2017 IEEE Trustcom/BigDataSE/ICESS

Security Modeling and Analysis of Cross-Protocol IoT Devices

Mengmeng Ge[1], Jin B. Hong[1], Hani Alzaid[2], and Dong Seong Kim[1]
[1] Department of Computer Science and Software Engineering,
University of Canterbury,
Christchurch, New Zealand.
[2] Center for CyberSecurity,
King Abdulaziz City for Science and Technology, Saudi Arabia
Email: {mge43, jho102}@uclive.ac.nz, hmalzaid@kacst.edu.sa, dongseong.kim@canterbury.ac.nz

***Abstract*—In the Internet of Things (IoT), smart devices are connected using various communication protocols, such as Wi-Fi, ZigBee. Some IoT devices have multiple built-in communication modules. If an IoT device equipped with multiple communication protocols is compromised by an attacker using one communication protocol (e.g., Wi-Fi), it can be exploited as an entry point to the IoT network. Another protocol (e.g., ZigBee) of this IoT device could be used to exploit vulnerabilities of other IoT devices using the same communication protocol. In order to find potential attacks caused by this kind of cross-protocol devices, we group IoT devices based on their communication protocols and construct a graphical security model for each group of devices using the same communication protocol. We combine the security models via the cross-protocol devices and compute hidden attack paths traversing different groups of devices. We use two use cases in the smart home scenario to demonstrate our approach and discuss some feasible countermeasures.**

I. Introduction

In the Internet of Things (IoT), smart devices are connected through heterogeneous communication techniques, for example, Wi-Fi [1], ZigBee [2], Z-Wave [3], Bluetooth [4], *etc*. Some IoT devices have multiple built-in communication modules. They are capable of connecting networks using different communication protocols. If these IoT devices are compromised by attackers using one communication protocol, they can be exploited as the entry points to the networks with other communication protocols via heterogeneous communication links. Thus, it is important to capture potential attack paths caused by such cross-protocol devices.

Graphical security models (e.g., attack graphs (AGs) [5], attack trees (ATs) [6]) have been widely used to assess the cyber security. In particular, an AG can capture possible sequences of an attacker's actions to compromise a target, and an AT can discover possible ways to achieve an attack goal via combinations of attacks. In order to improve the scalability problem of the graphical security models, the multi-layer hierarchical attack representation models (HARMs) [7] were proposed by combining AGs and ATs. In the two-layered HARM, the upper layer represents the network reachability information (i.e., nodes connected in the topological structure) and the lower layer denotes the vulnerability information of nodes, respectively. In our previous work [8], we developed a framework for modeling and assessing the security of the IoT. The framework is used to construct an IoT network, a graphical security model (i.e., a multi-layer HARM) for the IoT network and a security evaluator with various security metrics to automate the security analysis of the IoT network.

In this paper, we group IoT devices based on their communication protocols and construct a graphical security model (we used a HARM) for each group of devices using the same communication protocol. Given all the HARMs, we generate a meta-HARM that combines each HARM into one HARM and calculate extended attack paths. To the best of our knowledge, this work is the first approach to analyze the security of the IoT network using cross-protocol devices. The main contributions of this paper are summarized as follows:

- Divide the IoT network based on the communication protocols that the devices use;
- Construct a graphical security model to capture potential attack paths for the IoT devices using the same communication protocol;
- Develop a meta-model to compute attack paths traversing networks with different communication protocols via the cross-protocol devices to unveil hidden attack surfaces;
- Investigate the impact of cross-protocol devices with heterogeneous built-in communication modules.

The rest of the paper is organized as follows. Section II presents related work for security modeling of the IoT considering the heterogeneous features of devices. Our proposed approach is described in Section III. Use cases using the proposed approach are presented in Section IV. Limitations and discussions are presented in Section V. Finally, Section VI concludes the paper.

II. Related Work

There are a few work focused on considering the effect of device heterogeneity in the security analysis of the IoT network. Yu *et al.* [9] discussed cross-device interactions via services like IF-THIS-THEN-THAT (IFTTT) in terms of heterogeneous applications. As an example mentioned in the paper, an attacker is able to compromise the smart plug to turn off the air-conditioner and the increasing temperature can trigger the windows to open, thus causing

2324-9013/17 $31.00 © 2017 IEEE
DOI 10.1109/Trustcom/BigDataSE/ICESS.2017.350

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on February 23,2021 at 14:48:54 UTC from IEEE Xplore. Restrictions apply.

a home break-in. They proposed to build an abstract model to store different classes of devices and their interactions with the environment variables. They planned to use the model to explore possible device behaviors with various environment inputs and also suggested to use the model to identify multi-stage attacks. Mohsin *et al.* [10] proposed and implemented a formal framework for the security analysis of the IoT. The framework models interactions between IoT devices in terms of functionalities and network connections, user-defined policies (e.g., IFTTT) and threats using the Satisfied Modulo Theories logics. They used the framework to analyze a Building Management System to capture hidden attack vectors.

There is no previous work on constructing a formal graphical security model to explicitly capture the properties of different communication protocols that can create new attack paths. As a result, one cannot analyze the impact of cross-protocol devices with heterogeneous built-in communication modules in the IoT network.

III. The Proposed Approach

The aim of the proposed approach is to explicitly capture all potential attack paths arising from an attacker exploiting cross-protocol devices in the IoT network. We develop our approach based on the framework in [8]. The approach consists of three phases shown in Figure 1: 1) data input collection, 2) model construction, and 3) security analysis. We explain each phase in the following.

In phase 1, the security/network administrator needs to provide three types of inputs: the network topology (i.e., reachability information), communication protocol(s) used by each node and node vulnerability information. The vulnerability information can be found from the Common Vulnerabilities and Exposures (CVE) ID or other vulnerability databases. The Common Vulnerability Scoring System (CVSS) base score [11] and other metric-based values can also be assigned to the vulnerability (e.g., attack success probability, attack impact). The IoT generator takes the inputs and creates an IoT sub-network for the devices using the same communication protocol.

In phase 2, we perform the security model construction for each sub-network. In specific, the security model generator takes the outputs from the IoT generator, automatically generates a two-layered HARM for the sub-network and calculates the potential attack paths in the upper layer of the HARM [7].

In phase 3, we carry out the security evaluation for the sub-networks. The security evaluator generates a meta-HARM by combining the HARMs of different sub-networks via cross-protocol devices and calculates extended attack paths traversing different sub-networks [8].

IV. Use Cases

We present two use cases in a smart home to demonstrate the feasibility of the proposed approach. Home automation is one of the innovation domains in the emerging IoT [12]. Smart devices are usually controlled by a smart hub with multiple built-in communication modules. Besides, some smart devices (e.g., smart phones, smart tablets) also support multiple communication protocols to provide better user experience. However, these cross-protocol devices can connect several networks and lead to unpredictable attacks among different networks. We describe two attack scenarios in the smart home and analyze the impact of cross-protocol devices on the security of the smart home using the proposed approach. Our approach is not limited to the specific use cases but applicable to any cases with cross-protocol devices.

A. Use Case I of Direct Operation

Many IoT devices allow users to directly control them via the mobile apps. The smart hub/bridge connects to the home Wi-Fi, gets commands from the mobile apps and issues these commands to devices connected to them through other communication protocols (e.g., ZigBee, Z-Wave). In this use case, we will analyze the security of a cross-protocol hub/bridge and its impact on the security of the smart home.

1) Network Setting: We consider an IoT-enabled home network shown in Figure 2 as an example. A smart TV, a smart camera and an Android tablet are connected through the home Wi-Fi. We use the Philips Hue lighting system as it is a very popular product in the home automation market. The Hue bridge connects to the wireless router via the Ethernet cable and has a built-in ZigBee module to communicate with light bulbs via ZigBee Light Link protocol [13]. The Android tablet is installed with the Hue app to control light bulbs via the Hue bridge.

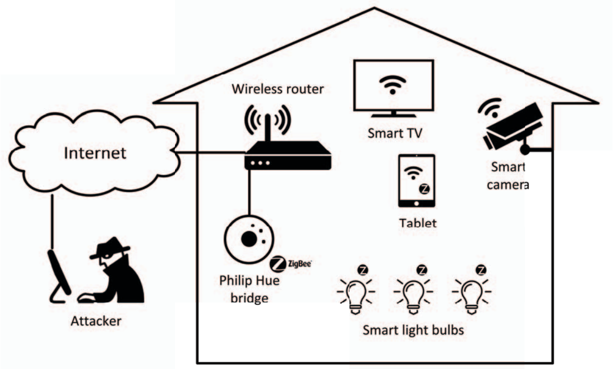


Fig. 2: A smart home with Philips Hue lighting system.

2) Attacker Model: As most IoT devices have constrained resources and limited computational capabilities, they can be easily compromised and controlled by attackers. There are many papers addressing the proof-of-concept attacks on a smart TV in [14], [15], a smart tablet in [16], and the Philips Hue lighting system in [17], [18], [19]. We collected the vulnerabilities from the existing papers and the CVE database. We choose some of them to be used in the attacker model shown in Table I.

We assume there is a remote attacker whose goal is to control home devices. Any smart home device can be the target

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on February 23,2021 at 14:48:54 UTC from IEEE Xplore. Restrictions apply.

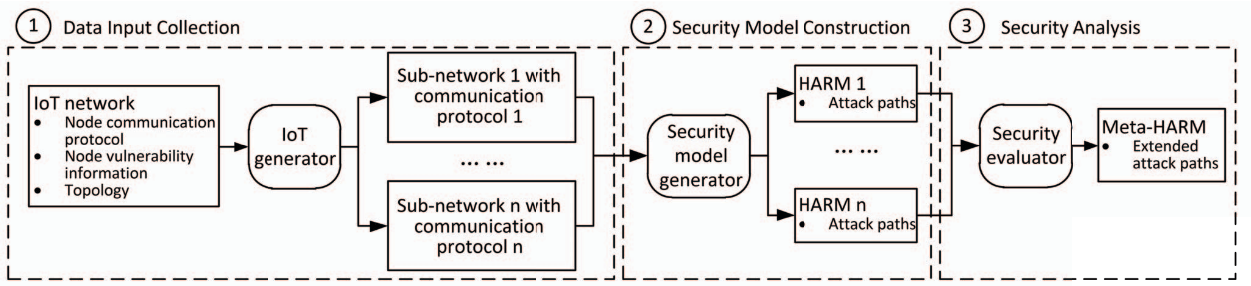


Fig. 1: The proposed approach.

TABLE I: Vulnerability information of the smart home in use case I.

Vulnerability	Description
$v1_{tv}$	CVE-2008-4886
$v2_{tv}$	CVE-2009-0385
$v1_{cam}$	CVE-2013-4977
$v1_{tab}$	Three bugs exploited in malware *Backdoor.AndroidOS.Obad.a* [16]
$v2_{tab}$	
$v3_{tab}$	
$v1_{hue}$	Request authentication using non-random whitelist token [17]

of the attacker. The assumptions about the attacker's capability are listed in the following.

- The attacker is able to remotely compromise the Smart TV using either $v1_{tv}$ or $v2_{tv}$, the Smart camera using $v1_{cam}$ and the Android tablet using the malware *Backdoor.AndroidOS.Obad.a* exploiting three bugs, $v1_{tab}$, $v2_{tab}$ and $v3_{tab}$.
- The attacker is able to write a malware exploiting $v1_{hue}$ in the Hue system to issue blackout command to the light bulbs via the Hue app.

3) Security Modeling and Analysis: We construct the two-layered HARM for the Wi-Fi network and visualize the attack paths in Figure 3. Let $HARM_{wifi}$ denote the HARM for the Wi-Fi network. The upper layer of the HARM captures the reachability of the devices in the network and the lower layer denotes a set of ATs for the devices. The connectivity of the devices is presented by using the solid lines. Each device is associated with an AT containing the vulnerability information by using the dotted line.

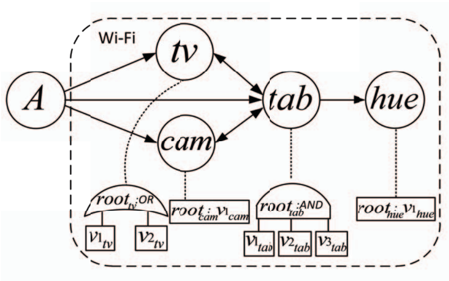


Fig. 3: Attacks paths in $HARM_{wifi}$ in use case I.

In the Wi-Fi network, the smart TV, smart camera and tablet are the entry points as they can be remotely exploited. We also set them as the targets of the attacker. The Hue bridge is also the target. It cannot be compromised directly but via the Hue app running on the tablet. Thus, the attacker can also reach the Hue bridge via the compromised tablet by exploiting $v1_{hue}$ in the Hue system. We list the attack paths captured in $HARM_{wifi}$ as follows: $\{tv$, cam, tab, $tv \rightarrow tab$, $cam \rightarrow tab$, $tab \rightarrow tv$, $tab \rightarrow cam$, $tab \rightarrow hue$, $tv \rightarrow tab \rightarrow cam$, $cam \rightarrow tab \rightarrow tv$, $tv \rightarrow tab \rightarrow hue$, $cam \rightarrow tab \rightarrow hue\}$.

In the Hue lighting system, the Hue bridge is the only entry point if the attacker is not located near the house. If the Hue bridge receives the blackout command from the compromised tablet, it will send the blackout command to the light bulbs directly via the ZigBee Light Link protocol to turn them off. We show the connectivity of the Hue bridge and light bulbs in Figure 4.

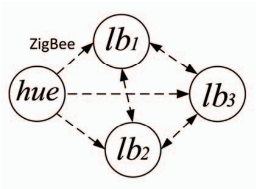


Fig. 4: The topology of the lighting system in the smart home.

As the Hue bridge connects to both the home Wi-Fi and the light bulbs, the attacker can compromise the tablet running the Hue app and exploit the vulnerability in the Hue system to eventually control the light bulbs via the Hue bridge. There are also many other cases that a remote attacker compromises the smart hub directly to maliciously operate the home devices connected to the hub. For instance, a remote attacker can exploit a cross-site request forgery vulnerability in the Honeywell Tuxedo Touch and use the Touch to unlock the door with the Z-Wave protocol; an attacker can launch a SQL injection to the Wink hub to gain root privilege and use the hub to issue malicious commands to the devices [20]. The smart hub/bridge links multiple networks based on their communication modules, extends attack paths for the attacker and allows the attacker from the Internet to reach devices residing inside the home network.

4) Potential Countermeasures: As all current smart hubs/bridges have multiple built-in communication interfaces for them to connect to both the Internet and the local home

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on February 23,2021 at 14:48:54 UTC from IEEE Xplore. Restrictions apply.

networks, attacks utilizing the heterogeneous communication of these devices are inevitable. Thus, improving the security design of the products is of critical importance.

In our use case, the vulnerability in the Hue lighting system has already been fixed. If there is no vulnerability to be exploited, a remote attacker cannot control the light bulbs. However, it is found in [18] that the communication between the app and the Hue bridge is not encrypted; an attacker can still compromise a device in the same network with the Hue bridge, eavesdrop the traffic and extract the useful information to eventually control the lighting system. Apparently, the new vulnerability requires more attack efforts in terms of time and cost compared with the old one. If the new vulnerability can be fixed, the attacker needs to find other ways to achieve the attack goal which may require more efforts. In reality, it is impossible to eliminate the attacks as an attacker can always find a way to reach the target. Our suggestion is to design products to make an attacker harder to compromise.

Besides, as home users are usually reluctant to apply patches for their home devices even if patches are released, mandatory updates can be applied. The SmartThings hub uses this mechanism to redirect the users to the update server to force the patching procedure.

B. Use Case II of Indirect Operation

In a smart home, besides the hub/bridge, some devices also support multiple communication protocols (e.g., smart phones, smart tablets, laptops). These devices can connect different networks and may lead to unpredictable attacks via hidden attack vectors. In this use case, we will analyze the security of a cross-protocol tablet and its impact on the security of the smart home.

1) Network Setting: We consider an IoT-enabled home network shown in Figure 5 as an example. We use the smart TV, the smart camera and the Android tablet in the use case I. The Android tablet is equipped with a ZigBee chip. It can act as a ZigBee router in the ZigBee network. We use a number of ZigBee devices presented in the emulated environment in [21]. The ZigBee devices consist of a switch electricity meter, a thermostat, several electricity meter plugs and temperature and humidity sensors. The switch electricity meter and electricity meter plugs have router functions to extend the limited range of the network. They can transfer packets to/from other ZigBee devices. The thermostat, temperature and humidity measurement sensors are end devices. They communicate wirelessly to the ZigBee gateway. The ZigBee gateway acts as the coordinator to form and maintain the mesh network. It connects to a personal computer via the Ethernet interface and the personal computer connects to the wireless router.

We also show the topology of the ZigBee sensor network with the tablet acting as a router in Figure 6. Let R_n denote the ZigBee device with router function, E_n denote the ZigBee end device, GW denote the ZigBee gateway, respectively.

2) Attacker Model: We use the same vulnerabilities for the smart TV, the smart camera and the tablet shown in Table I and a vulnerability for ZigBee devices proposed in [21]. We present the information of the exploitable vulnerability in Table II.

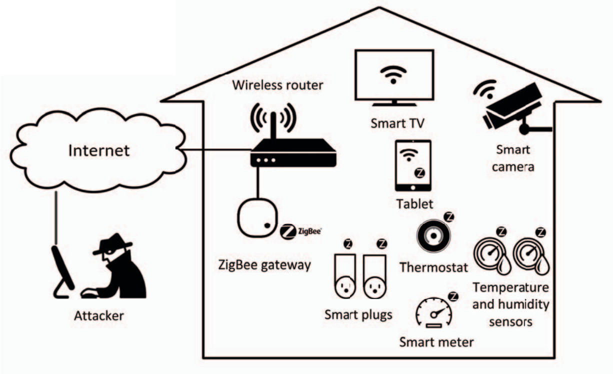


Fig. 5: A smart home with ZigBee sensors.

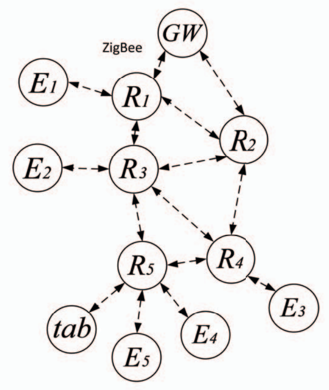


Fig. 6: The topology of the ZigBee network in use case II.

TABLE II: Vulnerability information of the smart home in use case II.

Vulnerability	Description
$v1_{zb}$	ZigBee routing algorithm prone to the Sinkhole attack [21]

In the Wi-Fi network, we assume there is a remote attacker whose goal is to control the home devices. Any smart home device can be the target of the attacker. The attacker is able to remotely compromise the Smart TV, the Smart camera and the Android tablet using the vulnerabilities listed in Table I.

In the ZigBee network, we assume there is a local attacker near the house whose goal is to control home devices using the ZigBee protocol. The assumptions about the attacker's capability are listed in the following.

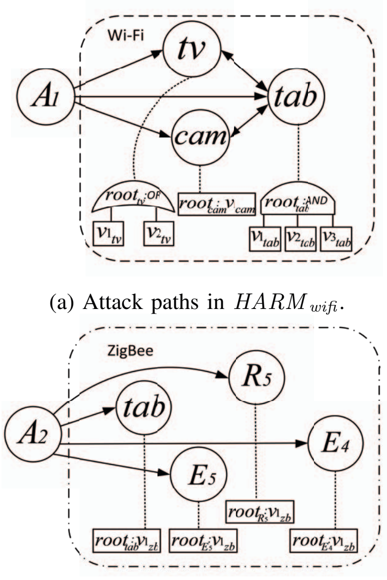
- The attacker can move physically around the house and carries a laptop-class device with the built-in ZigBee module and a special toolkit (i.e., KillerBee [22]).
- The attacker can use the device with a strong transmission range to eavesdrop the traffic in the home ZigBee network and intercept the network key to join the network legally

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on February 23,2021 at 14:48:54 UTC from IEEE Xplore. Restrictions apply.

(e.g., when the ZigBee gateway sends the network key unencrypted over-the-air to a new home device).

- As the ZigBee routing algorithm is prone to Sinkhole attacks, the attacker is able to use the device to advertise false routing table stating a shorter route to the ZigBee gateway, thus luring traffic of some ZigBee home devices from the ZigBee gateway to his device.
- It is very hard for the attacker to compromise the ZigBee gateway directly or via the personal computer connected to it as they have strong protection.

3) Security Modeling and Analysis: We construct two HARMs for the Wi-Fi network and the ZigBee network, respectively in Figure 7. Let $HARM_{wifi}$ denote the HARM for the Wi-Fi network, A_1 denote the remote attacker in the Wi-Fi network, $HARM_{zb}$ denote the HARM for the ZigBee network, A_2 denote the local attacker in the ZigBee network, respectively.



(a) Attack paths in $HARM_{wifi}$.

(b) Attack paths in $HARM_{zb}$.

Fig. 7: HARMs in use case II.

In the Wi-Fi network, the smart TV, smart camera and tablet are the entry points as they can be remotely exploited and are also the targets of the attacker. In the ZigBee network, the local attacker can use the device to lure traffic from some ZigBee devices within the communication range (i.e., tab, R_5, E_4, E_5). As the tablet has a built-in ZigBee module and is in the communication range of the attacker's device, it also connects to the attacker's device.

We generate a meta-HARM based on $HARM_{wifi}$ and $HARM_{zb}$ via the cross-protocol tablet and visualize the attack paths in Figure 8. Let $HARM_{meta}$ denote the meta-HARM. As the tablet has a built-in ZigBee module and acts as the router in the ZigBee network, the remote attacker can increase the transmission power of the tablet after the tablet is compromised and lure the traffic of some ZigBee devices from the ZigBee gateway. As the tablet is located inside the home network, more devices are affected due to its increased power (i.e., R_4, E_3). Other attacks can also be launched via the tablet (e.g., selective forwarding attack, drops or altered routing information, *etc*).

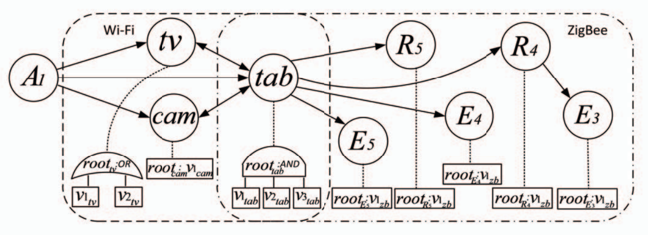


Fig. 8: Attack paths in $HARM_{meta}$ in use case II.

We calculate the number of attack paths in three HARMs in Table III. Any home device is set to be the target. For A_1 in $HARM_{wifi}$, the list of attack paths is shown as follows: $\{tv,\ cam,\ tab,\ tv \rightarrow tab,\ cam \rightarrow tab,\ tab \rightarrow tv,\ tab \rightarrow cam,\ tv \rightarrow tab \rightarrow cam,\ cam \rightarrow tab \rightarrow tv\}$. For A_2 in $HARM_{zb}$, each attack path consists of one devcie because they connect to the attacker's device as their parent. For A_1 in $HARM_{meta}$, besides the attack paths in $HARM_{wifi}$, the list of attack paths also includes: $\{tab \rightarrow R_4/R_5/E_4/E_5,\ tv \rightarrow tab \rightarrow R_4/R_5/E_4/E_5,\ cam \rightarrow tab \rightarrow R_4/R_5/E_4/E_5,\ tab \rightarrow R_4 \rightarrow E_3,\ tv \rightarrow tab \rightarrow R_4 \rightarrow E_3,\ cam \rightarrow tab \rightarrow R_4 \rightarrow E_3\}$. Compared with the attack paths in $HARM_{wifi}$, the number of the increased attack paths is 15 for A_1 in $HARM_{meta}$. Besides, the attacker can be remotely located and control the ZigBee sensor devices without the use of any special toolkit.

TABLE III: Number of Attack paths in three HARMs in use case II.

Attacker	HARM	Number of Attack paths
A_1	$HARM_{wifi}$	9
A_2	$HARM_{zb}$	4
A_1	$HARM_{meta}$	24

The built-in ZigBee module in the tablet enables a remote attacker to manage ZigBee devices maliciously. Unlike the direct operation in the use case I (i.e., home devices are directly controlled by the cross-protocol hub), the tablet creates additional paths to the ZigBee network and leads to unpredictable attacks.

4) Potential Countermeasures: As the tablet does not have direct control over the devices, the Sinkhole attack and further attacks caused by the tablet are hard to foresee and prevent. The manufacturers should be aware of possible interactions with the external devices and design flaws in the protocols and applications. In the Samsung SmartThings platform, a ZigBee device will hold onto their parent when it joins the network and choose a new parent once it completely loses connection with the parent. If this mechanism can be implemented in the ZigBee sensor devices in our use case, there will be no extended attack paths from the tablet to the ZigBee network.

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on February 23,2021 at 14:48:54 UTC from IEEE Xplore. Restrictions apply.

V. Limitations and Discussions

In the previous work [8], we developed a framework and a multi-layer HARM to model and evaluate the security of the IoT. In this paper, we designed an approach to analyze the security of the IoT with multiple communication protocols. The approach is used to generate sub-networks based on the communication protocols used by devices, construct a HARM for each sub-network, generate a meta-HARM using cross-protocol devices and compute the extended attack paths. We plan to complete the following extensions in our future work.

Scenarios: in the current analysis, we use two example networks in the smart home to demonstrate the use of our approach for the node controlling attack and Sinkhole attack. Analysis of other cases (e.g., healthcare) will be performed. Besides, we will consider different attacker models (e.g., Distributed Denial of Service attacks) and come up with countermeasures in both device and network levels.

Mobility: we assume smart devices are static in the use cases. In reality, IoT devices may have different movement patterns in different scenarios. The movement of devices has a great impact on the security of the IoT as the attack surface changes constantly. We will investigate current mobility models, modify them to capture the device movement in the network and analyze the impact of the movement of cross-protocol devices on the security of the IoT.

VI. Conclusions

As IoT devices are connected via heterogeneous communication protocols, devices with multiple communication protocols can provide connections among different networks. However, vulnerable cross-protocol devices may also create additional attack paths traversing different networks and lead to unpredictable attacks. In this paper, we have developed an approach to model and assess the security of the IoT with cross-protocol devices. Given the inputs of the communication protocols, network topology and node vulnerability information, we have generated sub-networks based on the communication protocols used by the devices, computed the HARM for each sub-network. Given all the HARMs, we have generated a meta-HARM to capture the hidden attack paths traversing different sub-networks. We have introduced two use cases, direct operation and indirect operation, and analyzed the cases using the proposed approach. We have also provided some potential countermeasures for the attacks presented in the use cases.

References

[1] P. S. Henry and H. Luo, "WiFi: what's next?" *IEEE Communications Magazine*, vol. 40, no. 12, pp. 66–72, Dec 2002.

[2] P. Kinney, "ZigBee Technology: Wireless Control that Simply Works," ZigBee Alliance, Tech. Rep., 2003.

[3] "Z-Wave," Last accessed: 2017-04-12. [Online]. Available: http://www.z-wave.com

[4] P. McDermott-Wells, "What is Bluetooth?" *IEEE Potentials*, vol. 23, no. 5, pp. 33–35, Dec 2005.

[5] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated Generation and Analysis of Attack Graphs," in *Proceedings of the 2002 IEEE Symposium on Security and Privacy (SP '02)*. IEEE Computer Society, 2002, pp. 273–284.

[6] V. Saini, Q. Duan, and V. Paruchuri, "Threat Modeling using Attack Trees," *Journal of Computer Science in Colleges*, vol. 23, no. 4, pp. 124–131, 2008.

[7] J. B. Hong and D. S. Kim, "Towards Scalable Security Analysis using Multi-Layered Security Models," *Journal of Network and Computer Applications*, vol. 75, pp. 156–168, 2016.

[8] M. Ge, J. B. Hong, W. Guttmann, and D. S. Kim, "A framework for automating security analysis of the internet of things," *Journal of Network and Computer Applications*, vol. 83, pp. 12–27, 2017.

[9] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a Trillion (Unfixable) Flaws on a Billion Devices: Rethinking Network Security for the Internet-of-Things," in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks (HotNets-XIV '15)*. ACM, 2015, pp. 1–7.

[10] M. Mohsin, Z. Anwar, G. Husari, E. Al-Shaer, and M. A. Rahman, "IoTSAT: A formal framework for security analysis of the internet of things (IoT)," in *Proceedings of the 2016 IEEE Conference on Communications and Network Security (CNS '16)*, Oct 2016, pp. 180–188.

[11] L. Gallon and J. Bascou, "Using CVSS in Attack Graphs," in *Proceedings of the 6th International Conference on Availability, Reliability and Security (ARES '11)*, 2011, pp. 59–66.

[12] A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home automation system," *Future Generation Computer Systems*, vol. 56, pp. 719–733, 2016.

[13] "Philips," Last accessed: 2017-04-12. [Online]. Available: https://www.developers.meethue.com/

[14] B. Michele and A. Karpow, "Watch and be watched: Compromising all Smart TV generations," in *Proceedings of the 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC '14)*. IEEE, 2014, pp. 351–356.

[15] Y. Bachy, F. Basse, V. Nicomette, E. Alata, M. Kaaniche, J. C. Courrege, and P. Lukjanenko, "Smart-TV Security Analysis: Practical Experiments," in *Proceedings of the 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '15)*. IEEE, 2015, pp. 497–504.

[16] R. Unuchek. Obad.a Trojan Now Being Distributed via Mobile Botnets. Last accessed: 2016-09-14. [Online]. Available: https://securelist.com/blog/mobile/57453/obad-a-trojan-now-being-distributed-via-mobile-botnets/

[17] N. Dhanjani, "Hacking Lightbulbs," Last accessed: 2017-04-12. [Online]. Available: http://goo.gl/RY252I

[18] S. Notra, M. Siddiqi, H. Gharakheili, V. Sivaraman, and R. Boreli, "An Experimental Study of Security and Privacy Risks with Emerging Household Appliances," in *Proceedings of the 2014 IEEE Conference on Communications and Network Security (CNS '14)*. IEEE, 2014, pp. 79–84.

[19] E. Ronen and A. Shamir, "Extended Functionality Attacks on IoT Devices: The Case of Smart Lights," in *Proceedings of the 2016 IEEE European Symposium on Security and Privacy (SP '16)*, March 2016, pp. 3–12.

[20] "Security holes in the 3 most popular smart home hubs and Honeywell Tuxedo Touch," Last accessed: 2017-04-12. [Online]. Available: http://www.networkworld.com/article/2952718/microsoft-subnet/

[21] L. Coppolino, V. D'Alessandro, S. D'Antonio, L. Lev, and L. Romano, "My Smart Home is Under Attack," in *Proceedings of the 2015 IEEE 18th International Conference on Computational Science and Engineering (CSE '15)*. IEEE Computer Society, 2015, pp. 145–151.

[22] O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, and P. Toivanen, "Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned," in *Proceedings of the 2014 14th International Conference on Hybrid Intelligent Systems (HIS '14)*. IEEE, 2014, pp. 199–206.

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on February 23,2021 at 14:48:54 UTC from IEEE Xplore. Restrictions apply.