SECURE HOME: AN APPROACH TO A GUARDED RESIDENTIAL IoT NETWORK

[1]DAVID PASKO, [2]VIYALETA PETERSON, [3]ERIC LUCE, [4]PHU PHAN, [4]KHALED ELLEITHY, [5]LAIALI ALMAZAYDEH

[1,2,3,4]University of Bridgeport, Computer Science and Engineering Department
Bridgeport, CT, USA
[5]Al-Hussein Bin Talal University, Software Engineering Department, Ma'an 71111, Jordan
E-mail: [1]dpasko@my.bridgeport.edu, [2]vipeters@my.bridgeport.edu, [3]ericluce@my.bridgeport.edu,
[4]phuphan@my.bridgeport.edu, elleithy@bridgeport.edu, [5]Laiali.almazaydeh@ahu.edu.jo

Abstract - As more devices become internet-connected, there is a greater need for secure and discrete device-to-device communication. Data shows that at the time of this writing the number of internet-connected devices is around 20 billion and is expected to increase to 29 billion by the end of 2022. In the early days of IoT the majority of the market was comprised of cellular phones, but by the end of 2018, the number of internet connected "things" is expected to surpass the number of cellular phones. While many of these devices perform low-risk tasks such as data measurement (temperature) or status alerts (home door/window open/closed), the security of these devices in a network is becoming increasingly important. While in the past a homeowner only needed to worry about a burglar physically breaking into their home using specialized physical tools, now they must worry about the same person entering their home through the use of hacking their home network. The need for a simple yet scalable method of securely adding and communicating to nodes on a home network will be investigated and proposed. Our approach includes creating a smart home infrastructure, which guarantees secure and effective communication between the IoT devices connected to a single Wi-Fi router.

Keywords - Access Control, Identity Management, IoT, Smart Home

I. INTRODUCTION

Internet of Things (IoT) is a growing technology that makes our lives easier. The term refers to over 20 billion devices or "things" connected to the internet, collecting and sharing data. This number is expected to grow to 29 billion by the end of 2022 [1]. Such devices can openly communicate with each other with little or no security [2]. IoT is especially vulnerable since devices have limited computing power and battery capacity. Moreover, their communication channel is typically wireless. A survey from Gartner found that, in the past three years, about 20 percent of organizations encountered at least one attack on their IoT network [3]. The traditional requirements of confidentiality, availability, and integrity still apply to IoT environments. With limited resources of devices, the biggest challenge for IoT is to minimize the devices' resource consumption while also satisfying the security requirements.

With the help of IoT, the smart home environment is developed to provide intelligent and innovative services to people. According to [4], the essential components of a Smart Home are:

- **Smart Devices** — Devices that can connect with the network or with each other devices via protocols like Wi-Fi, Bluetooth, ZigBee, etc. They can operate, share data and store the data to the Smart home Gateway system.
- **Central Control Box (CCB)** — This is the main component of a Smart Home System. It is a small computer with processing power and internet connection, acting as an interface for external devices like laptops, mobile phones, tablets, and computers.
- **Smart Home Network —** A network made of many elements like sensors, applications, and network protocols. Devices can operate and control within the network.
- **Applications —** Web or mobile applications, enabling access and control of Smart Devices after authentication.

Attacks on security play an essential role in defining smart home infrastructure and device network. Such threats include malware attacks on devices and breaching IoT devices to gain access to information or control the devices [5]. Proper access control and identity management are required to make a home system more secure as it can help meet confidentiality, integrity, and availability requirements [6]. Several approaches to deal with vulnerabilities exist. In [7], authors propose using One-Time Passwords (OTP) for secure access authentication in a smart home network. Research in [8] makes use of public key mutual authentication protocol, with pre-shared keys between a gateway and a new device (with elliptic curve cryptography) to address the access control problem. A two-phase mutual authentication process is used in [9] and involves two-stage authentication - registration followed by confirmation. One solution offered involves converting the IP address of home devices and the control server into an ID (Identifier) that can be recognized only within the trust domain [10]. Additionally, a star topology was used for routing in a smart grid home network to address the security concerns. Although various solutions exist to

address smart home security, a prominent approach will focus primarily on access control of the devices within the smart home network [11].

II. PROBLEM DEFINITION

The current infrastructure of home wireless networks allows all devices to communicate openly once connected to the central wireless signal [12]. Although more secure settings are available with most home routers, it is not easy for consumers to configure them. The combination of these facts is what causes the home network to be most vulnerable to attacks.

There are multiple scenarios in which an attacker can gain access to a network of IoT devices. One method would be a direct attack on a smart home hub, which, if compromised would allow them access to all devices connected to it. Similarly, if the Wi-Fi network is compromised, the same result could occur. Another scenario would involve an attacker installing malicious software on one of the devices connected to the network. This could get them access to data from that device but could also lead to the unwanted addition of other devices on the network. Lastly, data could be compromised by an attack outside the home, by targeting a third-party service provider that may not adequately protect against such an attack. All of these issues compromise the privacy of end-users, even if they believe that their data is anonymized or encrypted.

III. RELATED WORKS

One technique that attempts to solve the issue of user authentication is a messaging service known as Simple Messaging and Access Control (SMAC) [13]. In this technique, access control is moved from the device or shared server into the communication ports themselves. The SMAC server contains a significantly large enough number of ports that can be delegated to various devices. It can be safely assumed that only that specific device knows which port to use, therefore instantly verifying the identity of any user communicating on that port. The primary advantage of this technique is that it negates the need to store and maintain an Access-Control List (ACL), which can be very cumbersome as it increases in size.

IEEE 802.1X [14] is a strong reference when looking for a standard for port-based network access control as a large amount of the world's network traffic is sent using this underlying authentication mechanism. 802.1X authentication involves three parties: the supplicant, the authenticator, and the authenticating server. The authenticator responds to requests of new supplicants and acts as the middle-man to the authenticating server that performs the actual approval/denial. There are five stages of the authentication process within the 802.1X standard, and they include the following:

- **Initialization:** The supplicant begins communicating on a previously open port, and they are marked as "unauthorized" by the authenticator.
- **Initiation:** The authenticator will transmit a specific message to a particular address the supplicant should be listening for and waits for a response. The supplicant will reply with its identity, and this gets sent by the authenticator to the authenticating server.
- **Negotiation:** The authenticating server sends a message to the authenticator regarding the method of authentication that the supplicant must abide by.
- **Authentication**: Once a method has been agreed to, both the supplicant and the authenticating server will exchange messages through the authenticator. This process will continue until the authenticating server issues either a “Success” or “Failure” message. If a success message is transmitted, then the port is set to authorized, and the supplicant becomes a recognized device in the network. If a failure message is sent, then the port remains, and the authenticator will ignore any TCP or IP traffic from the device.

As the Internet of Things (IoT) becomes a more integral part of everyday life, the security surrounding it will also become equally important. When lights and electrical outlets were first controlled remotely, it could be argued that the worst a hacker could do was provide a light show for unsuspecting targets. With the migration of IoT to encompass home security alarms, cameras, and door locks the threat has become extremely serious. A. Kaur et al. [15] provide an analysis of various authentication methods while also performing a literature review on other research conducted on the subject. In the paper, it is highlighted that while some of the classical methods of authentication such as Access Control List (ACL), Role Based Access Control (RBAC), and Attribute Based Access Control (ABAC) have been used successfully, they all have flaws that could be improved. None of these methods are one-size fits all approach as is the difficulty in dealing with IoT devices. A system needs to be able to quickly and efficiently authenticate the smallest temperature sensor to the largest touch screen interface using the same basic algorithm.

Another topic discussed within the paper by A. Kaur et al. is how context awareness can be added to standard authentication methods to add an additional layer of protection from attack. The example provided is when IoT devices are authorized to access a network they must abide by specific communication data rates. If these rates are not followed, the device is blacklisted and removed from the network. This protection allows a network to have a slightly more robust authentication scheme than simple passcode or ID assignment at device addition if an authorized

device is compromised while on the network there is a chance that a context-aware network could more appropriately flag and eliminate the threat.

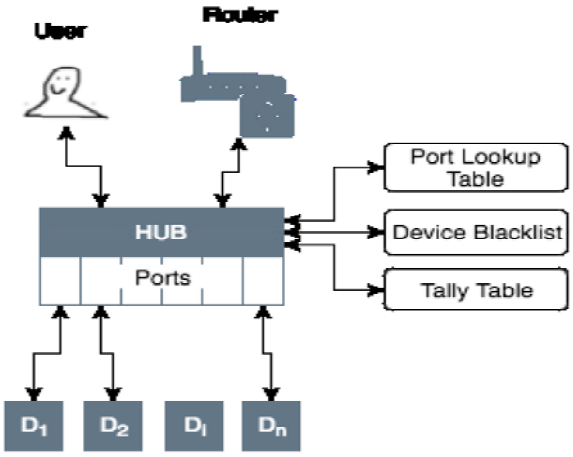


Figure 1. Smart Home Network Topology

IV. PROPOSED SOLUTION

To solve the problem regarding authentication and access control of IoT devices in a smart home network, given a set of assumptions, the following solution is proposed.

A. Smart Home Network Components

A typical smart home architecture involves three types of components: IoT devices, a router, and a hub. While the primary purpose of the router is to provide internet connection for all kinds of devices in a home network, the primary purpose of the hub is to connect IoT devices in the smart home to the router. The goal of the proposed model is to utilize the smart home hub to provide secure communication channels for IoT devices.

The hub acts as a central communication gateway for IoT devices and has m virtual ports through which bi-directional communication can take place. The hub also has a Port Lookup Table (PTL) which contains mapping between connected devices and ports through which they can communicate, a blacklist containing a list of MAC addresses associated with devices which are banned from interacting with the hub, and a Tally Table (TT) to track packet count for a rolling number of previous connections for each port and each device. Figure 1 depicts a visual example of a typical smart home network topology.
Any device, including the router, must follow the same protocol when attempting to communicate through the hub. Namely, every device must declare a port number through which a packet will be sent.

B. Assumptions

For this technique to be most effective, certain assumptions need to be established. The network must be set up as a hub-based star topology where all devices communicate through a centralized hub and never directly to each other. All communication through the hub happens within virtualized ports. The hub must be able to maintain a sufficiently large enough number of ports and additionally store data about each device. Each device in the network must also be able to store data about the ports they are assigned and the ratio of which they are expected to communicate through each of those ports. Each device will also require enough processing power to correctly determine which port to use each time a packet is sent. During the registration process, the hub becomes permanently known and trusted by the new device.

All communication that occurs within this network is expected to have its separate encryption scheme. The purpose of this paper is merely to propose an authentication method for the hub to be able to identify each device correctly.

TABLE I. TABLE OF NOTATIONS

Notation	Definition
D_A	Device A
H	Hub
U	User
E_A	Entry for D_A in the PLT
MAC	Media Access Control
PLT	Port Lookup Table
TT	Tally Table

C. Device Registration

The first step for the device to join the system is to register itself to the system.

1) $D_A \rightarrow H$: *Request*, *MAC*
   The device first sends a registration request along with its MAC to the hub to join the system.
2) $H \rightarrow U$: *Request*
   Upon receiving the registration request, the device forwards the request to the user.
3) $U \rightarrow H$: *Confirmation*
   The user sends a confirmation to deny or accept the request to the hub.
4) H: *Generate* E_A *and store it in PLT, create a new entry in TT*
   If the user denies the request, the hub would not reply to the device. If the user accepts the request, a random list of k virtual port numbers is created. A certain probability is assigned to each port.
5) $H \rightarrow D_A$: E_A
   The hub sends the ports and probabilities back to the device. The device stores this data and uses it for communicating with the hub/devices.

The user only needs to interact with the hub during registration as the rest of the authentication can take place automatically by the hub. For the remainder of this paper, we will discuss that process.

D. Instantaneous Authentication and Communication
The following describes the protocol for authenticating communication between an IoT device

in the network and the smart home hub for sending a single packet.

1) D_A:*Select a Port*
   The device which wishes to communicate with the Internet selects a random virtual port from a list of its assigned ports based on the probability established for that port.
2) $D_A \rightarrow H$: *Packet*The device sends a packet to the hub with the port number it wishes to connect through.
3) H: *Lookup* E_A
   The hub looks up the device via its MAC address and the port through which the packet came in the PLT.
   a) If the port-MAC addresses pairing is incorrect, the hub adds the device to its blacklist. Further steps are not taken.
4) H: *Lookup device in the blacklist*
   The hub checks for the device in the blacklist.
   a) If the device is in the blacklist, the packet is not forwarded. Further steps are not taken.
5) H: *Add device and port to TT*
   The device and the port are added to the top of the Tally Table.
6) H: *Remove the oldest entry from TT*
   If the number of tallies for the device exceeds some number *t*, the oldest entry for this device is removed from the Tally Table.
7) H: *Forward the packet*
   The hub forwards the packet.

E. Continuous Authentication and Communication

The following describes the protocol for providing authentication and communication services to devices in the network for more than one packet. This protocol requires a certain number of packets, *p*, to be sent such that the hub can calculate whether or not the ratio of ports used by a device matches the port usage probability assigned to the device.

1) $D_A \rightarrow H$: *Packet*
   A request to forward a packet has been received from the device
2) H: TT
   The hub checks the number of packets that have been received from the device since the registration in the Tally Table.
   a) If *p* packets have not yet been received by the hub from the device since the device has been registered, further steps are not taken.
3) H: TT
   If the number of forwarding requests is greater than or equal to *p*, the hub calculates the ratio of ports the hub expected the device to use and compares it with the ratio of the ports that the device used from the Tally Table.
   a) If the difference in ratios is greater than the predetermined allowed threshold, the device is added to the blacklist. No further steps are taken.

F. Security Analysis

Primarily, the instantaneous authentication protocol protects the network by verifying that the device attempting to establish communication has been registered and its MAC address is already stored in the PLT. Moreover, the protocol protects against masquerading attackers who are capable of spoofing the MAC address of the devices in the network from randomly guessing a port. Since the hub contains *m* virtual ports open for communication and each device is assigned *k* ports, then the probability of merely guessing a correct port while pretending to be a device in the network is $\frac{k}{m}$. This probability becomes increasingly small with an increase in the number of virtual ports. Moreover, if the guess is incorrect, the masquerading device is banned from communicating with the network with the stolen credentials until the correct device is registered again through the user's permission.

The primary purpose of the continuous authentication protocol is to make sure that an attacker who guesses one port correctly cannot continue to use that port without further knowing additional ports assigned to the device and the ratios at which the ports must be used by that device. Moreover, this scheme forces devices to diversify which ports they use to send data to.

Suppose that an attacker spoofs a device in the network and correctly guesses a single port. The attacker must use this port to continue to communicate through the hub because the probability of guessing another port is now $\frac{k-1}{m-1}$. However, since each device is assigned a specific ratio at which hub ports must be used, an attacker has a very limited number of requests it is allowed to send before the hub detects malicious behavior as the ratio of ports used by the device will become skewed towards a single port. However, the probability of guessing all ports correctly is $\frac{1}{\frac{m}{k}}$, which is relatively low. Furthermore, the likelihood of guessing proper ratios in addition to guessing the appropriate ports is improbable.

V. MATHEMATICAL MODEL

A. Instantaneous Authentication

Given m, the total number of ports on the hub and k, the number of ports assigned to each device, the immediate authentication requires only one port for authentication. Suppose the attacker can spoof the MAC address of the device, the probability of guessing one port associated with the device correctly is $\frac{k}{m}$. k should be chosen relatively small to m so that this ratio becomes small.

To determine the probability of an attacker correcting guessing the right combination of ports for any given device, we developed a formula that would show how the variable number of ports on the hub and number of ports assigned to each device would affect this probability.

$$\frac{(m-k)!\,k!}{m!}$$

For this calculation, we assume the following:

- The attacker knows the exact range of ports on the hub or has a list of all the possible port numbers.
- All devices connected to the hub have the same number of ports assigned to them, and the attacker knows this number.

If either of those assumptions is not true, the actual probability would be even smaller.

Figure 2 and Figure 3 show the results of this formula as the number of ports per device increases for 150, 500, and 1,000 total ports on the hub. Figure 2 shows the probability on a linear scale, and Figure 3 shows the probability on a logarithmic scale since the probability decreases exponentially with an increasing number of ports.

With these results, we concluded that if devices are assigned more than three ports, the probability of the attacker correctly guessing these three ports is insignificantly small, regardless of the total number of ports on the hub. This is why three ports was the primary number of ports assumed for the remainder of our simulation. However, as the logarithmic graph shows, applications with an increased need for security may still choose a higher number of ports per device and/or a higher total number of ports on the hub if desired.

B. Continuous Authentication

In a scenario when an attacker successfully guesses one port and given that his or her chances of guessing an additional port are too low, an attacker may use the same port to communicate with the hub. In this case, it is necessary to detect this abnormal behavior and block the intruder. Thus, two things must be defined: comparison measure between expected and received tally table port distributions and tolerance of bias toward a single port in the tally table.

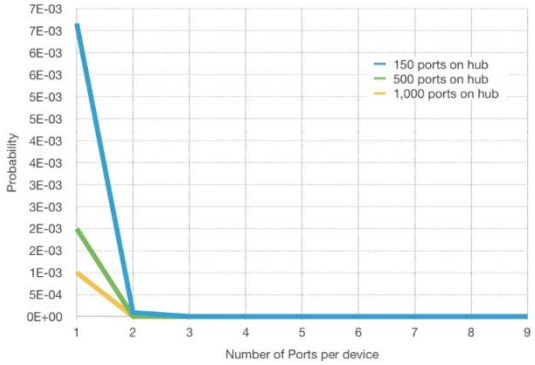


Figure 2: Number of Ports per Device

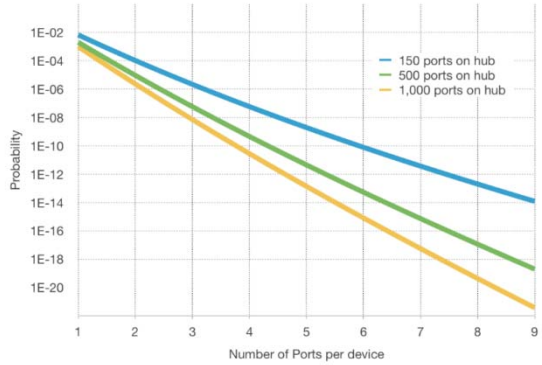


Figure 3: Number of Ports per Device

Traditional methods like Euclidean distance fall short in measuring the difference between the expected tally table and actual tally table. This is because their purpose is to measure the tally counts explicitly, while we are most interested in measuring the difference between the prior and posterior distributions. In other words, we are interested in seeing whether a change from expected port counts is due to randomness or due to intentional deviation from what we expected to observe. Since Kullback–Leibler (KL) divergence measures likeliness of one distribution function to another, it is the proposed measure.

Given received port distribution $P = \{p_i\}_n$ and expected distribution $Q = \{q_i\}_n$, KL divergence over discrete distribution sets is defined as

[redacted]

Since $\log(1) = 0$ and $D_KL\,(P||Q) \geq 0$, greater divergence implies that the bias in received port distribution is less likely to be due to randomness.

In that case, we can assume that an attacker randomly and successfully guesses port g. Let the expected prevalence of port in the tally table be q_g. Then we can express KL Divergence as

[redacted]

In the model above, if our tally table slowly starts filling up with port g counts, then p_g will increase, and p_i will decrease. Since

[redacted]

as the tally table gets filled with port,

[redacted]

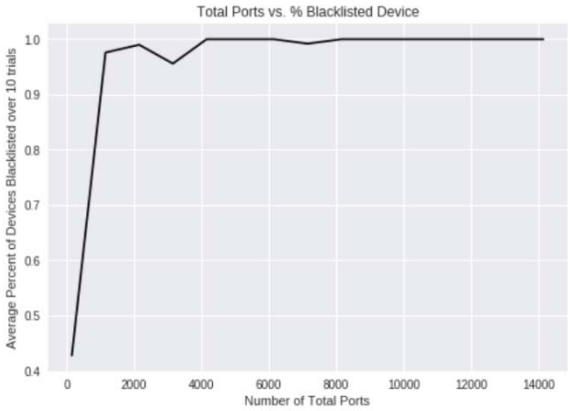


Figure 4: Total Ports vs. Number of Devices Blacklisted

Therefore, if the actual distribution has significantly more of port g than we expected, $D_KL\,(P||Q)$ will increase with every new packet, independent of the real probability assigned to port g. If we express the actual volume of g in the tally table as $p_g = q_g + x$, where x is a measure of the additional new number of packets arriving through port g, then

$$D_{KL}(p_g||q_g) \approx (q_g + x) \log \frac{q_g + x}{q_g}$$

and

$$\frac{\partial D_{KL}(p_g||q_g)}{\partial x} \approx \log \frac{q_g + x}{q_g} + 1 > 0$$

Which implies that divergence will continue to increase with the addition of new packets arriving through the single compromised port. Therefore, the optimal threshold does not necessarily have to be very high and can be determined through simulation.

VI. SIMULATION RESULTS

Simulation results in this section were performed in Python 3.6 on Google Colaboratory1 platform equipped with Intel(R) Xeon(R) CPU @ 2.30GHz processor.

Instantaneous communication can protect the network in the short term and depends solely on the number of

available ports in the hub. Given the mathematical results from the previous section, the expectation of proper guess is related to the number of total ports in the hub. Figure 4 depicts how many devices, on average over ten trials, would get blacklisted based on how many total virtual ports there are. Keeping the total number of devices in the system constant, this implies that the higher the number of ports, the less likely an attacker is to guess a correct port. Since it is not impossible for an attacker to guess a correct port, especially if there are very few virtual total ports in the hub, continuous authentication is required to further protect the network.

To understand how the network behaves under continuous authentication once an attacker has guessed at least one port correctly, it is essential to analyze the behavior of KL Divergence of the tally table for the mimicked device. Since it is more beneficial for an attacker to continue to use a single guessed port than guess an additional port, we can expect the tally table of the device which an attacker has mimicked to fill with the guessed port entries one packet at a time. The behavior of divergence in the tally table will depend on the distribution of assigned ports to the device as well as the number of new packets processed. Figure 5 depicts divergence for a malicious device if each port was guessed for a network where three ports were assigned to the device initially. It is evident that in this case, it does not make too much difference which port the attacker has guessed. Divergence appears to increase and its slope over time seems to increase as well.

Figure 6 depicts a scenario in which the expected distribution of ports is not uniform among the ports. This graph shows that divergence increases much faster when the expected port ratio is lower. This implies that it would be more difficult to detect a malicious device if an attacker guesses correctly a port which the device is expected to communicate through most of the time. Additionally, this implies that it would be beneficial to set a range for expected port
distribution, such that no bias exists toward a single port.

Divergence difference over time (as new compromised packets arrive) depends on how the port distribution was initialized. Figure 7 shows the randomly assigned port probabilities over ten trials. It is evident from the histogram that port assignments exhibit normal distribution about $\frac{1}{k}$, where k is the number of ports assigned to each device.

Setting a threshold tolerance level for detecting a malicious device requires setting the threshold high enough such that devices are not accidentally blacklisted and setting the threshold low enough, such that the malicious device cannot send too many packets and compromise the hub. A smart home network was simulated to determine how many devices,

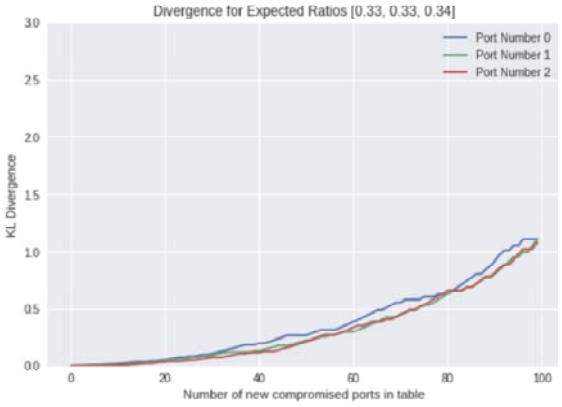


Figure 5: Divergence vs. Uniform Expected Ratios

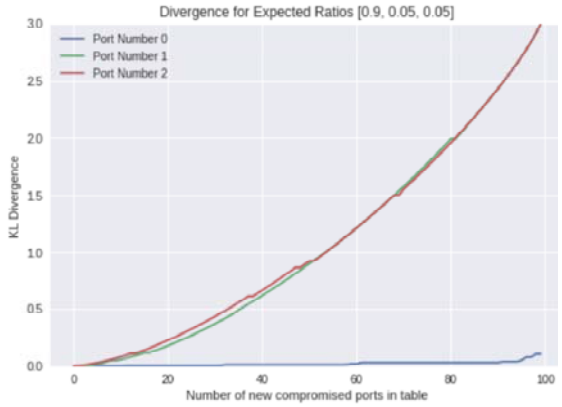


Figure 6: Divergence vs. Biased Expected Ratios

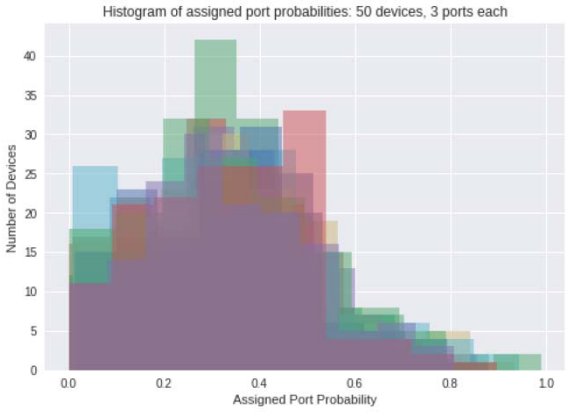


Figure 7: Randomly Assigned Port Probabilities

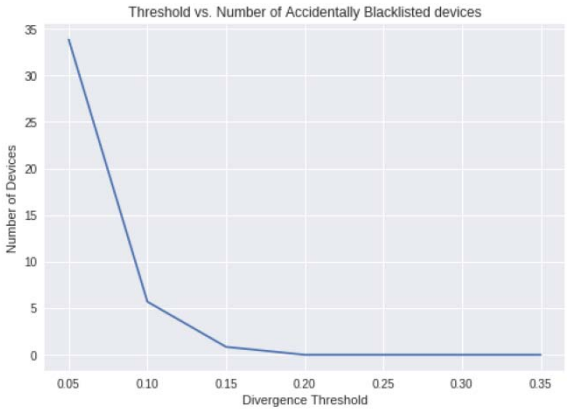


Figure 8: Accidental Blacklisting

on average, get accidentally blacklisted at each threshold level. The experiment involved 200 packets sent by 50 devices to the hub, where the size of the tally table for each device is 100 packets. Figure 8 shows the average number of accidentally blacklisted devices after 20 trials. This experiment substantiates that KL Divergence threshold is not required to be set high and a meager increase in threshold set significantly reduces the chances of accidentally blacklisting a healthy device.

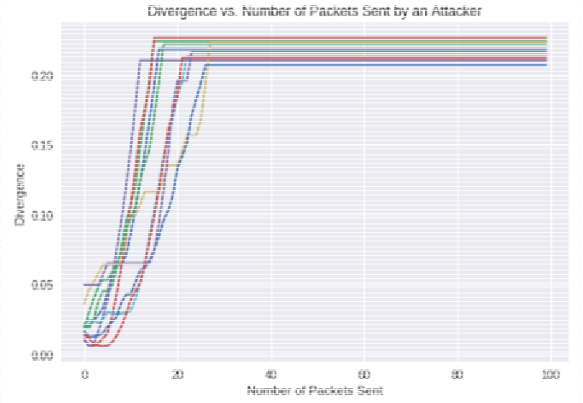


Figure 9: Threshold vs. Compromised Packet Count

Additionally, to determine the optimal threshold, it is necessary to analyze KL Divergence produced when a malicious device guesses a port correctly and uses that port solely to communicate through the hub. An experiment performed involved ten trials for a network with 50 devices with 100 tally table size and 0.2 KL Divergence threshold. A malicious device masqueraded as one of the healthy devices in the network, guessed a port correctly, and sent 100 packets (equal to the size of the tally table) through the hub. Figure 9 shows the results of KL divergence after each new packet is sent by the malicious device. It is evident from this analysis that KL divergence increases dramatically after several packets and the network does not require a full tally table to be populated with malicious packets to detect and blacklist the malicious device.

Finally, to establish a relationship between the number of devices in the network, threshold set, and an average number of packets required to determine whether a malicious device is communicating through the hub, the following experiment was designed. The network included a hub with 1000 available ports; 3 ports were assigned per device. The simulation involved a different number of devices between 50 and 300 in increments of 50. The threshold was set between 0.05 and 0.35 in increments of 0.05. The results, as seen in Figure 10, show that at any network density, demonstrated by the number of devices in the network, an increase in threshold corresponds to an increase in average packets required. Moreover, detection of the malicious device does not seem to correlate with the number of devices in the network (and thus, the number of unused ports).

CONCLUSION

In this paper, we proposed a simple protocol for authentication and access control of IoT devices in a smart home system. The protocol is based on the communication between the device using pre-assigned virtual ports on the central hub. Instantaneous authentication prevents an attacker from masquerading as a device in the network and accessing the central hub while continuous authentication blacklists any suspicious device which has gained access to the network. Our results show that the implementation of both authentication techniques provides secure and effective communication between the IoT devices, yet, ensures high scalability.

Additional effort is required to enhance our solution. The future work will contain an analysis of different attack methods (e.g., Botnet, Denial of service, Man-in-the-middle) and simulation to test against them. Moreover, one future avenue of our work is to implement the protocol in a real smart home system.

REFERENCES

[1] Ericsson: The Connected Future (2016). “Internet of Things Forecast” [Online]. Available: https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

[2] W. Ali, G. Dustgeer, M. Awais and M. A. Shah, "IoT based smart home: Security challenges, security requirements and solutions," 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, 2017, pp. 1-6.

[3] J. Han, Y. Jeon and J. Kim, "Security considerations for secure and trustworthy smart home system in the IoT environment," 2015 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2015, pp. 1116-1118.

[4] A. K. Ray and A. Bagwari, "Study of smart home communication protocol's and security & privacy aspects," 2017 7th International Conference on Communication Systems and Network Technologies (CSNT), Nagpur, 2017, pp. 240-245.

[5] M. Schiefer, "Smart Home Definition and Security Threats," 2015 Ninth International Conference on IT Security Incident Management & IT Forensics, Magdeburg, 2015, pp. 114-118.

[6] S. Erfani, M. Ahmadi and L. Chen, "The Internet of Things for smart homes: An example," 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON), Bangkok, 2017, pp. 153-157.

[7] T. Li, J. Ren and X. Tang, "Secure wireless monitoring and control systems for smart grid and smart home," in IEEE Wireless Communications, vol. 19, no. 3, pp. 66-73, June 2012.

[8] F. K. Santoso and N. C. H. Vun, "Securing IoT for smart home system," 2015 International Symposium on Consumer Electronics (ISCE), Madrid, 2015, pp. 1-2.

[9] S. Chang, T. William, W. Wu, B. Cheng, H. Chen and P. Hsu, "Design of an authentication and key management system for a smart meter gateway in AMI," 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), Nagoya, 2017, pp. 1-2.

[10] E. Kim and C. Keum, "Trustworthy gateway system providing IoT trust domain of smart home," 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, 2017, pp. 551-553.

[11] M. Nguyen, L. Nguyen and T. Nguyen, "On the design of gateway node for smart grid home network," 2015 International Conference on Communications, Management and Telecommunications (ComManTel), DaNang, 2015, pp. 57-61.

[12] I. Sanchez, R. Satta, I. Fovino, G. Baldini, G. Steri, D. Shaw and A. Ciardulli, "Privacy leakages in Smart Home wireless technologies," 2014 International Carnahan Conference on Security Technology (ICCST), 2014.

[13] A. Saxena, P. Duraisamy and V. Kaulgud, "SMAC: Scalable Access Control in IoT," 2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), 2015.

[14] Wikipedia: IEEE 802.1X (2018). [Online]. Available: https://en.wikipedia.org/wiki/IEEE_802.1X [15] A. Kaur, Isha, G. Rai, A. Malik, "Authentication and Context Awareness Access Control in Internet of Things: A Review," 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 1-6.

★★★