Electric Vehicle Authentication and Secure Metering in Smart Grids

Yutaka Yamaguchi
Faculty of Engineering,
Kyushu University
Fukuoka, Japan
1TE20110W@s.kyushu-u.ac.jp

Dirceu Cavendish
Department of Computer Science and Elect.,
Kyushu Institute of Technology
Fukuoka, Japan
cavendish@net.ecs.kyutech.ac.jp

Hiroshi Koide
Research Institute of Info. Tech.,
Kyushu University
Fukuoka, Japan
koide@cc.kyushu-u.ac.jp

***Abstract*—Electric vehicles have been recently produced at a very aggressive pace as a way to curb carbon emissions in the 21st century. Public utility companies are rushing to provide electric vehicle charging station infrastructure needed to serve a rapidly growing fleet of EV users in various countries around the world. Equipped with smart meters, charging stations must check vehicle's characteristics prior to charging, as well as securely report charging data back to public utility companies. In this paper, we propose to leverage an Authentication and Key Agreement protocol used in cellular networks into an electric vehicle authentication and secure metering framework. Starting with a vehicle Subscriber Identification Module, we show how generic vehicle services can be securely provided, including mutual authentication, key agreement, and key management issues.**

Index Terms*—*Smart Grids; Electric Vehicle Charging; Authentication and Key Agreement.

I. Introduction

Electric Vehicles have become very popular in recent years, with hybrid and all electric models being sold in large numbers in developed countries. In addition, residential solar panels have also become popular in new house developments across the world. As a result, power utility companies in the United States and other developed countries are installing Smart Meters at residential and business buildings, in order to manage renewable energy generation and consumption to efficiently manage the electric grid [2]. These efforts are seen as evolutionary steps towards Smart Grids, which consists of intelligent power generation and transmission utilities, equipped with meters, sensing devices, and information gateways that controls energy distribution and consumption in near real time. Aggressive Smart Grid projects are currently being pursuit in US, EU, and Asia [3]. As Power Utility Companies rely on accurate metering information from smart meters, secure metering is key to a reliable electric grid management system. From a consumer's perspective, accurate billing is important. For instance, some charging stations may charge extra for vehicles staying in the stations longer than needed. Authentication and encryption mechanisms for reliably transmitting and recording data consumption of users between power companies and users via smart meters are needed.

Symetric key based authentication and encryption requires a Public Key Infrastructure (PKI) that is complex to manage, in addition to requiring more computational power than symmetric key based counterparts. About complexity, maintaining a mobile device uptodate about certificates that have been revoked is not a trivial matter. As far as processing power, although smart meters are not typically limited in power consumption, they do not necessarily come equipped with state of the art processing chipsets. Finally, symmetric key encryption is more suitable to cellular wireless interface, usually the interface of choice of Smart Meters. In this work, we propose a vehicle to Power Utility Company (PUC) authentication and secure metering scheme based on symmetric keys and cryptographic one way functions widely used in the cellular industry. We first advocate for an extension of Subscriber Identity Module (SIM) card industry to vehicles. Then, we show how to realize authentication and key agreement protocols between Power Utility Companies and EV vehicles, in order to support secure charging via smart meters. Provided that smart meters are physically protected within charging stations, the framework proposed obviates the need to manage meter credentials while still supporting secure metering.

There has been a number of research work on Security of Smart Grids in the last several years. A comprehensive survey on security issues in Smart Grids can be found at [5]. Similar to our work, [10] have proposed authentication mechanisms using credentials stored in the Electric Vehicle, using a Hardware Security Module. Due to economy of scale, a vehicle SIM is likely to be as secure and a cheaper solution than an onboard EV HSM. A Trusted Platform Module (TPM) has been proposed to safely store credentials within EVs [11]. We see such proposal to be complementary, rather than competing with our framework, as we can use TPM to store and process master keys generated by the AKA algorithm safely.

The paper material is organized as follows. Section II describes EV charging Ecosystem, its functionalities, security requirements and credential management. Section III shows how to leverage cellular authentication and key agreement protocols to provide EV/PUC mutual authentication and secure metering of charging services. Section IV discusses smart grid standards and their relation to or aka authentication protocol proposal. Section VI provides a security threat analysis of our protocol proposal. Section VII summarizes our contributions and discusses future work.

II. Smart Grid EV System and Security

Figure 1 defines the scope of the system our work is focused on. A Public Utility Company (PUC) retails energy from distribution grid via sub-stations (not shown). For that purpose,

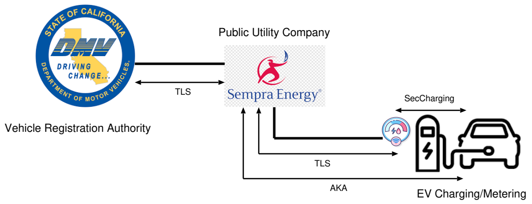

Figure 1: EV Registration and Public Utility Company Ecosystem

PUCs own and control smart meters (SM), which provides energy metering of users at energy consumption end-points, such as residential homes and commercial buildings. SMs are connected to EV charging stations, which provide both home and on the road EV charging services. Consumers EV ownership is controlled by a Vehicle Registration Authority, which manages vehicle ownership during the lifetime of the vehicle, issuing registration and license plates.

A. *Secure EV charging*

Secure EV charging consists of the following components:

- **Mutual authentication of service provider (PUC) and consumer/vehicle:** PUC needs to recognize a licensed vehicle and associate it with a legitimate owner upon which charging fees are assessed. Consumers, on the other hand, need to have trust that the charging station and its SM belongs to a trustworthy PUC.
- **Secure charging metering:** Energy consumption metering needs to be reliable and confidential between PUC service provider and user/vehicle. In this paper, we assume a separate mechanism to ensure Smart Meters/EV chargers can be trusted by the PUC. Several mechanisms are possible to authenticate a SM, from a X.509 certificate to Physically Unclonable Functions [6].

For authentication between PUCs and user/vehicle, we propose a symmetric cryptographic based Authentication and Key Agreement mechanism, similar to the one widely used in cellular networks [1]. We advocate that an alternative asymmetric key scheme, based on Public Key Infrastructure (PKI), is not appropriate for mobile devices, due to complexities in managing certificate revocations and other key management issues.

B. *Vehicle SIM Credential*

A Subscriber Identity Module is an integrated circuit that securely stores an International mobile subscriber number (IMSI) and a unique cryptographic symmetric key. Authentication of the mobile device is predicated on the verification of the device possession of the key, and hence the key must be kept hidden into the Universal Integrated Circuit Card (SIM card/UICC) at all costs. The authentication of the device is based on the sharing of this key only between the user and the service provider, in this case the mobile network operator. The sharing of the device key with operators is executed between UICC manufacturer and network operators via secure ceremonies, which are secure protocols to ensure that no other entity has knowledge of a valid mobile cryptographic key and its IMSI association.

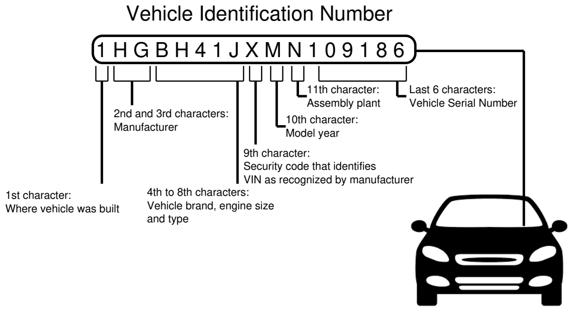
Vehicle Identification Number
1 H G B H 4 1 J X M N 1 0 9 1 8 6
1st character: Where vehicle was built
2nd and 3rd characters: Manufacturer
4th to 8th characters: Vehicle brand, engine size and type
9th character: Security code that identifies VIN as recognized by manufacturer
10th character: Model year
11th character: Assembly plant
Last 6 characters: Vehicle Serial Number

Figure 2: Vehicle Identification Number

TABLE I: LIST OF VARIABLES

K	EV Vehicle key: shared secret between user and provider
RAND	Random challenge: challenges user identity
SQN	Sequence number: prevents replay attacks
AMF	Authentication Management Field: manages multiple AKA protocols
CK	Confidentiality key: encrypts data between user and provider
IK	Integrity key: provides data integrity between user and provider
AK	Anonymity key: obfuscates SQN
MAC	Message authentication code: verifies integrity of authentication msgs.
XMAC	Expected message authentication code: verifies provider
RES	Challenge response: produced by user for authentication
XRES	Expected challenge response: verifies user response
PUC-MSK	Master session key between a PUC and vehicle
SN id	Serving Network: In EV charging context, unique id of a PUC

As SIM card industry has proven to be reliable and scaleable, we propose the extension of it to vehicles. That is, a cryptographic key is associated with the Vehicle Identification Number (VIN), which is a unique but readily available vehicle number etched into every car chassis. As shown in Figure 2, a VIN encodes vehicle manufacturer, model, engine size, among other characteristics. For our purposes, manufacturer and model information may be used to verify the type of charger required, useful if charging stations are not standardized. In addition, charging parameters specific to a vehicle model can be supported.

III. Vehicle and Utility Company Authentication and Key Agreement

Figure 1 depicts mutually authenticated and encrypted communication protocols for secure communication between entities. PUC communicates securely with vehicle registration authority via mutually authenticated TLS session. Secure communication between PUC and EV is supported via an Authentication and Key Agreement protocol, as per Figure 3.

Upon reading of the vehicle license plate, PUC requests authentication vectors to the vehicle registration authority for the vehicle to be charged via a secure TLS connection. A stolen/fake license plate will result in vehicle authentication failure, and hence denial of EV charging service.

Authentication vectors are generated as per Figure 4 (see Table I for a glossary), as follows. A sequence number SQN is maintained between the registration authority and the vehicle, to prevent replay attacks. A fresh random number RAND is generated for each set of authentication vectors. RAND

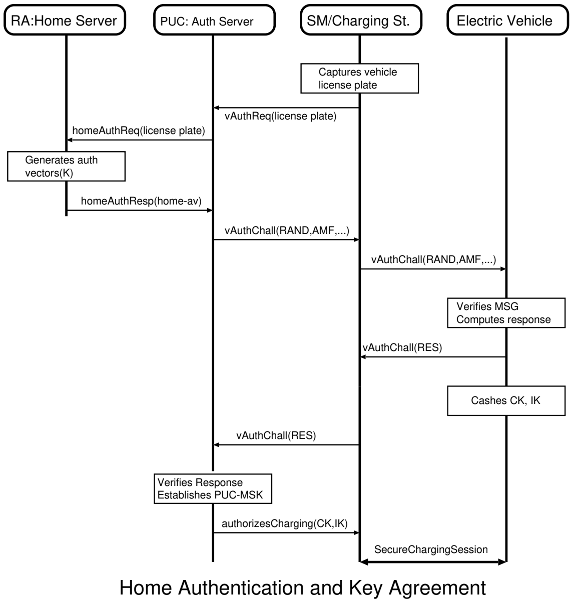

Figure 3: Home Authentication and Key Agreement

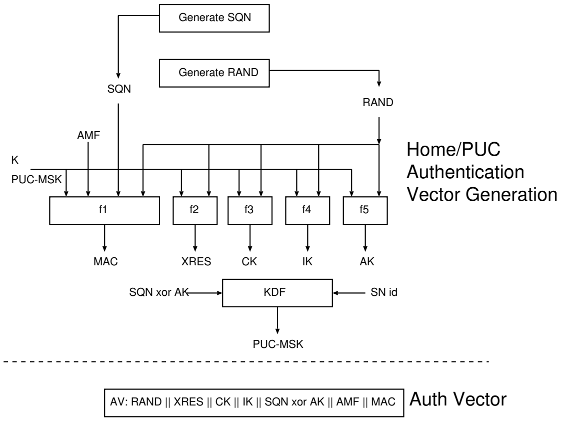

Figure 4: Authentication Vector Generation

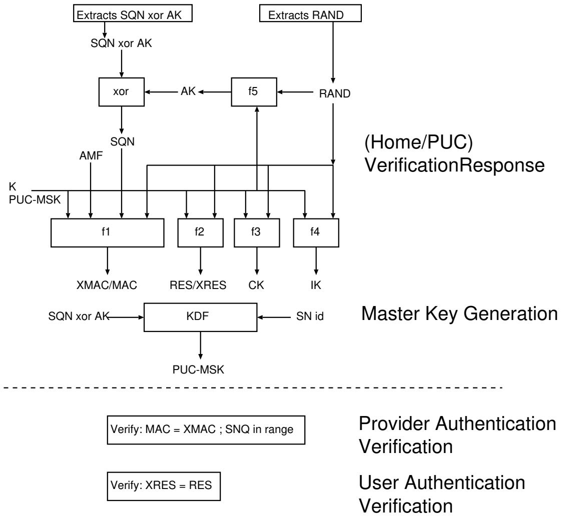

Figure 5: Provider/User Verification

and SQN, together with the vehicle cryptographic key K and authentication management field AMF (to be described later) are fed into five one way functions, as per [1]. A Message Authentication Code MAC is generated to verify the authenticity of the vector. An expected response XRES to challenge RAND is also produced. In addition, a confidentiality key CK (encryption), identity key IK (authentication), and anonymity key AK are produced. The authentication vector results from the concatenation of RAND, XRES, CK, IK, IK, SQN xor AK, AMF, and MAC. Upon reception of the authentication vector, PUC challenges the identity of the EV by passing the random challenge RAND, SQN xor AK, and AMF to the vehicle, for challenge response computation. It also sends MAC for message verification.

Vehicle computes challenge response as per Figure 5. Vehicle first uses RAND and its key K to retrieve AK using one way function f5. AK then is used to retrieve SQN, which, together with vehicle key K and challenge RAND, are used to compute an expected message authentication code XMAC, a challenge response RES, and confidentiality and identity keys CK and IK, respectively. The vehicle then validates the message by comparing XMAC with MAC received from the PUC, and then sends the challenge response RES computed back to PUC, which authenticates the vehicle if XRES=RES. Finally, both PUC and vehicle use a key derivation function KDF (e.g., SHA-256) to generate a master session key PUC-MSK, which becomes a shared key between PUC and the vehicle. A serving network id is used to constraint the scope of the PUC-MSK to a specific PUC provider. We hence suggest the use of the AMF as SN id in the generation of PUC-MSK.

Once vehicle is authenticated, PUC authorizes the smart meter to initiate a charging secure session with PUC, using CK and IK keys. We assume the smart meter software has not been compromised. Mechanism to verify smart meter software vulnerabilities and secure updates is beyond the scope of this paper. Notice that during the authentication process no credential is exchanged between the parties involved. If the vehicle key K is safely stored at registration authority and the electric vehicle, authentication and key agreement process can not be compromised. In addition, user confidentiality is protected by requiring only the vehicle license plate to jump start the authentication process, and not even its VIN number. This help mitigate VIN number based cyber attacks. For additional protection, encryption of license plate information by a PUC managed symmetric key residing in the Smart Meter/charging station can mitigate even the harvesting of license plate information during authentication. This key can be securely distributed from PUC to its smart meters via secure TLS connection.

Once a master session key PUC-MSK is established between PUC and the vehicle, a variant version of the authentication protocol can be run, by replacing vehicle cryptographic key K with PUC-MSK in the figures above. This way, after first authentication of a vehicle, PUC no longer requires

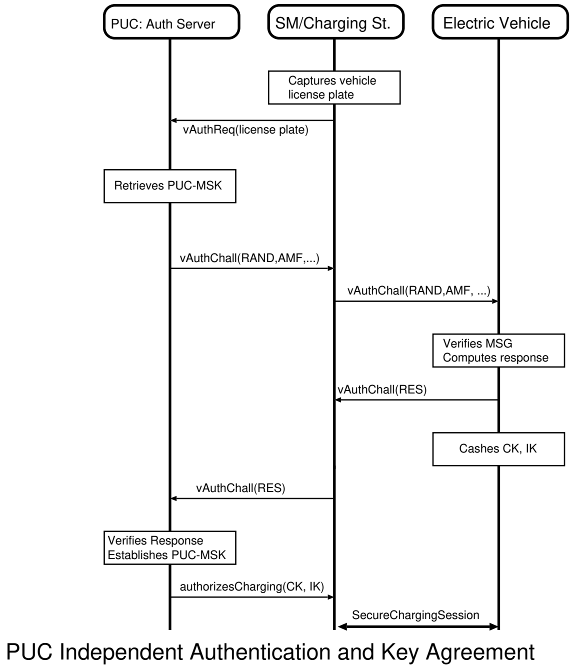
PUC: Auth Server
SM/Charging St.
Electric Vehicle
Captures vehicle license plate
vAuthReq(license plate)
Retrieves PUC-MSK
vAuthChall(RAND,AMF,...)
vAuthChall(RAND,AMF, ...)
Verifies MSG Computes response
vAuthChall(RES)
Cashes CK, IK
vAuthChall(RES)
Verifies Response Establishes PUC-MSK
authorizesCharging(CK, IK)
SecureChargingSession
PUC Independent Authentication and Key Agreement

Figure 6: PUC Authentication and Key Agreement

contacting the registration authority to authenticate the vehicle. We call the first version of the protocol home-AKA, and the second version puc-AKA. As the vehicle needs to differentiate which AKA variant is engaging with, a different AMF is used for home-AKA and puc-AKA. Generalizing it, AMF becomes a pointer to the cryptographic key to be used by the vehicle to authenticate itself. Figure 6 illustrates PUC independent authentication protocol.

Mutual authentication of PUC/EV should be executed as a pre-requisite for every charging operation. In addition, authentication should be enabled only if the charging station cable is physically connected to the vehicle charging outlet. Any disconnect of the charging cable should trigger the need for a fresh authentication handshake upon re-establishing physical connectivity to resume charging.

A. Service key management

Key management of a fleet of Smart Meters within Smart Grids is not a trivial matter. A recent survey on multiple approaches for Smart Grid Key management can be fond in [4], where various key generation and distribution schemes are compared. Our Vehicle-SIM based secure metering framework obviates the need to distribute keys across the Smart Grid, as shared master keys between PUCs and vehicles are generated at the endpoints. Key management then reduces to two issues: i- defining when these keys are generated and under which conditions they should be renewed/rotated; ii- how to support multiple PUCs.

B. Power Utility Company Key Rotation

Rotation of Public Utility Company master session key PUC-MSK is driven by the following use cases:

- **New user use case:** A Smart Meter is assigned to a home, attached to a home EV charger. SM allows the running of a home-AKA algorithm, with generation of a public utility company master session key (puc-MSK).
- **Vehicle change of ownership:** A new master session key must be generated for the same vehicle. This requires the rotation of PUC-MSK at a cadence, perhaps once a month, to ensure the vehicle is still owned by the same utility user. A side use case would be a vehicle that is reported stolen. In this case, registration authority may stop issuing authentication vectors to the vehicle, effectively preventing the vehicle from being charged.
- **House change of ownership:** A new PUC-MSK must be generated, as the Home Smart Meter changes ownership.

PUC-MSK rotation may be supported by the home smart meter only. In addition, multiple PUCs will typically need to provide charging services along multiple jurisdictions. In this case, different AMFs must be used among multiple PUCs. We propose the use of a hash function with low collision probability, with a unique PUC input, such as the private key of a PUC X.509 certificate, to generate an unique AMF.

C. Multiple Public Utility Company key management

As travel typically involves charging stations from multiple PUCs, each PUC requires fetching of authentication vector from the vehicle regulatory body. As each authentication vector generated increments SEQN, and given the fact that the vehicle verification involves checking a valid range of SEQNs, it is possible that the vehicle gets out of sync about the acceptable range of SEQN and RA:Home Server in a multiple PUC scenario. A synchronization mechanism between the registration authority and the vehicle needs to be established. We propose to execute this synchronization at a trusted EV charging station, such as the one at home. That is, when the smart meter engages in home-aka authentication with the vehicle, the vehicle resets its SEQN valid window around the SEQN resent in the challenge received, as per Figure 5 (replacing the SEQN in range verification with expected SEQN - XSEQN - assignment to the received SEQN).

D. Supporting other Smart Grid services beyond EV Charging

The secure metering framework proposed in this work can be extended in few ways.

- **Secure Vehicle Services:** Smart devices controlling parking lot gates can be used to automatically grant entrance access to vehicles equipped with SIM cards. For instance, in some countries with advanced smart grid systems, airports may grant free parking to EV vehicles which allows one cycle charging during their stay, so as to smooth airport energy peak hours. In this case, a PUC is replaced by another service provider, which interacts with the vehicle registration authority. The authority then may provide a “authentication as a service” business model to help with operational costs.
- **Non-vehicle Secure Metering Services:** Power utility companies may use user electronic credentials other than

vehicle to generate master service keys at smart meters for smart grid services other than vehicle charging. As a first step towards that scenario, PUCs may use vehicle generated master key to provide secure metering services for smart home. In this case, a PUC would simply rotate the ev charging master key for charging, but retain the previous key in the smart meter for other home services. In future, PUCs could engage with a network operator owning a cellular network SIM card to retrieve authentication vectors, and generate master keys for generic metering services. Smart meters then could engage with user cellular phone in order to enable the generation of smart grid service keys.

IV. Leveraging Standards and Protocols

The management of charging operation within EV charging ecosystem has evolved via different protocols, some of which have been standardized. ISO 15118 [7] allows EVs and SMs to dynamically exchange information for a proper charging. In terms of security, ISO 15118 supports a Plug & Charge feature, upon which a secure EV to SM secure communication link is established. In ISO 15118, secure EV to SM link requires agreement between EV and SM on a symmetric key - our proposal fulfills this requirement, providing a different key per EV.

Another widely used protocol is Open Charge Point Protocol (OCPP) [8], which supports all communication between the SM and its "control center" (within PUC). Various versions of the protocol exist, with version 2.0 having the most advanced security features, such as secure communication channel, secure firmware update, logging of security events. OCPP allows the SM to behave as a communication gateway between the EV and PUC backend system. This architecture blends well with our security framework. In fact, the symmetric cryptographic keys generated by our AKA framework may be used to mitigate lingering protocol vulnerabilities [9].

V. Implementation Proof of Concept

This section describes a proof of concept implementation of the security protocols introduced in this paper. Authentication and Key Agreement algorithms were simulated in Python. Using a library called Pykka, we created an actor model of the four components of secure metering ecosystem: Home Server, PUC, Smart Meter, and Electric Vehicle (Figure 7). Pykka allows messages to be sent to other actors by tell() function. Key exchanging was implemented by using tell() with a dictionary type list in tell(), such as message = [”order”: ”start , ”key”:00112233]. Since on_receive() is a message handler, it reads the ”order” of the message and performs the following conditional branching according to transactions name.

As per Figure 8, the output of the program uses print() to output the name of the actor sending message data, the name of the transaction, and the generated key to visually track how communication between entities is taking place. Even though the figure shows Home AKA output, a similar output from PUC-AKA has also been verified, omitted for space's sake.

```
class HomeServer(pykka.ThreadingActor):
    def __init__(self):
        super(HomeServer, self).__init__()

    def link_class(self, instance_name):
        self.PUC_ref = instance_name

    def on_receive(self, message):
        print(””)
        print(”HS”)
        self.message = message
        self.order = message[”order”]

        if(self.order ==
        ”Send_License_Plate”):
            print(”(Home_AKA) Generate_Key”)
            self.license_plate =
            message[”license_plate”]
            self.Generate_Key()

    def Generate_Key(self):
        self.key = 0x0011223344556677
        8899aabbccddeeff
        – self.license_plate
        self.PUC_ref.tell
        ({”order”:
        ”Send_Registration_Complete_Message”,
        ”key”:self.key})
```

Figure 7: Software Implementation

VI. Authentication and Key Agreement enhanced Charging - Security Evaluation

In this section, we evaluate our AKA EV charging framework vis a vis security threats. The analysis is structured around three actors: EV, Charging station(CS)/Smart Meter(SM), PUC/Charging control center.

- **EV:** The following threats are devised:
  - Impersonation: Impersonating an arbitrary vehicle is impossible as long as the vehicle cryptographic key is safely stored in the v-sim card. As a consequence, the protocol supports non-repudiation of charging session.
  - Denial of Service: Assuming a EV to SM (WiFi/cellular) wireless link, DoS attack may be staged, for instance, via radio jamming.
  - Distributed DOS: As charging section is initiated via AKA by the reading of the vehicle license plate, staging a DDoS from the vehicle would require multiple fake license plates. To mitigate such attacks, PUC control center may keep track of license plates that have failed authentication in the past, as in a blacklist concept, and discard charging requests coming from vehicles that have failed authentication multiple times.

```
SM
home AKA communication initiation

PUC
(Home_AKA)Send_License_Plate

HS
(Home_AKA)Generate_Authentication_Vector
SQN: 4738849701895016728
(Home_AKA)Generate_XRES_MAC
XRES: 15568641829527999796
MAC: 968201358740978223

PUC
(Home_AKA)Extract_RAND_AMF_SN_SQN_XRES_MAC

SM
(Home_AKA)Send_RAND_AMF_SQN_MAC

EV
(Home_AKA)Extract_RAND_AMF_SQN_MAC
(Home_AKA)Generate_RES_AK_CK_IK_XMAC
RES: 15568641829527999796
XMAC: 968201358740978223
AK: 22205989251187
CK: 302442567435870355165888583869651823 40
IK: 204382471729976753096951681390175295497
OK! MAC = XMAC

(Home_AKA)Generate_PUC_MSK
PUC_MSK = 88649950777707439318863624181421982 2

SM
(Home_AKA)Forward_Encrypted_RES

PUC
(Home_AKA)Compare_RES_and_XRES
OK! XRES = RES
PUC_MSK: 88649950777707439318863624181421982 2
```

Figure 8: Software Output

  - Data tampering: To mitigate data tampering, cryptographic storage/operations should be executed within a secure hardware in the vehicle and SM.
- **SM:** The following threats are devised:
  - Privacy: License place is read by the charging station and sent to charging control/PUC via a secure TLS session. This information does not need to be retained by the charging station/SM, once transmitted to PUC, mitigating leakage. All data exchanged between vehicle and SM is protected by the crypto keys generated by AKA algorithm, within the secure session.
  - Data tampering: Any attempt to alter data exchanged between the vehicle and the SM will be detected via the integrity key IK, and should be discarded.
- **PUC/Control Center:** The following threats are devised:
  - Denial of Service: Communication between the smart meter and the PUC can be supported via cloud service infrastructure (such as Amazon Web Services), for which DoS protection techniques do exist.
  - Data tampering: Communication between Smart Meter and PUC is protected via server authenticated TLS session. This ensures not only data integrity, but also prevents man-in-the-middle attacks.

VII. Conclusion and Future work

We have proposed a symmetric key based authentication and key agreement protocol to support Electric Vehicle Charging in Smart Grids. PUC and vehicle mutual authentication and secure metering are achieved without the need for the Smart Meter to store credentials. In addition, new cryptographic keys are used by the smart meter on every charging session, rendering key stealing via SM tampering unprofitable. The framework hence reduces Smart Meter security requirements, as well as its attack surface. We have analyzed service keys' management on multiple Power Electricity Company scenarios. In addition, we have provided a proof of concept implementation of the authentication and symmetric keys generation involved in the framework. As future work, we plan to evaluate our proposal via prototyping.

Acknowledgments

This work is supported by JSPS Kakenhi Grant Number 21K11888 and Hitachi Systems, Ltd.

References

[1] "Specification of the MILENAGE algorithm Set: An Example algorithm set for the 3GPP authentication and key generation functions f1; f1*, f2, f3, f4, f5, and f5*," Document 2: Algorithm specification (3GPP TS 35.206 version 14.0.0 Release 14), 2017-04.

[2] H. M. Rehmani et al., "Integrating Renewable Energy Resources into the Smart Grid: Recent developments in information and communication technologies," In IEEE Trans. Ind. Informat., Vol. 14, no. 7, pp. 2814-2825, Jul. 2018.

[3] L. Alejandro et al., "Global Market for Smart Electricity Meters: Government policies driving strong growth," US Int. Trade Commission, Washington, DC, USA, Rep. ID-037,2014.

[4] A. Ghosal and M. Conti, "Key Management Systems for Smart Grid Advanced Metering Infrastructure: A Survey," In IEEE Communications Surveys & Tutorials, Vol. 21, No. 3, pp. 2831-2847, Third Quarter 2019.

[5] P. Kumar et al., "Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues," In IEEE Communications Surveys & Tutorials, Vol. 21, No. 3, pp. 2886-2927, Third Quarter 2019.

[6] B. Harishma et al., "Safe is the New Smart: PUF-Based Authentication for Load Modification-Resistant Smart Meters," In IEEE Transactions on Dependable and Secure Computing, Vol. 19, No. 1, pp. 663-680, January/February 2022.

[7] "Road vehicles - Vehicle-to-grid communication interface-Part 2: Network and application protocol requirements," Int. Org. Stand., Geneva, Switzerland, Rep. ISO/CD 15118-2, 2014.

[8] F. Buve, P. Klapwijk, and R. de Leeuw, "OCPP 2.0.1, part 0-Introduction," Open Charge Alliance, Arnhem, The Netherland, Rep. 2020-03-31, 2020.

[9] Z. Garofalaki et al., "Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP)," In IEEE Communications Surveys & Tutorials, Vol. 24, No. 3, pp. 1504-1532, Third Quarter 2022.

[10] A. Fuchs et al., "HIP: HSM-based identities for plug-and-charge," In ACM 14th Int. Conf. Availability Rel. Security, Dublin, Ireland, Aug. 2020, pp. 1-33.

[11] A. Fuchs et al., "TrustEV: trustworthy electric vehicle charging and billing," In ACM 35th Annual Symposium on Applied Computing, Brno, Czech Republic, Mar. 2020, pp. 1706-1715.