Earthline Journal of Mathematical Sciences
E-ISSN: 2581-8147
Volume 13, Number 2, 2023, Pages 543-553
https://doi.org/10.34198/ejms.13223.543553

A Multi-Indicator Light Weight Defense Scheme for Smartphone Camera-Based Attacks

Arnold Mashud Abukari*, Abukari Abdul Aziz Danaa,
Diyawu Mumin and Shiraz Ismail

Department of Computer Science, Tamale Technical University, Tamale, Ghana
e-mail: amashud@tatu.edu.gh*

Abstract

Over the years, cyber criminals have succeeded in exposing some vulnerabilities in smartphones and have exploited those vulnerabilities in several ways. In recent years, one of the growing attacks on smartphones is the camera-based attacks. Attackers are able to exploit smartphone vulnerabilities to cause harm to smartphone users by using cameras of the smartphones to capture images and videos. Privacy leakage and confidentiality remains a big threat to smartphone users and this has gained attention from researchers and industry players across the world. In this research paper, a multi-indicator light weight defense scheme is presented to address the rising smartphone camera-based attacks. The random forest algorithm, the Gini coefficient index and the entropy method are adopted in the designing of the proposed scheme. The means of the threat indicators and the Mean Square Deviation (MSD) is also calculated in order to ensure accurate scores and weight assignments of the threat indicators. The proposed multi-indicator light weight scheme demonstrated to be consistent with real situations. A review of literature in camera-based attacks is also presented in this research paper.

Introduction

The use of smartphones has increased dramatically in recent years, with Android-based handsets dominating the market because of their high availability and intuitive user interfaces (Statista [3]). Android phones are now profitable targets for many types of cyberattacks and data breaches thanks to the rise in smartphone usage, which has also caught the attention of hackers. It is very essential for the research community and the

Received: August 11, 2023; Accepted: September 16, 2023; Published: September 29, 2023

2020 Mathematics Subject Classification: 68-XX.

Keywords and phrases: camera-based attack, smartphone, cyber attack, random forest, light weight defense scheme, cyber security.

*Corresponding author

industry collaborates to mitigate the dangers that these cyber criminals pose to smartphone users. This research work seeks to focus on study of the vulnerabilities and security implications of smartphones in the wake of camera-based attacks. The objective of this research paper is to propose an effective light weight security scheme that minimizes the impact on device performance and battery life, thereby ensuring security and a seamless user experience. The research work adopted a combination of techniques that seek to increase efficient malware detection, smartphone integrity verification and secure data transmission.

The random forest algorithm and the entropy methods optimize the threat indicators selection, data processing methods that will offer real-time protection for smartphone users and minimize the computational overhead caused by a wide range of threats.

In order to achieve an efficient malware detection, a defense scheme should incorporate a machine learning-based techniques and neural networks because it has the potential to identify malicious software (Gao et al. [2]).

Large datasets of known malware or threat indicators are fed into a light weight scheme to help in classifying and mitigating potential threats. This approach ensures a proactive protection against malware, threats and their variants.

Franklin et al. [1] argues that a defense scheme should integrate strong encryption algorithms such as the Advanced Encryption Standard (AES) to contribute in ensuring confidentiality and data integrity. The AES also incorporates a secure communication protocols such as the Transport Layer Security (TLS) which helps to establish a trusted connections between smartphones and servers remotely. This reduces the risk of man-in-the-middle attacks.

At the software level, a secure bootstrapping and digital signatures that will ensure verification of the integrity of the smartphone operating system (OS) and applications during the booting process to help the smartphone to run genuine and unaltered software (Weichbrodt et al. [4]).

Light Weight Defense Schemes

There are several light weight defense schemes that have been implemented across various industries and encryption schemes as well as devices. A light weight defense is a security framework which adopts very efficient mechanisms and algorithms to minimize resources consumption and to ensure the effective protection of a device (Deshpande et

al. [13]). Light weight defense schemes do not compromise its performance and usability for its malware detection and secure data transmission. It strikes a fair balance to achieve its objectives between resource efficiency and security of the device. The most important objective of every light weight defense scheme is to ensure a real-time protection against cyber criminals, unauthorise modifications, data breaches and various malware. The adoption of light weight defense scheme helps to optimize system utilization resources like the Central Processing Unit (CPU).

Lightweight Cryptography

The security of devices especially smartphones and Internet of Things (IoT) devices has caught the attention of users and the research community. These smartphones and Internet of Things (IoT) devices largely operate in very vulnerable environments that require connectivity which leads to security challenges. The traditional cryptography schemes are not able to properly address the security challenges facing smartphones and the Internet of Things (IoT) devices and this has compelled researchers to develop a concept called Light Weight Cryptography (LWC) scheme (Eisenbarth et al. [22]). Light weight cryptography is cryptographic algorithms and protocols that are designed to ensure security of devices that are resource-constrained like the smartphones and IoT devices. The size of the device, the ROM, RAM, Power and the power consumption are essential in the determination of the light weight cryptographic algorithm. The processing speed with much emphasis on throughput and delays are also essential in LWC schemes.

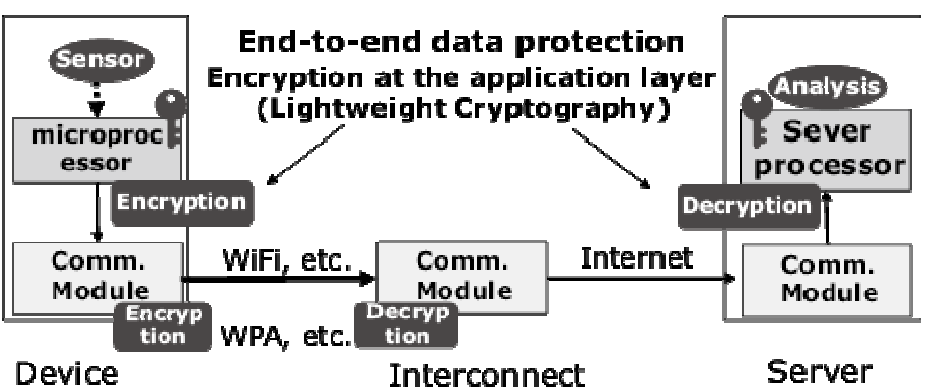

Figure 1: Light Weight Cryptography (LWC) (Okamura [23]).

The Proposed Light Weight Defense Scheme

Analysis of the permission levels of smartphones is critical in putting measures to prevent camera-based attacks in smartphones. The permission analysis is to enable the user of the smartphone to be able to identify harmful attacks and has the power to disable the suspected application with such permission. This research paper is mindful of the fact that some camera-based attacks can be controlled by the attacker remotely. The light weight defense scheme is built based on the information of the kind of permissions used by the attacker to develop the malicious application. The proposed light weight defense scheme is designed to serve as a counter measure mechanism for the detection and prevention of malicious software in smartphones. The research work applied random forest algorithm to classify the mobile applications on the smartphone to either safe or malicious. The random forest algorithm is adopted in this research because it has been proven to be very good in solving pattern recognition problems (Rogez et al. [18]). The Classification and Regression Trees (CART) approach of the Random Forest Algorithm is used with the Gini index to calculate the contribution of the features or parameters to aid in the classification of the mobile applications to safe or malicious in order to avoid camera-based attacks. Our proposed system introduces a pre-selection of some of the datasets with indicators to make the indicator set more purposeful and efficient. The dataset is then trained in the random forest network and the contribution of each indicator set is calculated and converted into a weight or a score. The indicators with high score are selected and those with low score are discarded. Let S_i be the indicator set of the random forest:

$$S_i = S_1, S_2, S_3, S_4, S_5, S_6, \ldots, S_n, \quad (1)$$

where i is the i-th indicator of the indicator set and n is the last indicator in the list of indicators.

Table 1: The proposed indicator set of the random forest algorithm.

Indicator (S_i)	Indicator Name
S_1	External Apps communicating with Smartphone
S_2	Non-standard port connection (without either 80 or 443)
S_3	Honeytoken alerts
S_4	Excessive SMTP Traffic
S_5	Malware reinfection after removal
S_6	Multiple user login from different regions

Proposed Threat Indicators Selection Criteria

The selection of the threat indicators is based on the application of the Gini coefficient index since it can handle a combination of binary trees. The Gini coefficient index $G_n(p)$ is defined in equation 2 below:

$$G_n(p) = 2p_n(1 - p_n), \tag{2}$$

where $G_n(p)$ is the Gini coefficient, n is the number of nodes and p_n is the probability that node n has at least one sample. The score of the indicators are identified and sorted and the indicators with the highest score are evaluated and the indicators with the less scores are eliminated due to unimportant threat indicators.

Table 2: Threats labeled dataset for random forest algorithm training.

SMARTPHONES	S_1	S_2	S_3	S_4	S_5	S_6	**Status**	**Label**
Smartphone 1	Yes	Yes	Yes	Yes	Yes	Yes	Attacked	1
Smartphone 2	No	Yes	No	No	No	No	Attacked	1
Smartphone 3	No	No	Yes	No	No	No	Attacked	1
Smartphone 4	No	No	No	Yes	No	No	Attacked	1
Smartphone 5	No	No	No	No	Yes	No	Attacked	1
Smartphone 6	No	No	No	No	No	Yes	Attacked	1
Smartphone 7	No	No	No	No	No	No	Safe	0

Table 2 is the threat labeled dataset that is used to train the random forest algorithm. Label 1 signifies the possibility of the smartphone being attacked and label 0 signifies safety. The research work used Seven (7) suspected smartphones against the threat labeled dataset for the random forest algorithm and the labels recorded and presented in Table 3. As indicated in Figure 2, S_1 (External Apps communicating with smartphones), S_3 (Honeytoken alerts) and S_4 (Excessive SMTP Traffic) are the most common form of attacks adopted in the camera-based attack process on smartphones. S_5 (Malware reinfection after removal) is also another threat indicator that was identified among the smartphones used for this research work.

Table 3: Threat indicators.

SMARTPHONES	S_1	S_2	S_3	S_4	S_5	S_6
Smartphone 1	1	1	0	1	0	0
Smartphone 2	1	0	1	0	0	0
Smartphone 3	0	0	1	1	1	1
Smartphone 4	1	1	1	1	1	1
Smartphone 5	0	0	0	1	1	0
Smartphone 6	1	0	1	1	0	0
Smartphone 7	1	0	1	0	1	0

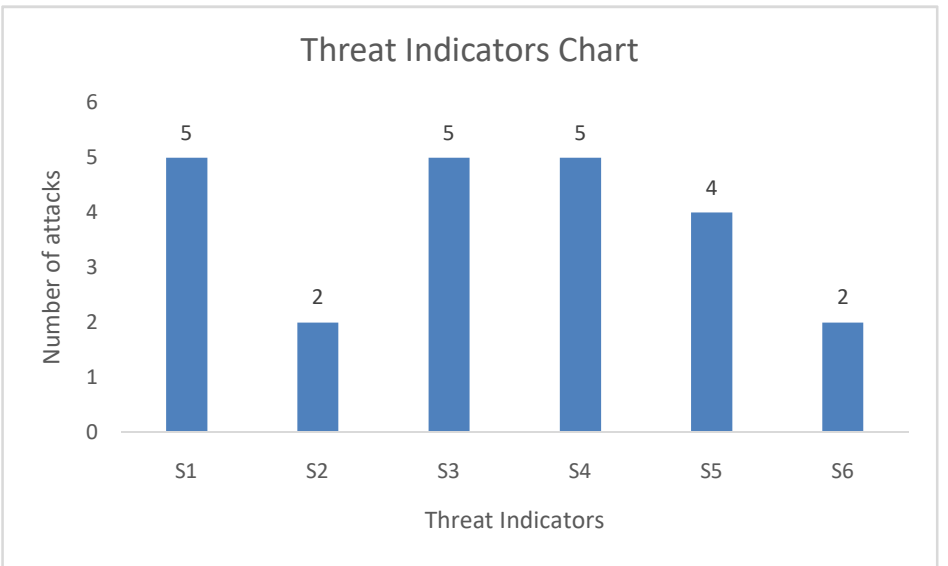

Figure 2: Threat indicators chart.

Proposed Evaluation System

The research work proposed the building of a threat dataset largely centered on camera-based attacks threat models with labels. The random forest algorithm is trained on the threat models dataset in order to calculate the significance of the threat indicators. The highest threat indicators and the threat indicators that meets the threshold is selected

and subjected to the entropy method to determine the weight and total scores of the selected threat indicators. The means of each random variable or threat indicators with multiple test is calculated using equation 3.

$$M(S_j) = \frac{1}{n}\sum_{i=1}^{n} z_{ij}, \tag{3}$$

where $M(S_j)$ is the mean of the random threat indicators, z_{ij} is the values of the combination of the *i*-th and *j*-th threat indicators of the S_j. After calculating the means of each random threat indicator, the Mean Square Deviation (MSD) is determined using equation 4 below:

$$MSD(S_j) = \sqrt{\sum_{i=1}^{n}\left(z_{ij} - M(S_j)\right)^2}. \tag{4}$$

The weight of each threat indicator is calculated and evaluated by applying equation 5.

$$W_j = \frac{M(S_j)}{\sum_{j=1}^{m} M(S_j)}, \tag{5}$$

where W_j is the weight of the various threat indicators, m is the number of the selected threat indicators under consideration.

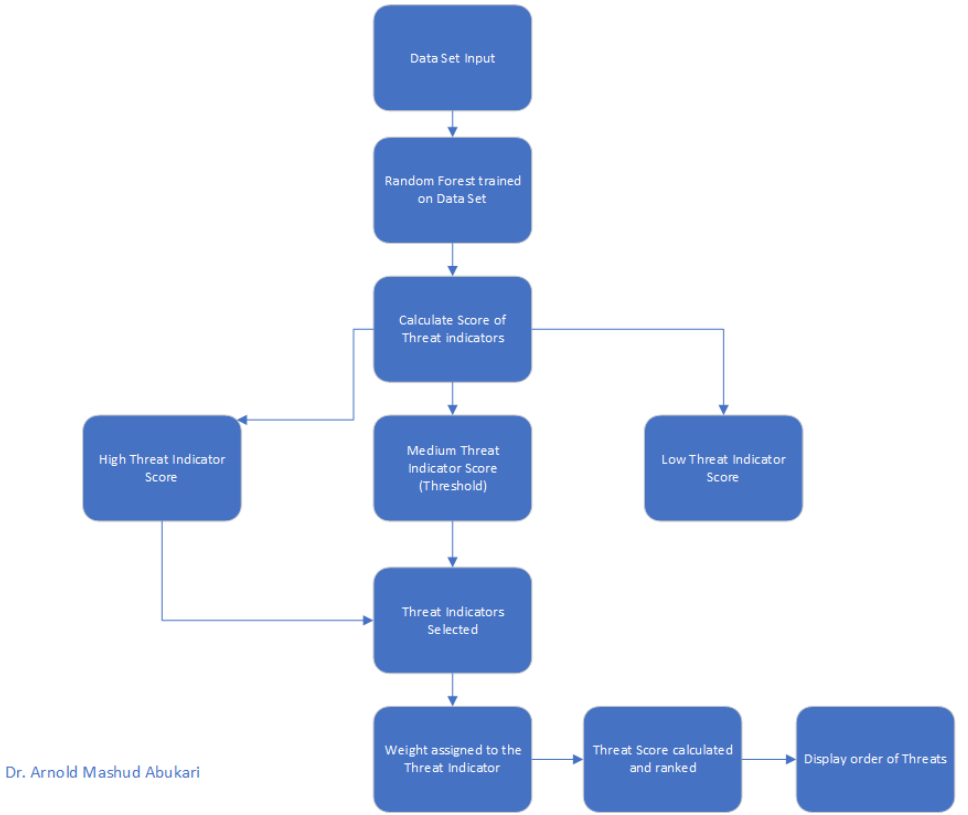

Figure 3: Proposed evaluation system.

Conclusion

As the number of smartphones usage keep growing coupled with security challenges especially camera-based attacks, there have been frantic efforts made by researchers and industry leaders to patch all vulnerabilities. This research has also contributed to the fight in addressing the challenges of security concerns in smartphones. In this paper, a multi-indicator light weight scheme using the random forest algorithm and entropy method is presented. This proposed scheme can be used to classify indicators based on their threats levels. A scenario is also presented for the purposes of this research and the outcome of the research has demonstrated that the proposed multi-indicator scheme presented using random forest and entropy method is consistent with the actual situations. This research work recommends the application of fuzzy logic or any other method to look at how to select the threat indicators in future.

References

[1] Franklin, M. K., Ray, A., & Bhattacharyya, D. K. (2017). Lightweight cryptographic module for secure communication in Android. *International Journal of Network Security*, 19(6), 954-962.

[2] Gao, D., Li, K., & Yao, Y. (2018). Efficient malware detection for Android using deep neural networks. *Future Generation Computer Systems*, 86, 1171-1179.

[3] Statista (2021). Android OS platform version market share worldwide from 2013 to 2021. Retrieved from https://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-google-play/

[4] Weichbrodt, N., Tölle, D., & Lukasiewycz, M. (2018). Lightweight secure bootstrapping of Android devices. *IEEE Transactions on Dependable and Secure Computing*, 15(4), 578-590.

[5] Al-Riyami, S. S., & Paterson, K. G. (2003). Lightweight authentication protocols for securing RFID. *Proceedings of the 8th Australasian Conference on Information Security and Privacy* (*ACISP 2003*) (pp. 149-164). Springer.

[6] Bogdanov, A., Knežević, M., Leander, G., Toz, D., Varici, K., & Verbauwhede, I. (2007). PRESENT: An ultra-lightweight block cipher. In *Lecture notes in computer science: Vol. 4727. Cryptographic hardware and embedded systems - CHES 2007* (pp. 450-466). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74735-2_31

[7] Großschädl, J., & Indesteege, S. (2014). Lightweight cryptography: Cryptographic engineering for a pervasive world. *International Journal of Cryptography and Information Security*, 4(1), 11-24.

[8] Molnar, D., & Wagner, D. (2004). Privacy and security in library RFID: issues, practices, and architectures. *Proceedings of the 11th ACM Conference on Computer and Communications Security* (*CCS '04*) (pp. 210-219). ACM. https://doi.org/10.1145/1030083.1030112

[9] Sarkar, P., Singh, A., & Karmakar, A. (2019). Lightweight symmetric key encryption algorithm based on diffusion and substitution. *Journal of Ambient Intelligence and Humanized Computing*, 10(10), 4151-4164.

[10] Bernstein, D. J. (2005). Salsa20 Specification (Version 1.0). Retrieved from https://cr.yp.to/snuffle/salsa20.html

[11] Bertoni, G., Daemen, J., Peeters, M., & Van Assche, G. (2017). The Gimli permutation. In *International Conference on Cryptographic Hardware and Embedded Systems* (pp. 3-28). Springer.

[12] Guo, J., Peyrin, T., & Poschmann, A. (2011). The PHOTON family of lightweight hash functions. In *International Conference on Selected Areas in Cryptography* (pp. 157-175). Springer.

[13] Deshpande, S. P., Pattalwar, S. V., & Lohiya, P. B. (2017). Light weight defense mechanism against camera based attacks. *IRA-International Journal of Technology & Engineering*, 7, 137-147. https://doi.org/10.21013/jte.icsesd201714

[14] Wu, L., Du, X., & Fu, X. (2014). Security threats to mobile multimedia applications: Camera-based attacks on mobile phones. *IEEE Communications Magazine*, 52, 80-87. https://doi.org/10.1109/mcom.2014.6766089

[15] Nage, G., Jadhav, A. R., Kazi, A. N., & Mundhe, S. (2016). Camera based attacks on mobile phones. *International Journal of Modern Trends in Engineering and Research*, 3.

[16] Ramesh, G., Pooja, B. R., Shilpa, B., Sujatha, B., & Suma, M. (2018). Security threats to mobile multimedia applications: Camera-based attacks on mobile phones. *International Journal of Advance Research and Innovative Ideas in Education*, 4(2), 3015-3020.

[17] Hussain, M., Al-Haiqi, A. M., Zaidan, A. A., Zaidan, B. B., Kiah, M. L., Anuar, N. B., & Abdulnabi, M. (2016). The rise of keyloggers on smartphones: A survey and insight into motion-based tap inference attacks. *Pervasive Mob. Comput.*, 25, 1-25. https://doi.org/10.1016/j.pmcj.2015.12.001

[18] Rogez, G., Rihan, J., Ramalingam, S., Orrite, C., & Torr, P. H. S. (2008). Randomized trees for human pose detection. In *2008 IEEE Conference on Computer Vision and Pattern Recognition* (pp. 1-8). Anchorage, AK, USA. https://doi.org/10.1109/cvpr.2008.4587617

[19] Zhang, K. et al. (2019). Random forest algorithm-based lightweight comprehensive evaluation for wireless user perception. *IEEE Access*, 7, 173477-173484. https://doi.org/10.1109/ACCESS.2019.2956285

[20] Vennam, P., Pramod, T. C., Thippeswamy, B. M., Kim, Y.-G., & Pavan Kumar, B. N. (2021). Attacks and preventive measures on video surveillance systems: A review. *Applied Sciences*, 11(12), 5571. https://doi.org/10.3390/app11125571

[21] Deshpande, S., Pattalwar, S., Lohiya, P. (2017). Light weight defense mechanism against camera based attacks. *Proceedings of the International Conference on Science & Engineering for Sustainable Development (2017)*, 137-147. https://doi.org/10.21013/jte.icsesd201714

[22] Eisenbarth, T., Gong, Z., Güneysu, T., Heyse, S., Indesteege, S., Kerckhof, S., Koeune, F., Nad, T., Plos, T., Regazzoni, F. et al. (2012). Compact implementation and

performance evaluation of block ciphers in ATtiny devices. In *Progress in Cryptology - AFRICACRYPT 2012* (pp. 172-187). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-31410-0_11

[23] Okamura, T. (2017). Lightweight cryptography applicable to various IoT devices. *NEC Technical Journal*, 12(1), 67-71.