6-26-2018

A Redundancy-based Security Model for Smart Home

Monjur Ahmed
Waikato Institute of Technology, monjur.ahmed@protonmail.com

A Redundancy-based Security Model for Smart Home

Research-in-Progress

Monjur Ahmed
Waikato Institute of Technology
Hamilton 3240, New Zealand
e-mail: Monjur.Ahmed@wintec.ac.nz

Abstract

Recent developments in smart devices, Cloud Computing and Internet of Things (IoT) are introducing network of intelligent devices. These intelligent devices can be used to develop smart home network. The home appliance in a smart home forms an ad-hoc network. A smart home network architecture can be exploited by compromising the devices it is made up of. Various malicious activities can be performed through such exploitation. This paper presents a security approach to combat this. By using a collaborative and redundant security approach, the ad-hoc network of a smart home would be able to prevent malicious exploitation. The security approach discussed in this paper is a conceptual representation on the proposed security model for smart home networks.

Keywords: Ad-Hoc Networking, Collaboration, Redundancy, Security, Smart Home.

Introduction

In a smart home, intelligent devices create ad-hoc smart network or connect to an existing one; and a smart home network is made up of different services, applications and devices (Batalla, Vasilacos & Gajewski 2017). The concept of smart home is accelerated by developments in recent computing approaches, for example Cloud Computing and IoT. Better service and surveillance are possible as the devices in a smart home can form an ad-hoc network and carry out real time monitoring for better service, surveillance and for other purposes (Singh, Sharma & Park 2017). However, security has always been a concern in computing networks, and smart home networks are no exception (Olawumi, Väänänen, Haataja and Toivanen 2017). The integration of Cloud Computing and IoT in pre-existing computing context raises further security concerns. Cloud Computing and IoT come with security issues (Botta, Donato, Persico & Pescape 2015) that a smart home network may inherit due to such integration. In a smart home, the ad-hoc network of smart devices is also prone to malicious attacks. One such scenario could be compromising the whole network and using the smart home network to carry out further attacks my masquerading or spoofing. If a security approach that provides protection through redundancy and collaborative surveillance against threats, a network wide attack may be countermeasure successfully. This paper presents a collaborative security approach to combat this. By using a collaborative and redundant security approach, the devices in a smart-home network will be able to prevent such exploitation. The security approach discussed in this paper is a conceptual representation and a research in progress. Though the proposed work confines its context within smart home, the approach is a generic one that can be employed in any network made up of computing devices.

The rest of the paper is structured as follows: Related Study section presents literature review. The security approach is discussed in The Model section. The conceptual view of the underlying security mechanism for the model is discussed in Security Mechanism section, followed by Validation Process section that portrays the logic of the proposed security model to validate a transaction and/or to detect a compromised transaction. The presented work is a research in progress. Planned future research is discussed under Further Developments section.

Related Study

A network of devices in a smart home is essentially an ad-hoc computer network which may also be an ad-hoc network. Due to this, security aspects or concerns of both traditional computer networks and ad-hoc computing networks equally apply to smart home networks. Security has been a major concern in computing. Apart from this, and the emergence of Cloud Computing and IoT and their integration into smart homes makes security a concern for smart home networks. Cloud Computing comes with numerous benefits, but not without security vulnerabilities and threats (Kandukuri, Paturi & Rakshit, 2009). IoT has security issues (Bhabad & Bagade 2015; Suo, Wan, Zou & Liu 2012; Maple 2017) where data transfer, data processing and application security are some related factors (Bhabad & Bagade 2015; Suo et al. 2012; Maple 2017). Chetty, Sung and Grinter (2007), Singh, Sharma and Park (2017), and Mantas, Lymberopoulos and Komninos (2011) discuss various security related aspects and concerns for smart home networks. Security for technology-specific smart home network is also taken into consideration by researchers. For example, Konidala, Kim, Yeun and Lee (2011) propose a security framework for RFID-based applications in smart home. The framework defines secure communications between smart phones and home servers of a smart home network. Konidala and Kim (2007) proposes another similar security approach for smart home networks. On security management in smart home, Khoury, Busnel, Giroux and Li (2009) discuss the use of security patterns to enforce security. The authors state that the complexity of smart home networks makes it challenging to embed security solutions.

Smart home networks may counter different types of attacks (He, Xiao, he & Pathan 2017). The attack may be carried out at traffic level, control level or the backbone level of a smart home network (Ali & Awad 2018). A network gateway in a smart home network can be compromised to eventually take control of the whole network (Granzer, Kastner, Neugschwandtner and Praus 2006), which enables the compromised network to establish connection to the outside world (Ricquebourg, Menga, Durand, Marhic, Delahoche & Loge 2006). Various related attacks are discussed by Yoo, Shin and Choi (2007), Nixon, Wagealla, English and Terzis (2005), Can and Sahingoz (2015), and Rubio-Loyola, Sala and Ali (2008).

Kim, Li, Han and Kim (2007) argue that smart home networks are prone to all legacy security threats. They state that a smart home network is a heterogeneous network and thus are open to various internet related security threats. To counter security threats, the authors propose a security model through secure home gateway. Marsa-Maestre, Hoz, Alarcos and Velasco (2005) discuss a hierarchical, agent-based approach to secure smart networks. They propose an architecture that relies on smart spaces that are self-contained and specific locations within the environment. Schaefer, Ziegler and Mueller (2006) propose a Secure Profile Server system to which is a security architecture for smart home. It provisions secure access to application and user profiles. Other examples of research on security models, frameworks, or architectures for secure smart home network are found in Singh, Sharma & Park (2017), Kidd et al. (1999), Argyroudis and O'Mahony (2004), OSGI (1999), Wu, Liao and Fu (2007), Ganti, Jayachandran, Abdelzaher and Stankovic (2006), Al-Muhtadi, Ranganathan, Campbell and Mickunas (2003), Augusto and Nugent (2004), Jaszczyk and Krol (2010). Literature suggest that a collaborative and redundant approach in securing smart home network is not given much research focus, and thus warrants further exploration.

The Model

All the intelligent devices of an ad-hoc network in a smart home may be thought of as nodes of that network. The devices may be further classified into different groups (e.g. kitchen appliance,

entertainment gadgets and so on). Thus, the network can be thought of as grouped arrangement of devices where the group is defined based on the category of the devices. Each group of devices make their own sub-network which in turn become part of the smart home network. Thus, the smart home network becomes a collection of sub networks. These sub networks may be defined as layer-A network. For example, all the smart kitchenware appliances (e.g. microwave, fridge, washing machine) could form one Layer-A, all the smart computing gadgets (e.g. TVs, gaming console, computers, smart phones) could form another Layer-A network, and so on. The total number of Layer-A network thus variable for a smart home depending on the number of types of smart devices and gadgets available in a smart home.

There are further sub-networks of the devices that may be termed as layer-B sub networks. This is a redundant layer of sub-networks. All the nodes of a layer-B sub network are chosen from each different layer-A network. That is, one member from each layer-A network forms a layer-B network. There can be more than one (and typically is) layer-B network. Each member node of a layer-A network becomes node of a layer-B network to which no other node from its native network may become a member. Figure 1 illustrates both sub networks.

As illustrated in Figure 1, the network is made up of three layer-A sub networks having members {A, B, C, P}, {D, E, F, Q} and {G, H, I, R}. Three nodes from these three layer-A networks form a layer-B network with nodes {P, Q, R}.

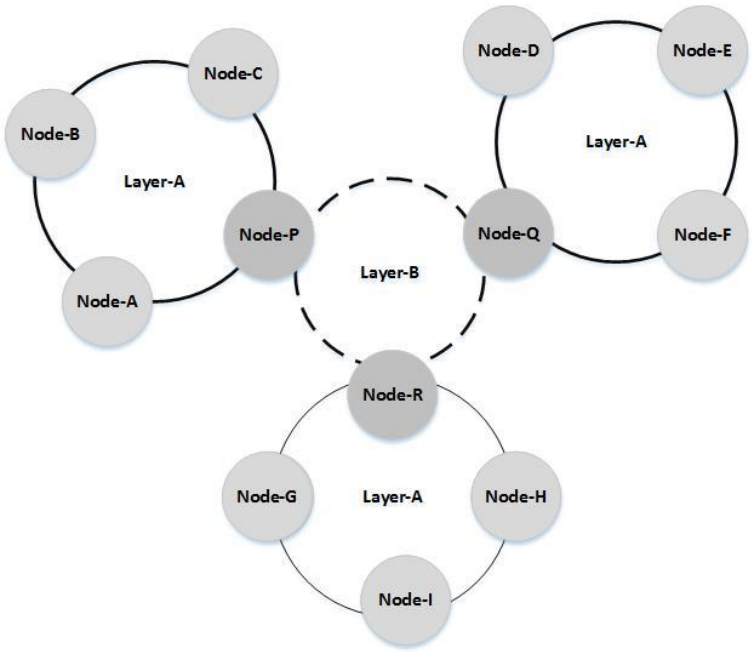

Figure 1. Layered Sub Networks

It is important to note that the above arrangement needs a security mechanism that would be capable of detecting compromised nodes in a network. Upon detecting a compromised node, any layered network can broadcast this message to other networks. The nodes in other network can then blacklist the compromised node and stop all communications. The security mechanism for incident detection is described in next section.

Security Mechanism

All nodes are 'validator' and 'vault' at the same time. Validator validates transactions, while vault keeps a copy of the transaction details. One transaction cannot be stored in more than one node, and the same node cannot be the validator and vault for the same transaction. Both validator and vault for a transaction are chosen at random. The information kept in vault can be examined at random and by any validator.

The scope of validators is defined both in terms of layer-A and layer-B sub networks, while the scope of vaults is defined only in terms of layer-B sub networks. A validator cannot be a validator for any

node of its own layer-A sub network. In addition, if the validator is a member of a layer-B network, it cannot be a validator for any other members of a layer-B network. Node-P cannot be a validator for Node-P and Node-R; it also cannot be a validator for Node-A, Node-B and Node-C. Figure 2 illustrates the base conditions for validator nodes where Node-P and Node-I are considered, and shows which nodes they cannot be a validator of. On the other hand, the conditions for a node to serve as a vault are that, it cannot serve as its own vault, and one specific transaction cannot be stored in more than one vault.

Given the above, let us assume that,

α = a node

λ = a transaction

β = validator for α

Thus, α can be expressed as,

$$\alpha = \sum_{n=1}^{\infty}(\lambda_n) \quad (1)$$

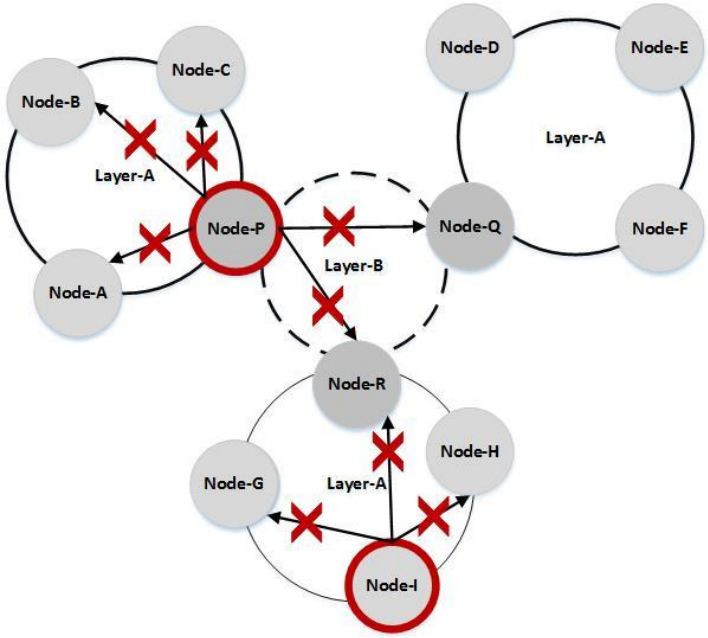

Figure 2. Conditions for Validator Node

So, a validator β can be noted as,

$$\exists\beta: (\beta \neg \alpha) \wedge (\forall\lambda_n \exists!\beta) \wedge (\alpha \in X: \beta \notin X) \quad (2)$$

X = a sub network. Thus,

$$X = \sum_{i=1}^{\infty}(\alpha_i + \beta_i) \quad (3)$$

There needs to be at least two sub networks to construct the security model. Thus, the security model,

$$M = \sum_{j=2}^{\infty}(X_j) \quad (4)$$

Validation Process

A node as a validator has twofold functions – allocating a validation stamp while a transaction is committed, and then, at later time randomly checking the validation of the transactions stored in vaults. Let us call the latter as re-validation. The random approach to re-validation prevents an attacker to be context-aware of the validation process. When a transaction occurs, the validator will put a validation

stamp on the transaction and the vault will store the transaction details. At any given time, a validator may broadcast a request of re-validation of any transaction in a random manner. If a validation request receives multiple responses, it indicates a possible compromise that leads to raise alarm, since a transaction cannot be stored in two nodes. If a node is compromised and keeps itself silent by not responding to the re-validation request, it may not use the transaction in any future processing, as the requesting validator will keep a track of nodes as well as responses, and will publish it to other nodes too. Thus, the validation database from each validator will be shared to other nodes. The high level conceptual flow of the validation check to determine transaction security is illustrated in Figure 3. The validation and re-validation is an ongoing process for the network.

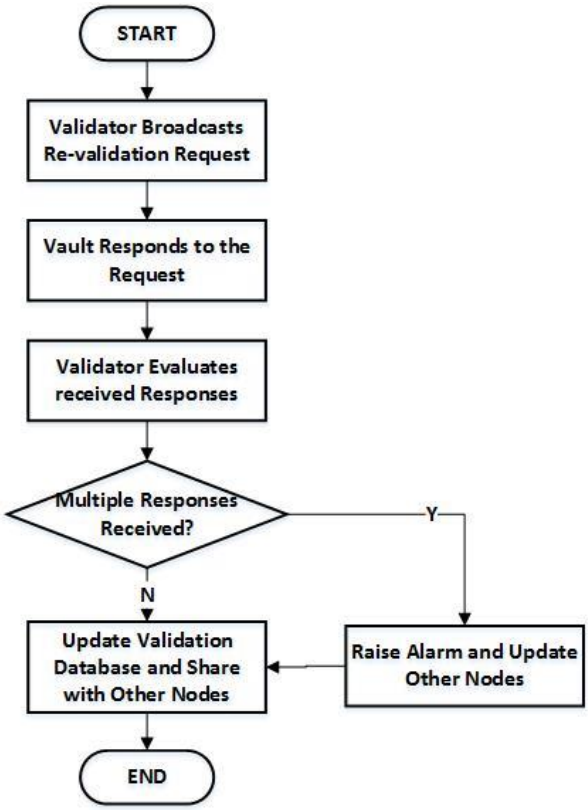

Figure 3. Validation of a Transaction

The objective of the proposed security model is to enable the network to continue its operation without being forced to shut down in case of a breach. This is achieved through validation and re-validation, where a compromised node, upon detection, is excluded from the network.

Future Developments

The conceptual high-level view of the proposed security model is presented in this paper. Future developments would include defining the algorithm for security mechanism. Besides, development of a prototype is another planned future research. Performance overheads are anticipated to be an issue in the current proposed architecture of the model. Further research will focus around this aspect, where performance evaluation will be carried out once the prototype is developed, and optimised if required. The proposed model is applicable to any computing scenario. However, when targeted for home appliances, the processing capability and memory limitations of the computing units of home appliance will also be considered to analyse the performance trade-offs.

The validation process presented is a high-level view of the process. Further research will involve developing detailed steps for validation. It will also include a mechanism on what to do when an alarm is raised. The database in vaults that keeps the transaction details also requires further development. This involves, among other factors, considerations in volume of data to be kept by a vault and its

memory capacity. Upon detection of a compromised node, an automated process might help to erase the memory of the compromised node, and a re-installation of the base system might help the node to join the network again to start 'fresh' as if it is a new device added to the network. This would also be investigated further.

Conclusion

The arrangements of layer-A and layer-B network described create a mesh of networks and would make the scenario complex for an attacker to launch a network wide breach, that is, to take control of the smart home. The goal of proposing the security model is to create a complex scenario of sub networks with decentralised autonomy. This creates distributed points of attacks. As a result, to successfully take-over the smart home, an attacker is required to compromise several sub-networks within a network. The presented security model is high-level view of security approach for smart home networks. Contemporary computing approaches are converged and overlapping. The proposed security approach is applicable in any networked scenario.

References

Ali, B., and Awad, A.I. 2018. "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," *Sensors*, (817:18), pp. 1-17

Al-Muhtadi, J., Ranganathan, A., Campbell, R.H. and Mickunas, M.D. 2003. "Cerberus: a context-aware security scheme for smart spaces," *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom 2003)*, pp. 489-496

Argyroudis, P.G., and O'Mahony, D. 2014. "Securing Communications in the Smart Home", *EUC2004*, LNCS 3207

Augusto, J.C. and Nugent, C.D. 2004. "The Use of Temporal Reasoning and Management of Complex Events in Smart Homes," *ECAI*

Batalla, J.M., Vasilakos, A., and Gajewski, M. 2017. "Secure Smart Homes: Opportunities and Challenges," *ACM Computing Survey*, (50:5), https://doi.org/10.1145/3122816

Bhabad, M.A., and Bagade, S.T. 2015. "Internet of Things: Architecture, Security Issues and Countermeasures," International Journal of Computer Applications (125:14), pp. 1-4

Botta, A., Donato, W., Persico, V., and Pescape, A. 2015. "Integration of cloud computing and Internet of Things: A survey", *Future Generation Computer Systems*, http://dx.doi.org/10.1016/j.future.2015.09.021

Can, O., Sahingoz, O.K. 2015. "*A Survey of Intrusion Detection Systems in Wireless Sensor Networks*", In Proceedings of the 2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), Istanbul, Turkey, 27–29May 2015, pp. 1–6.

Chetty, M., Sung, J., and Grinter, R.E. 2007. *UbiComp 2007*, LNCS 4717, pp. 127–144, Berlin: Springer-Verlag

Ganti, R.K., Jayachandran, P., Abdelzaher, T.F., and Stankovic, J.A. 2006. "SATIRE: a software architecture for smart AtTIRE," *MobiSys*.

Granzer, W., Kastner, W., Neugschwandtner, G., and Praus, F. 2006. "Security in Networked Building Automation Systems", *in Proceedings of the 2006 IEEE International Workshop on Factory Communication Systems*, Torino, Italy, 28–30 June 2006, pp. 283–292

Jaszczyk, P., and Krol, D. 2010. "Updatable Multi-agent OSGi Architecture for Smart Home System," *KES-AMSTA 2010, Part II, LNAI 6071*, pp. 370-379

He, J., Xiao, Q., He, P., and Pathan, M.S. 2017. "An Adaptive Privacy Protection Method for Smart Home Environments Using Supervised Learning", *Future Internet*, (7:9), doi:10.3390/fi9010007

Kandukuri, B.R., Paturi, R., and Rakshit, A. 2009. "Cloud Security Issues," *2009 IEEE International Conference on Services Computing*, pp. 517-520

Khoury P.E., Busne, P., Giroux, S., and Li, K. 2009. "Enforcing Security in Smart Homes using Security Patterns," *International Journal of Smart Home* (3:2), pp. 57-70

Kidd, R.J., Orr, G.D., Abowd, C.G., Atkeson, I.A., Essa, B., MacIntyre, E.D., Mynatt, T.E., Starner, W. 1999. "The Aware Home: A Living Laboratory for Ubiquitous Computing Research", *CoBuild99*, Pittsburgh, PA, USA, 1999, www.cc.gatech.edu/fce/ahri

Kim, G.W., Lee, D.G., Han, J.W., and Kim, S.W. 2007. "Security Technologies based on Home Gateway for making Smart Home secure," *IFIP International Federation for Information Processing*.

Konidala, D.M., Kim, D., Yeun, C.Y., and Lee, B. 2011. "Security Framework for RFID-based Applications in Smart Home Environment," Journal of Information Processing Systems (7:1), DOI: 10.3745/JIPS.2011.7.1.111

Konidala, D.M., and Kim, K. 2007. "Security for RFID-based Applications in Smart Home Environment," *The 2007 Symposium on Cryptography and Information Security (SCIS 2007)*, Sasebo, Japan, Jan. 23-26

Mantas, G., Lymberopoulos, D., and Komninos, N. 2011. Security in Smart Home Environment, IGI Global, DOI: 10.4018/978-1-61520-805-0.ch010

Maple, C. 2017. "Security and privacy in the internet of things," Journal of Cyber Policy (2:2), pp. 155-184, DOI:10.1080/23738871.2017.1366536

Marsa-Maestre, I., Hoz, E., Alarcos, B., and Velasco, J.R. 2006. "A Hierarchical, Agent-based Approach to Security in Smart Offices," *http://www.it.aut.uah.es/ist/papers/TR2006-101.pdf*

Nixon, P.A., Wagealla, W., English, C., and Terzis, S. 2005. "*Security, Privacy and Trust Issues in Smart Environments*", in Smart Environments, JohnWiley & Sons, Inc.: Hoboken, NJ, USA, pp. 249–270

OSGI. 1999. "The Open Services Gateway Initiative Platform - Dynamic services for networked devices (OSGi)", The OSGi Alliance, www.osgi.org

Olawumi, O., Väänänen, A., Haataja, K. and Toivanen, P. 2017. "Security Issues in Smart Home and Mobile Health System: Threat Analysis, Possible Countermeasures and Lessons Learned," *International Journal on Information Technologies & Security* (1:9), pp. 31-52

Ricquebourg, V., Menga, D., Durand, D., Marhic, B., Delahoche, L., and Loge, C. 2006. "The Smart Home Concept: Our Immediate Future", *in Proceedings of the 2006 1st IEEE International Conference on E-Learning in Industrial Electronics*, Hammamet, Tunisia, 18–20 December 2006, pp. 23–28

Rubio-Loyola, J., Sala, D., and Ali, A.I. 2008. "Maximizing Packet Loss Monitoring Accuracy for Reliable Trace Collections", *In Proceedings of the 16th IEEE Workshop on Local and Metropolitan Area Networks (LANMAN2008)*, Chij-Napoca, Transylvania, Romania, 3–6 September 2008, pp. 61–66

Schaefer, R., Ziegler, M., Mueller, W. 2006. "Securing Personal Data in Smart Home Environments", *Workshop on Privacy-Enhanced Personalization (PEP2006).*

Sethi, M. 2012. "Security in Smart Object Networks," *Master's Thesis*, School of Science, Aalto University.

Singh, S., Sharma, P.K., and Park, J.H.. 2017. "SH-SecNet: An Enhanced Secure Network Architecture for the Diagnosis of Security Threats in a Smart Home," *Sustainability 2017*, (9:513), DOI: 10.3390/su9040513, pp. 1-19

Suo, H., Wan, J., Zou, C., and Liu, J. 2012. "Security in the Internet of Things: A Review," *2012 IEEE International Conference on Computer Science and Electronics Engineering*, DOI 10.1109/ICCSEE.2012.373

Wu, C., Liao, C., and Fu, L. 2007. "Service-Oriented Smart-Home Architecture Based on OSGi and Mobile-Agent Technology," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* (37), pp. 193-205

Yoo, D.Y., Shin, J.W., Choi, J.Y. 2007. "*Home-network Security Model in Ubiquitous Environment*", Proc. World Acad. Sci. Eng. Technol. 26. Available at: http://waset.org/publications/2785