionSetupReq>
<ns2:EVCCID>A07817A65779</ns2:EVCCID>
</ns2:SessionSetupReq>
</ns0:Body>
</ns0:V2G_Message>
```

* Example of normal SessionID: C3917A55A2BA8118

```
<ns0:V2G_Message xmlns:ns0="urn:iso:15118:2:2013:MsgDef" xmlns:ns1="urn:iso:15118:2:2013:MsgHeader"
xmlns:ns2="urn:iso:15118:2:2013:MsgBody" xmlns:ns3="urn:iso:15118:2:2013:MsgDataTypes">
<ns0:Header>
<ns1:SessionID>74F18B6F1F222CA5</ns1:SessionID>
</ns0:Header>
<ns0:Body>
<ns2:PowerDeliveryReq>
<ns2:ChargeProgress>-1</ns2:ChargeProgress>
<ns2:SAScheduleTupleID>1</ns2:SAScheduleTupleID>
<ns2:ChargingProfile>
<ns3:ProfileEntry>
<ns3:ChargingProfileEntryStart>0</ns3:ChargingProfileEntryStart>
<ns3:ChargingProfileEntryMaxPower>
<ns3:Multiplier>3</ns3:Multiplier>
<ns3:Unit>W</ns3:Unit>
<ns3:Value>11</ns3:Value>
</ns3:ChargingProfileEntryMaxPower>
<ns3:ChargingProfileEntryMaxNumberOfPhasesInUse>3</ns3:ChargingProfileEntryMaxNumberOfPhasesInUse>
</ns3:ProfileEntry>
</ns2:ChargingProfile>
</ns2:PowerDeliveryReq>
</ns0:Body>
</ns0:V2G_Message>
```

* Example of ChargeProgress: “Start” or “Stop”

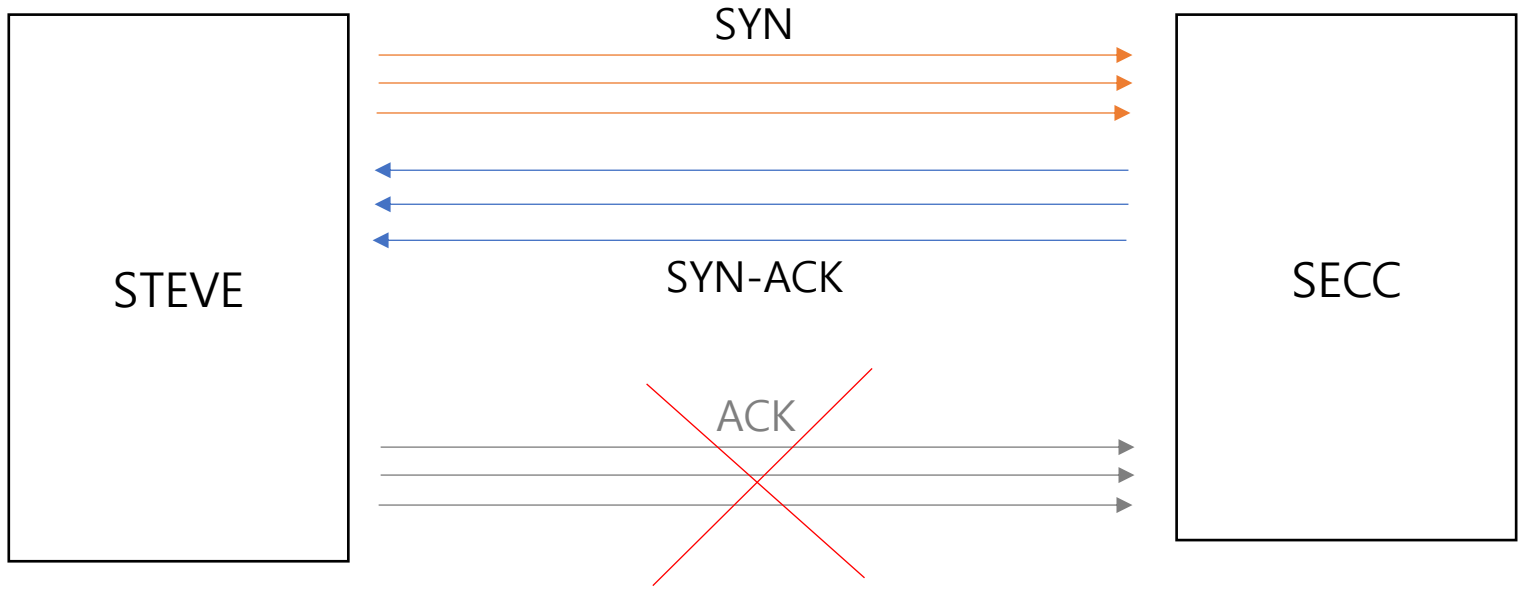
4. DoS 공격 Prevention

기존 네트워크 DoS 공격들에 대한 대비 필요 (단, ISO 15118-2는 IPv6 환경)

→ Rate limit 설정, 과도한 데이터 전송하는 client는 차단 (블랙리스트 관리)

DoS 공격 예제: SYN flooding attack

대량의 "SYN" 패킷을 서버에 전송한 뒤 돌아오는 "ACK" 패킷에는 응답하지 않는 공격



5. XML Injection Prevention

XML 메시지들에 공격 코드가 포함되어 있는지 검증 필요

→ XML injection 공격에 주로 사용되는 패턴, 공격 코드들을 filtering 해야함

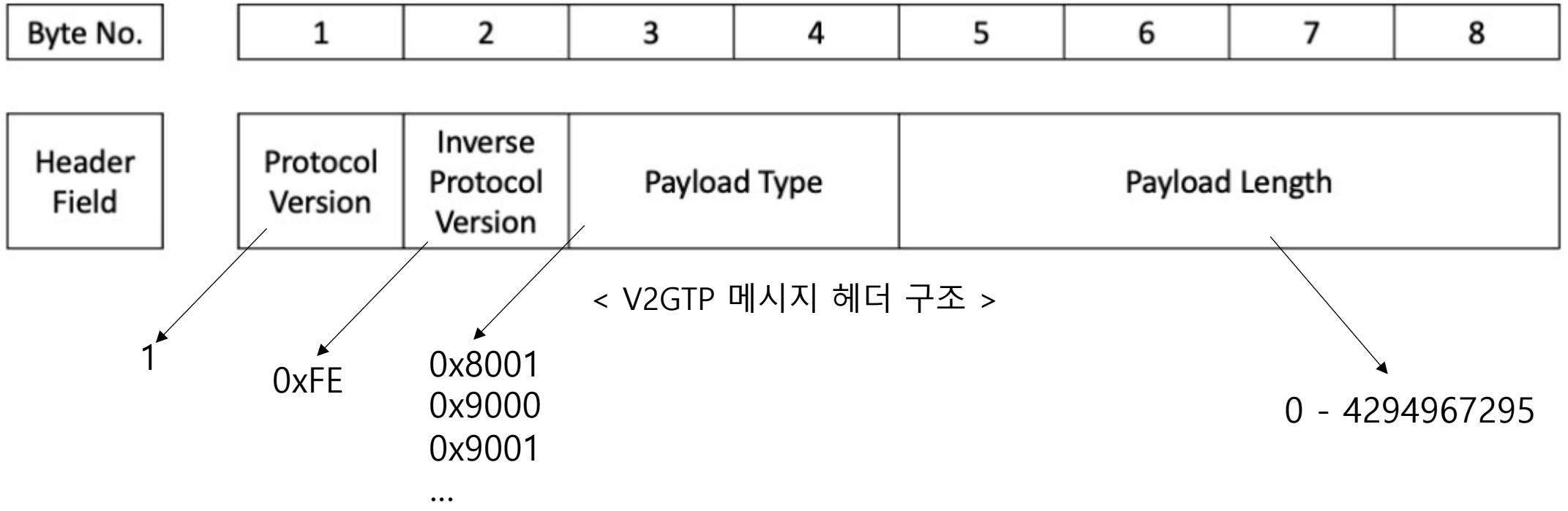
```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<foo>&xxe;</foo>
```

< XXE injection 공격 payload 예제>

6. V2GTP Data 검증

SECC/EVCC는 서로 주고 받는 V2GTP 메시지에 대해 검증을 해야 한다.

→ V2GTP 구조를 지키는지, 각 filed가 가지는 type 및 restriction을 지키는지 확인 필요



결론

전기차 충전 환경에서의 사이버보안 위협들에 대해 대비가 필요하다.

- 일반 네트워크 환경에서 가능했던 공격들에 대해 대비 필요
- XML 데이터를 이용한 공격들에 대해 대비 필요
- 새로 적용되는 프로토콜들에 대한 충분한 검증 필요

AUTOCRYPT

Secure First, Then Ride

SEOUL · SEJONG · SHANGHAI · WUXI · TORONTO · TOKYO

www.autocrypt.io