Security and Privacy Implementations within the AnyPLACE Energy Management Solution

Christian Kudera[1], Viktor Ullmann[1], Markus Kammerstetter[1], and Wolfgang Kastner[2]

[1] Secure Systems Lab Vienna, Research Division of Automation Systems, Institute of Computer Engineering, TU Wien, Vienna, Austria
{ckudera,viktor,mk}@seclab.tuwien.ac.at
[2] Research Division of Automation Systems, Institute of Computer Engineering, TU Wien, Vienna, Austria
{k}@auto.tuwien.ac.at

***Abstract*—With the increasing number of energy aware devices, energy management solutions can provide the necessary means to visualize, overlook and automate devices as well as communication with external services. To protect users from malicious attacks and data abuse, security and privacy aspects need to be included into the design and implementation from the very beginning. Within the AnyPLACE solution, we set out to create a security and privacy centric energy management solution. We present a survey of best practice guidelines and EU-wide security and privacy regulatory frameworks including the General Data Protection Regulation (GDPR). Based on the results of our survey, we defined implementation requirements and present the security and privacy architecture of the AnyPLACE implementation.**

I. Introduction

The increased use and promotion of renewable energy are accompanied by significant changes in the electricity market. To support decentralized generation and domestic microgeneration at the user's premises, classical power grids are transformed into *smart grids* through the integration of Information and Communication Technology (ICT) technologies and smart devices. The use of ICT technologies thus allows automatic monitoring of energy flows and demands so that the overall generation within the power grid can be adjusted accordingly. At the user's premises, the ongoing change is primarily visible through the exchange of conventional analog Ferraris meters with digital *smart meters*. In 2014, the European Commission (EC) published a report on the deployment of smart metering [1]. According to the report, about 200 million smart meters for electricity and 45 million for gas will be rolled out in the European Union (EU) until 2020. Furthermore, an increasing energy awareness and availability of microgeneration technology have driven users to increase household energy efficiency as well. Primary motivators are cost saving, self sustainability and environmental protection. As a side effect of the energy awareness, users have an increasing desire to know more about their own consumption of electricity, water and gas. To address the desire and to support the end-users claim of more self-control and energy efficiency, the Adaptable Platform for Active Services Exchange (AnyPLACE) solution was developed.

The solution is funded by the European Union's Horizon 2020 research and innovation program and provides a modular, secure and flexible energy management system. The platform comprises a bidirectional service exchange gateway with management and control functionalities, enabling the interaction between end-users, market representatives, electricity networks operators and ICT providers. Among other features, it allows end-users to manage their energy expenditure and take advantage of dynamic price tariffs to minimize their energy costs. The AnyPLACE platform is based on an embedded system that resides on the end-user's premises. While recent publications have shown that embedded systems often raise security and privacy concerns [2]–[4], the development of the AnyPLACE platform followed a secure development lifecycle and best practice recommendations from the very beginning. Connecting multiple stakeholders and their infrastructures, the development of the solution had to take into account the EU-wide and member-specific recommendations and regulations for smart metering as well as the best practices for embedded systems security.

In this paper, we provide an overview of the security and privacy implementations within the AnyPLACE solution. The contributions are as follows:

- We present an up-to-date summary of EU-wide and member country specific recommendations and regulations for smart metering.
- We present an analysis of existing best practice security and privacy recommendation frameworks for embedded systems.
- We summarize the requirements of the General Data Protection Regulation (GDPR) and study its consequences.
- Distinguishing between hardware and software implementations, we illustrate the security and privacy implementations of the AnyPLACE solution.

II. Related Work

A. Security and Privacy in the Area of Energy Management, End-User Engagement, and Smart Meter Integration

There are several security and privacy centric publications covering the areas of energy management, end-user engagement and smart meter integration. According to Aman et al. [5], security and privacy are key requirements of energy management systems. On one side, the communication of data and control signals poses security challenges. On the other side, there are privacy issues related to disclosing personal

consumption profiles of customers. The end-user's data and control operations thus have to be transmitted in a secure manner to prevent unauthorized access to third parties. Kailas et al. [6] published a survey of communications and networking technologies for energy management in buildings and home automation. Their paper includes a discussion on the integration of a social network service to send power consumption profiles and to receive company data, power costs, and power consumption of each appliance in neighboring homes. Within their discussion, they highlight concerns regarding the privacy of the user's data. These concerns were subsequently reviewed by Rottondi and Verticale [7]. In their work, they describe a method for privacy-friendly load scheduling of deferrable and interruptible domestic appliances in smart grids. Mo et al. [8] present an overview of the cyber-physical security within smart grid infrastructures including the risks of smart meter integrations into home area networks (HANs). The authors present fundamental security approaches including key management, a secure communication architecture as well as system and device centric security measures.

B. Security and Privacy related to Embedded Systems

The area of embedded system security and privacy has been widely covered in recent publications. According to Cai and Zuhairi [9], classical embedded systems are commonly only locally connected within their specific application domain. Due to a lack of large scale interconnectivity (such as Internet connections among Internet of Things devices), the authors' argument that the inherent security and privacy threats and requirements for these systems can be considered low since an attacker would require physical access to the local communication interfaces in the first place. In contrast, modern embedded systems are widely connected to the outside world and new embedded system security challenges arise. The authors summarize these challenges as attacks that compromise information confidentiality, integrity, privacy and availability that can be mitigated or even prevented through intrinsic security methods such as secure protocols and cryptographic measures. Kocher et al. [10] argue that security is a new dimension in embedded systems design. They specify the common security requirements for embedded systems from an end-user perspective. Specifically, these are basic security functions, tamper resistance, content security, secure storage, availability, secure network access and user identification. Furthermore, they illustrate existing security mechanisms like symmetric ciphers, secure hash algorithms and asymmetric algorithms that need to be considered during embedded systems design. However, according to Schaumont et al. [11], embedded system security is always a tradeoff between risk, flexibility and performance that needs to be chosen in accordance with the system requirements and the intended application. Similarly, this tradeoff is also mentioned by Fournaris et al. [12]. According to the authors, the physical hardware design decisions have to be in line with the intended application of the embedded system. For this reason, the threats to which the embedded system is exposed to must be assessed and the resulting security requirements need to be determined accordingly. In 2012, Fiaschetti et al. [13] presented the nSHIELD approach. The nSHIELD framework aims to address security, privacy and dependability issues in the context of embedded systems. The main idea of the framework is to provide an architectural solution and design paradigm to enable security functionalities in complex systems. Therefore, a security agent monitors a set of selected measurements and parameters taken from the embedded system. Using the measured values, the security monitor can dynamically activate or deactivate different security modules. In 2015, Papp et al. [14] provided a comprehensive overview of embedded systems security by analyzing typical attack vectors and vulnerabilities. They present an attack taxonomy that was applied to classify and describe common attack scenarios against embedded systems. According to the authors, the attack taxonomy can assist the design and analysis of embedded systems within a system development lifecycle. In contrast, Joe Grand [15] focuses on practical design solutions from a security point of view. For the enclosure of the embedded system, anti-tamper mechanisms such as switches and sensors are recommended. The components of the printed circuit board should be protected with glue or epoxy against physical access. Furthermore, the author points out different implementation attacks such as side-channel attacks (SCA) and fault injection (FI) attacks that can be prevented with hardened integrated circuits that include countermeasures against these kinds of attacks.

III. The AnyPLACE Solution

The AnyPLACE solution is a modular, secure and flexible energy management system. The AnyPLACE research project had several design objectives, including end-user engagement strategies, the evolution of integration strategies for smart home appliances, the integration of energy management algorithms as well as compliance with regulatory security and privacy requirements and the implementation of near-market prototypes. Overall, two prototypes have been developed: A basic version and an advanced version with additional features. Both versions have undergone initial lab tests and a field trial in a model region. The solution utilizes a modular architecture that is illustrated in Fig. 1. The components of the basic version are highlighted in dark gray while the optional extension modules of the advanced version are colored light gray.

In general, a distinction has been made between internal and external communication. Internal communication is defined as communication with devices on the customer's premises while external communication concerns the remote communication with actors, services and components such as utilities or Internet services. The modules of the solution can be individually exchanged, allowing the customization and adaptation to member-specific recommendations and regulations.

The *AnyPLACE Central Module* includes a *Cybersecurity Module* and provides the modules interconnection as well as

the core QT[1] application. The core application includes *Energy Management Algorithms*, a *Firmware Upgrade Manager*, an *Internet Services Manager*, an *Alarm Manager*, a *Security Module*, a *Device Manager Interface* and the *Interface to the End-User Interface*. The *Energy Management Algorithms* process end-user preferences and device characteristics to produce an optimal dispatch considering demand response incentives [17]. The *Firmware Upgrade Manager* provides a way to update the firmware while the *Internet Services Manager* integrates third party services such as the current weather forecasts. The *Alarm Manager* provides logging and system auditing functionalities. Alerts and security critical incidents are stored in a tamper-proof log file. The *Security Module* is responsible to encrypt and sign as well as to decrypt and verify exchanged messages and data. The *Device Manager Interface* connects the central module to the openHAB[2] framework. The framework allows the connection to a wide range of smart devices from arbitrary manufacturers and the use of automation rules to interconnect the components [16]. The *Interface to the End-User Interface* enables the communication between the central module and the Graphical User Interface (GUI). To interact with the AnyPLACE solution, the user can either use the attached touchscreen or the local web interface available on the Local Area Network (LAN) interface. In addition, the GUI allows the user to monitor the current load balancing actions and to control attached smart home appliances [18].

IV. Security and Privacy Requirements

Since compliance with international, EU and EU member country specific security and privacy recommendations and regulations was one of the AnyPLACE goals, we surveyed existing regulatory documents, recommendations and frameworks. In the following, we provide an overview of the relevant documents.

[1]https://www.qt.io/
[2]https://www.openhab.org/

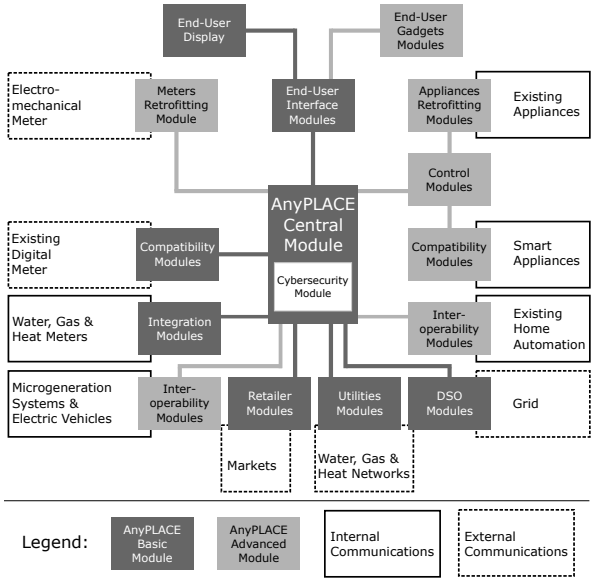

Fig. 1. Modular Architecture of AnyPLACE [16]

A. International Recommendations and Regulations

The International Electrotechnical Commission (IEC) published various standards in the area of smart grids. The IEC 62351 [19] series defines data and communication security aspects. Although the series focuses on smart grids in general, the interconnection of smart meters with the HAN is considered as well. The IEC 62056 [20] series summarizes recommendations for data exchange between smart meters and HANs including meter readout, tariff and load control.

The IEEE 2030 Smart Grid Interoperability Series of Standards [21] include recommendations to address security and reliability concerns for smart grid interoperability with end-user applications and loads.

The National Institute of Standards and Technology (NIST) published the NISTIR 7628 Revision 1 Guidelines for Smart Grid Cybersecurity [22]. The guidelines are divided into three volumes: The first one illustrates smart grid cybersecurity strategies, architectures and high-level requirements. The second one addresses privacy aspects and the third one discusses auxiliary analyses and references concerning smart grid cybersecurity.

B. EU-wide Recommendations and Regulations

Based on the directives 2009/72/EC [23] and 2012/27/EU [24], the member states of the EU are encouraged to achieve a 80 % smart metering roll-out by 2020. Furthermore, according to EC Recommendation 2012/148/EU [25], every smart metering system for electricity should provide readings directly to the customer and to any third party designated by the consumer (Art. 42(a)). In addition, the recommendation requires compliance with directive 95/46/EC [26], the predecessor of today's General Data Protection Regulation (GDPR).

The EU has conducted a study resulting in 10 security recommendations defined in the ENISA Smart Grid Security Recommendations [27]. In general, the recommendations are high-level and non-technical security recommendations suggesting the promotion of the development of security certification schemes and the creation of security test beds to support security assessments.

The CEN-CENELEC-ETSI Smart Meters Coordination Group has issued a three-part privacy and security approach describing privacy and security requirements. The fist part [28] recommends public key cryptography so that clients and third parties can be provided with the smart meter public keys and key establishment algorithms can be utilized as well. Furthermore, specific cipher suites, cryptographic algorithms and protocols are suggested. In addition, a separation between message protection (communication layer) and data protection (information layer), end-to-end security and different security levels are recommended.

C. General Data Protection Regulation

In 2016, the EU agreed to a major reform of their data protection framework. The GDPR [29] has become directly applicable by May 25th, 2018.

In general, the GDPR regulates how organizations operating within the EU (Art. 3, *Territorial scope*) have to deal with personally identifiable information (Art. 1, *Subject-matter and objectives*; Art. 2, *Material scope*). In principle, all information that relates to an identified or identifiable natural person is considered to be personal data (Art. 4, *Definitions*). In that scope, identifiable means that even if it is only theoretically possible to identify individual persons by combining partial information, the partial information already represents personally identifiable information. According to the EC, this also concerns personal data that has been anonymized, encrypted or pseudonymized, but could be later on used to re-identify a person (Art. 6(4)e, *Lawfulness of processing*; Art. 31, *Security of processing*). Only if the data has been anonymized in a way that even with greater effort no conclusions can be drawn on the data subjects, data is considered no longer personal data.

The processing of personally identifiable information is thus only lawful if there exists a proper justification to do so (Art. 6(1), *Lawfulness of processing*). If processing is based on consent, the controller must be able to prove that the data subject has consented to the processing of his or her personal data (Art. 7(1), *Conditions for consent*) and the data subject has the right to withdraw his or her consent at any time (Art. 7(3), *Conditions for consent*). Furthermore, the conditions for consent of under-age persons is strictly regulated (Art. 8, *Conditions applicable to child's consent in relation to information society services*). Consents are only valid for children who have reached the age of sixteen. However, this limit can be lowered by the member states to an age limit of thirteen years.

An important part of the GDPR consists of the privacy rights for affected data subjects. These consist of the rights of transparency and modalities (Art. 12), information and access to personal data (Art. 13–15), rectification and erasure (Art. 16–20), right to object and automated individual decision-making (Art. 21–22), and restrictions (Art. 23).

Member states have to install one or more supervisor authorities, which are independent public authorities responsible for monitoring the application of the GDPR (Art. 51, *Supervisory authority*). The supervisory authority has to ensure that the imposition of administrative fines shall in each individual case be effective, proportionate and dissuasive (Art. 83(1), *General conditions for imposing administrative fines*). The administrative fines can be up to 20M EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Art. 83(5), *General conditions for imposing administrative fines*). The controller as well as the processor shall cooperate on requests with the supervisory authority (Art. 31, *Cooperation with the supervisory authority*). In the case of a personal data breach, the controller has to inform the supervisory authority (Art. 33, *Notification of a personal data breach to the supervisory authority*). In this case, the notification should include the details and consequences of the breach. Furthermore, the controller has to inform the data subject about a personal data breach (Art. 34, *Communication of a personal data breach to the data subject*). Each data subject must have the possibility to complain at a supervisory authority if the data subject considers that the processing of personal data relating to him or her infringes the GDPR (Art. 77, *Right to lodge a complaint with a supervisory authority*).

D. EU Member-Specific Recommendations and Regulations

In this section, we focus on member country specific implementations of EU-wide recommendations and regulations with a particular focus on contries of the AnyPLACE consortium partners. Due to the upcoming GDPR, we do not discuss national privacy regulatory requirements.

Austria Österreichs Energie[3] released a requirements catalog which describes the minimum requirements for smart metering end-to-end security [30]. The catalog requires encrypted end-to-end communication between the end-user's smart meter and the utility's infrastructure. The architecture describes two possible scenarios for the connection: In the first scenario, the smart meter is connected via a wide area network (WAN) interface to the utility. In the second scenario, the smart meter is connected via a gateway using the end-user's local area network (LAN). Nevertheless, the gateway must be transparent and shall not store any cryptographic material. Furthermore, the smart meter must provide a customer interface providing current consumption information to the end-user. The customer interface shall support application-layer encryption, whereas the allowed encryption algorithms should follow the NIST SP 800-57 Part 1 Rev. 4 recommendations (Section IV-E).

Germany In Germany, the so called Smart Meter Gateway (SMGW) is used as central communication unit. According to the applicable BSI Protection Profile BSI-CC-PP-0073-2014 [31], the SMGW is a device or unit responsible for collecting meter data, processing meter data, providing communication capabilities for devices in the local metrological network (LMN), protecting devices in the HAN against attacks from the WAN and providing cryptographic primitives. Smart meters are part of the LMN and it is possible to connect multiple smart meters (e.g. electricity, gas, water) to one SMGW. Furthermore, smart meters of different households, for example in the same building, can be connected to one SMGW. On the HAN interface, the SMGW offers three logical interfaces: the end-user interface, the service technician interface and the controllable local system (CLS) interface [32]. The end-user interface is a read-only interface and can be used to receive the current consumption information. The protection profile defines multiple security and privacy requirements for the interface. Transmitted smart meter data shall be protected by a hash or signature to verify the origin and validity of the data. Regarding privacy, it shall be enforced that no personally

[3]https://oesterreichsenergie.at

identifiable information can be obtained by an analysis of the communication data characteristics.

Netherlands Netbeheer Nederland[4] published the Dutch Smart Meter Requirements [33] to ensure the interoperability of smart meters. In the Dutch smart meter architecture, the smart meter shall provide five interfaces denoted *communication ports*. The read-only communication port P1 enables the end-user to monitor the current consumption information. For the interface itself, no special security and privacy requirements are specified. However, a general requirement is specified requesting all communication involving privacy sensitive data to be secured in a way that data integrity, authenticity, confidentiality and uniqueness are guaranteed.

E. Embedded Systems Recommendations and Best Practices

Although the application range of embedded systems is exceptionally wide, there are several recommendations and best practices that can be applied to the AnyPLACE solution as well.

The NIST Federal Information Processing Standards (FIPS) 140-2 [34] specify requirements for cryptography. FIPS 140-2 defines four levels of security, where Level 1 is the lowest security level with significantly limited requirements. Level 2 adds requirements for physical tamper-evidence and role-based authentication. Level 3 augments the tamper-evidence to tamper-resistance and the role-based authentication to identity-based authentication. The highest level adds the requirement of countermeasures against implementation attacks such as side-channel attacks (SCA), fault injection (FI) attacks, semi-invasive and invasive attacks.

The NIST SP 800-57 Part 1 Rev. 4 [35] standard provides guidance and best practices for the management of cryptographic key material. It requests the usage of FIPS-approved or NIST-recommended cryptographic algorithms whenever cryptographic services are required. Furthermore, the general key management and protection requirements for cryptographic information are described.

The International Organization for Standardization (ISO) 27034 [36] standard contains recommendations for secure software development and a secure software lifecycle that is also applicable to AnyPLACE software development.

The IEEE Internet Initiative published a white paper regarding security best practices for Internet of Things (IoT) devices and networks [37]. Although the white paper focuses on the IoT development, the best practices regarding the device security and the network security are applicable to the AnyPLACE development as well.

V. Security and Privacy Implementations

In the following, the security and privacy implementations are described in detail. Furthermore, Table I gives an overview of the implementations and the effects on the CIA (confidentiality, integrity and availability) triad.

[4]https://www.netbeheernederland.nl/

A. Hardware Design

The AnyPLACE goal was to implement near-market prototypes in basic and advanced versions with the intention to evaluate the different design objectives in field studies. During development and prototyping, a Raspberry Pi[5] 3 with a custom printed circuit board (PCB) add-on was utilized to enable rapid development times and easy integration of different in-house appliances. For the final product, a custom board including all necessary interfaces is envisioned. One of the major challenges during development was to minimize production costs while still retaining the necessary hardware functionalities to achieve the required security and privacy protection levels. Since the developed solutions store personally identifiable information in the form of the end-user's energy consumption, suitable protection mechanisms had to be chosen. At the same time, a trade-off between risk, flexibility and performance has been made to avoid high system complexity and maintainability issues that could ultimately lower the overall security due to increased system complexity and a large attack surface. The resulting trade-off solution comprises of a system on a chip (SoC) centric base system in combination with a smart card processor. To harden the system and to impede unauthorized firmware access, the SoC shall contain an integrated flash memory, an integrated random access memory (RAM), and a debugging interface that can be deactivated. Further, the firmware shall be signed to prevent the manipulation of the system. The smart card processor is used for secure key storage and tamper-proof cryptographic operations. For the prototypes, we used the Yubico[6] YubiKey, a tamper-proof smart card processor solution with a Universal Serial Bus (USB) interface. The smart card processor can be used for key generation and storage, encryption and decryption as well as for signing and signature verification operations. An important security feature of the smart card solution is that private key material can not be read out and security certified countermeasures are in place to detect and/or avoid tampering. In the envisioned final product, the relatively costly Yubikey used during development shall be replaced with an on-board or integrated smart card processor.

B. Secure Development Lifecycle

During the development of the AnyPLACE platform, a secure development lifecycle was followed. The individual phases are described below and illustrated in Fig. 2.

Security Requirements In the first step, it was necessary to define the security and data privacy requirements to identify the necessary security functions in the AnyPLACE design and in the subsequent hardware and software implementation of this design.

Design and Implementation In the next step, a *secure by design* solution was developed. Once the design was complete, the implementation of the design was started. Throughout the technical implementation, it was necessary to adhere to

[5]https://www.raspberrypi.org/

[6]https://www.yubico.com

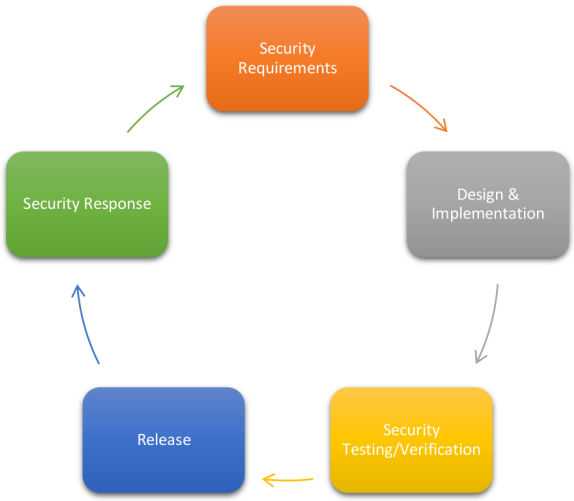

Fig. 2. Secure Development Lifecycle (SDL)

established implementation security guidelines and best practices to avoid technical vulnerabilities. For instance, a *secure by design* system could include a set of cryptographically secured authentication messages that are exchanged between devices. While this message exchange itself could be *secure by design*, the actual software implementation of the message exchange handling code could include a software vulnerability such as a buffer overflow flaw that could jeopardize the security of the overall system. Proper security training of the developers and building up upon established implementation security guidelines and practices minimized implementation flaws. Ultimately, these techniques significantly lowered the likelihood of vulnerabilities, but at the same time, it was impossible to prove the correctness of the system or the absence of vulnerabilities (Rice's theorem [38]).

Security Testing/Verification Once the design had been implemented, it was necessary to perform security tests on the actual implementation. An important goal during these tests was to (1) verify that the implementation actually performs the security functions defined in the design, and (2) to test the robustness of the hardware and software implementation with regard to common implementation security flaws. In addition to common software implementation vulnerabilities and attacks, physical hardware implementation attacks had to be considered as well since the AnyPLACE solution is located within the customer's premises and thus easily accessible by potential adversaries. While for software implementation security testing established analysis tools were utilized, for the hardware security testing we developed a custom fault injection testing tool [39].

Release In this step, the solution had been already thoroughly scrutinized and it was released to the customers.

Security Response Even though the likelihood of vulnerabilities has been significantly lowered through security tests and validation, it is still possible that vulnerabilities are discovered. The security response process allows addressing this case so that subsequent security fixes and patches can be created throughout the cyclic SDL process.

C. Security Module

The security module is responsible to encrypt and sign as well as decrypt and verify exchanged messages and data. It is implemented in the Qt core application and provides its functionalities to other core modules. The keys for the cryptographic methods are stored on the YubiKey smartcard processor to hinder attackers from obtaining the key material.

D. Remote Maintenance Service

Since the AnyPLACE solution offers complex configuration settings via the end-user interface, a remote maintenance service to provide assistance to end-users is necessary. The remote maintenance service is provided by a reverse secure shell (SSH) tunnel. This means that the device itself opens the connection, as opposed to an always open service that anyone can connect to. The access method thus minimizes the attack surface and prevents attackers from connecting to the end-user's local area network (LAN). Furthermore, due to the connection setup from the inside of the end-user's local area network (LAN) to the outside, no configuration of the end-user's firewall or network address translation (NAT) technology is required. In the envisioned final product, an end-user would request assistance through the user interface. Subsequently, the tunnel is opened and maintainers are able to connect to the device. During the field trial, these tunnels are always open to troubleshoot with less interaction required from the end-user. The authentication of a device is performed with the key material stored on the YubiKey smart card processor to prevent attackers from abusing the remote maintenance service.

E. Firmware Update Functionality

The firmware update process is implemented in a way that the authenticity of the firmware is verified before applying it. The device queries the update server every day (during the nighttime) to determine if a new update is available. This connection is secured with the Transport Layer Security (TLS) protocol. Furthermore, the new packages (Debian software package format) are signed by the developers, ensuring that packages with wrong signatures are denied.

F. Graphical User Interface

The graphical user interface enables end-users to interact with the AnyPLACE solution. To allow the interaction either with a touch screen attached to the solution as well as with a remote device (e.g. smart phone, computer), the graphical user interface was implemented as Web service. The technologies used are nginx[7] for the Web server, PHP[8] as script language for the dynamic webpage and PostgreSQL[9] as database. To minimize the attack surface, the Open Web Application Security

[7]https://nginx.org
[8]http://php.net
[9]https://www.postgresql.org/

TABLE I
EFFECTS OF THE SECURITY AND PRIVACY IMPLEMENTATIONS ON THE CIA TRIAD

Category	Implementation	Confidentiality	Integrity	Availability
Hardware Design	SoC: Integrated flash memory	x	x	
Hardware Design	SoC: Integrated RAM	x	x	
Hardware Design	SoC: Deactivation of debugging interface	x	x	
Hardware Design	Secure key storage on smart card	x	x	
Security Module	Decryption and encryption of messages	x		
Security Module	Signature and verification of messages		x	
Remote Maintenance Service	SSH cryptographic network protocol	x	x	
Firmware Update Functionality	Signature verification of update		x	
Firmware Update Functionality	Encrypted connection to update service	x		
Graphical User Interface	Input validation to prevent XSS attacks	x	x	x
Graphical User Interface	Prepared statements to prevent SQL injection	x	x	x
Graphical User Interface	Encryption via HTTPS	x	x	
Graphical User Interface	Session cookie protection with HTTPOnly flag	x	x	
Graphical User Interface	Session cookie protection with secure flag	x	x	
Privacy	Personal data is stored encrypted	x	x	
Privacy	Personal data is transferred encrypted	x	x	
Privacy	If possible, personal data is anonymized	x		

Project (OWASP)[10] recommendations for Web development were considered. To prevent injection attacks, each input is validated before it is used by the application. The validation was implemented with a whitelist approach, where only the required characters are allowed to pass the validation. Also the output is validated to prevent cross-site scripting (XSS) attacks. To prevent SQL injection attacks, only prepared statements are used in addition to the input validation. To protect the user credentials and the session identification, the user interface is only accessible via the HTTP Secure (HTTPS) protocol. Furthermore, the session cookie is protected with the HTTPOnly and the secure flag. The Web server was hardened by utilizing best practice guidelines to ensure a high security standard.

G. Privacy

To ensure the protection of the end-user's privacy and the compliance with the legal requirements and the GDPR, we focused on data avoidance, data protection and data filtering during the design phase of the AnyPLACE solution. This corresponds to the best practice recommendations known as *privacy by design* and *privacy by default*. In a first step, we analyzed which personal data are particularly necessary to fulfill requirements of the AnyPLACE solution. Therefore, we mapped the collection, storage and use of consumer data, whereas the main focus was to avoid the collection of data if it was not truly required for the operation of the solution. In addition, we conducted a privacy impact assessment for the collected data, where we evaluated the risk and performed gap analyses. In the next step, we discussed if there are any personal data which needed to be transferred out of the end-user's home area network. Finally, we defined the privacy specific implementation policy that is described in the following: If personal data is collected, it must be stored encrypted. The decryption is only allowed during operation whenever absolutely necessary. Furthermore, personal data must be transferred encrypted, whereas the data should be anonymized if possible. In addition, an emergency policy was drafted in order to be able to react immediately in the event of security and privacy breaches.

[10]https://www.owasp.org

VI. CONCLUSION AND FUTURE WORK

In this paper, we presented an up-to-date summary of EU-wide and member country specific recommendations and regulations for smart metering. We provided an analysis of existing best practice security and privacy recommendation frameworks for embedded systems. Furthermore, we summarized the requirements of the GDPR and study its consequences. Regarding the AnyPLACE solution, we illustrated the security and privacy implementations of the solution. Overall, we presented a viable approach to design and implement a modular, secure and flexible energy management system which fulfills the EU-wide and member country specific recommendations and regulations for smart metering. In future work, we plan to compare the AnyPLACE solution with other energy management systems to evaluate our security and privacy implementations with respect to other system implementations.

ACKNOWLEDGMENT

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 646580. The hardware security tests during development were supported by Trustworks (https://www.trustworks.at).

REFERENCES

[1] European Commission, "Benchmarking smart metering deployment in the eu-27 with a focus on electricity," *COM/2014/0356 final*, 2014.

[2] J. Viega and H. Thompson, "The state of embedded-device security (spoiler alert: It's bad)," *IEEE Security Privacy*, vol. 10, no. 5, pp. 68–70, Sept 2012.

[3] P. Koopman, "Embedded system security," *Computer*, vol. 37, no. 7, pp. 95–97, Jul. 2004. [Online]. Available: http://dx.doi.org/10.1109/MC.2004.52

[4] M. M. Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, "Emerging frontiers in embedded security," in *2013 26th International Conference on VLSI Design and 2013 12th International Conference on Embedded Systems*, Jan 2013, pp. 203–208.

[5] S. Aman, Y. Simmhan, and V. K. Prasanna, "Energy management systems: state of the art and emerging trends," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 114–119, January 2013.

[6] A. Kailas, V. Cecchi, and A. Mukherjee, "A survey of communications and networking technologies for energy management in buildings and home automation," *Journal of Computer Networks and Communications*, 2012.

[7] C. Rottondi and G. Verticale, "Privacy-friendly load scheduling of deferrable and interruptible domestic appliances in smart grids," *Computer Communications*, vol. 58, pp. 29 – 39, 2015, special Issue on Networking and Communications for Smart Cities. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366414002825

[8] Y. Mo, T. H. J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, Jan 2012.

[9] L. Z. Cai and M. F. Zuhairi, "Security challenges for open embedded systems," in *2017 International Conference on Engineering Technology and Technopreneurship (ICE2T)*, Sept 2017, pp. 1–6.

[10] P. Kocher, R. Lee, G. McGraw, and A. Raghunathan, "Security as a new dimension in embedded system design," in *Proceedings of the 41st Annual Design Automation Conference*, ser. DAC '04. New York, NY, USA: ACM, 2004, pp. 753–760, moderator-Ravi, Srivaths. [Online]. Available: http://doi.acm.org/10.1145/996566.996771

[11] P. Schaumont and A. Aysu, "Three design dimensions of secure embedded systems," in *Security, Privacy, and Applied Cryptography Engineering*, B. Gierlichs, S. Guilley, and D. Mukhopadhyay, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 1–20.

[12] A. P. Fournaris and N. Sklavos, "Secure embedded system hardware design - a flexible security and trust enhanced approach," *Computers & Electrical Engineering*, vol. 40, no. 1, pp. 121 – 133, 2014, 40th-year commemorative issue. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0045790613002930

[13] A. Fiaschetti, V. Suraci, and F. D. Priscoli, "The SHIELD framework: How to control Security, Privacy and Dependability in complex systems," in *2012 Complexity in Engineering (COMPENG). Proceedings*, June 2012, pp. 1–4.

[14] D. Papp, Z. Ma, and L. Buttyan, "Embedded systems security: Threats, vulnerabilities, and attack taxonomy," in *2015 13th Annual Conference on Privacy, Security and Trust (PST)*, July 2015, pp. 145–152.

[15] J. Grand, "Practical secure hardware design for embedded systems," *Proceedings of the 2004 Embedded Systems Conference*, 2004.

[16] D. Henneke, C. Freudenmann, M. Kammerstetter, D. Rua, L. Wisniewski, and J. Jasperneite, "Communications for anyplace: A smart metering platform with management and control functionalities," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, Sept 2016, pp. 1–8.

[17] C. Abreu, D. Rua, T. Costa, P. Machado, J. A. P. Lopes, and M. Heleno, "Anyplace — an energy management system to enhance demand response participation," in *2017 IEEE Manchester PowerTech*, June 2017, pp. 1–6.

[18] D. Rua, C. Abreu, T. Costa, and M. Heleno, "Automation and user interaction schemes for home energy management - a combined approach," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, Sept 2016, pp. 1–5.

[19] IEC 62351, "Power systems management and associated information exchange - data and communications security," International Electrotechnical Commission, Standard.

[20] IEC 62056, "Electricity metering data exchange - the dlms/cosem suite," International Electrotechnical Commission, Standard.

[21] IEEE 2030, "Guide for smart grid interoperability of energy technology and information technology operation with the electric power system (eps), and end-use applications, and loads," Smart Grid Interoperability Series of Standards, Standard, 2011.

[22] NISTIR 7628 Rev. 1, "Guidelines for smart grid cybersecurity," National Institute of Standards and Technology, Standard, 2014. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final

[23] European Parliament, "Directive 2009/72/ec of the european parliament and of the council of 13 july 2009 concerning common rules for the internal market in electricity and repealing directive 2003/54/ec," *Official Journal of the European Union*, 2009.

[24] ——, "Directive 2012/27/eu of the european parliament and of the council of 25 october 2012 on energy efficiency, amending directives 2009/125/ec and 2010/30/eu and repealing directives 2004/8/ec and 2006/32/ec," *Official Journal of the European Union*, 2012.

[25] European Commission, "Commission recommendation of 9 march 2012 on preparations for the roll-out of smart metering systems," *Official Journal of the European Union*, 2012.

[26] European Parliament, "Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," *Official Journal of the European Union*, 1995.

[27] ENISA, "Smart grid security recommendations," European Union Agency for Network and Information Security, Tech. Rep., 2012. [Online]. Available: https://www.enisa.europa.eu/publications/ENISA-smart-grid-security-recommendations

[28] Smart Meters Coordination Group, "Privacy and security approach – part i," CEN-CENELEC-ETSI, Tech. Rep., 2013. [Online]. Available: https://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartMeters/Pages/default.aspx

[29] European Parliament, "Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec," *Official Journal of the European Union*, 2016.

[30] European Network for Cyber Security, "End-to-end security for smart metering," Österreichs Energie, Requirements Catalog, 2018. [Online]. Available: https://oesterreichsenergie.at/files/Downloads%20Netze/E2E-Sicherheit-Anforderungskatalog-EN_1.1_final.pdf

[31] BSI-CC-PP-0073-2014, "Protection profile for the gateway of a smart metering system," Federal Office for Information Security, Protection Profile, 2014. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0073.html

[32] C. Freudenmann, D. Henneke, C. Kudera, M. Kammerstetter, L. Wisniewski, C. Raquet, W. Kastner, and J. Jasperneite, "Open and secure: Amending the security of the bsi smart metering infrastructure to smart home applications via the smart meter gateway," in *Smart Energy Research. At the Crossroads of Engineering, Economics, and Computer Science*, C. Derksen and C. Weber, Eds. Cham: Springer International Publishing, 2017, pp. 136–146.

[33] Netbeheer Nederland – WG DSMR, "Dutch smart meter requirements v4.2.2," Netbeheer Nederland, Requirements Catalog, 2014. [Online]. Available: https://www.netbeheernederland.nl/_upload/Files/Slimme_meter_15_7b581ff014.pdf

[34] FIPS 140-2, "Security requirements for cryptographic modules," National Institute of Standards and Technology, Standard, 2001. [Online]. Available: https://csrc.nist.gov/publications/detail/fips/140/2/final

[35] NIST SP 800-57 Part 1 Rev. 4, "Recommendation for key management, part 1: General," National Institute of Standards and Technology, Standard, 2016. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final

[36] ISO 27034, "Application security," International Organization for Standardization, Standard, 2011.

[37] G. Corser, G. A. Fink, M. Aledhari, J. Bielby, R. Nighot, S. Mandal, N. Aneja, C. Hrivnak, and L. Cristache, "Internet of things (iot) security best practices," IEEE Internet Initiative, White Paper, 2017. [Online]. Available: https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_may_2017.pdf

[38] H. G. Rice, "Classes of recursively enumerable sets and their decision problems," *Transactions of the American Mathematical Society*, vol. 74, no. 2, pp. 358–366, 1953. [Online]. Available: http://www.jstor.org/stable/1990888

[39] C. Kudera, M. Kammerstetter, M. Müllner, D. Burian, and W. Kastner, "Design and Implementation of a Negative Voltage Fault Injection Attack Prototype," in *2018 IEEE International Workshop on Physical Attacks and Inspection of Electronics (PAINE)*, Jun 2018, pp. 1–6.