SVN: SOFTWARE VULNERABILITY PREDICTION BY NEURAL NETWORK

B Noorul Sajini ,P. Vijaya Sarathy

Abstract—**The vogue and advanced functionality of mobile devices to create them striking targets for malevolent and invasive applications (apps). They need security measures are in the own place for mobile system. The user to make decisions that crash the security of a device, where these system often to fail. Say for example, Android depends on users to identify the permissions that an app is requesting and to base the fitting decisions on the list of permissions. In the proposed model we creating a monitoring neural learning for a software verifications (SVN). This model to tracked, if there any misbehaved application accessed by user it will be blocked it.**

Index Terms—**Android, Mobile device, SVN.**

I. INTRODUCTION

Mainly we can take care of the detection and prevention of mobile system if they vulnerable. In recent days mobile phones are static and does not report for other devices such as tablets, computers. Also they are running similar mobile operating system. Android devices are geographical acquisition for both personal and official uses [1] [2] [3].

The pervasive usage of these mobile gadget create new privacy and security threats. Our entire digital world we want to often stored on the devices. Which contains contact details, emails, messages, passwords, and the accessed files stored locally and in the cloud. If they any possible conditions, the unauthorized user to access the personal information of user. It may be risk, and this is not where the risk end [4] [5].

Every device they won have the sensors, and they are nearly always with devices. The GPS system to identify our own places. It identify exactly where you are, also they recording our audio with use microphone, and camera can to stored the images. Even though mobile phones frequently connected directly to some pecuniary risks. These links are made by messages, phones calls, and data usages. It can be smash the users bills [6-15].

Beginning stage they provide several useful functionalities, but sometimes other plots it may be accessed to collect a particular amount of personal information and even though to some crash the system [16].

II. RELATED WORKS

A. Android System

In present situation we are all to interests on the Android platform. Because of its popularity, how they to access the open sources, and the way of handles and access the sensitive resources. Android apps, we have must to request a particular permission to be access to a given resources. If the user to warns the Android apps if they got permission that an app, then only Android may be installed [17] [18].

An Android is a very risk communication mechanism. It has been limited effectiveness. It is mobile operating system. Android system with a user interface based on direct access. It is designed only for touch screen mobiles devices. Such as smartphones and tablet computers, it will be specially user interface. Android is the most widely used mobile OS [19].

B. Existing Usage

We propose the addition of a summary risk rating for each app. A summary risk rating enables easy risk comparisons among apps that provide similar functionalities. We believe that one reason why current permission information is often ignored by users is that it is presented in a “stand-alone” fashion and in a way that requires a lot of technical knowledge and time to distill useful information, making comparison across apps difficult. An important feature of the mobile app ecosystem is that users often have choices and alternatives when choosing a mobile app. If a user knows that one app is significantly riskier than another but provides the same or similar functionality, then this fact may cause the user to choose the less risky one. This will in turn provide incentives for developers to better follow the least-privilege principle and request only necessary permissions [20] [21].

Peng et al. presented one possible method for generating a principled metric to rank an app’s risk based on the set of permissions it requests. The method can rank the risk of any Android app among all apps available in Google Play, Google’s online market for Android apps. Such a risk ranking can be translated into categorical values such as very low, low, medium, and high risk, to provide a summary risk rating [22] [23].

B. Noorul Sajini*, M.E. CSE , Krishnasamy College of Engineering and Technology, Affiliated to Anna University (Chennai), S. Kumarapuram, Cuddalore, 607109, Tamil Nadu , India.*

P. Vijaya Sarathy*, Assistant Professor, Krishnasamy College of Engineering and Technology, Affiliated to Anna University (Chennai), S. Kumarapuram, Cuddalore, 607109, Tamil Nadu , India.*

C. Implementation of SVN

In the proposed model we initiate the validating neural network. This may learning for software verification. Neural network is an data processing paradigm that is inspired by the way biological nervous information. The key element of this paradigm is the novel structure of the information processing system. Learning in biological system involves adjustments to the synaptic connections that exist between the neurons.

Many important advances have been boosted by the use of inexpensive computer emulations. During this period when funding and professional support was minimal important advances were made by relatively few researchers.

The dummy system is used by the server to learn the behavior of the new applications. The JAVA is used in this system which enhances the wide application of the system.

If they any unauthorized user to crash the system, it will be tracked by server and the blocks the applications if it is vulnerable. It is not restricted to apps and can be applied for any type of software.

III. METHODS

The proposed system to implement this SVN we follow below methods:

A. Server and Client Creation

A simple server that will accept a single client connection and display everything the client says on the screen. If the client to quit the connection the client and the server will both quit. A server as before, but this time it will remain open for additional connection once a client has quit. The server can handle at most one connection at a time. A server as before, but this time it can handle multiple clients simultaneously.

The output from all connected clients will appear on the server's screen. A server as before, but this time it sends all text received from any of the connected clients to all clients. This means that the server has to receive and send, and the client has to send as well as receive. Wrapping the client from client server connection into a very simple GUI interface but not changing the functionality of either server or client. The client is implemented as an Applet, but a Frame would have worked just as well (for a stand-alone program). The network topology will be created for communication.

The client to register their information in server. There are two kinds of registration process initiated by server, such as original database and fake database. The original database to contains exact information of client, the fake database to contains relevant information of original one.

Server will waiting to watch the apps to installed the apps. It will allow the request to give by user for the apps verification. The user will download the app only if they verified by server.

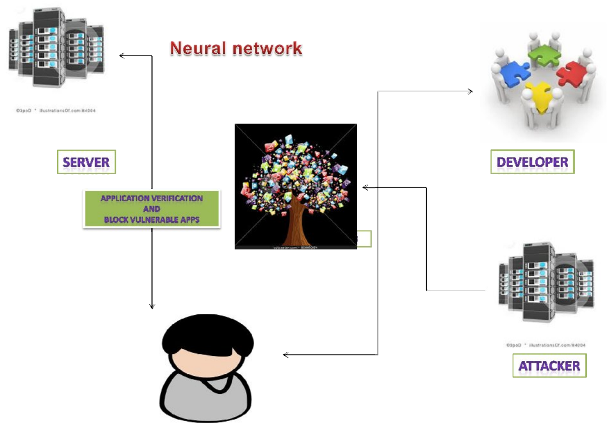

Fig. 1 Neural network implementation.

From the above figure we implement the neural network. Client to request for apps in server using some Google application. The developer to develop the several application for client. The provide our details in server. Application to contains several advantages. It will be used for several personal and official usages. The attacker to hack the user data using malicious applications. Attacker to do some vulnerable applications. If any vulnerable action is occurred the neural network provide fake data about user.

B. Developing and Providing the Apps

Every apps will be developed by some developers. After the developing the apps it will be sold in the internet market. Once the new apps is generated in internet it will be viewed for the user. In internet marketing there are several apps will be generated. It will contain either good apps or some vulnerable apps. They are mixed up in internet. That kind of vulnerable apps are to attack the server all of the sudden or after some particular period of time [24-31].

C. Server Heuristics

The apps which displayed in the online shopping mart will be verified by the user. If any of this apps to selected by user, it will be send the details about the apps and request the server to check for its vulnerability. The sever once got the request then it will start verification by installing that.

After some threshold time it will ask the user to install that if it doesn’t harms. It will check initially the heuristics for vulnerable application [32] [33].

D. SVN Creations

Once the application is verified with heuristics and if it founds to be a new one then it will be under neural learning. This software will be installed in server and it will be in leading for a particular period [34].

So that if any attack is initiated by the apps in later then it can block the application for clients in advance. It will learn the properties of new vulnerable apps for future use.

IV. CONCLUSIONS

Compared to desktop and laptop computers, mobile devices have a different paradigm for installing new applications. For computers, a typical user installs relatively few applications, most of which are from reputable vendors, with niche applications increasingly being replaced by web-based or cloud services. In contrast, for mobile devices, a person often downloads and uses many apps from multiple unknown vendors, with each app providing some limited functionality. Additionally, all of these unknown vendors typically submit their apps to a single or several app stores where many other apps from other vendors may provide similar functionality. This different paradigm requires a different approach to deal with the risks of mobile devices, and offers distinct opportunities [35] [36].

The results from user studies to validated our heuristics that when risk ranking is presented in a user friendly. We expect that adding a summary risk metric would cause positive changes in the app ecosystem. When users prefer lower-risk apps, developers will have incentives to better follow the least-privilege principle and request only necessary permissions. It is also possible that the introduction of this risk score will cause more users to pay for low risk apps. Thus, this creates an incentive for developers to create lower risk apps that do not contain invasive ad networks and in general over-request permissions.

REFERENCES

[1] A.I. Anton, J.B. Earp, Q. He, W. Stufflebeam, D. Bolchini, and C. Jensen, “Financial Privacy Policies and the Need for Stand-ardization,” IEEE Security and Privacy, vol. 2, no. 2, pp. 36-45, Mar./Apr. 2004.

[2] D. Balfanz, G. Durfee, D.K. Smetters, and R.E. Grinter, “In Search of Usable Security: Five Lessons from the Field,” IEEE Security and Privacy, vol. 2, no. 5, pp. 19-24, Sept./Oct. 2004.

[3] R. Biddle, P.C. van Oorschot, A.S. Patrick, J. Sobey, and T. Whalen, “Browser Interfaces and Extended Validation SSL Certificates: An Empirical Study,” Proc. ACM Workshop Cloud Computing Security, pp. 19-30, 2009.

[4] E. Chin, A.P. Felt, V. Sekar, and D. Wagner, “Measuring User Confidence in Smartphone Security and Privacy,” Proc. Eighth Symp. Usable Privacy and Security (SOUPS ’12), pp. 1-16, 2012.

[5] L.F. Cranor, M. Arjula, and P. Guduru, “Use of a P3P User Agent by Early Adopters,” Proc. ACM Workshop Privacy in the Electronic Soc., pp. 1-10, 2002.

[6] L.F. Cranor, P. Guduru, and M. Arjula, “User Interfaces for Pri-vacy Agents,” ACM Trans. Computer-Human Interaction (TOCHI ’06), vol. 13, no. 2, pp. 135-178, 2006.

[7] N. Dell, V. Vaidyanathan, I. Medhi, E. Cutrell, and W. Thies, “Yours is Better!: Participant Response Bias in HCI,” Proc. Conf. Human Factors in Computing Systems, pp. 1321-1330, 2012.

[8] A. Diederich and J.R. Busemeyer, “Judgment and Decision Making,” Experimental Psychology, A.F. Healy and R.W. Proctor, eds., second ed., pp. 295-319, John Wiley & Sons, 2013.

[9] S. Egelman, L.F. Cranor, and A. Chowdhury, “An Analysis of P3P -Enabled Web Sites among Top-20 Search Results,” Proc. Eighth Int’l Conf. Electronic Commerce, pp. 197-207, 2006.

[10] S. Egelman, J. Tsai, L.F. Cranor, and A. Acquisti, “Timing Is Everything?: The Effects of Timing and Placement of Online Pri-vacy Indicators,” Proc. 27th Int’l Conf. Human Factors in Computing Systems, pp. 319-328, 2009.

[11] B. Fathi, Engineering Windows 7: User Account Control, MSDN blog on User Account Control, http://blogs.msdn.com/b/e7/ archive/2008/10/08/user-account-control.aspx, Oct. 2008.

[12] A.P. Felt, K. Greenwood, and D. Wagner, “The Effectiveness of Application Permissions,” Proc. Second USENIX Conf. Web Applica-tion Development (WebApps ’11), 2011.

[13] A.P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wag-ner, “Android Permissions: User Attention, Comprehension, and Behavior,” Proc. Eighth Symp. Usable Privacy and Security, 2012.

[14] M.L. Finucane, A. Alhakami, P. Slovic, and S.M. Johnson, “The Affect Heuristic in Judgments of Risks and Benefits,” J. Behavioral Decision Making, vol. 13, no. 1, pp. 1-17, 2000.

[15] M. Gondan, C. Gotze,€ and M.W. Greenlee, “Redundancy Gains in Simple Responses and Go/no-Go Tasks,” Attention, Perception, & Psychophysics, vol. 72, no. 6, pp. 1692-1709, 2010.

[16] K.A. Juang, S. Ranganayakulu, and J.S. Greenstein, “Using Sys-tem-Generated Mnemonics to Improve the Usability and Security of Password Authentication,” Proc. Human Factors and Ergonomics Soc. Ann. Meeting, vol. 56, no. 1, pp. 506-510, 2012.

[17] D. Kahneman, Thinking, Fast and Slow. Farrar, Straus and Giroux, 2011.

[18] P.G. Kelley, S. Consolvo, L.F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, “A Conundrum of Permissions: Installing Applications on an Android Smartphone,” Proc. Workshop Usable Security (USEC ’12), Feb. 2012.

[19] P.G. Kelley, L.F. Cranor, and N. Sadeh, “Privacy as Part of the App Decision-Making Process,” Proc. Conf. Human Factors in Com-puting Systems (CHI ’13), pp. 3393-3402, 2013.

[20] T. H.-J. Kim, P. Gupta, J. Han, E. Owusu, J. Hong, A. Perrig, and D. Gao, “OTO: Online Trust Oracle for User-Centric Trust Estab-lishment,” Proc. ACM Conf. Computer and Comm. Security, pp. 391-403, 2012.

[22] J. Lin, S. Amini, J.I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang, “Expectation and Purpose: Understanding Users’ Mental Models of Mobile App Privacy Through Crowdsourcing,” Proc. ACM Conf. Ubiquitous Computing (UbiComp ’12), pp. 501-510, 2012. R.D. Luce, Response Times: Their Role in Inferring Elementary Mental Organization. Oxford Univ. Press, 1986.

[23] S. Mishra, M. Gregson, and M.L. Lalumi_ere,

"Framing Effects and Risk-Sensitive Decision Making," British J. Psychology, vol. 103, no. 1, pp. 83-97, Feb. 2012.

[24] S. Motiee, K. Hawkey, and K. Beznosov, "Do Windows Users Fol-low the Principle of Least Privilege?: Investigating User Account Control Practices," Proc. Sixth Symp. Usable Privacy and Security, 2010.

[25] H. Peng, C.S. Gates, B.P. Sarma, N. Li, Y. Qi, R. Potharaju, C. Nita-Rotaru, and I. Molloy, "Using Probabilistic Generative Models for Ranking Risks of Android Apps," Proc. ACM Conf. Computer and Comm. Security, pp. 241-252, 2012.

[26] E.E. Schultz, "Web Security, Privacy, and Usability," Handbook of Human Factors in Web Design, K.-P.L. Vu and R.W. Proctor, eds., pp. 663-677, CRC Press, 2011.

[27] J. Schwarz and M. Morris, "Augmenting Web Pages and Search Results to Support Credibility Assessment," Proc. SIGCHI Conf. Human Factors in Computing Systems, pp. 1245-1254, 2011.

[28] J. Staddon, D. Huffaker, L. Brown, and A. Sedley, "Are Privacy Concerns a Turn-Off?: Engagement and Privacy in Social Networks," Proc. Eighth Symp. Usable Privacy and Security (SOUPS '12), pp. 1-13, 2012.

[29] S. Sternberg, "Inferring Mental Operations from Reaction-Time Data: How We Compare Objects," An Invitation to Cognitive Sci-ence: Methods, Models and Conceptual Results, D. Scarborough and S. Sternberg, eds., pp. 703-863, MIT Press, 1998.

[30] J. Sun, P. Ahluwalia, and K.S. Koong, "The More Secure the Bet-ter? A Study of Information Security Readiness," Industrial Man-agement and Data Systems, vol. 111, no. 4, pp. 570-588, 2011.

[31] A. Tversky and D. Kahneman, "The Framing of Decisions and the Psychology of Choice," Science, vol. 211, no. 4481, pp. 453-458, 1981.

[32] W. Van Wassenhove, K. Dressel, A. Perazzini, and G. Ru, "A Comparative Study of Stakeholder Risk Perception and Risk Com-munication in Europe: A Bovine Spongiform Encephalopathy Case Study," J. Risk Research, vol. 15, no. 6, pp. 565-582, 2012.

[33] K.-P.L. Vu, V. Chambers, B. Creekmur, D. Cho, and R.W. Proctor, "Influence of the Privacy Bird User Agent on User Trust of Differ-ent Web Sites," Computers in industry, vol. 61, no. 4, pp. 311-317, 2010.

[34] K.-P.L. Vu, R.W. Proctor, A. Bhargav-Spantzel, B. Tai, J. Cook, and E.Eugene Schultz, "Improving Password Security and Memorabil-ity to Protect Personal and Organizational Information," Int'l J. Human-Computer Studies, vol. 65, no. 8, pp. 744-757, 2007.

[35] S. Werner and C. Hoover, "Cognitive Approaches to Password Memorability—The Possible Role of Story-Based Passwords," Proc. Human Factors and Ergonomics Society Ann. Meeting, vol. 56, pp. 1243-1247, 2012.

[36] XF. Xie, M. Wang, R. Zhang, J. Li, and QY. Yu, "The Role of Emo-tions in Risk Communication," Risk Analysis, vol. 31, no. 3, 450-465, 2011.

Noorul Sajini B has received her B.E.(CSE) degree in THE YEAR 2013. At present she is pursuing M.E. (CSE) in Krishnasamy College of Engineering and Technology, Cuddalore, Tamil Nadu, India. Her research interests lies in the areas of Artificial Intelligence, Neural Network, Image Processing, Data Mining and Cloud Computing .She attended many workshop over various technologies.

P. Vijaya Sarathy, Completed her B.E. (EEE) degree in the year 2007, M. E(SE) degree in the year 2009. Currently she is working as an Assistant professor in Computer Science and Engineering department at Krishnasamy College of Engineering & Technology, Cuddalore, Tamil Nadu, India. Her research interests lies in the areas of Networking , DBMS, Image processing, Cryptography & Network Security, and Cloud Computing. She has published papers in National/ International conferences. She attended many workshops & National seminars in various technologies and also attended Faculty Development Programme.