An Concert Review on Proximity Based IOT Device Authentication

Dr. Padmaja. Pulicherla
Professor, Dept. of CSE, TKR engineering College, Hyderabad, Telangana, India

Abstract- **To predictors trust that the Internet of Tings (IoT)grips great promise for many life-improving applications. In this paper, we propose a singularthe proximity-primarily based mechanism for IoT device authentication, known asMove2Auth, for the purpose of improving IoT device security. InMove2Auth, we require user to keep telephone and perform oneof two hand-gestures (moving in the direction of and away, and rotating)in front of IoT tool. By combining (1) large RSS-variation and(2) matching among RSS-hint and phone sensor-trace,Move2Auth can reliably stumble on proximity and authenticate IoTthe device henceforth.**

***Index Terms*-Wireless Communication; Security; Internet of Thingsng.**

I. INTRODUCTION

The Internet of Things (IoT) has quickly moved from hypeto reality. Gartner estimates that the number of deployedIoT devices will reach 20.8 Billion in 2020 [1]. Like otherdisruptive technologies, such as smartphones and cloud computing, IoT holds the potential for societal scale impact bytransforming many industries as well as our daily lives.However, IoT also brings security challenges due to its largescale and embedded device nature [2]. In this paper we discusssecurity of a basic IoT device function, i.e., associating toInternet gateway (e.g., Wi-Fi access point). In particular, wefound authenticating an IoT device is non-trivial, and existingdesign actually leads to security vulnerability in practice. Forexample, according to our experimental study on a popularhome automation brand, we can obtain the secrets that aresufficient for stealing home Wi-Fi password from all (millionof) the devices based on our attack on one device. From furtherdiscussion on this real world example, we show the need for acarefully designed IoT device authentication mechanism.In Figure 1, we take home automation scenario as anexample to describe IoT device authentication. Home Wi-Firouter needs to authenticate home automation devices (e.g.,smart power switch) before allowing them to connect. On themean time, a nearby attacker (e.g., deployed attacking devicearound home) can perform (1) passive attack by sniffing allmessage exchanges on Wi-Fi channel, or (2) active attack byimpersonating the home automation device and connecting tohome router. Therefore, a successful attack may obtain sensitive information (e.g., home Wi-Fi password), or get the access to home network whichenables further attack.

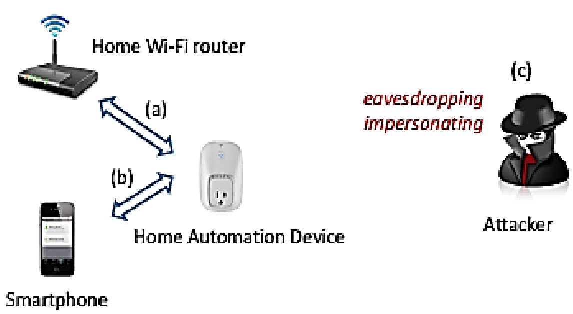

Figure.1. We take home automation device as an example to illustrate the IoTdevice authentication problem. (a) Home Wi-Fi router needs to authenticatethe device before connecting. (b) Smartphone is leveraged to input Wi-Fipassword. (c) An attacker can eavesdrop by sniffering Wi-Fi channel, orimpersonate the IoT device to connect to router/smartphone.

The imaginative and prescient of the IoT will advance primarily based on many newcapabilities and could address new demanding situations, as proven inFigure 2, inclusive of cloud computing, M2M, IoS, IoE, IoT,social networks, software-defined optical networks (SDO),and fifth generation (5G) cell networks. TeIoTdataso one can be made out of billions of interactions amongdevices and people are going to be not only large but additionallycomplicated and it will suffer from many safety and privatenesstroubles, especially concerning the authentication amongdevices. To clear up those security problems, researchers inside thefield of system protection has advanced many authentication protocols implemented inside the context of the IoT. The aim ofthe current survey paper is to offer a comprehensive andthe systematic overview of new research on posted authentication protocols for the IoT in four environments, such as,M2M, IoT, IoE, and IoS.

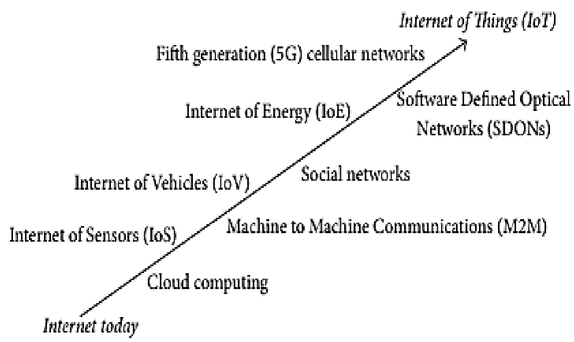

Figure 2: Vision of the IoT with main features and challenges

The temporal and spatial variations in the radio channelhave been exploited by researchers in RF-based localization,secure key extraction, and proximity estimation. In RFbased localization [7, 6], the range between a device and thereference points is estimated by means of RSSI. Afterwards,techniques such as triangulation can be used to estimate therelative location. Key extraction approaches [4, 8, 10] usethe reciprocal behavior of communication links to generatea secure key between two end-points. These approaches arecomplementary to our work, since they aim at securing thecommunication between two nodes without prior knowledge,whereas we provide proximity-based authentication.Prominent RF-based proximity estimation approaches are:

Amigo [3], Ensemble [2], and ProxiMate [9]. Amigo relieson observing the channel in promiscuous mode for 802.11frames. The observed packets and their corresponding RSSIreadings are fed to a classifier which determines proximity.In order to reach low false positive rates, more than 5 s areneeded. Ensemble relies on RSSI readings of packets generated by a network of trusted devices. It requires at least3 trusted devices in communication range, each sending 40packets per second for 70 s. ProxiMate relies similar to ourapproach on ambient RF signal. However, they focus on TVsignals and require software-defined radios to extract the required features (amplitude and phase) from the signal.Proximity estimation can as well be achieved by othermeans such as Time-of-Arrival (TOA). Rasmussen et al.[5] introduce an RF distance bounding technique based onTOA, which requires high processing time in the range ofnanoseconds, since an error of 3 ns results into an estimationerror of approx. 1 m. They achieve this high precision witha custom designed radio-chip.

II. METHODS ANDOUTLINES

In this paper, we propose a proximity based mechanism forsmartphone to authenticate IoT devices, called Move2Auth.As shown in Figure 2, we require user to hold smartphoneand perform one of two hand gestures (randomly picked bysmartphone) in front of the IoT device, while on the mean timethe IoT device is keep sending packets. The two gestures, i.e.,moving smartphone towards and away from IoT device, androtating smartphone, both lead to significant (around 15dB)variation in Received Signal Strength (RSS) because of fastchanging attenuation and antenna polarization, respectively. InMove2Auth, we combine (1) large RSS-variation detection,and (2) matching between RSS-trace and smartphone’s sensortrace, to perform reliable proximity detection, where (1) caneffectively differentiate devices in-proximity and far-away,and (2) can protect against powerful active attacker who canarbitrarily tune transmission power.

To conclude our experiments, the protection implementedby device vendor (i.e., Wemo designer) is indeed not sufficientto fix the password leakage issue. In the following, we discussthis defeated solution as well as other two possible solutions.We will show that carefully-designed device authenticationmechanism is a must for secure device association.

1) Defeated Vendor Solution: Encrypting Wi-Fi passwordactually provides a low cost solution for device authentication,i.e., even an attacker is connected to smartphone, it will not beable to retrieve the Wi-Fi password if the secrets are

unknown.Unfortunately, the secrets are identical to all the devices,therefore we can defeat the entire solution by attacking onlyone device.

2) Unique Secrets for Every Device: Security will beenhanced if unique secrets are allocated for every device, asattacking one device will not help in cracking other devices.However, we would argue that the cost of unique secrets canbe too high to afford, because IoT devices come in large scale.Specifically, every device can be assigned a unique key duringmanufacturing. The key can be (1) printed on device, or (2)recorded in a database and indexed by device ID or MACaddress. When the device needs to be authenticated, the printedkey can be directly read by user and inputted in the other party(e.g., smartphone), or the stored key can be queried from thedatabase. In case (1), the problem is that the same key shouldbe stored simultaneously at two places, i.e., hardcoded insidefirmware and printed on device. While manufacturing in largescale, maintaining a sufficiently low mismatch rate will be abig challenge to device vendors. In case (2), for symmetrickey, we need additional means for determining which usercan query the key of a device ID. Otherwise, the key will beleaked to attackers. Private/public key pair might mitigate theproblem, for which each vendor can build an infrastructuresimilar to the Public Key Infrastructure (PKI) [18]. Again, themaintenance cost will be a big challenge when devices comein large scale.

3) Encrypting the Channel between Smartphone and IoT device: Encrypting the channel can prevent eavesdroppersfrom capturing the message exchanges. However, while encrypting the channel is not difficult, for example, generatingsymmetric key using Diffie-Hellman key exchange or providing private/public key pair from either side, encryption doesnot prevent active attackers. In the Wemo case (as well asmany other home automation devices we tried), device setsitself as Wi-Fi access point for smartphone to connect. As inFigure 1, an active attacker can impersonate the Wemo deviceby broadcasting the same SSID and using the same MACaddress. If smartphone is connected to the attacker, home WiFi password will be sent to the attacker directly.

III. MOVE2AUTH DESIGN

From Wi-Fi router point of view, an IoT device is all the same as a mobile device (e.g., smartphone or tablet), on which Pre-Shared Key (PSK) is widely used for device authenticate. Specifically, 802.11 standards incorporate a Diffie-Hellman key exchange based mechanism, called Simultaneously Authentication of Equals (SAE) [3], for mutual authentication between router and device. SAE plus a limited number of retries provides solution against the attacks shown in Figure 1. However, from device point of view, IoT brings new challenge because the devices usually lack means for PSK (e.g., Wi-Fi password) input, as they are mostly embedded devices. Specifically, in this paper we assume the IoT device (1) does not contain sophisticated user interface like screen or keyboard, (2) does not equip sensors like camera, accelerometer, gyroscope, NFC, microphone, etc. (3) is not easy to move (e.g., power switch plugged on walls).

A. Goal and Threat Model

Our goal is to build a device-authentication mechanism forthe purpose of facilitating IoT device to securely associateto Wi-Fi router. In particular, we leverage smartphone inthe way that connecting IoT device to smartphone first, andinput the password of Wi-Fi router on smartphone, as wediscussioned in the Introduction and Figure 1. As a result,the whole process can be considered secure as long as theIoT-smartphone connection is secure.We consider attacker who can receive the packets fromIoT device and smartphone, but is not physically close toIoT device, e.g., outside of the home as in home automationscenario. We consider powerful attackers. For example, theattacker can sniff all the Wi-Fi channels and capture all thepackets; he may have arbitrarily high-sensitivity receiver; hecan actively connect to smartphone by impersonating the IoTdevice; he may have arbitrarily high transmission power andcan adjust the transmission power arbitrarily; he may have fullknowledge of our scheme; he may have exact copy of the IoTdevice; he may know the exact location of the IoT device.In the following, we focus on one-way authentication, i.e.,smartphone authenticates IoT device.

B. Basic Scheme

We assume IoT device is not moveable. When an IoT device is in pairing mode, it keeps sending encrypted packets. On the mean time, we require user to hold smartphone in front of (e.g., 20cm distance) the IoT device and perform small gesture for a while (e.g., three seconds). User will be asked to perform one of two gestures, i.e., moving towards and away from IoT device and rotating, as shown in Figure 2. The gesture is randomly picked by smartphone. While the gesture is performed, smartphone receives a series of packets with significantly-varying RSS.

Smartphone determines whether the packets are sent from a nearby device based on two criteria, i.e., (1) RSS-variation exceeds a threshold, (2) RSS-trace matches with smartphone sensor trace. In our design, we set 10dB as the RSS-variation threshold for both gestures.

Matching between RSS-trace and sensor-trace is an important building block of Move2Auth. The idea behind trace matching is that, both traces can precisely describe smartphone emovement when two devices are in proximity, but when twodevices are far-apart, RSS-trace will not reflect the movementwell. In our design, we not only consider shape of traces, butalso involve timing for trace-matching. Timing informationcreates big-barrier for attacker who can fake large RSSvariation (e.g., by tuning its transmission power). Even if thefaked RSS-variation reflects the pace of smartphone-movementwell, the faked RSS trace will not exactly match smartphonemovement because of their different start time. In our design,both sensor-trace and RSS-trace are recorded on smartphoneso that we can easily synchronize them using smartphoneclock.

C. Trace Transformation - Moving Towards and AwayWe require user to move smartphone for around 20cm,and the shortest distance to IoT device is around 20cm. Thissmartphone movement causes around 15dB RSS-variation.In our design, moving smartphone towards and away fromIoT device is captured by accelerometer. For the sake ofsimplicity, we assume smartphone moves strictly on a line(towards IoT device). Therefore, the accelerometer-reading canbe reduced from 3-dimension to 1-dimension.

IV. CONCLUSION

Inspired by our comment of IoT safety vulnerability in real international, we recommend a singular proximity based authentication mechanism for IoT gadgets called Move2Auth.Move2Auth detects proximity by way of checking (1) big RSS version and (2) matching between RSS-trace and telephone sensor-hint during user gestures, i.e., shifting phone toward or far away from IoT device, and rotating smartphone.

REFERENCES

[1] “Gartner says 6.4 billion connected "Things" will be in use in 2016, up 30 percent from 2015,” http://www.gartner.com/newsroom/id/3165317.

[2] A. Kalamandeen et al. Ensemble: CooperativeProximity-based Authentication. MobiSys’10.

[3] A. Varshavsky et al. Amigo: Proximity-basedAuthentication of Mobile Devices. UbiComp’07.

[4] J. Croft et al. Robust Uncorrelated Bit ExtractionMethodologies for Wireless Sensors.IPSN’10.

[5] K.B. Rasmussen et al. Realization of RF DistanceBounding. USENIX Security’10.

[6] M. Youssef et al. Challenges: device-free passivelocalization for wireless environments. Mobicom’07.

[7] N. Patwari et al. Relative Location Estimation inWireless Sensor Networks.Transactions on SignalProcessing, 51(8), 2003.

[8] S. Jana et al. On the Effectiveness of Secret KeyExtraction from Wireless Signal Strength in RealEnvironments.MobiCom’09.

[9] S. Mathur et al. ProxiMate: Proximity-based SecurePairing Using Ambient Wireless Signals. MobiSys’11.

[10] S. Mathur et al. Radio-Telepathy: Extracting a SecretKey from an Unauthenticated Wireless Channel.MobiCom’08.

[11] “Owners of heatmiserwifi thermostats warnedof password leaks and other vulnerabilities,”https://www.grahamcluley.com/2014/09/heatmiser-wifi-thermostatspassword-leak/.

[12] "Kettles are leaking wifi passwords (and other failures of the internetof things)," http:// www.newstatesman.com/science-tech/futureproof/2015/10/kettles-are-leaking-wifi-passwords-and-other-failuresinternet.
[13] "Belkinwemo home automation,"http://www.belkin.com/us/Products/ home-automation/c/wemohome-automation/.
[14] "Base64," https://en.wikipedia.org/wiki/Base64.
[15] "Binwalk firmware analysis tool," http://binwalk.org/.