COMPUTERS & SECURITY 78 (2018) 336–346

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

The Kano model analysis of features for mobile security applications

*Mei-Ling Yao**, *Ming-Chuen Chuang*, *Chun-Cheng Hsu*

Institute of Applied Arts, NCTU, Hsinchu, Taiwan

ARTICLE INFO

Article history:
Received 8 April 2018
Revised 21 May 2018
Accepted 17 July 2018
Available online 29 July 2018

Keywords:
Mobile security
Mobile security application
Kano model
Mobile security risk
Antivirus

ABSTRACT

The Google Play app store is providing more than 200 mobile security applications (MSAs) with abundant features. This study consolidates and extracts 12 main mobile security and antivirus features out of the top 25 MSA vendors to find out how users evaluate and classify quality attributes for these features with the Kano Model two-dimensional questionnaire. The analysis result shows that all features could be classified as either one-dimensional or indifferent quality. These 12 features could be further grouped into 5 quality types (O, OA, OI, IO and I) based on SI and DSI values assigned to each feature for its impact on customer satisfaction. Overall, the top four features with greater impact on customer satisfaction are "malware prevention", "safe browsing", "parental control" and "privacy protection". The MSA vendors should emphasize these 4 features. The "secure app advisor" and "app lock" may enjoy less attention as they bear little impact on customer satisfaction. The "data backup", "garbage file cleanup", "Wi-Fi security", "message and call filter", "remote wipe" and "remote lock and locate" have the higher impact on increasing customer satisfaction than reducing dissatisfaction. For MSA vendors with above average quality, they have to put more design efforts on these features to gain more customer satisfaction. Female users pay more attention to "remote lock and locate" and "Wi-Fi security" while users with little technological knowledge focus on "garbage file cleanup", "remote lock and locate" and "secure app advisor".

1. Introduction

The global smartphone markets delivered 380 million units in Q1 2017, 9.1% up over the same period last year. Average unit price of the smartphone is up as users tend to buy smartphones with more advanced features according to the survey by Gartner in 2017. The Android OS now accounts for 86.1% of the market share, iOS 13.7%, and the remaining 0.2% goes to others. The first two OSs are dominating the smartphone OS markets. This growth comes from global acceptance of Android smartphones made by China as share up by 2% from Q1 2016 to Q1 2017. Still stronger growths are expected after Google announced that it is planning to launch the low end smartphone OS, Android Go (Gartner, 2017). Global smartphone users may reach 2.5 billion in 2019 up from 2.1 billion in 2016. That is, up to 40% of the world's population will be using smartphones by then. With its huge population base, China is playing a key role in growing the smartphone markets. With 563 million smartphone users in 2016, it is expected to grow to 675 million in 2019. Almost a half of the Chinese population will be using smartphones by 2020. This is the same case with the United States where there will be 247.5 million

* Corresponding author.
E-mail addresses: ammy_yao@trend.com.tw (M.-L. Yao), cming@faculty.nctu.edu.tw (M.-C. Chuang), chuncheng@mail.nctu.edu.tw (C.-C. Hsu).

https://doi.org/10.1016/j.cose.2018.07.008
0167-4048/

smartphone users by 2019 from 233 million in 2017 (eMarketer, 2016).

Huge amount of smartphones and diversified apps are bringing us unprecedented convenience and great user experiences. Mobile applications including messaging, social networking, web surfing and shopping, video streaming, and mobile payment, are dominating our daily life while exposing much of our privacy in the form of photos, videos, contacts, location, credit card numbers, bank accounts, ID, name, address, birthday, health records and certificates among others. Conveniences blessed by smartphones are great, yet the risks of mobile security, privacy concern and data loss mandate more attention. Hackers do not overlook the vulnerability of apps as they quickly apply PC-aimed viruses and malwares to smartphones to steal personal data or defraud victims. There are around 3,520,690 Android apps now available on the Google Play with 13% of them of lower quality and higher security concerns. The number of Android apps soared 25% from 2,664,044 to 3,329,754 in the first 10 months of 2017. Yet the number of low quality ones soared 46% from 273,404 to 398,496 in the same period. That is, low quality apps are fast outgrowing normal ones (AppBrain, 2018). A survey by Cambridge University in 2015 showed that 87% of Android smartphones are suffering at least one vulnerability easily exploited by hackers. Zimperium Labs found 95% of Android devices have been invaded by hackers by SMS (short message service) at least once (Kaspersky Lab, 2015). Malware attacks against smartphones tripled to 8.5 million cases in 2016 from a year earlier with ransomware and IoT viruses accounting for the lion's share (TechRepublic, 2017). Most users are unaware of the existence of malwares or suspicious applications on the Android App store let alone knowing about the damages they can inflict by abusing the stolen personal information (Kelley et al., 2012). Mobile security is now a topic which we should do our best to know its impact and find ways to protect us against mobile security risk.

App developers can easily access personal data saved in or obtain permission for smartphone with applications that they have developed by including contacts, call logs, browsing history, personal photos and videos, financial information, personal message, GPS location, camera or microphone access. It's also easy to track or monitor personal mobility, communication and surroundings by their smartphone. App developers frequently acquire more privileges than they actually need while users cannot fully understand the risks associated with granting these permissions (Jorgensen et al., 2015). In addition, most App developers are not security experts and seldom notice potential security risks buried in the software development process. A survey by Trend Micro in 2015 and data available in its Smart Protection Network warned that some Chinese iOS app developers code their programs with tampered Xcode development tools from non-Apple official websites. They have no idea that Apps developed by them are infected by malicious codes embedded in their development tools. These malicious codes containing Apps may lead to attacks in the form of fraud, phishing, and data theft. Apple Apps have long been deemed to be relatively safer by its strict app review process. This has not been the case since attacks against Apple Xcode development tools have been revealed. It's clear now that hackers are not leaving Apple iOS free from their attacks and more threats by them can be expected with more ways to detour the Apple App review mechanism (Trend Micro 2015).

In spite of 200 mobile security apps (MSA) available on Google Play, some are provided in the premium model, none seems successful in attracting users' interest and attention as very few of them enjoy relatively higher downloads. Smartphone users seem failing to apply their PC (personal computer) antivirus experience to smartphones. The reasons include overlooking mobile security risks fooled by poor knowledge about them, failing to learn about protection provided by MSA, fearing costs of device performance paid by mobile security applications, being confused by so many unnecessary MSA features, and poor MSA user interface designs which do not meet their requirements. MSAs tend to come with many features beyond antivirus or mobile security protection and result in distractions and operating clumsiness and interferences. Designers are required to learn about user requirements for MSA and identify features of better use before they can improve customer satisfaction with MSAs. This study is aimed to identify Kano model quality attribute on major MSA features and difference over MSA feature among different user groups with Kano model two-dimensional questionnaire survey to help designers in the feature elicitation.

2. Literature review

Mobile security research covers many different topics, including malware detection technology, privacy and permission, and mobile security risk awareness. Many users just ignore the list of permission during installation process, only 17% of Android smartphone users are consciously aware of the specific permissions and app demands during installation, and more than 75% of them have no idea about mobile security risks inflicted due to permission granted (Felt et al., 2012). Most users ignore the permission grant screen and tend to select Apps based on easy to understand, e.g. App ranking, user appraisal and word of mouth, due to poor knowledge about impact of permission granting (Kelley et al., 2012). Due to usability issue in Android default permission UI design, users are not aware of the risks of privacy exposure due to their granting the installed Apps to access their photos, GPS location and camera. In spite of studies by scholars on privacy issues caused by Android OS and also proposed many detection mechanisms to prevent permission over granting issues, hackers may still develop malwares to steal personal data without being blocked by these mechanisms (Trend Micro, 2009). It remains crucial to install legitimate MSAs against malware attacks. Differing from mobile privacy and permission studies, technical researches on malwares are concentrated on creating innovative detection mechanism against them. The TaintDroid system detects key data saved in smartphones being transmitted by untrusted applications and alerts users on the fly (Enck et al., 2010). Gilbert et al. (2011) designed a mechanism (AppInspector) against smartphone application information security verification to identify possible security risk. It provides users with reports covering potential security and privacy threats

Table 1 – Summary of mobile security application features of 25 brands (by the author).

MSA brand / feature	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
AhnLab V3 Mobile Security	V	V			V		V		V								
Alibaba mobile security	V	V	V	V		V	V		V	V							
Antiy AVL	V	V						V						V			
Avast Mobile Security	V	V	V	V	V		V	V	V								
Bitdefender Mobile Security	V	V	V	V	V		V		V								
Cheetah Mobile Security Master	V	V	V	V	V	V	V	V	V	V							
ESET Mobile Security Master	V	V	V	V		V				V							
F-Secure Safe	V	V	V	V	V	V					V			V			
G Data Internet Security	V	V	V	V	V	V	V				V					V	
Google Play Protect	V	V	V	V													
Ikarus mobile security	V	V	V	V	V	V					V						
Kaspersky Lab Internet Security	V	V	V	V	V	V	V				V			V		V	
McAfee Mobile Security	V	V	V	V	V	V	V	V	V	V		V			V		
Norton Mobile Security	V	V	V	V	V	V						V	V				
NSHC Droid-X	V																V
PSafe DFNDR	V	V	V	V			V	V	V	V							
360 Mobile Security	V	V	V	V		V	V		V	V							
Quick Heal Mobile Security	V	V	V	V	V	V		V			V	V	V				
Sophos Mobile Security	V	V	V	V	V	V	V	V		V	V		V				
Tencent WeSecure	V	V										V					
Trend Micro Mobile Security	V	V	V	V	V	V	V	V			V						
Webroot	V	V	V	V	V	V											
AVG free	V	V	V	V		V	V		V	V		V			V		
Avira	V	V	V	V	V		V										
Lookout	V	V	V	V	V			V				V					V
Total	25	24	21	21	16	15	14	9	9	8	7	6	3	3	2	2	2

to make users learning about information security risks came with their smartphone. The MAETROID framework by Dini et al. is aimed to determine whether an app is safe or risky to be installed by evaluating its trustworthiness. The assessment criteria cover permission requested and data provided by app stores including app quality and popularity of the individual App (Dini et al., 2016). These studies are focused at detecting, judging and blocking malwares rather than user requirements and expectations in terms of cognition, behavior, interface design and user experience on mobile antivirus and attacks by malware. 96% of smartphones do not have pre-installed mobile security application. This lack in security is an opportunity for malicious cyber attackers to hack into the various devices that are popular. Compared to PCs, smartphones are even more vulnerable than personal computers because more people are using smartphones to do personal tasks including sending and receiving mails, social networking, downloading various apps, monetary transactions such as buying goods, redeeming coupons and tickets. Monetary transactions are especially attractive to cyber attackers because they can gain access to bank account information after hacking a user's smartphone (Wright and Dawson, 2012). Trend Micro surveyed 1000 mobile phone and iPhone users 18 years older in 2009 and found that only 23% of them had smartphone antivirus software installed while 20% of those without antivirus software installed deem these apps are useless. Nonetheless, most of them are aware of the security threats from smartphones and 50% of those respondents have been attacked by malware, 45% of them received spams on their smartphone; 50% opened attachments of emails received; 39% clicked URL links contained in email (Trend Micro, 2009). All these are mechanisms often employed by malware in invading mobile devices. Installing a legitimate MSA is the best solution to prevent malware from mobile devices of most users. Their research result confirmed that MSAs are capable of blocking most malwares aimed at mobile devices (Fan et al., 2014).

Android Google Play with keyword "mobile security" may end up with more than 200 mobile security applications telling the importance and market competition in this area. AV-TEST, (a global IT-security research institute focused on information technology security and virus research) unveils regular rankings of computer and mobile antivirus software providers on its website. Based on the top 21 mobile security applications ranked in November 2017

AV-TEST, 2017) and another top 4 mobile security applications in the market (Webroot, AVG free, Avira, Lookout), this study counted the frequency of each security feature been included in the 25 mobile security applications. There are 17 security features been included at least by 2 mobile security applications, as shown in Table 1, which are regarded as important security features for further investigation in this study.

1) Malware prevention (25/25, all of these 25 MSAs come with this feature): which an auto scanning for viruses and malware during app downloads to identify infection by Trojan. 2) Safe browsing (24/25): Block malicious links, fraud links and phishing websites to prevent linking to malicious website or clicking on fraudulent URLs contained in SMS, Line or Facebook posts which imposes a threat of loss of privacy on credit card. 3) Remote wipe (21/25): Erase data contained in lost smartphone remotely to prevent them from being viewed, stolen, or deleted. 4) Remote lock and locate (21/25): Lock lost smartphone remotely with web page interface or identify its current position to locate where it was lost. 5) Privacy protec-

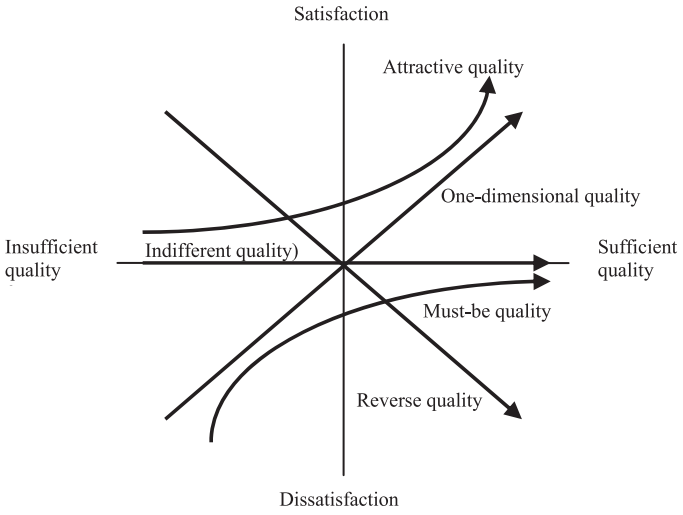

Fig. 1 – Kano model of customer satisfaction (Kano, 1984).

tion (16/25): Detect applications suspected of stealing mobile phone data and displays these programs in scanning results page or alerts users when downloading or installing Apps to relieve users from worrying about personal data leakage, unintended exposure of photos or chat sessions or even financial losses. 6) Call and message filter (15/25): Block specific or unknown messages and incoming calls to avoid fraud or harassing messages or phone calls. 7) Data backup (14/25): Back up personal data in SD card or cloud storage space. 8) Secure app advisor (9/25): Recommend secure applications to users for mobile App installation with confidence. 9) App lock (9/25): Lock desired applications with PINs to maintain security and privacy of sensitive data. 10) Wi-Fi security (8/25): Provide encryption and protection over public wireless network connections to avoid data exposure over unsecured public WiFi connections. 11) Parental control (7/25): Control or monitor children's activities on the Internet through permission, regulates children's use of the Internet or prohibits them from browsing certain types of websites. 12) Garbage file cleanup (6/25): Erase cache files in the system to find and remove unused files in disk space to free up space for smooth system operations. 13) Battery optimizer (3/25): Shutdown unnecessary features to save battery charges. 14) Secure payment (3/25): Ensure payment system security before making online payments. 15) Network data monitor (2/25): Set smartphone network traffic and tariffs to avoid over quota. 16) Encryption (2/25): Encrypt smartphone or its network communication data. 17) Rooting detection (2/25): Identify whether the user cracked the Android OS and gained permissions beyond user roles as this may help hackers in easing up invading the device with malware.

The Kano model was an important theoretical model proposed by Japanese quality management guru Noriaki Kano in 1984 aimed to illustrate and identify quality attributes for the research targets. The customer satisfaction over specific quality of a product or service may vary with his/her preference over the quality attribute as shown in Fig. 1: here the X-axis represents the level of each quality performance and the Y-axis is the customer satisfaction level. There can be 5 attributes of quality as described below (Kano, 1984):

(1) One-dimensional quality (O): Customer is satisfied when this quality element is sufficient and vice versa. Customer satisfaction level in liner relation with quality attribute adequacy. That is, the typical quality.
(2) Attractive quality (A): sufficiency of this quality attribute will boost customer satisfaction yet a lack of it does not lead to dissatisfaction and the product remains acceptable to customers.
(3) Must-be quality (M): customers tend to take this quality attribute for granted. That is, improve it makes no difference and worsen it leads to dissatisfaction.
(4) Indifferent quality (I): this quality, whether sufficient or not, does not affect customer satisfaction. That is, product or service quality and customer satisfaction are irrelevant to each other.
(5) Reverse quality (R): customer satisfaction has nothing to do with this type of quality.

Define Kano quality attributes based on the results of a Kano model "two-dimensional questionnaire" (Table 2) composed of pairs of opposite questions in the format of: how is customer satisfied when quality is adequate and when it is not? Answers to either of the two are limited to "Like," "Neutral" and "Dislike".

The quality attribute conceived by participants can be determined by pairing these two answers and matching them with their feeling over quality "sufficiency" and "insufficiency" in Table 3 (Kano, 1984). The final result for quality attribute can be defined by different group of participants depends on the user groups you want to compare.

Kano model provides a framework which could enable the elicitation of product requirements. It helps increase customer satisfaction if the elicited requirements are met. Requirements, met or unmet, can influence customers' satisfaction or dissatisfaction for a product or service, because from

Table 2 – Example of Kano two-dimensional questionnaire for privacy scanner.

Please give your satisfaction level when mobile security and antivirus software comes with "privacy scanner" feature?		
☐ Dislike	☐ Neutral	■ Like
Please give your satisfaction level for mobile security and antivirus software comes without "privacy scanner" feature:		
☐ Dislike	■ Neutral	☐ Like

Table 3 – Quality attribute evaluation table (3 x 3).

Product requirements		Quality insufficiency		
		Like	Neutral	Dislike
Quality sufficiency	Like	–	A	O
	Neutral	R	I	M
	Dislike	R	R	–

customer point of view, products with the right functionality satisfying them implies that such product are with good quality. The Kano model has been applied in the elicitation of requirements for a proposed e-Ebola awareness System. The result of the Kano analysis indicated that eliciting customer satisfying requirements increase the satisfaction level of potential customers of the proposed product. It also improves the perceived quality of such product in the eyes of the potential customers as evidenced from their satisfaction scores and self-stated importance rating (Hussain and Mkpojiogu, 2016). Customer satisfaction is proportionally related to the perceived requirements importance, it is then necessary to give adequate attention to customer satisfying requirements from elicitation to design and the final implementation (Mkpojiogu and Hashim, 2016). Kano model not only could be used for requirement clarification in the early stage, but also for different stages in the service delivery lifecycle. Kano survey helps to add value by focusing efforts in service design, development and verification stages to encompass features on use case level, supported by early prototypes and conducted with real customers (Lubinski and Oppitz, 2012). By applying Kano model on mobile payment customer requirement classification, Krisztina and Isabel (2017) indicated that customer requirements for mobile payment have transformed and new requirements appeared in comparison to former research conducted on payment method in general. Some requirements like security, fake-proof nature, reputation and reliability of the method has transformed and become more important. Incorporating customer satisfying requirements elicited by Kano survey in products design is of great worth to the potential users or customers of the product.

3. Method

This study is designed to identify Kano quality attribute for the 17 important security features which were built in the mobile security applications developed by 25 main MSA vendors. The participants were required to answer the "two-dimensional questionnaire" of the Kano model. It will help to understand users' preference and also figure out the differences over Kano quality attributes for each MSA feature among different user groups.

3.1. *MSA feature selection*

Figures shown in Table 1 suggest 5 out of the 17 MSA features, including "battery optimizer", "secure payment", "network data monitoring", "encryption" and "rooting detection", are provided by only 2–3 MSA brands. This is a clear indicator that these 5 MSA features are the less important features of the MSA. This study is designed to identify quality attributes over the remaining 12 MSA features including: "malware prevention", "safe browsing", "remote wipe", "remote lock and locate", "privacy protection", "message and call filter", "data backup", "secure app advisor", "app Lock", "Wi-Fi security", "parental control" and "garbage file cleanup" .

3.2. *Questionnaire design*

The questionnaire is composed of two sections: the first one is aimed at profiling the participant in terms of gender, age, education, family size, number of computer possessed, and familiarity with technology in 5-level Likert scale from very familiar to very unfamiliar. The second one is a Kano quality two-dimensional questionnaire addressing the 12 key MSA features mentioned earlier. The questionnaire was then released online as a Google form for the participants' easy review and reply.

3.3. *Participant sampling and questionnaire implementation*

There are fewer users practicing or knowing about MSA when compared with computer antivirus software. Netizens are more likely to use computer antivirus software and be familiar with MSA relevant information. This study publishes a questionnaire link on social networking websites targeted at netizens in Taiwan. The questionnaire was available on the Internet for anyone who' d like to take the survey for 3 days. Questionnaire availed through social networking websites may cover a wider range of users and get inputs from users with varying degrees of technology familiarity.

3.4. *Data analysis*

Quality attribute of each feature by individual participant are determined by applying the "Kano quality attribute evaluation table" (Table 3) to their scores in the aforementioned questionnaire. Quality attributes are set by "mode" of all participants

Table 4 – Difference between male and female participants over familiarity with technology.

	Very familiar	Familiar	Neutral	Unfamiliar	Very unfamiliar	Total
Male	18(26%)	23(34%)	24(35%)	2(3%)	1(2%)	68
Female	4(9%)	15(33%)	24(54%)	0(0%)	2(4%)	45
Total	22(19%)	38(34%)	48(42%)	2(2%)	3(3%)	113

over individual feature quality attribute. That is, the quality attribute perceived by most participants are the one of the group. To identify whether or not the different groups differ in their preference over MSA feature quality attributes, the participants are divided into sub-groups by gender and technology familiarity level to analyze and explore any differences and causes to the latter.

4. Research results

4.1. *Demographic characteristics*

A total of 113 valid questionnaires were collected in this survey, with 45 from female participants and 68 from the male ones. With 84.1% of them aged between 30% and 50%; 78% had at least a college degree; 80% of them from a family size 1–4 people, they seem to represent the demographic profile of netizens in Taiwan. 63.7% of them have 1–2 computers in their home while 31.3% have 3–5 ones. Figures in Table 4 suggest 53% of the total participants are familiar or very familiar with computers and smartphone technology information. Among those very familiar with technology, the male ones (26%) outnumber the female ones (9%) constituting a big gap. More than half of the female participants show only average familiarity with technology.

Regarding technology familiarity calculated by converting the Likert scale replies into scores 1–5: overall average of technology familiarity is 3.65 with a standard deviation at 0.896; 3.79 and 0.90 for male and 3.42 and 0.839 for female participants, respectively; with a difference of 0.05 in terms of the *t*-test, it's clear that male participants are more familiar with technology than their female peers.

4.2. *Preliminary quality attributes classification on MSA features*

Quality attributes of individual participants are determined by their replies to the two-dimensional questionnaire subject to rules set in Table 3. Count and ratio of evaluation result by individual participants over quality attributes of each feature are then tallied. The quality attribute of the highest ratio is set the attribute perceived by the entire group as shown in Table 5. Take "malware prevention" for example. There are 65 out of 113 participants (62.5%) who perceive it as a one-dimensional quality which is of the highest ratio among all quality attributes. This leads to set it with quality attributes of one-dimensional (O) as shown in the Major Kano Model column. Table 5 suggests every MSA feature is of quality attributes one-dimensional (O) or indifferent (I). There are 8 MSA features bearing one-dimensional quality attributes. They are, in descending sequence of quality attribute performance ratio: malware prevention (63.5%), safe browsing (61.32%), parental control (50%), privacy protection (49.53%), data backup, garbage file cleanup (43.81%), Wi-Fi security (42.06%), message and call filter (40.95%). The four indifferent quality attributes are, in descending sequence of ratio: app lock (57.28%), secure app advisor (41.82%), remote lock and locate (39.05%), remote wipe (38.32%). Despite being utility app, most users are less likely to be familiar with MSA features and relevant knowledge compared to social networking or other apps essential in daily life. MSA features with indifferent quality attribute are deemed unable to improve user satisfaction even with increasing quality fulfillment. Therefore they bear less importance in MSA design. The "app lock" is recognized with indifferent quality attribute of the highest percentage. Users have virtually no need for it as smartphones always come with an internal key lock or other locking mechanism and so have no requirements for extra program based.

This study divided participants by factors of "familiarity with technology" and "gender" to further identify different user groups' difference in MSA feature quality attribute clarification. The "high technology familiarity (HTF)" group contained those who were very familiar or familiar with technology with the remaining participants in the "low technology familiarity (LTF)" group. It's quite straightforward that the gender groups are male and female ones. Regarding the "garbage file cleanup" function of MSAs: its quality attribute by the entire and LTF groups was type "O" while the HTF group had an equal share of type "O" and "I" . Regarding "remote lock and locate" and "secure app advisor" of MSAs: their quality attribute by the entire and HTF groups was type "I" while the LTF group had type "O". These three features are of greater necessity to the LTF group than to the HTF group. Regarding gender differences for the "Wi-Fi security" of MSAs: Quality attribute by the female group was type "A" while the whole and male group had type "O". Regarding the "remote lock and locate" of MSAs: Quality attribute by the female group was type "O" while the whole and male group had type "I". This tells us that females are more concerned with "Wi-Fi security", that is, better quality on this may improve the MSA satisfaction of female users. Female users impose more necessity over "remote lock and locate".

4.3. *Further quality attributes classification on MSA features*

As shown in Table 5, no MSA features are clarified as attractive quality from evaluation result. However, there are still some users who set certain features of MSAs as attractive quality. This is the case with one-dimensional quality as well. Some features are of high ratio for indifferent quality; this is also the

Table 5 – Results of Kano quality attributes survey of mobile security application features.

Item	Kano model distribution					Kano model distribution (%)					CS coefficient			
	M	O	A	I	R	M	O	A	I	R	Major Kano model	Extent of satisfaction (SI)	Extent of dissatisfaction (DSI)	Secondary Kano model
1. Malware prevention	5	65	15	18	1	4.81%	62.50%	14.42%	17.31%	0.96%	O	0.77670	−0.67961	O
2. Safe browsing	3	65	13	25	0	2.83%	61.32%	12.26%	23.58%	0.00%	O	0.73585	−0.64151	O
3. Parental control	6	54	34	14	0	5.56%	50.00%	31.48%	12.96%	0.00%	O	0.81481	−0.55556	OA(A/O = 0.63)
4. Privacy protection	2	53	18	31	3	1.87%	49.53%	16.82%	28.97%	2.80%	O	0.68269	−0.52885	OI(I/O = 0.58)
5. Data backup	1	48	17	33	8	0.93%	44.86%	15.89%	30.84%	7.48%	O	0.65657	−0.49495	OI(I/O = 0.69)
6. Garbage file cleanup	2	46	23	34	0	1.90%	43.81%	21.90%	32.38%	0.00%	O	0.65714	−0.45714	OI(I/O = 0.74)
7. Wi-Fi safety	1	45	32	29	0	0.93%	42.06%	29.91%	27.10%	0.00%	O	0.71963	−0.42991	OA(A/O = 0.71)
8. Message and call filter	3	43	30	27	2	2.86%	40.95%	28.57%	25.71%	1.90%	O	0.70874	−0.44660	OA(A/O = 0.70)
9. Remote wipe	1	30	28	41	7	0.93%	28.04%	26.17%	38.32%	6.54%	I	0.58000	−0.31000	IO(O/I = 0.73)
10. Remote lock and locate	2	40	20	41	2	1.90%	38.10%	19.05%	39.05%	1.90%	I	0.58252	−0.40777	IO(I/O = 0.98)
11. Secure app advisor	9	28	18	46	9	8.18%	25.45%	16.36%	41.82%	8.18%	I	0.45545	−0.36634	IO(I/O = 0.61)
12. App lock	3	18	20	59	3	2.91%	17.48%	19.42%	57.28%	2.91%	I	0.38000	−0.21000	I

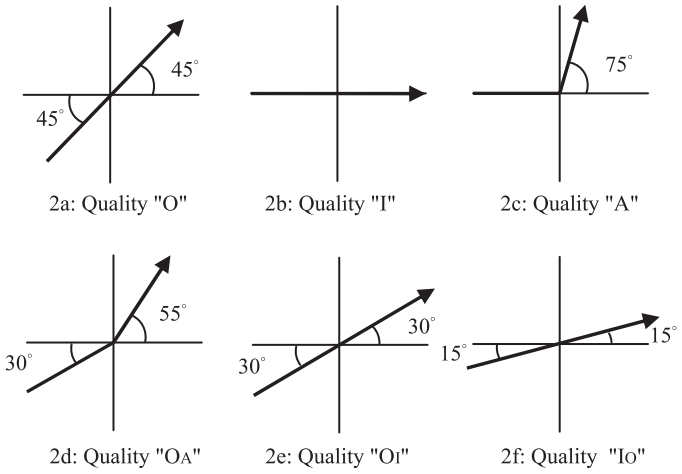

Fig. 2 – Kano model graph.

case with features of Indifferent quality: some features are of a high ratio for attractive quality or one-dimensional quality. That is, one-dimensional quality or indifferent quality is not distinct property among all MSA features. It may be feasible to further categorize quality attributes to MSA features. MSA features of quality M (must-be quality) and R (reverse quality) appears very infrequently as shown in Table 5. Their impact is ignored in further analysis. This study defines sub-quality attributes as described below. Acquire frequency of two quality attributes other than the main one; calculate their ratio over that of the main one. If the greater of the two is above 0.5 then it is a sub-quality attribute. If neither is above 0.5 then the quality has no sub-quality attribute, i.e. a pure one-dimensional quality or indifferent quality. The main quality attribute of "malware prevention" is one-dimensional quality. Both its A/O and I/O rates are less than 0.5 and so it is of pure "O" quality as defined in this study. The main quality attribute of "parental control" is one-dimensional. Its A/O and I/O rates are 0.63 and 0.26 respectively (A/O value above 0.5), and so it is of OA quality attribute, that is, one-dimensional quality with an attractive sub-quality attribute. The main quality attribute of the "privacy protection" is one-dimensional. Its A/O and I/O rates are 0.34 and 0.58 respectively (I/O value above 0.5), and so it is of OI quality attribute, that is, one-dimensional quality with an indifferent sub-quality attribute. The main quality attribute of "remote locate and lock" is indifferent quality. Its A/I and O/I rates are 0.49 and 0.98 respectively (O/I value above 0.5), and so it is of IO quality attribute, that is, indifferent quality with a one-dimensional sub-quality attribute. The main quality attribute of "app lock" is indifferent. Both A/I and O/I rates are less than 0.5, and so is of pure "I" attribute. The sub-quality attributes of each feature are O, I, OA, OI and IO (no IA is in existence) as shown in the last column of Table 5.

The fulfillment and satisfaction association of quality attribute "O" and "I" in Fig. 1 are transformed into an inclined line (a 45° angle from the upper right to lower left) in Fig. 2a and horizontal line in Fig. 2b. The "A" quality attribute in Fig. 1 is simplified into two lines as shown in Fig. 2c. That is, negative quality fulfillment (lower than average) bears no impact on satisfaction and is represented by a horizontal line similar to attribute "I" while positive quality fulfillment (above average) improves satisfaction at a faster pace represented by an inclined line (a 45° angle from the upper right to lower left). The 1:0.5 mix of main quality attribute "O" and sub-quality attribute "A" can be expressed with the formula (1xO + 0.5xA)/1.5 which can be illustrated by two lines with one inclined line "$(1 \times 45^{\circ}) + (0.5 \times 0^{\circ})/1.5 = -30^{\circ}$" in the negative fulfillment area and another "$(1 \times 45^{\circ}) + (0.5 \times 75^{\circ})/1.5 = 55^{\circ}$" in the positive fulfillment area as shown in Fig. 2d. The same rule can be used to illustrate OI and IO quality attributes in Fig. 2e and 2f. These 5 quality attribute types and the MSA features covered are described below:

(1) Quality "O": This is a pure one-dimensional quality attribute which covers MSA features of "malware prevention" and "safe browsing". It features a positive association between quality fulfillment and satisfaction: Better quality fulfillment would improve satisfaction and vice versa.
(2) Quality "I": This is a pure indifferent quality attribute which covers the MSA feature of "app lock". This quality has no impact on satisfaction regardless of its fulfillment level.
(3) Quality "OA": This is a combined quality type of main quality attribute "O" and sub-quality attribute "A" covering the MSA features of "message and call filter", "parental control", and "Wi-Fi security". Differing from the impact of a pure "O" quality attribute on satisfaction, this mixed quality attribute has less impact on decreasing satisfaction than its pure counterpart when below average and vice versa when above average.
(4) Quality "OI": This is a combined quality type of main quality attribute "O" and sub- quality attribute "I" covering the MSA features of "privacy protection", "data backup", and "garbage file cleanup". Impact of this quality on satisfaction appears parallel with that of quality "O": Quality fulfillment is weaker associated with customer satisfaction and it could be presented with a inclined line (a 30° angle from the upper right to lower left) as shown in Fig. 2e.
(5) Quality "IO": This is a combined quality type of main quality attribute "I" and sub-quality attribute "O" covering the

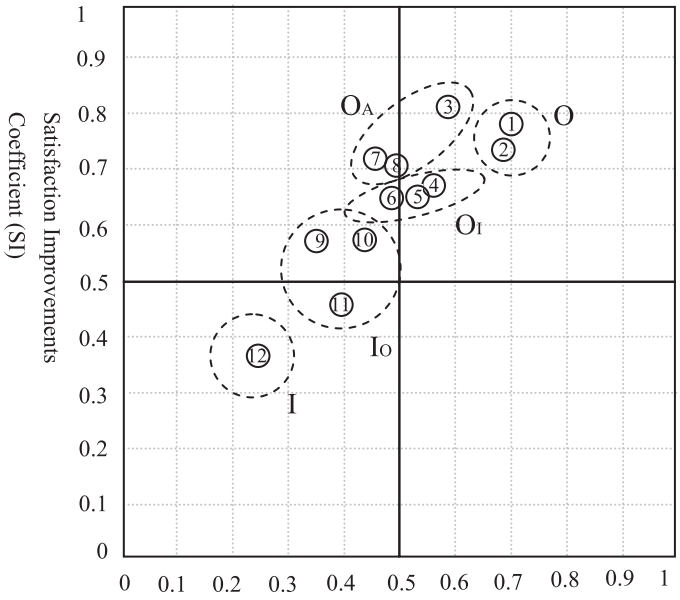

Fig. 3 – Association of satisfaction impact. Dissatisfaction coefficient (absolute value of DSI).

MSA features of "remote lock and locate", "remote wipe", and "secure app advisor". Impact of this quality on satisfaction appears parallel with that of quality "O": Quality fulfillment is still weaker associated with customer satisfaction, even weaker than OI and it could be presented with an inclined line (a 15° angle from the upper right to lower left) as shown in Fig. 2f.

4.4. *Customer satisfaction coefficient analysis on MSA features*

The Kano questionnaire may be supplemented by a "customer satisfaction coefficient" to identify the impact of quality fulfillment on customer satisfaction when quality attributes are not distinct. The "customer satisfaction coefficient" contains both "extent of satisfaction" (SI) and "extent of dissatisfaction" (DSI) (Berger et al., 1993) [9]. $SI = (A + O) / (A + O + M + I)$ and $DSI = -(M + O) / (A + O + M + I)$ where the letters "A, O, M, I" are number of persons who recognize a feature as attractive, one-dimensional, must-be, and indifferent (Sauerwein et al., 1996). The SI and DSI value of each quality can be calculated with the aforementioned formula. The SI values fall in a range of 0–1. The greater the value is the heavier the impact it may impose on satisfaction by quality improvements; the DSI values fall in a range of 0 to −1 and the lower the value is the heavier the impact it may impose on dissatisfaction. The impact on overall satisfaction may be illustrated with quality defined by the SI value on the *Y*-axis and the absolute value of DSI on the *X*-axis: Qualities with a position further away from the home point bear a larger impact on satisfaction (Xinbin, 2012). This study calculates SI and DSI values of individual MSA features (shown in the last 2 and 3 columns of Table 5) and plots them into the satisfaction impact association shown in Fig. 3. The latter displays the distribution of individual features and classifies them by the 5 quality attribute types. The distribution is further divided into four sections (by halving both SI and DSI) and the impacts and variances of each feature on satisfaction are described by each section:

(1) Upper right section (both SI and absolute DSI values above 0.5): Features in this section would have customer satisfaction improved and dissatisfaction reduced by increasing quality fulfillment. That is, they deserve more attention. Features in this section are "malware prevention", "safe browsing" (quality O); "parental control" (quality OA); and "privacy protection" (quality OI).
(2) Upper left section (SI value above 0.5 and absolute DSI values below 0.5): Features in this section have a greater impact on customer satisfaction with better quality fulfillment and less on customer dissatisfaction. Brands with qualities in the leading position need to pay more attention to them. Features in this section are: "Wi-Fi security" and "message and call filter" (quality OA); "data backup" and "garbage file cleanup" (quality OI); and "remote wipe" and "remote locate and lock" (quality IO).
(3) Lower right section (SI value below 0.5 and absolute DSI values above 0.5): Features in this section have a greater impact on customer dissatisfaction with better quality fulfillment and less on customer satisfaction. Brands with qualities in the trailing position need to pay more attention to them (features in this section are not covered by this study).
(4) Lower left section (SI and absolute DSI values below 0.5): Features in this section have little impact on customer satisfaction and dissatisfaction, i.e. no need to improve them. Features in this section are: "secure app advisor" and "app lock" (quality I).

Conclusions

This study explores Kano quality attributes of the 12 key functions of MSAs with a Kano two-dimensional questionnaire and identifies their relative importance to users. Our results suggest all of them belong to one-dimensional and indifferent quality attributes. These 12 functions are then defined with 5 quality attribute types based on their relative frequency of each function quality attribute: O, OA, OI, IO and I; their importance in the positive quality fulfillment area are: OA>O>OI>IO>I and O>OA = OI>IO>I in the negative quality fulfillment area. The impact of SI and DSI values on customer satisfaction and dissatisfaction are examined in this study as well. In summary, the top four features with the greatest impact on customer satisfaction are "malware prevention", "safe browsing", "parental control" and "privacy protection". All of these need more attention in design. "secure app advisor" and "app lock" may be ignored in design as they bear little impact on customer satisfaction improvements. "data backup", "garbage file cleanup", "Wi-Fi security", "message and call filter", "remote wipe", and "remote locate and lock" impose heavier impacts on customer satisfaction improvements than dissatisfaction reduction. MSA brands with above average quality have to increase the design effort for these functions for better customer satisfaction.

Participant profile analysis suggests that males have high technology familiarity than their female peers. Females are more concerned with "remote locate and lock" and "Wi-Fi security" than their male peers. Users with low technology familiarity (LTF) are more concerned with "garbage file cleanup", "remote locate and lock" and "secure app advisor" than those with high technology familiarity (HTF).

Result of this study may help mobile security and antivirus software vendors understand the Kano quality attributes of MSA features and their impacts on customer satisfaction for prioritizing requirements. Further classifying Kano quality attributes by this study may serve as a reference for relevant research. This study focused on users' preference of Kano model quality attribute evaluation for existing MSA features rather than exploring their real scenario and use cases and pain points on using MSA to identify more MSA design shortcomings and opportunities. These may be a direction for more research in future.

There are limitations in this study. Sample size may be too small and its diversity is limited to the netizen. Although netizen should be more knowledgeable for technology because of their rich experience to explore the internet world, the mobile phone users are not limited to netizen. It could be extend to other types of users to validate the applicability of the research result. This research focuses on MSA in Google Play because Android OS has higher security risk than iOS has, due to its nature of open platform. Definitely, it is also valuable to know how users classify the Kano quality attribute for the major MSA features of iOS. However, fewer vendors have developed MSA for iOS platform because iOS has less hacker attacks than Android platform, there are not so many specific security features developed for iOS to be explored. We could consider to better understanding mobile security risk for iOS users by deep interview or contextual inquiry.

REFERENCES

AppBrain. Number of android applications. accessed April 6, http://www.appbrain.com/stats/number-of-android-apps;; 2018 accessed April 6,.

AV-TEST, The best antivirus software for Android, https://www.av-test.org/en/antivirus/mobile-devices/android/november-2017/ accessed November 2017.

Berger C, Blauth R, Boger D, Bolster C, Burchill G, Wi DuMouchel, et al. Kano's methods for understanding customer-defined quality. Center Quality Manag J 1993:3–36.

Dini G, Martinelli F, Matteucci I, Petrocchi M, Saracino A, Sgandurra D. Risk analysis of android applications: a user-centric solution. Elsevier; 2016 May.

eMarketer, Number of smartphone users worldwide from 2014 to 2020 (in million), https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/, accessed June 2016

Enck W, Gilbert P, Chun B, Cox L, Jung J, McDaniel P, et al. TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. Proceedings of the symposium on operating systems design and implementation (OSDI), 2010.

Fan W, Narang H, Clarke D. An overview of mobile malware and solutions. J Comput Commun 2014;2:8–17.

Felt A, Ha E, Egelman S, Haney A, Chin E, Wagner D. Android permissions: user attention, comprehension, and behavior. Symposium on usable privacy and security (SOUPS), 2012.

Gartner, Worldwide sales of smartphones grew 9 percent in first quarter of 2017. https://www.gartner.com/newsroom/id/3725117; accessed May 23 2017.

Gilbert P, Chun B, Cox L, Jung J. Vision: automated security validation of mobile apps at app markets. MCS'11, 2011.

Hussain A, Mkpojiogu E. An application of kano method in the elicitation of stakeholder satisfying requirements for an e-Ebola awareness System. WSEAS Trans Bus Econ 2016 April.

Jorgensen Z, Chen J, Gates C, Li N, Proctor R, Yu T. Dimensions of risk in mobile applications: a user study. CODASPY '15: proceedings of the 5th ACM conference on data and application security and privacy, 2015.

Kano N. Attractive quality and must-be quality. J. Jpn. Soc. Quality Control 1984:39–48 April.

Kaspersky Lab., Mobile malware, 2015. https://usa.kaspersky.com/resource-center/threats/mobile; [accessed October 2017].

Kelley P, Consolvo S, Cranor L, Jung J, Sadeh N, Wetherall D. A conundrum of permissions: installing applications on an android smartphone. FC 2012 Workshops; 2012. p. 68–79 LNCS 7398.

Krisztina K, Isabel H, Mobile payment analyzed from the aspects of the Kano model, OAI: oai:DiVA.org:hh-33436, 2017.

Lubinski G, Oppitz A. Applying the Kano model in mobile services world: a report from the frontline. Eighth international conference on the quality of information and communications technology, 2012.

Mkpojiogu OCE, Hashim N. Understanding the relationship between Kano model's customer satisfaction scores and self-rated requirements importance. SpringerPlus 2016;5:197. doi:10.1186/s40064-016-1860-y.

Sauerwein E, Bailom F, Matzler K, Hinterhuber H. The Kano model: how to delight your customer, preprints volume I of the IX. International working seminar on production economics; 1996. p. 313–27 Innsbruck/Igls/Austria, Feb 19-23.

TechRepublic, Report: 2016 saw 8.5 million mobile malware attacks, ransomware and IoT threats on the raise. https://www.techrepublic.com/article/report-2016-saw-8-5-million-mobile-malware-attacks-ransomware-and-iot-threats-on-the-rise/ [accessed Feb 28 2017].

Trend Micro, Smartphone users: not smart enough about security. https://www.darkreading.com/risk/report-smartphone-users-not-smart-enough-about-security/d/d-id/1131765?piddl_msgorder=;, 2009, August 18; [accessed October 2017]

Trend Micro, software vulnerability in iOS platform. http://www.trendmicro.tw/cloud-content/tw/pdfs/security-intelligence/reports/rpt-hazards-ahead_111315_c.pdf, 2015; [accessed October 2017]

Wright J, Dawson Jr M, Omar M. Cyber security and mobile threats: the need for antivirus application for smart phones. J. Inf. Syst. Technol. Plann. 2012;5(14):40–60.

Xinbin F, Improving the product and service quality for Topray, 2012

Mei-Ling Yao is a PHD student at National Chiao-Tung University in Taiwan, a lecturer for user experience design in Fu-Jen University and also a user experience design manager at Trend Micro for 8 years who leads both designers and researchers to study security needs for SMB customers, managed service providers and resellers who sells security products for Trend Micro.

She focuses on helping product and design team to figure out user pains and needs across regions by different research methodologies like onsite customer visit, remote interview, contextual inquiry, user behavior tracking, NPS survey, fake door, usability testing and etc. She is also an evangelist to share with team how to deliver a good user experience and evaluate the business impact bringing from design improvement. Her ambition is to help team know more about users and make their life easier and safer from security threats during her career at Trend Micro. Her belief will definitely be beneficial and extendable to other areas as well in the future.

Ming-Chuen Chuang earned his Ph.D. degree in 1988 from the Department of Engineering Design of Tufts University, majoring in ergonomic design of products. Now, he is the emeritus professor of the Institute of Applied Arts of National Chiao Tung University in Taiwan. His research interest is in Kansei engineering, ergonomic design of products, interface design, and color theory.

Chun-Cheng Hsu is an associate professor in the industrial design group, Institute of Applied Arts, National Chiao Tung University, Taiwan. He was a visiting scholar at Massachusetts Institute of Technology during 2013–2014. His research is devoted to applications of theory in design practices, with interests including interaction design, user experience, and application of new media technology into social and cultural issues.