Enhancing Mobile Internet user Security with Threat Detection and Multi Authentication System

Navin Kumar Sehgal
Department of Computer Science
Kalindi College, University of Delhi
New Delhi, India

Krishan Kumar
Department of Computer Science
Kalindi College, University of Delhi
New Delhi, India

***Abstract*—As the number of internet enabled mobile devices grow exponentially, a new pattern of user behavior is evolving. In this scenario the access to internet resources moves beyond boundaries of time and cost. The purpose of the paper is to build a system that intelligently detects such flaws in mobile usage. It make user experience more secure by using a multi authentication system Mobile usage patterns may vary across users as well their category of use. There is growing need to detect and prevent associated threats**

Keywords--mobile usage, security threats, detection , prevention

I. INTRODUCTION

Mobile usage is growing at an exponential rate. There are estimated two billion cell phone users in the world .As the number of users increases and internet access becomes easier a usage pattern starts emerging among the users. The usage pattern depends on existing technologies and their applications. It can be broadly categorized into work, social, media, gaming and commerce. A varying amount of time and resources are spent on each of them. Users increasingly spend more and more time on their cell phones. According to a survey cell phone is an invention that has impacted more people than any other.

A threat exists if a user spends more resources than allocated. It reflects in the amount of time spent by them. Another way to measure is the amount data used. As the phones use greater amount of data it adds up to the cost. Mobile companies provide a number of billing options. AT&T has a service to limit the number of calls made by a user. Still the degree of freedom given to the user requires some analysis and evaluation.

Another form of threat arises from user behavior. It relates to actions taken by the user while interacting with mobile phone and its applications. Since humans are responsible for their own decisions, their concern for information security becomesimportant. It can be perceived bythe decisions they make. It is influenced by location, time and other people. IT is important to consider various situations faced by a mobile user. Number situations can cause a threat to the user. It involves giving permissions to applications to access contacts, media and location. Most applications have the share option through which can share the information. The user normally relies on a set of applications used by him a number of times and at different places.

It is possible to detect anomalies in use based on cost and security These can categorized into mobile usage for work, usage for social purposes, usage for media streaming, usage for gaming and usage for commercial transactions. Mobile usage anomaly for work includes spending more time on a particular application or sharing official documents among other users. Social usage involves overspending time and giving permissions to access personal information. Media usage anomaly involves wasting bandwidth on multimedia content or watching in appropriate content. Gaming usage makes a user end spending more time and money. Commercial usage includes using e-commerce sites which are a threat to a user's financial security.

This paper detects such anomalies in mobile usage. It relies on a mechanism to detect the threat in he form of over drafting. The usage types and corresponding threats are categorized.

It also tries to build a prevention mechanism. It uses a number of influencers as authorization agents. Security policies can be formulated involving a user and a number of influencers. It leads to multi criteria decision

II. THEAT DETECTION

A. Detection Method

Detection is important for cost related problems and usersecurity. Instead of using simplistic method of threat detection, we rely on a method that senses the environment and continuously updates the cost and security parameters. It doesn't use a single scenario but a usage pattern

There a number of mobile application which have some mechanisms for reducing threats. Gaming applications have limited number of lives for players which prevents over spending of time on the application. Many applications specifically request for access permissions from the user. Privacy settings in most applications reduce security threat. There is no mechanism however which calculates both overspending limits and user threats simultaneously.

SNO	USAGE CATEGORY	User Behaviour	Priority Cost Wise	Priority Security Wise
1	WORK	Browsing	2	2
		Sharing	3	3
		Giving Permissions	2	4
		Downloading	4	3
2	SOCIAL	Browsing	2	2
		Sharing	3	4
		Giving Permissions	2	4
		Downloading	4	2
3	MEDIA	Browsing	4	2

Table 1. Threat Priorities associated with user actions

B. *Detection System*

We can compare the system to a THERMOSTAT. This device tries to maintain a temperature value in a heating device. Beyond a temperature limit it cuts the access of the device to electrical input. We measure the cost and threat of an ongoing process and update the threat values The threat values are priority values as shown in table 1. It uses control theory which uses a feedback system to control thesystem.

The system is a feedback system that senses the current status of the threat level and upgrades the overall threat value. Initially all values are set to zero. As the user starts using the mobile, the system checks the threat priorities in terms of cost and security. With user performing more actions the values of priorities change. This helps the system to upgrade the overall threat value.

Detection process in turn alerts the mobile user about a cost related or security threat. The first method involves signaling the user of a potential threat. The second prompts the user to input confirmation of threat awareness. The third method stops the current process altogether.

C. *Equations*

If the overall threat is represented by Tv, threat due to cost by Tc and threat due to security Ts. Then-

$$\mathrm{Tv} = \mathrm{Tc} + \mathrm{Ts} \qquad (1)$$

According to Vander Vaals equations for non linear feedback systems-

$$\frac{dTv}{dt} = \frac{dTc}{dt} + \frac{dTs}{dt} \qquad (2)$$

$$\frac{d^2\,Tv}{dt^2} = \frac{d^2\,Tc}{dt} + \frac{d^2\,Ts}{dt} \qquad (3)$$

$$\frac{d^2Tc}{dt} = A(1 - Tc)^2\,\frac{dTc}{dt} - B\,dTc \qquad (4)$$

$$\frac{d^2Ts}{dt} = A(1 - Ts)^2\,\frac{dTs}{dt} - B\,dTs \qquad (5)$$

III. THREAT PREVENTION

Prevention involves multi authentication system. It is a similar to a lock with multiple keys. The keys time, location, application, people and passwords. Mobile usage is largely

A. *Prevention Method*

The prevention system therefore checks locations to be home, workplace, travelling. It then checks time to be early morning, afternoon, evening or night. It can check people around to be friends, colleagues and family. Finally it checks user permissions, application to be used and action to be performed. It then provides the status to the user about the feasibility of his actions..

B. *Diagrmmatic Representation*

The Prevention system can be represented with the help of a diagram as shown in fig 1 .

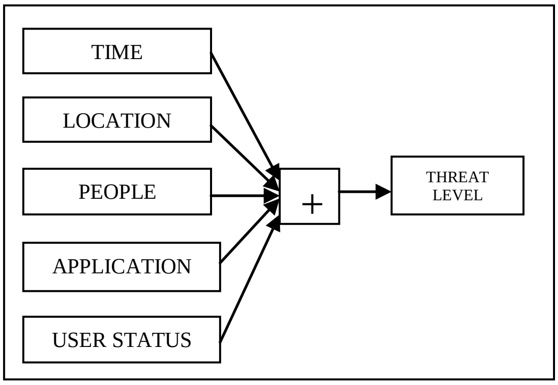

Fig 1. Calculating threat levels from influencing factors

Iteration	d^2Tv/dt	d^2Tc	dTc	Pc	d^2Ts	dTs	Ps	Usage
0	5	0	0	0	0	0	0	Initializing
1	3.56	-0.072	0.2	0.2	-0.07	0.2	0.2	Browsing gmail
2	3.56	-0.051	0.1	0.3	0.051	-0.1	0.3	Chatting
3	3.56	0.036	-0.1	0.2	-0.04	0.1	0.2	Browsing Facebook
4	2.28	0	0	0.2	-0.13	0.2	0.4	Facebook Permissions
5	1.72	-0.128	0.2	0.4	0.072	-0.2	0.2	Watching News
6	1.21	0	0	0.4	-0.05	0.1	0.3	Downloading Movie
7	1.72	0.051	-0.1	0.3	0	0	0.3	Chatting
8	1.72	0	0	0.3	0	0	0.3	Sharing documents
9	1.08	0	0	0.3	-0.06	0.1	0.4	Uploading a picture
10	1.44	0.036	-0.1	0.2	0	0	0.4	Buying a book
11	2.16	0	0	0.2	0.072	-0.2	0.2	Browsing Facebook

Table 2. A simulating experimenting showing change in values for user actions

IV. SIMULATION EXPERIMENT

The Based on the above method we carry out a simulation experiment. We start with initial values for Pc and Ps to be zero.

As shown in table 2 next step involves recording the action performed by the user. Its priority in terms of cost and security are updated. The change in the priority values are reflected in the table. The total change in the priority values is updated. If the overall threat value reaches a minimum value the user is warned with a signal or a message. In extreme conditions the internet connection may be terminated.

The experiment also updates the positive actions taken by the user like moving from a high threat action to a low threat action.

V. BENEFITS

- The user is informed of any threat instantly.
- The user can control the total cost. The system can be upgraded to take drastic actions like stopping internet services altogether
- Before stating an internet session a user can confirm that it is safe to browse the internet.
- It can be used in desktop applications as well to check the safety of browsing.
- It can be included in firewalls and anti viruses to asses the safety of the user.
- E-commerce applications can use the system to warn the user that he has exceeded his spending limit or he is under threat from hackersIt can inform about internet browsing at a particular location like a market or a mall
- It helps in measuring the actions performed by the user at a social networking site.
- Media applications can inform the user that he is using a higher bandwidth.
- It can be used in a workplace to check the efficiency of the employees.

VI. CONCLUSION AND FUTURE WORK

The system is helpful in assessing safety. It can be modified in a number of ways to find the cost and safety patterns in mobile internet usage

The future work involves creating software to efficiently use the system. The detection mechanism can be made more robust by finding user actions that more harmful than others and include it in the system. A number of factors can be added to prevention measures.

REFERENCES

[1] Kivi, Antero. "Measuring mobile user behavior and service usage: methods, measurement points, and future outlook." Proceedings of the 6th Global Mobility Roundtable (2007): 1-2.

[2] Hong, SeJoon, James YL Thong, and Kar Yan Tam. "Understanding continued information technology usage behavior: A comparison of three models in the context of mobile internet." Decision Support Systems 42.3 (2006): 1819-1834.

[3] Morisset, C., et al. Formalization of influencing in information security. Technical Report CS-TR-1423, Newcastle University (May 2014), 2014..

[4] Srikala, D., and Siva Reddy. "Detecting, Determining and Localizing Multiple Spoofing Attackers in Wireless Networks."

[5] Ghosh, Anup K., and Tara M. Swaminatha. "Software security and privacy risks in mobile e-commerce." Communications of the ACM 44.2 (2001): 51-57.

[6] Buchanan, George, et al. "Improving mobile internet usability." Proceedings of the 10th international conference on World Wide Web. ACM, 2001..

[7] Ngai, Eric WT, and Angappa Gunasekaran. "A review for mobile commerce research and applications." Decision Support Systems 43.1 (2007): 3-15.

[8] Turunen, Matti. "Mobile internet access." U.S. Patent No. 6,477,644. 5 Nov. 2002..