

[DOI: 10.20472/IAC.2016.024.090](https://doi.org/10.20472/IAC.2016.024.090)

GURKAN TUNA

Trakya University, Turkey

RESUL DAŞ

Fırat University, Turkey

SECURE WEB-BASED COMMUNICATION FRAMEWORK FOR SMART HOME SYSTEMS DESIGNED FOR THE ELDERLY AND DISABLED

Abstract:

As a result of the increasing awareness about common daily problems of the elderly and disabled in recent years, novel technology solutions have been designed and developed. Thanks to smart homes which involve a set of various sensors and devices to make the daily lives of the elderly and disabled easier and provide remote monitoring ability to the family members, nowadays the elderly and disabled stay in their houses instead of assisted-living centres. On the other hand, elderly and disabled people living alone may be exposed to potential security threats. In this study, a framework is proposed in order to achieve secure communication over the Internet. In the proposed framework, information to be transferred is first encrypted using RSA algorithm and then sent to the recipient. For security reasons, after the recipient reads the encrypted information, traces of the communication should be removed. For this objective, before the transfer, the sender determines how many seconds the message will be available to the recipient via a link. When the recipient receives the link, he/she can open the message with the secret key. After the predefined time, the message is deleted from the database used by the framework. The framework can be used to enable confidential messaging between smart home inhabitants and people they would like to communicate. The framework can easily be integrated into smart home control panels or web-based interfaces of smart home systems.

Keywords:

Smart homes; web-based communication; information security; the disabled; the elderly.

JEL Classification: C88, L86, L63

Introduction

Although generally the elderly and disabled prefer living in their houses, their health and daily activities must be constantly monitored since elderly people are prone to different types of accidents and disabled people cannot perform some movements and activities. Continuous remote monitoring enables to provide immediate help in case of an urgent situation.

Smart homes are technologically advanced homes with domestic task automation, easier communication, and higher security abilities. Since they provide abilities to provide the special needs of the elderly and disabled, they play a key role in improving the quality of services provided by healthcare companies. Basically, smart homes typically consist of a control panel, a web-based remote management tool, a set of wireless/wired sensors and motion detectors, a set of audio-visual based systems, and a state-of-the art monitoring system supported by a set of machine learning algorithms and analytics (Gaddam, Mukhopadhyay and Gupta, 2010; Suryadevara and Mukhopadhyay, 2011; Tuna, Daş and Tuna, 2015). Smart home systems are generally installed and maintained in residential environments without any complexity and their components are either barely visible or almost invisible since the acceptance level of smart home automation systems is higher if invisible components are preferred (Gaddam, Mukhopadhyay and Gupta, 2010; Suryadevara and Mukhopadhyay, 2011). Thanks to smart homes, data collected by distributed sensor nodes and audio-visual based systems enable monitoring the daily activities of inhabitants and learning the personal activity patterns (Gaddam, Mukhopadhyay and Gupta, 2010; Suryadevara and Mukhopadhyay, 2011; Lê, Nguyen and Barnett, 2012; Tuna, Daş and Tuna, 2015; Daş, Tuna and Tuna, 2015). As soon as the monitored patterns deviate from the patterns accepted as normal, an alert is generated to let both healthcare providers and family members take immediate actions (Jin Wang et al., 2014; Moutacalli et al., 2013; Jalal and Kamal, 2014; Jovanov et al., 2003).

Although smart homes provide remote monitoring ability and contribute to the enhancement of the daily lives of the elderly and disabled, potential security threats still exist, especially in terms of information security. Information leakage to outside world may have bad consequences in terms of the safety and security of the inhabitants since the idea of smart home technology creates new vulnerabilities and complexity. In this context, we propose a framework to provide web-based secure communication for smart home inhabitants.

Related Work

Smart homes provide their owners comfort, security, low operating costs and convenience at all times. In addition, with advanced sensor technologies they constitute

in-home and self-learning care solutions to take some of the worry of family members off by helping in constantly monitoring the inhabitants. Although they provide many benefits, security related concerns arise if their services are not designed without considering information security (Yoon, Park and Yoo, 2015; Han, Jeon and Kim, 2015). Because, smart homes can be remotely controlled via smart phones, tablets or personal computers; since, they are typically connected to the Internet. Once a device such as a smart phone is connected to smart home network, it is vulnerable to any hacker who is able to get in since it becomes a single point of failure. Therefore, careful analysis is required to find out security vulnerabilities of smart homes and propose countermeasures since network-controlled embedded devices introduce many security threats into smart homes.

In recent years, many smart home appliances and various wearable devices which have communication functions to connect the Internet and thus can be interacted have been developed. While those devices provide a wide range of services to their users, because of the nature of the Internet of Things (IoT) environment, appropriate security functions should be applied to enable secure and trustworthy smart home services (Han, Jeon and Kim, 2015). The security requirements of different smart home components are explained in (Han, Jeon and Kim, 2015). Similarly, a new quality of service (QoS) concept and a new integrated concept for smart home security systems are proposed in (Hager et al., 2012). In the proposed approach in (Hager et al., 2012), all communication channels, all system and user-data, and all kinds of access to the smart home system are secured by a state-of-the art security framework. In addition, based on the classification of each specific smart home service, the authors also present a solution to prevent congestion situations inside the smart home network.

A cyber-physical system (CPS) can be described as a composition of independently interacting components and include a control system, computational elements, and a communications system. CPSs are used in different applications including smart grid, smart home, and healthcare systems. Although CPSs transmute how human interact with the physical world, since each system requires different levels of security based on the information carried, security and trust measures are needed to counter possible security violations and privacy leakage. Security and privacy concerns of CPSs are reviewed and solutions to ensure their security and trust are presented in (Konstantinou et al., 2015).

Although IoT technologies enable to realize the state-of-the art energy-efficient smart homes, information security risks related to the use and potential misuse of sensitive information, the integration of security-enhancing measures in the design and development of the IoT devices is not straightforward and requires substantial investigation. In this respect, a risk analysis applied on a smart home automation system is presented in (Jacobsson, Boldt and Carlsson, 2014). As proven in the study, while the implementation of standard security features can minimize most of information serious

risks, the integration process is complex in nature and requires careful consideration. In this regard, for the IoT technologies in smart home domain, a new paradigm called the Information-Centric Networking (ICN) provides many features including content-based security, in-network caching, native multicast support, and easy data access by leveraging location-independent, unique and content names. A solution which encompasses the definition of a flexible, expressive naming scheme for data/command exchanges and configuration/ management operations for smart homes is proposed in (Amadeo et al., 2015).

For smart home systems, data security and privacy must be handled throughout the complete data lifecycle, namely data generation/collection, transfer, storage, processing and sharing (Chakravorty, Wlodarczyk and Chunming Rong, 2013). In this respect, for analysis of sensor data from smart homes, a framework to maintain information security and preserve data privacy without compromising on data utility is presented in (Chakravorty, Wlodarczyk and Chunming Rong, 2013). If necessary security measures are not taken into considerations and not applied, internet-enabled smart home devices can be turned into highly dangerous spots for distributed internet-based attacks (Hoang and Pishva, 2015).

Proposed Secure Web-Based Communication Framework

The framework proposed in this paper relies on well-known RSA algorithm. RSA (Rivest, Shamir and Adleman, 1978) was developed by Ron Rivest, Adi Shamir and Leonard Adleman in 1978 and is a public-key cryptography method based on algorithmic difficulty of separating factored integers. The framework basically consists of two main steps. In the first step of the framework, the recipient selects the prime p , q , and e values or can use prime numbers suggested by the framework. Moreover, the framework automatically checks whether the numbers entered by the users are prime or not. After the prime values are entered, when the "Create Key" button is clicked, public and private (secret) keys are obtained. Finally, the recipient sends the public key to the sender. In the second step of the framework, the sender encrypts the text, creates a link with the public key received from the recipient, and finally transmits the link created to the recipient. Then, the recipient displays the message with the secret key created in the first step. The messages created by the framework are stored in the database as RSA-encrypted. Hence, access to the messages manually without using the framework is prevented. The framework enables confidential messaging between two users and can be integrated into smart home control panels or their web-based interfaces.

User interface of the proposed communication framework is shown in Figure 1. It appears when the user starts the software application developed to implement the proposed framework. It has three main buttons, namely Create Message, Create Key and How to Use, respectively. When the user clicks Create Key button, as shown in Figure 2, he/she chooses primes p and q values and then clicks Create Key button in the screen. Or

he/she can prefer clicking Create Random Value button instead. After Create Key button is clicked, the framework generates public and secret key values as shown in Figure 3. The recipient sends the public key to the sender in the last step.

Figure 1: Homepage of the user interface

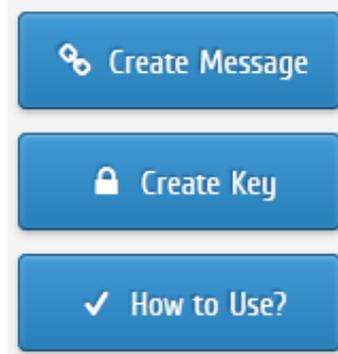


Figure 2: Prime numbers created by the recipient using

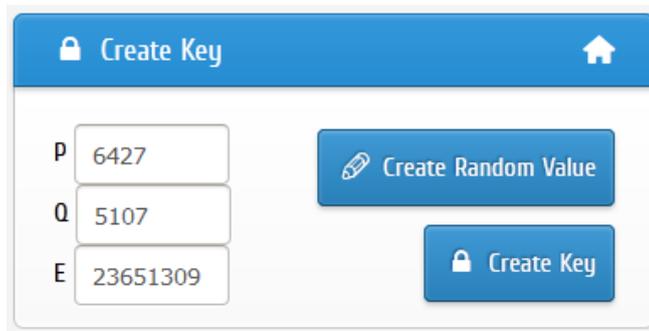


Figure 3: Public and secret keys generated by the framework

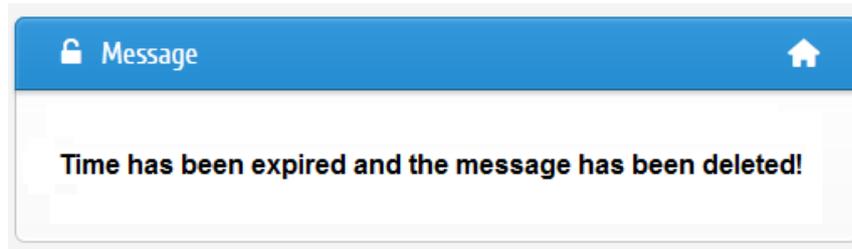


As shown in Figure 4, when the sender receives the public key from the recipient, he/she creates the message and adjusts message-related parameters. When the encrypted message is ready, the sender clicks Create Link button. Then the link created and transmitted to the recipient.

Figure 4: Creating a message and its link

As shown in Figure 5, the recipient enters the secret key values and clicks Show Message button. As shown in Figure 6, the recipient can read the message for the specified time. As shown in Figure 7, when the specified time is over, a message which expresses that time is over so the message has been deleted is shown in the screen. Thus, taking the screenshot is prevented.

Figure 5: The message is shown
Figure 6: Message interface

Figure 7: Time is over and the message has been deleted

After the recipient reads the message in the specified time, the message is deleted from the database. If the recipient clicks on the link that he/she received earlier, he/she will not be able to read the message again and he/she will see the screen shown in Figure 8.

Figure 8: No message interface

Conclusion

Digital information and the expansion of the Internet have transformed both industrial activities and social life. With the idea of using electronics in smart home appliances and enabling them to connect the Internet, in recent years, mankind has witnessed an upsurge in the use of smart home appliances. Although internet-controlled functions have made smart home appliances quite attractive to most consumers, serious challenges must be addressed since those devices are designed for specific domestic functions and lack processing capacity required for information security components.

Smart homes enable the elderly and disabled to enjoy the comfort of living at home with full confidence and offer peace of mind to the family members and relatives. On the other hand, the elderly and disabled living alone may be exposed to potential information security threats since smart homes involve a set of wireless/wired sensors and rely on various communication technologies. In this paper, we proposed a web-based secure communication framework to eliminate potential information security threats. The framework is based on the well-known RSA algorithm and this way user messages can be transferred to recipients securely. The framework is supported by an easy-to-use graphical user interface for user comfort and can be integrated into smart home control panels or web-based smart home interfaces.

Acknowledgment

This work was supported by Research Fund of the Trakya University. Project Number: 2016/112.

References

- Amadeo, M., Campolo, C., Iera, A. and Molinaro, A. (2015). Information Centric Networking in IoT scenarios: The case of a smart home. *2015 IEEE International Conference on Communications (ICC)*, pp. 648-653.
- Chakravorty, A., Wlodarczyk, T. and Chunming Rong, (2013). Privacy Preserving Data Analytics for Smart Homes. *2013 IEEE Security and Privacy Workshops*, pp. 23-27.
- Daş, R., Tuna, G. and Tuna, A. (2015). Design and Implementation of a Smart Home for the Elderly and Disabled. *International Journal of Computer Networks and Applications (IJCNA)*, 2(6), pp. 242-246.
- Gaddam, A., Mukhopadhyay, S. and Gupta, G. (2010). Towards the Development of a Cognitive Sensors Network Based Home for Elder Care. *2010 6th International Conference on Wireless and Mobile Communications*, pp. 484-491.
- Hager, M., Schellenberg, S., Seitz, J., Mann, S. and Schorcht, G. (2012). Secure and QoS-aware communications for smart home services. *2012 35th International Conference on Telecommunications and Signal Processing (TSP)*, pp. 11-17.
- Han, J., Jeon, Y. and Kim, J. (2015). Security considerations for secure and trustworthy smart home system in the IoT environment. *2015 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 1116-1118.
- Hoang, N. and Pishva, D. (2015). A TOR-based anonymous communication approach to secure smart home appliances. *2015 17th International Conference on Advanced Communication Technology (ICACT)*, pp. 517-525.
- Jacobsson, A., Boldt, M. and Carlsson, B. (2014). On the Risk Exposure of Smart Home Automation Systems. *2014 International Conference on Future Internet of Things and Cloud*, pp. 183-190.
- Jalal, A. and Kamal, S. (2014). Real-time life logging via a depth silhouette-based human activity recognition system for smart home services. *2014 11th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, pp. 74-80.
- Jin Wang, Zhongqi Zhang, Bin Li, Sungyoung Lee, and Sherratt, R. (2014). An enhanced fall detection system for elderly person monitoring using consumer home networks. *IEEE Transactions on Consumer Electronics*, 60(1), pp.23-29.
- Jovanov, E., O'Donnell Lords, A., Raskovic, D., Cox, P., Adhami, R. and Andrasik, F. (2003). Stress monitoring using a distributed wireless intelligent sensor system. *IEEE Eng. Med. Biol. Mag.*, 22(3), pp.49-55.
- Konstantinou, C., Maniatakos, M., Saqib, F., Hu, S., Plusquellic, J. and Jin, Y. (2015). Cyber-physical systems: A security perspective. *2015 20th IEEE European Test Symposium (ETS)*, pp. 1-8.
- Lê, Q., Nguyen, H. and Barnett, T. (2012). Smart Homes for Older People: Positive Aging in a Digital World. *Future Internet*, 4(4), pp.607-617.
- Moutacalli, M., Marmen, V., Bouzouane, A. and Bouchard, B. (2013). Activity pattern mining using temporal relationships in a smart home. *2013 IEEE Symposium on Computational Intelligence in Healthcare and e-health (CICARE)*, pp. 83-87.

- Rivest, R., Shamir, A. and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), pp.120-126.
- Suryadevara, N. and Mukhopadhyay, S. (2011). Wireless sensors network based safe home to care elderly people: A realistic approach. *2011 IEEE Recent Advances in Intelligent Computational Systems*, pp. 1-5.
- Tuna, A., Daş, R. and Tuna, G. (2015). Integrated Smart Home Services and Smart Wearable Technology for the Disabled and Elderly. *Proceedings of 4th International Conference on Data Management Technologies and Applications*, Colmar, France, pp. 173-177.
- Yoon, S., Park, H. and Yoo, H. (2015). Security Issues on Smarthome in IoT Environment. *Computer Science and its Applications*, 330, pp.691-696.