RSSI Localization: A Study to Found Targeted Social Engineering Victim Using 4 Dollar Wireless Device

Galang P. N. Hakim[1], Ahmad Firdausi[2]
[1, 2]Electrical Engineering Department, Universitas Mercu Buana, Jakarta, Indonesia
Email: [1]galang.persada@mercubuana.ac.id, [2] ahmad.firdausi@mercubuana.ac.id
* galang.persada@mercubuana.ac.id

***Abstract*—Social engineering is a common method to collect more information from victim trough socialization. This method employs human psychology to manipulate other people. In cyber society today, the attacker could use various methods to tapping into victim smartphone, and after that the attacker can get victim persona profiling information. The attacker can select random victim and then using wireless localization methods, the attacker could found its victim. After the random victim has been found the attacker can start social engineering directly to the victim based on persona profiling information, to gain trust and more personal information that can lead inflicting damage to the victim. In this paper, we demonstrate to localize victim using green obaidat calibrate Path loss Propagation models and $4 dollar device based on victim Smartphone RSSI Wi-Fi Signal. With this device we could localize a person within 15 meter with just only 0.64 dbm in difference between our RSSI measurement and simulation.**

Keywords— wireless localization, RSSI signal, Pathloss Model

I. Introduction

In this golden age of information, one of the things that have a value more than money would be information itself. Furthermore attackers usually launch not only cyber-attack but also social engineering to obtain information by manipulating people [1]. Social engineering is one of most powerful tool to attack security system [2]. Because people remain susceptible to manipulation [3], It's easier to trick someone into revealing a password than hacking into the system [4]. Social engineering can defeat the best of the best security system, even though they have their robust firewalls, best cryptography methods, best intrusion detection system, and best antivirus to protect their system [5]. Social engineering is a common method to collect information from victim trough socialization. This method employs human psychology to manipulate people to gain access to system or other sensitive information [6]. A lot of social engineering methods such as Trojan, impersonation, persuasion, bribery, shoulder surfing, dumpster diving [7], and one of popular is phishing and reverse social engineering [8].

Today, security problem arises because lot of people stores their personal information on their trusted device such as smartphone [9], [10]. Sometimes it not just to store, but also process organizational data [11]. This persona profiling such as age, sex, cultural and professional background, habits, and others that serve as preliminary information [12]. Social engineering methods can be using also whether the victim or the attacker just meet (incidental), even if attacker don't know the face of the victim (random target on attacker local area). As long as the attacker can get access to its smartphone such as using exploit in the NFC (Near Field Communication) [13], Rowhammer attack [14], UI (User Interface) state inference attack [15], and others, the attacker could know the position of the victim. This could be done using gps (Global Positioning System) tracking application if the victim is on the outdoor area [16], and using wireless localization if the victim is inside building [17], [18] where gps signal lost or couldn't penetrated the building [19]. Even though many companies have started to educate their employees to prevent social engineering attacks [20], [21], but when victim is located using wireless localization and the attacker using preliminary information before as initial information, the victim didn't know that they have been fallen into reverse social engineering methods. Thus with this the attacker can easily gain more confidential information such as password, username and even companies secret.

In this paper we presented indoor and outdoor personal wireless localization to raise awareness of an attacker if one of our wireless features on smartphone (such as WiFi, NFC, and others) is turn on even though we don't use it. Wireless localization basically is the process of determining the device physical coordinate using triangulation, time of arrival, RSSI (Receive Signal Strength Indicator) signal, and others [22]. One of the cheap, simple, and easier wireless localization technique is using RSSI Signal. Table 1 show Matrix Related Research.

TABLE I. Matrix Related Research

Researcher	Application	Measurement Device
David B. Green and M. S. Obaidat [23]	Computer Communication Ad hoc Network	Cisco Aironet 340 LAN
Galang P. N. Hakim [24]	IoT WSN Forest environment Data Communication	IoT Node Microcontroller Wemos

Researcher	Application	Measurement Device
Tony & Margo[25], [26]	Indoor and Outdoor measurement	IoT Node Microcontroller Wemos

II. Wireless Localization Component

There are 2 main component for personal wireless localization which is $4 dollar device and pathloss propagation model. pathloss propagation model is a function of a reduction in power density (attenuation) of an electromagnetic wave signal propagates through space. Researcher has been develop several pathloss propagation model with their own respective application. In this paper we are using 2.4 GHz pathloss propagation model that has been develop by Green-Obadiat [23].

A. Green-Obaidat Pathloss Propagation Model

This pathloss model develop from free space path loss model. The merits of this model was to consider the use low antenna height between 1-2 meter, where people usually use their smartphone to call and to texting. Therefore a fresnel zone will limits the electromagnetic wave propagation distance with high attentuation [23].

- For distance (d) function develop from free space model Therefore, the model will be :

$$40 \log_{10} d \quad (1)$$

- For frequency (f) function still the same with free space model, and thus its model was :

$$20 \log_{10} f \quad (2)$$

- For Antenna Height (H) Gain the equation will become :

$$20 \log_{10} Hr\, Ht \quad (3)$$

The full pathloss propagation model for low antenna height develops by green-obadiat become:

$$40 \log_{10} d + 20 \log_{10} f + 20 \log_{10} Hr\, Ht \quad (4)$$

Where :

f = frequency in gigahertz (GHz)

$H\,t, H\,r$ = antenna heights for Tx and Rx in meter

d = distance between Tx & Rx in meter

B. Maintaining the Integrity of the Specifications

Wemos is a one of IoT Node that popular because it was cheap, simple, and easy to use. Basically it was a microcontroller that has been equipment with WiFi Chipset [27] therefore allows it to be use in wireless Sensor Network application. To make it simple to use this device for wireless localization, we equip with LCD I2C to show the result RSSI measurement, powered using 9 volt battery, and placed inside cardboards cube for a better handling [25], [26]

III. RSSI Signal Measurement

A simulation and real time measurement is carried out to compare the Green-Obaidat Pathloss Propagation Model theory with real world for outdoor and indoor application. We proposed a walk test method, and for each meter we do RSSI measurement both for outdoor and indoor application. For outdoor measurement we proposed the use of football field and for indoor measurement we propose an auditorium which has non obstacle, also wide, and bigger space. Table 2 and figure 2 shows measurement versus simulation for 15 meter.

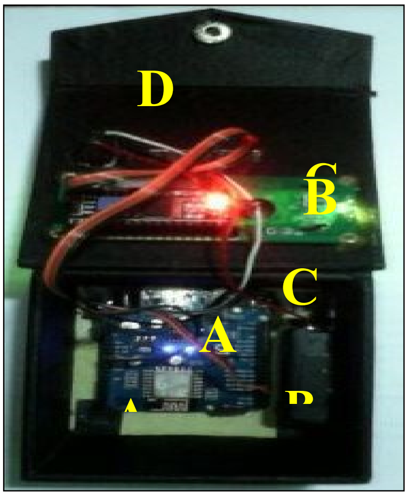

Fig 1. Indoor Outdoor Wireless Localization Device

A	= Wemos IoT Node
B	= Hitachi LCD 16x2 I2C
C	= 9 Volt Battery
D	= Cardboards Cube

TABLE II. RSSI MEASUREMENT VERSUS SIMULATION

Distance (m)	Simulation (dBm)	Outdoor Measurement (dBm)	Indoor Measurement (dBm)
1	9.40	-49	-50
2	-2.64	-47	-52
3	-9.68	-57	-59
4	-14.68	-57	-61
5	-18.56	-56	-58
6	-21.73	-58	-63
7	-24.40	-65	-67
8	-26.72	-61	-66
9	-28.77	-60	-68
10	-30.60	-67	-72
11	-32.26	-66	-73
12	-33.77	-68	-75
13	-35.16	-70	-73
14	-36.45	-70	-68
15	-37.64	-71	-72

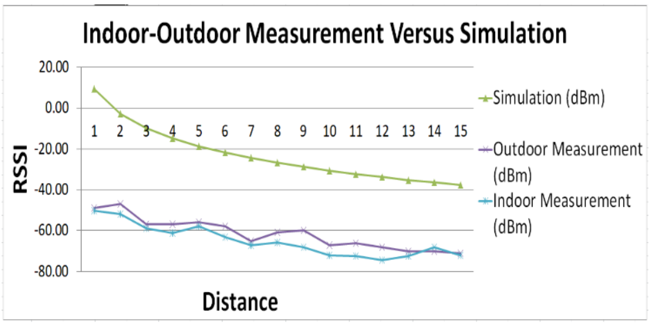

Fig 2. Indoor Outdoor Localization Measurement Versus Simulation

From figure 2 above and table 2 above we see between simulation and measurement there is a big gap. From our previous research we know this is an effect because of shielding [28]–[30] that cause high attenuation. In this research the use of cardboards cube for handling simplicity also caused high attenuation. Therefore we proposed calibration for additional attenuation caused by cardboards cube which is 35 dB losses. Table 3 and figure 3 shows measurement versus calibrated simulation for 15 meter.

TABLE III. RSSI MEASUREMENT VERSUS CALIBRATED SIMULATION

Distance (m)	Calibrated Simulation (dBm)	Outdoor Measurement (dBm)	Indoor Measurement (dBm)
1	-25.60	-51	-50
2	-37.64	-50	-52
3	-44.68	-52	-59
4	-49.68	-54	-61
5	-53.56	-58	-58
6	-56.73	-61	-63
7	-59.40	-67	-67
8	-61.72	-61	-66
9	-63.77	-68	-68
10	-65.60	-70	-72
11	-67.26	-66	-73
12	-68.77	-74	-75
13	-70.16	-73	-73
14	-71.45	-74	-68
15	-72.64	-72	-72

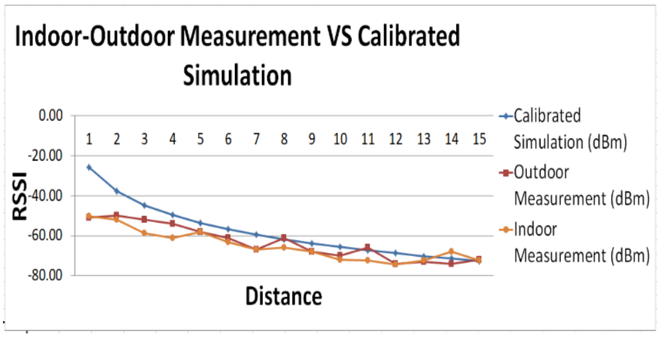

Fig 3. Indoor Outdoor Localization Measurement Versus calibrated Simulation

For personal wireless localization in indoor and outdoor environment we propose additional attenuation (loss) in effect of device boxing. Therefore the pathloss propagation model becomes:

$$40 \log_{10} d + 20 \log_{10} f + 20 \log_{10} Hr\ Ht + 35 \quad (5)$$

Using this Pathloss Propagation models for measurement below 4 meter fails to produce accurate result with average gap at about 16.16 dbm for indoor measurement and gap at about 12.35 dbm for outdoor measurement. The models shows accurate result for 5 meter to 15 meter measurement, with very accurate in 15 meter where the gap only 0.64 dBm between outdoor measurement and calibrated simulation and the gap only 0.39 between indoor measurement and calibrated simulation.

IV. CONCLUSION

In this paper, we raised awareness for user that using smartphone to store their persona profiling data. In this paper we demonstrated how to localize victim using low cost device. Using green obaidat calibrate Pathloss Propagation models and $4 dollar device an attacker could build low cost, simple, but yet powerful enough to perform personal localization trough victim WiFi or NFC signal. After victim has been localizing, reverse social engineering could be performed by the attacker based on their initial persona profiling data. With these two things we could localize a person within 15 meter with just only 0.64 dbm in difference between our measurement and simulation.

ACKNOWLEDGMENT

The Authors would like to Fauzi Atsani to help with the Field Measurement.

REFERENCES

[1] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Social engineering attacks on the knowledge worker,” *Proceedings of the 6th International Conference on Security of Information and Networks - SIN ’13*, pp. 28–35, 2013, doi: 10.1145/2523514.2523596.

[2] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “ScienceDirect Advanced social engineering attacks *,” *Journal of Information Security and Applications*, vol. 22, pp. 113–122, 2014, doi: 10.1016/j.jisa.2014.09.005.

[3] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, “Social engineering attack framework,” 2014, doi: 10.1109/ISSA.2014.6950510.

[4] C. Hadnagy, “Social Engineering: The Art of Human Hacking,” *The Art of Human Hacking*, 2010.

[5] F. Salahdine and N. Kaabouch, “Social Engineering Attacks: A Survey,” *Future Internet*, vol. 11, no. 4, p. 89, 2019, doi: 10.3390/fi11040089.

[6] A. Kumar, M. Chaudhary, and N. Kumar, “Social Engineering Threats and Awareness: A Survey,” *European Journal of Advances in Engineering and Technology*, vol. 2, no. 11, pp. 15–19, 2015, [Online]. Available: www.ejaet.com.

[7] S. D. Applegate, “Social engineering: Hacking the wetware!,” *Information Security Journal*, 2009, doi: 10.1080/19393550802623214.

[8] M. Chinta, J. Alaparthi, and E. Kodali, “A Study on Social Engineering Attacks and Defence Mechanisms,” *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 14, no. Icetcse, pp. 225–231, 2016.

[9] A. Eboka and A. A. Ojugo, “A Social Engineering Detection Model for the Mobile Smartphone Clients,” *African Journal of Computing*,

vol. 7, no. September 2014, 2018.

[10] Y. Zhou, X. Zhang, X. Jiang, and V. W. Freeh, “Taming information-stealing smartphone applications (on android),” 2011, doi: 10.1007/978-3-642-21599-5_7.

[11] S. Allam, S. V. Flowerday, and E. Flowerday, “Smartphone information security awareness: A victim of operational pressures,” *Computers and Security*, 2014, doi: 10.1016/j.cose.2014.01.005.

[12] D. Ariu, E. Frumento, and G. Fumera, “Social Engineering 2.0: A Foundational Work,” in *ACM International Conference on Computing Frontiers 2019*, 2017, no. July, pp. 1–7, doi: 10.1145/123.

[13] C. Bermejo and P. Hui, “Steal Your Life Using 5 Cents: Hacking Android Smartphones with NFC Tags,” *arXiv Computer Science Cryptography and Security*, 2017, [Online]. Available: http://arxiv.org/abs/1705.02081.

[14] P. Frigo, C. Giuffrida, and H. Bos, “Grand Pwning Unit: Accelerating microarchitectural attacks with the GPU,” 2018.

[15] Q. A. Chen, Z. Qian, and Z. M. Mao, “Peeking into your app without actually seeing it: Ui state inference and novel android attacks,” *Proceedings of the 23rd USENIX Security Symposium*, no. August, pp. 1037–1052, 2014.

[16] K. Al Zaabi, “Android device hacking tricks and countermeasures,” *2016 IEEE International Conference on Cybercrime and Computer Forensic, ICCCF 2016*, 2016, doi: 10.1109/ICCCF.2016.7740441.

[17] K. Chintalapudi, A. P. Iyer, and V. N. Padmanabhan, “Indoor localization without the pain,” 2010, doi: 10.1145/1859995.1860016.

[18] A. S. Paul and E. A. Wan, “RSSI-Based indoor localization and tracking using sigma-point kalman smoothers,” *IEEE Journal on Selected Topics in Signal Processing*, 2009, doi: 10.1109/JSTSP.2009.2032309.

[19] N. Kohtake and S. Morimoto, “Indoor and Outdoor Seamless Positioning using Indoor Messaging System and GPS,” *2011 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 2011.

[20] D. Rountree, “Organizational and Operational Security,” in *Security for Microsoft Windows System Administrators*, 2010, pp. 135–159.

[21] M. Junger, L. Montoya, and F. J. Overink, “Priming and warnings are not effective to prevent social engineering attacks,” *Computers in Human Behavior*, 2017, doi: 10.1016/j.chb.2016.09.012.

[22] A. R. Kulaib, R. M. Shubair, M. A. Al-Qutayri, and J. W. P. Ng, “An overview of localization techniques for wireless sensor networks,” *2011 International Conference on Innovations in Information Technology, IIT 2011*, pp. 167–172, 2011, doi: 10.1109/INNOVATIONS.2011.5893810.

[23] D. B. Green and A. S. Obaidat, “An accurate line of sight propagation performance model for ad-hoc 802.11 wireless LAN (WLAN) devices,” *Proceedings of IEEE International Conference on Communications (IEEE ICC ’02)*, vol. 5, pp. 3424–3428, 2002, doi: 10.1109/ICC.2002.997466.

[24] G. P. N. Hakim, M. Alaydrus, and R. B. Bahaweres, “Empirical Approach of Ad hoc Path Loss Propagation Model in Realistic Forest Environments,” *International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications, ICRAMET*, vol. 978-1–5090, pp. 1–5, 2016.

[25] T. Chandra and F. Bachruddin, “RANCANG-BANGUN ALAT PENGUKUR JARAK BERDASARKAN SINYAL RSSI WIFI YANG DI TERIMA,” 2016.

[26] M. Yonathan and F. Bachruddin, “ANALISA ALAT PENGUKUR JARAK BERDASARKAN SINYAL RSSI WIFI IEEE 802.11 b/g/n,” 2016.

[27] E. Datasheet, “ESP8266 Serial Esp-01 WIFI Wireless,” *ESP8266 Serial Esp-01 WIFI Wireless*, 2004.

[28] A. S. Wardoyo and M. Alaydrus, “Degradation of Shielding Performance of Metallic Sheet due to Aperture Configuration and Dimension at 2.4 GHz,” *Jurnal Elektronika dan Telekomunikasi*, vol. 18, no. 1, p. 9, 2018, doi: 10.14203/jet.v18.9-14.

[29] G. P. N. Hakim, A. Firdausi, and M. Alaydrus, “A low cost electromagnetic sensor for detecting holes in metallic sheet,” *Telkomnika*, vol. 17, no. 5, 2019, doi: http://dx.doi.org/10.12928/telkomnika.v17i5.12684.

[30] S. Celozzi, R. Araneo, and G. Lovat, *Electromagnetic Shielding*. Wiley Interscience, 2018.