S3MP: A SCION based Secure Smart Metering Platform

Tony John
Networks and Distributed Systems (Netsys) Lab
Otto von Guericke University Magdeburg
Magdeburg, Germany
tony.john@st.ovgu.de

David Hausheer
Networks and Distributed Systems (Netsys) Lab
Otto von Guericke University Magdeburg
Magdeburg, Germany
hausheer@ovgu.de

***Abstract*—The number of smart meters deployed around the world is increasing every day. Soon, all energy meters will be smart meters, especially in developed countries. The data from smart meters will enable energy companies to manage their distribution more efficiently and reduce wastage. It eliminates the monthly manual meter readings and enables energy companies to implement services like dynamic pricing. Along with the many benefits of smart meters, it raises various privacy and security concerns. Hackers gaining access to them can cause blackouts and other catastrophic failures. The energy consumption data can reveal many household characteristics using off the shelf statistical methods raising privacy concerns. Energy companies should make sure that the smart meter data does not fall into the wrong hands. Smart metering infrastructures ultimately use the Internet for communication, making it vulnerable to present-day Internet security flaws. The SCION network architecture is a secure next-generation Internet architecture that aims to overcome the flaws of today's Internet, especially in terms of security and privacy. This paper presents the design of a secure smart metering platform on top of the SCION network. Furthermore, a prototypical implementation of the proposed approach is developed and evaluated. We show that with our approach it is possible to achieve a high resilience against potential attacks without compromising on performance.**

***Index Terms*—SCION, Smart Metering, privacy, security**

I. Introduction

Internet of Things (IoT) applications are getting more and more widely adopted. The number of IoT devices is growing exponentially every year. Bain predicts that the IoT market will grow to over $500 Billion in 2021 [1]. At the same time, security is still considered the most significant concern in adopting IoT technology, especially in enterprises. Potential threats include weak authentication facilitating unauthorized access, unencrypted communication leaking privacy-sensitive data, and insufficient availability for critical infrastructures.

Our aim in this paper is to provide a secure IoT platform for smart metering. Smart meters are intelligent power meters deployed at customers' premises, enabling a remote reading and processing of measured power data and thus allowing a more efficient and sustainable handling of the power grid [2]. With the number of deployed smart meters increasing day by day, the privacy and security concerns regarding the collected data are also increasing [3], [4]. Privacy of the smart meter data is of high importance as granular energy consumption data can reveal much information about a household [3]. With many smart meters having remote power disconnection capabilities, an attack against the smart metering network can have serious consequences [5]. Today's smart metering infrastructures rely on the Internet as its backbone network for data, making them vulnerable to the attacks possible on today's Internet [6].

SCION [14], which stands for "Scalability, Control, and Isolation On Next-Generation Networks" is a secure next-generation Internet architecture that inherits the benefits of today's Internet while addressing its limitations, especially in the case of security [7]. The path-aware networking capability of SCION provides high resilience against BGP hijacking, and its native multi-path feature provides a high availability and better protection against DDoS attacks. Moreover, SCION's Dynamically Recreatable Key (DRKey) approach [15] provides a fast and secure authentication mechanism.

In this paper, we provide the design and implementation of a secure smart metering platform that uses the SCION network to overcome the vulnerabilities of today's Internet. We developed a prototype of our platform based on real hardware, and performed an evaluation to show that our approach is able to achieve a high reliability without compromising on delay.

To this end, our paper provides the following contributions:

1) Design of a smart metering platform using the SCION Internet architecture for communication
2) Implementation of a SCION based smart metering prototype
3) Evaluation of different methods based on the implemented prototype

The remainder of this paper is structured as follows. Section 2 delves into the current state of security in smart metering infrastructures and their vulnerabilities, the most relevant medium and protocols currently used in smart metering and the SCION Internet architecture. Section 3 presents the design of a smart metering platform using SCION, while Section 4 discussed the implementation of a SCION-based smart metering prototype. Two alternative methods of using SCION in smart metering are evaluated using the prototype, and the results are compared in Section 5. Finally, the paper is concluded and the possible future works are discussed in Section 6.

978-3-903176-32-4

II. Background and Related Work

This section describes the technologies used in current smart meter infrastructures and the SCION Internet architecture.

A. Smart Metering Infrastructures

Figure 1 shows a typical smart metering infrastructure using Power Line Communication (PLC) at the endpoints. A collection of smart meters communicate with a data concentrator through PLC. This collection of smart meters can be the meters in a neighbourhood or a housing complex. The data concentrator communicates with the head end system via the Internet through LTE, Ethernet or other WAN communication links. The head end system consists of data collection applications run by the Energy distribution company [2].

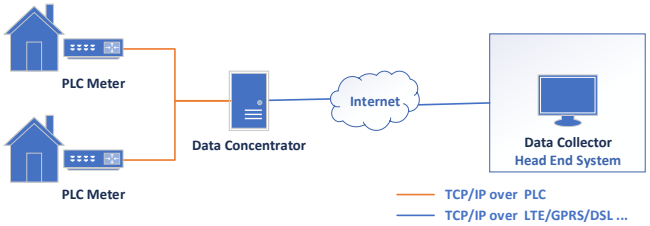

Fig. 1. A typical Smart Meter Infrastructure

1) Vulnerabilities of Current Smart Metering Infrastructures: Current smart metering infrastructures use the Internet for their communication, which brings the vulnerabilities of today's Internet to smart meters, making the smart meters vulnerable to DDoS attacks and man in the middle attacks. Hackers gaining access to a smart meter can even cause house fires and explosions [9]. A comprehensive survey of security and privacy issues in Smart Grids and Smart Metering Infrastructures is provided in [8].

The smart meters' data privacy is of paramount importance as it can reveal household activities. Molina-Markham et al. [4] show that even without prior knowledge of household activities, intricate power usage patterns can be extracted from the smart meter data using commonly available statistical methods. The Border Gateway Protocol (BGP) based routing in the Internet does not provide mechanisms to specify a particular path to use [6]. This can result in the data passing through a country or region that may intercept it and use it for malicious activities [10].

B. DLMS/COSEM

DLMS/COSEM is a global standard for smart energy metering, control and management [11]. It is the de facto standard for smart metering. DLMS/COSEM specifies an object-oriented data model, an application layer protocol and communication profiles for specific media. DLMS stands for Device Language Message Specification, and COSEM stands for Companion Specification for Energy Metering. The DLMS User Association does the development and maintenance of this standard.

1) jDLMS: jDLMS is an open-source Java library implementing the DLMS/COSEM communication standard [13]. It is licensed under GNU Public License v3, and maintained by OpenMUC.

C. SCION

Scalability, Control and Isolation on next-generation Networks (SCION) is a secure next-generation Internet architecture, designed to provide route control, failure isolation, and explicit trust information for end-to-end communication [14].

1) Isolation Domains: SCION inherits the concept of Autonomous Systems (ASes) from the Internet and introduces the concept of Isolation Domains (ISD). An ISD groups ASes with independent routing planes. Different ISDs interconnect to provide global connectivity. The isolation provided by the ISD facilitates protection of ASes from routing attacks by foreign ASes and misconfigurations, endpoints to have robust control of both inbound and outbound traffic and scalable routing updates while maintaining high path freshness.

SCION end hosts learn about new path segments through Path Construction Beacons (PCB), combining these segments can create end to end paths. Embedded cryptographic mechanisms ensure that path construction is constrained to routing policies of ISDs and the receiving AS. These mechanisms make communication in SCION path aware. It also enables multi-path communication.

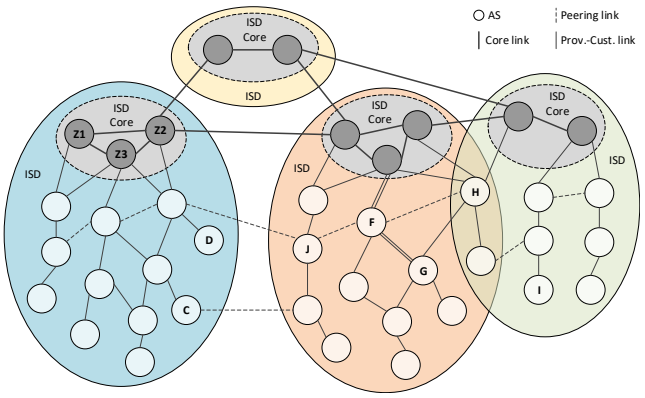

Fig. 2. Autonomous systems (ASes) grouped into four ISDs. [14]

2) Dynamically Recreatable Key: Dynamically Recreatable Key (DRKey) enables routers and end hosts to derive symmetric cryptographic keys on the fly efficiently from a single local secret in the certificate server. Each certificate server is responsible for the selection of the secret value. This value is the root for a symmetric key hierarchy, and the keys of a level are derived from the keys of the previous level using an efficient Pseudo-Random Function (PRF) [15]. DRKey can be used to authenticate data plane packets.

3) SCION-IP Gateway (SIG): SCION-IP Gateway (SIG) enables SCION to interoperate with legacy IP applications. Forwarding legacy IP packets through the SCION network requires encapsulation of IP packets in SCION packets. SIG takes care of IP packets' encapsulation and decapsulation and provides a transparent IP link between two ASes.

4) SCIONLab: SCIONLab is a global research network based on the SCION Internet architecture [16]. The testbed comprises a globally connected network of ASes, enabling the creation of personal ASes and running experiments in a SCION network.

III. Secure Smart Metering Infrastructure

This section presents the security requirements of a smart metering infrastructure and how we integrated SCION into our platform in order to achieve these requirements.

A. Security Requirements

The specific security requirements that we aim to achieve for our smart metering platform are as follows:

1) Geofencing: limit the packet routing to a predefined area
2) Resilience against DDoS attacks
3) Resilience against man in the middle attacks
4) Failure recovery

In the following, we discuss and compare to what extent these requirements are met in today's Internet and in a SCION network.

*1) **Today's Internet**:*

Geofencing: The Internet relies on the Border Gateway Protocol (BGP) to achieve reliable routing. It is prone to thousands of attacks every year [17]. BGP routing is not path aware, and it does not have mechanisms to ensure that packets follow a particular path. The most common attack on BGP is BGP hijacking [18]. By BGP hijacking, a bad actor can reroute the packets to a malicious location.

DDoS attacks: The Internet does not provide network-level access control. The attempts to mitigate DDoS attacks are not 100% successful in all types of DDoS attacks [19]. All of these fixes used BGP and carry the flaws of BGP with them.

Man in the middle attacks: Authentication of paths on a packet level is not possible using the Internet, making it prone to man in the middle attacks, especially in constrained devices such as smart meters.

Failure recovery: BGP is slow to react in case of failures in a connecting AS. It can take minutes to react to the change [20].

*2) **SCION Network**:*

Geofencing: SCION routing is path aware. ISDs provide isolation to intra-domain routing. Furthermore, the ability to choose paths can guarantee geofencing even in case of inter-domain communication. Since SCION is BGP free, BGP hijacking is not applicable here. Geofencing can ensure the privacy of smart meter data by ensuring that the data does not leave the intended path.

DDoS attacks: SCION provides a host of mechanisms to fight against DDoS attacks.

1) SCION supports multi-path communication. An attacker will have to attack all the paths to ensure a failure making it harder to accomplish an attack.
2) SCION supports hidden paths. These paths are not advertised, making it much harder to mount an attack on it.
3) As SCION supports network-level access control, it can be used to create a DDoS defence mechanism.

Man in the middle attacks: Using DRKey the path can be authenticated on a packet level, making it harder to mount a man in the middle attack on a SCION network.

Failure recovery: SCION supports multi-path communication, making it possible to have a fast failover if one path fails.

The above comparison shows that with SCION all the desired security requirements of a smart metering infrastructure can be achieved, whereas today's Internet falls short.

B. SCION Smart Metering Infrastructure

Figure 3 depicts the design of our proposed SCION-based smart metering infrastructure.

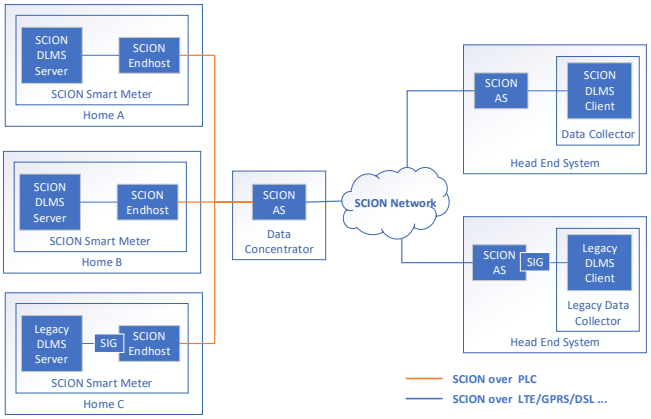

Fig. 3. Smart Meter Infrastructure using SCION

A SCION endhost is deployed on each SCION smart meter. To enable the communication over the SCION network, these SCION endhosts are connected with a SCION AS hosted on the data concentrator. Likewise, the data collector is connected to another SCION AS hosted on the head end system in order to fetch the data from the smart meters. Equal to the original infrastructure depicted in Figure 1, the communication between the smart meter and data concentrator happens over PLC. The data concentrator's connection to the SCION network can be through various media such as Ethernet, LTE or GPRS. Multiple SCION connections can be established from the data concentrator to the head end system, to utilize the multi-path communication of SCION. For example, a connection to the SCION network can be through LTE and another through a leased line.

1) DLMS/COSEM over SCION: Each smart meter runs a DLMS server and the data collector runs a DLMS client. There are two alternative methods to enable DLMS/COSEM communication over the SCION network:

1) The use of SIG enables legacy DLMS/COSEM applications to communicate over SCION.
2) The extension of a DLMS/COSEM library with SCION enable a native communication over the SCION network.

Both methods are depicted in Figure 3. Applying SIG provides a lower barrier for the use of SCION as its significant advantage is that legacy DLMS/COSEM libraries and applications can be used without any changes, reducing the development time. However, this approach has some significant drawbacks, such as:

1) Additional configuration is required at the head end system and the smart meter.
2) Additional overhead is introduced to the whole system.
3) Key features of SCION such as path selection and DRKey cannot be utilized.

A DLMS/COSEM application that supports SCION natively facilitates the full utilization of all the features of SCION. However, development effort is required for writing or extending a DLMS/COSEM library and application to support a native SCION communication.

C. SCION DLMS Implementation

The jDLMS library was selected to be extended for native SCION support. jDLMS is an open-source Java library maintained by OpenMUC [13]. It has a server stack and a client stack that supports communication via TCP/IP.

SCION is written in the Go programming language [21]. It provides the package 'appnet' to develop Go applications that can communicate through SCION. To enable SCION communication in Java, a Java binding for the 'appnet' Go package needed to be created. The 'gojava' application by sridharv [22] provides a method to create Java bindings for Go packages.

A wrapper for the appnet package with the required methods was created in Go in the format suitable for the 'gojava' application. Then, a java binding was created for this wrapper called 'javaappnet'. The 'javaappnet' package enables path selection and failover to another path in case of a failure. The current Go implementation of SCION supports both UDP and QUIC for communication. Using 'javaappnet', a SCION UDP library was created to facilitate communication over SCION in Java applications. Finally, the server and client stack of the jDLMS library was extended to use the newly created Java SCION libraries. The resulting SCION jDLMS library can be used to create DLMS/COSEM applications that can communicate over SCION natively.

1) DRKey for Authentication: The jDLMS library provides a built-in authentication mechanism. Instead of using pre-shared keys for authentication, the 'javaappnet' package was further extended to support DRKey. The keys derived by DRKey based on the client/server pair can be used for authentication of DLMS connections. As the keys are renewed periodically, the security flaw from using fixed keys [23] can be mitigated.

IV. SCION Smart Metering Prototype

To evaluate our approach, we have implemented a prototype of the SCION smart metering infrastructure. Figure 4 depicts the hardware and software components of the prototype implementation.

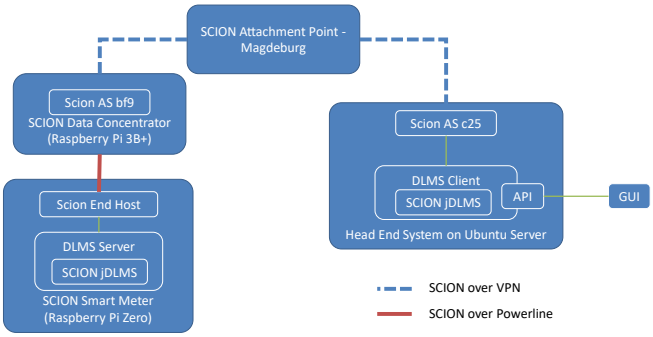

Fig. 4. Prototype SCION Smart Meter Infrastructure

A. SCION Smart Meter

This is the smart electricity meter part of the SCION smart metering infrastructure. It has an electric input and an electric output where electrical appliances can be connected simulating the electric power usage in a home. This meter also has the ability to remotely shutdown the electricity output.

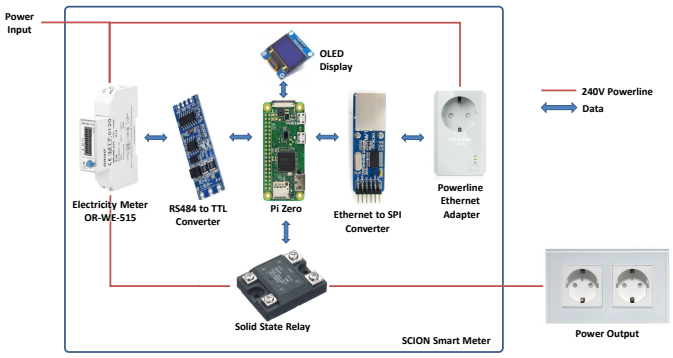

Fig. 5. Hardware Configuration of the SCION Smart Metering Prototype

1) Hardware: Figure 5 illustrates the hardware configuration of the SCION smart metering prototype. The heart of our SCION smart meter is a Raspberry Pi Zero v3.1 (PiZero). Orno OR-WE-514 is a single-phase electricity meter with a Modbus interface for accessing the electricity consumption data [24]. The solid-state relay connects or disconnects the electricity output from the supply. The TL-PA4010 Powerline Adapter enables Ethernet communication through power lines. The OLED screen displays the SCION address of the meter and displays messages from the client if any.

2) Software: The PiZero runs the Raspbian operating system. SCION endhost applications are installed on the PiZero from the SCIONLab package repositories [25]. Furthermore, a DLMS server is implemented based on the SCION jDLMS library and deployed. It models the electric meter so that a DLMS client can access all the parameters. It also has COSEM methods to disconnect the power output remotely by a client and display messages sent from a client.

B. SCION Data Concentrator

The SCION data concentrator acts as a bridge between the SCION smart meter and the head end system. It runs a SCION AS. For our prototype, the data concentrator is hosted on a Raspberry Pi 3B+. The use of a power line adapter enables the power line communication with the SCION smart meter on the Raspberry Pi Zero.

C. Head End System

The head end system is based on a PC running Ubuntu 20.1. A SCION AS is installed on this system using the SCIONLab packages. Furthermore, a DLMS client is developed using the SCION jDLMS library and deployed. It exposes an API to access the parameters of the SCION smart meter. It also provides API calls for setting the message on the meter's OLED screen and remote disconnection of the power. A node-red-based graphical user interface is also provided to visualize the meter's electricity consumption and to control the meter. Figure 6 depicts the GUI of the prototype head end system. The GUI provides the option to read the meter continuously every second and also to read just once. There are buttons to connect and disconnect the power output from the meter remotely. The graph on the right updates every second to show the live power usage while the meter is read continuously. A demo video of the prototype is available here: [26]

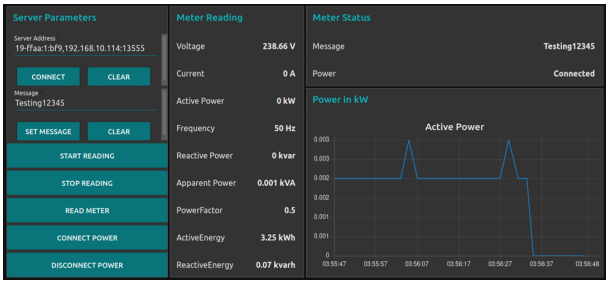

Fig. 6. Graphical User Interface of the Head End System Prototype

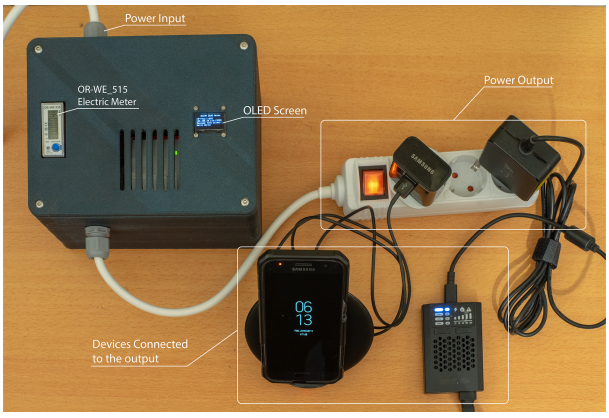

Fig. 7. SCION Smart Meter Prototype

V. Evaluation

This section provides the results of the prototype evaluation. We evaluated both methods of using SCION in a smart meter infrastructure: a) through SIG and b) by using SCION natively. In the case of SIG, the DLMS/COSEM applications use the unmodified version of the jDLMS library, while in the native SCION case, they use the SCION jDLMS library.

A. Evaluation Method

The following steps describe the evaluation method. These steps were carried out for both SIG and native SCION cases, and the results recorded.

1) Meter reading delay measured for 500 readings 500 milliseconds apart.
2) Delay measurement carried out every hour from 8am to 7pm in a day and values were averaged across the hours for each reading number.
3) CPU and memory utilization measured using 'htop' during one delay measurement session, and the results averaged.

B. Results

Table I compares the results of SIG vs native SCION. While using SIG provides the benefit of reusing legacy DLMS/COSEM applications, it performs poorly compared to the native SCION setup. There is a significant overhead in terms of CPU and memory utilization when using SIG. The reading delay is larger by six milliseconds, and SIG requires extensive configuration at all infrastructure levels. Another drawback is that not all SCION features such as path selection and DLMS connection authentication using DRKey can currently be used with SIG. Figure 8 shows the difference in reading delay using a cumulative distribution function.

TABLE I
Evaluation result of Native SCION vs SIG configurations

	Native SCION	**SIG**
CPU utilization of PI Zero	14.1%	24.35%
Memory utilization of Pi Zero	85Mb	106Mb
Average reading delay	32.8 ms	38 ms

VI. Conclusion and Future Work

Privacy and security are of paramount importance for a smart metering infrastructure. As shown in related work, the complex energy usage patterns and household characteristics can be derived from the smart meter data without any prior knowledge. Moreover, hackers gaining access to smart meters could cause significant damages. We infer that securing the smart metering infrastructure is non-negotiable. In the following, we review the contributions claimed in Section 1.

1. *A smart metering platform using the SCION Internet architecture for communication:* The SCION next-generation Internet architecture provides a number of security properties that are not available on today's Internet, including geofencing capabilities, resilience against DDoS attacks, network-level

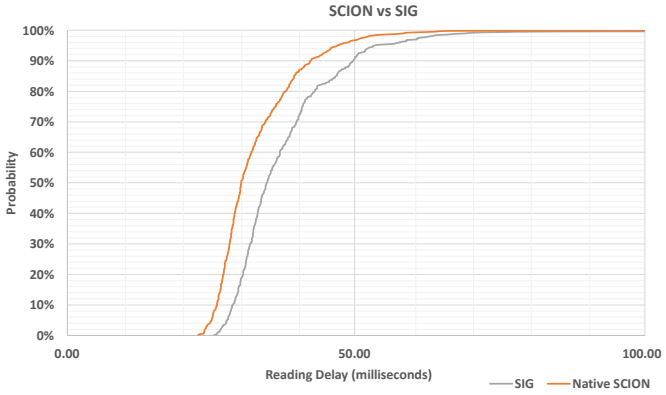

Fig. 8. Reading delay: Native SCION vs SIG

access control and hidden paths. Moreover, failure recovery and high availability is achieved through multi-path communication. To use these properties, we have developed a SCION-based smart metering infrastructure as described in Section 3. Our implementation includes a SCION jDLMS library which uses DRKey for authentication instead of fixed keys.

2. *Implementation of a SCION based smart metering prototype:* Section 4 describes the prototypical implementation of the SCION smart metering infrastructure. The implementation includes a DLMS application which is based on our SCION jDLMS library. The hardware of the prototype was realized using off the shelf components and Raspberry Pi single-board computers.

3. *Evaluation of different methods based on the implemented prototype:* We evaluated and compared two methods of using SCION in a smart metering infrastructure: a) through SIG and b) by using SCION natively. As discussed in Section 5, the native SCION implementation required more development effort, but it showed better performance in the evaluation. A native SCION implementation is required to take full advantage of SCION's security features.

A. Future Work

Currently, the SCION jDLMS library uses a Java binding to the SCION appnet package to enable Java to communicate with SCION. In a very resource-constrained device, this can lead to crashes. Development efforts are ongoing to integrate SCION into the Linux kernel. When completed, this will remove the aforementioned additional overhead.

The SCION smart metering prototype presented in this paper runs on a Raspberry Pi Zero. The Smart meters available in the market today have less powerful processors and resources. Additional development and testing efforts are required to optimize the library to run on these resource-constrained devices.

Acknowledgment

We would like to extend our sincere gratitude and appreciation for all the help provided by our colleagues in the SCION IoT team.

References

[1] "IoT Market Size Will More Than Double — Bain & Company." https://www.bain.com/about/media-center/press-releases/2018/bain-predicts-the-iot-market-will-more-than-double-by-2021/ (accessed Jan. 20, 2021).
[2] Wang, Yi, et al. "Review of smart meter data analytics: Applications, methodologies, and challenges." IEEE Transactions on Smart Grid 10.3 (2018): 3125-3148.
[3] Beckel, Christian, et al. "Revealing household characteristics from smart meter data." Energy 78 (2014): 397-410.
[4] Molina-Markham, Andrés, et al. "Private memoirs of a smart meter." Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building. 2010.
[5] "Trump Declares National Emergency As Foreign Hackers Threaten U.S. Power Grid." https://www.forbes.com/sites/daveywinder/2020/05/02/trump-declares-national-emergency-as-foreign-hackers-threaten-us-power-grid/ (accessed Dec. 07, 2020).
[6] Goldberg, Sharon, et al. "How secure are secure interdomain routing protocols." ACM SIGCOMM Computer Communication Review 40.4 (2010): 87-98.
[7] Zhang, Xin, et al. "SCION: Scalability, control, and isolation on next-generation networks." 2011 IEEE Symposium on Security and Privacy. IEEE, 2011.
[8] Kumar, Pardeep, et al. "Smart grid metering networks: A survey on security, privacy and open research issues." IEEE Communications Surveys Tutorials 21.3 (2019): 2886-2927.
[9] "Smart electricity meters can be dangerously insecure, warns expert — Smart homes — The Guardian." https://www.theguardian.com/technology/2016/dec/29/smart-electricity-meters-dangerously-insecure-hackers (accessed Jan. 01, 2021).
[10] "The Dark Side of the Smart Grid." https://www.powermag.com/the-dark-side-of-the-smart-grid/ (accessed Jan. 01, 2021).
[11] "Specification — dlms." https://www.dlms.com/dlms-cosem (accessed Jan. 01, 2021).
[12] "Security in DLMS A White Paper by the DLMS User Association," 2019.
[13] "jDLMS Overview – DLMS/COSEM – OpenMUC." https://www.openmuc.org/dlms-cosem/ (accessed Jan. 01, 2021).
[14] Perrig, Adrian, et al. SCION: a secure Internet architecture. Springer, 2017.
[15] "Dynamically Recreatable Key (DRKey) Infrastructure — SCION documentation." https://scion.docs.anapaya.net/en/latest/cryptography/DRKeyInfra.html (accessed Jan. 01, 2021).
[16] Kwon, Jonghoon, et al. "SCIONLab: A next-generation internet testbed." IEEE ICNP. 2020.
[17] "14,000 Incidents: A 2017 Routing Security Year in Review — Internet Society." https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/ (accessed Jan. 01, 2021).
[18] Cloudflare, "What Is BGP? BGP Routing Explained — Cloudflare," 2017. https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/ (accessed Jan. 01, 2021).
[19] "What Is a Distributed Denial-of-Service (DDoS) Attack? — Cloudflare." https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (accessed Jan. 01, 2021).
[20] Labovitz, Craig, et al. "Delayed Internet routing convergence." ACM SIGCOMM Computer Communication Review 30.4 (2000): 175-187.
[21] "GitHub - scionproto/scion: This repository represents the main SCION version." https://github.com/scionproto/scion (accessed Jan. 01, 2021).
[22] "GitHub - sridharv/gojava: GoJava - Java bindings for Go packages." https://github.com/sridharv/gojava (accessed Jan. 01, 2021).
[23] Shuaib, Khaled, et al. "Resiliency of Smart Power Meters to Common Security Attacks." ANT/SEIT. 2015.
[24] "OR-WE-514 Single-phase meter 100A with port RS-485." Accessed: Jan. 01, 2021. [Online]. Available: www.orno.pl
[25] "Configuration - SCIONLab Tutorials." https://docs.scionlab.org/content/config/ (accessed Jan. 01, 2021).
[26] "S3MP Demo Video." https://youtu.be/YvT-otHCpA8