International Journal of Science and Technology

http://www.ejournalofsciences.org

Social Attackability Metrics for Software Systems

[1]Samuel Mungai Mbuguah , [2]Waweru Mwangi , [1]Pang Chol Song, [3]Geoffrey Muchiri Muketha
[1]Department of Computer Science
Masinde Muliro University of Science and technology ,Kakamega , Kenya
[2]ICSIT, Jomo Kenyatta University of Agriculture and Technology, Nairobi , Kenya
[3]Department of Computer Science Meru University, Meru, Kenya

ABSTRACT

Software based system have become ubiquitous in modern day activities. Software system based system are being increasing attacked, leading to the need for software system administrators, and managers to have some metrics at predicting the social engineering attackability of a such system. Researchers have identified seven human traits/attributes that make human susceptible to social engineering attacks. Yet they did not model nor come up metrics. The author has published a conceptual a holistic predictive attackability metric model and corresponding metrics to assist the system designers. The model considers the technical metrics based on cohesion, coupling and complexity as used to predict attackability. It also consider the social metrics based on human traits that make the human operators become susceptible to social engineering attacks. The identified human traits are dishonesty, social compliance, Kindness,Time pressure, Herd mentality, greed/need and distraction. This paper considers only the social metrics part of the model.To measure human traits the authors relies on the HEXACO model and Big Five personality trait models. In these model the personality trait are measured using a ranking scale based on Lickert scale. Hence each trait is measured as a percentile. However, for purpose of this paper, to postulate the metric the author considered the discrete case. Why the value of trait take either a value of "1" or "0". To determine the relationship between traits between and attackability experts were asked to assess the trait versus attackability from which after aggregating for all traits a social attackability metrics was determined. To determine the predictive social attackability metrics each trait was considered to be equally likely to occur and hence a probability of 1/7 and this acts as factor to transform the social attackability metric into predictive attackability metrics.

Key words: *Probability, Metrics, attackability, attributes/traits, model*

1. INTRODUCTION

Computer system systems are socio technical system in that apart from the hardware and software the human operator is involved. The reliability of such system will be a product of reliability of the software, reliability of hardware and finally the reliability of the human operator. Similarly, it has be suggested that from a holistic security engineering point of view, real world systems are often vulnerable to attack despite being protected by elaborate technical safeguards. The weakest point in any security strengthened system is usually the human element; an attack is possible because the designers of the system thought only about their strategy for responding to threats, without anticipating how real users would react [1]

This then forms the gist of this paper, has research being done in this area? Are there existing models and metrics. The structure of the remaining part of the paper is: related work, summary social attackability model, metrics, results, discussion and references.

2. RELATED WORK

This section highlights related work on social metrics. The seven principles, the social models

2.1 Understanding Scam Victims: Seven Principles For Systems Security

Researchers have tried to find out on the psychology of scam victims[2]. Researchers have identified traits that make people vulnerable to scams. These traits were published in ACM vol 54 journal as shown in table 1.

Table 1—Scam Victims source(ACM Vol 54)

Principle	Cialdini (1985-2009)	Lea et al, (2009)	Stajano-wilson (2009)
Distraction		~	X
Social compliance(Authority)	X	-	-
Herd (Social proof)	X		-
Dishonesty			X

Kindness	~		X
Need and greed (Visceral Triggers)	~	X	-
Scarcity (related Time)	X	-	~
Commitment and Consistency	X	-	
Reciprocation	X		~
~ -------Lists a related Principle Also lists this principle X First identified this principle			

Wilson says that the finding support their thesis that systems involving people can be made secure only if designers understand and acknowledge the inherent vulnerabilities of the human factor[1].

Their three main contributions were: First hand data not otherwise available in literature; Second they abstracted seven principles; Third they applied the concept to more a general system point of view. They argue that behavioral patterns are not just opportunities for small scale hustlers but also of the human component of any complex system. They suggested that system –security architect should acknowledge the existence of these vulnerabilities as unavoidable consequence of human nature and actively build safeguards to prevent their exploitation [1] However they did not attempt to model the relationship between the traits and system attackability.

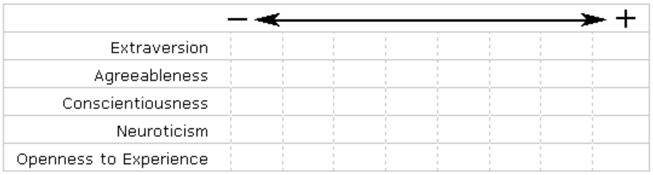
2.2 Measuring the Personality Traits

Literature review indicate that a lot of research has been carried out in this area measurement of personality traits and is standard practice especially for human resource department. For the purpose of this paper only two models will be highlighted.

2.2.1 Five Factor Theory

In the final decades of the twentieth century an increasing number of psychologists came to the conclusion that the three factor model was too simple and that 16 factors were too many. In 1990 Paul Costa and Robert McCrae presented their '**Five Factor Theory**' and introduced the associated NEO Personality Inventory. Table 1 depicts the model. Each of these 5 personality traits describes, relative to other people, the frequency or intensity of a person's feelings, thoughts, or behaviours[3].

Table 1 Five factor theory (Source Costa &McCrae 1990)



Everyone possesses all 5 of these traits to a greater or lesser degree. But there could be a significant variation in the degree to which they are both agreeable. In other words, all 5 personality traits exist on a continuum rather than as attributes that a person does or does not have.

Each of the big 5 personality traits is made up of 6 facets or sub traits. These can be assessed independently of the trait that they belong to. Table 2 shows the traits and their facets[4].

Table 2: Personality traits Source(MacCrae & Costa,1990)

Personality Trait	Facets
Extraversion	Friendliness Gregariousness Assertiveness Activity Level Excitement-Seeking Cheerfulness
Agreeableness	Trust Morality Altruism Cooperation Modesty Sympathy
Conscientiousness	Self-Efficacy Orderliness Dutifulness Achievement-Striving Self-Discipline Cautiousness
Neuroticism	Anxiety Anger Depression Self-Consciousness Immoderation Vulnerability

Openness to experience	Imagination Artistic Interests Emotionality Adventurousness Intellect Liberalism

From the literature it can be seen that measurement of the known personality traits is through a percentile scale. This based on self reports, questionnaire and peer assessments [5].

2.2.2 HEXACO Personality Model

Kibeom et al.[6] carried out research on predicting integrity based on HEXACO Model. The model is an improvement on the big five model that has a six-dimension. It has been suggested that the framework may have particular value in organizational settings because of its ability to predict integrity-related outcomes. In the study, they examined the potential value of the HEXACO factor known as Honesty–Humility. First, the empirical distinctness of this construct from the other major dimensions of personality was demonstrated in a high-stakes personnel selection situation. Second, Honesty–Humility was found to predict scores on an integrity test and a business ethical decision making task beyond the level of prediction that was possible using measures based on a traditional Big Five model of personality. This finding was also observed when Honesty–Humility was assessed by familiar acquaintances of the target persons. The applicability of the HEXACO model within industrial and organizational psychology was then discussed.

Hence the HEXACO model would be appropriate measuring the identified seven traits. This could be used in the measurement of identified seven traits. Several researcher have experimented on how to measure the personality [7],[8],[9],[10],[11],[12] and [13]. However this paper aims to use discrete value for each traits that is 1 or 0.

2.2 The Conceptual Holistic predictive attackability metric model

Mbuguah et al.[14] published the above model that combined the technical attributes and the social attributes that affects system attackability. The researcher postulated that each had a positive correlation with meanattackability of the system. However, for technical attributes, since a strong cohesion is normally equated to a weak coupling the two were considered to work in opposition.

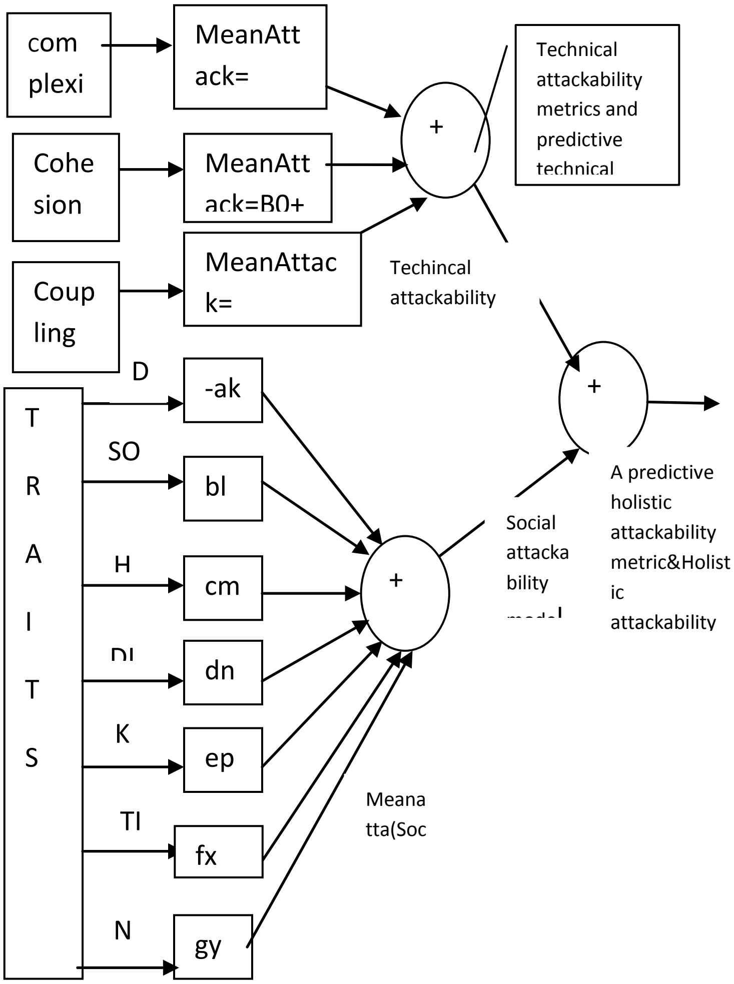

com plexi
MeanAtt ack=
Technical attackability metrics and predictive technical
Cohe sion
MeanAtt ack=B0+
+
Coup ling
MeanAttac k=
Techincal attackability
T R A I T S
D
-ak
SO
bl
H
cm
DI
dn
K
ep
TI
fx
N
gy
+
Social attacka bility model
+
A predictive holistic attackability metric&Holist ic attackability
Meana tta(Soc

Figure 1 The Holistic attackability model source (Mbuguah et al.2012)

This model and metrics have not being validated. This paper picks on social aspects attempts to validate the model and metrics.

Figure 1 shows this model. The upper block indicates technical attributes modelling while the lower block indicate the social attributes. The two blocks are then combined to generate the holistic model and the accompanying metrics. The researcher assumes that each of the seven attributes occur in equal measure. If this be the case the factor labelled “a” to “g” will be 1/7.This can be verified by carrying out a research through, questionnaires, interviews, penetration tests and observations. If this is not the case then data collected can then be used to determine the frequency of of each which will be used to determine the factors “a” to “g”. It can also be assumed that each of the trait contribute in equal measure to social attackability. This may not be the case the variables "k" to "y" assessment of weighting of the probable contribution to each them. It is assumed that the model of each will be a probability and all of them can be combined to generate a social attackability model and hence metric.

To generate a holistic predictive model and metric the technical model and social model should be combined to produce a metric. In the ideal case the metric should a numerical value. But there could be issues on whether this is justifiable. The researchers proposed to avoid this by proposing that the final metric M= mT + nS where small m represents the technical metric and n represents social metric.

3. SOCIAL MODEL AND METRICS

In this the social attackability model is developed, the researcher illustrates the model can be developed from the basic probability models which well grounded in mathematics.

3.1 Probability Model

A probability model is a mathematical representation of a random phenomenon. It is defined by its sample space, events within the sample space, and probabilities associated with each event. The sample space S for a probability model is the set of all possible outcomes. An event A is a subset of the sample spaces [16].

The social attributes then can form a probability model whose sample space is

S = {Dishonest(Dishon), Distraction(Dist),
Kindness(Kind), Greedy/need(greed),
TimePressure(Timep), Social compliance(Socom) ,Herd
mentality(Herd)

S={Dishon, Dist, Kind, Greed, TimeP, Socom, Herd}

An event A, being a subset of sample space such as considering Dishon only.

A probability is a numerical value assigned to a given event *A*. The probability of an event is written *P(A)*, and describes the long-run relative frequency of the event. The first two basic rules of probability are the following [16]:

Rule 1: Any probability P(A) is a number between 0 and 1 ($0 \le P(A) \le 1$).

Rule 2: The probability of the sample space S is equal to 1 (P(S) = 1).

If there are *k* possible outcomes for a phenomenon and each is equally likely, then each individual outcome has probability 1/*k[16]*.

$$p(A) = \frac{count\ of\ outcomes\ in\ A}{count\ of\ outcomes\ in\ S} = \frac{count\ of\ outcomes\ in\ a}{k}$$

For the social model the frequency of occurrence of an event A should be determined. This can will done by use of a Questionnaire tool in data collection and use SPSS software frequency for descriptive analysis. Using five scale Likert scale the participants will be asked rate in scale comprising of {Strongly agree, Agree, Do not Know, disagree and strongly disagree) whether any of traits in sample space contribute to Social attackability of system. This scale will then quantified as { 5,4,3,2,1}.Assuming that the number of participant is N then

Count of outcome in S, k=5N.

Count of outcome in A , j= (5*(no of strongly agree)+4*(no of agree) +3*(no of DNK) + 2*(no of disagree) +1*(Strongly disagree)

P(A) = j/k

If two events have no outcomes in common, then they are called ***disjoint***. The addition of probabilities for disjoint events is the third basic rule of probability[9]:

Rule 3: If two events A and B are disjoint, then the probability of either event is the sum of the probabilities of the two events:P(A or B) = P(A) + P(B).

The chance of *any* (one or more) of two or more events occurring is called the ***union*** of the events. The probability of the union of disjoint events is the sum of their individual probabilities.

Rule 4: The probability that any event A does not occur is $P(A^c) = 1 - P(A)$.

In social model has seven disjoint events and rule 4 will apply .

P(S)={P(Dishon), P(Dist), P(Kind), P(Greed), P(TimeP), P(Socom), (P)Herd}

If two events occur in succession and If the outcome of the first event has no effect on the probability of the second event, then the two events are called independent. The fifth basic rule of probability is known as the multiplication rule, and applies only to independent events[16]:

> Rule 5: If two events A and B are independent, then the probability of both events is the product of the probabilities for each event: P(A and B) = P(A)P(B).

The chance of *all* of two or more events occurring is called the intersection of events. For independent events, the probability of the intersection of two or more events is the product of the probabilities.

The social model should also be predictive, for this to happen then it can be assumed that each trait in the sample space is equally likely to occur and since sample space is seven then

P(A) = 1/7.

But there also is Probability(Union) duo to the union of individual probabilities. Hence this two probabilities can be considered sequential and independent and rule five applies

Predictive probability (Intersection)= 1/7*P(union)

3.2 The Social Metrics

Several researches [17],[18] and [19]have looked at the issue studied the metrics for quite some time. Weyukker came up with the nine principles on which to evaluate a metric. The principles have be critiqued as being ideal for complexity metrics only. Briand et al. looked at this and expanded on them by including a criterion for evaluating size metrics. Since the proposed attackability metrics are size based then Briand et al.[19] approach is more applicable in this case.

3.2.1 Goal Question Metrics(GQM)

Briand et al.[19]postulates that measurement should be based on Goal Question metrics paradigm developed at University of Maryland. The paradigm states that you have to have a goal of measurement. Then determine the right question to achieve the your goals, then metrics are based on this question. The procedure involves the following steps:

i. Define experimental goals.
ii. State assumptions.
iii. Formalize relevant measurement concept.
iv. Define product abstractions refine properties.
v. Define metrics.
vi. Experimental validation of metrics.

3.2.1 Representation of Systems and Module

According to Briand et al.[19], A *system* S will be represented as a pair <E,R>, where E represents the set of elements of S, and R is a binary relation on E ($R \subseteq E \times E$) representing the relationships between S's elements. Given a system S = <E,R>, a system m = <Em,Rm> is a *module* of S if and only if $Em \subseteq E$, $Rm \subseteq E \times E$, and $Rm \subseteq R$. This will be denoted by $m \subseteq S$.

3.2.2 Concept of Size

Briand et al.[19] says size is recognized as being an important measurement concept and defines size of a system S as function Size(S) that is characterized by the following properties Size.1 - Size.3.

Property *Size.1*: Non-negativity

The size of a system S = <E,R> is non-negative
$Size(S) \geq 0$ (Size. I)

Property *Size.2*: Null Value

The size of a system S = <E,R> is null if E is empty
$E = \varnothing \Rightarrow Size(S) = 0$ (Size. II)

Property *Size.3*: Module Additivity

The size of a system S = <E,R> is equal to the sum of the sizes of two of its modules m1 = <Em1,Rm1> and m2 = <Em2,Rm2> such that any element of S is an element of either m1 or m2
($m1 \subseteq S$ **and** $m2 \subseteq S$ **and** $E = Em1 \cup Em2$ **and** $Em1 \cap Em2 = \varnothing$)$\Rightarrow$ Size(S) = Size(m1) + Size(m2) (Size.III)
The last property Size.3 provides the means to compute the size of a system S = <E,R> from the knowledge of the size of its—disjoint—modulesme = <{e},Re> whose set of elements is composed of a different element e of
E2. $Size(S) = \sum e \in E\ Size(me)$ (Size. IV)

Therefore, adding elements to a system cannot decrease its size

For each me, it is either $Re=\varnothing$ or $Re=\{<e,e>\}$.

$$(S' = <E',R'> \textbf{ and } S'' = <E'',R''> \textbf{ and } E' \subseteq E'') \Rightarrow Size(S') \leq Size(S'') \ (Size.\ V)$$

From the above properties Size.1 - Size.3, it also follows that the size of a

system S = <E,R> is not greater than the sum of the sizes of any pair of its

modules m1 = <Em1,Rm1> and m2 = <Em2,Rm2>, such that any element of S

is an element of m1, or m2, or both, i.e.,

$$(m1 \subseteq S \textbf{ and } m2 \subseteq S \textbf{ and } E = Em1 \cup Em2) \Rightarrow Size(S) \leq Size(m1) + Size(m2) \ (Size.VI)$$

The size of a system built by merging such modules cannot be greater than the sum of the sizes of the modules, due to the presence of common elements (lines of code, operators, and class methods). These properties will be used to interrogate the theoretical validity of define metrics.

Social Attackability Metrics

The metric is defined as summation of each attributes probabilities

(i)SocAttack =aGreed +bTimep +cKind+dDish+eHerd +fSocom +hDist

The attributes are measured as percentile scale and taking the floor and ceiling function for attributes ie 0 and 1. Then theoretical maximum value is 7 since a, b, c, d, e, f and h are fractions. The minimum value for metrics will be zero.This metrics satisfies Size I-III

(ii) Predictive SocAttack metrics= 1/7(aGreed +bTimep +cKind+dDish+eHerd +fSocom +hDist). The maximum is 1 and minimum zero. Which follows with the range of probability and also satisfies Size(I-III).

4. VALIDITION OF THE METRICS

Theoretical validation of metrics is appropriate; the metrics so designed appear to meet the threshold for size metrics. But for metrics to be useful they required empirical validation to enable them be used in industrial setting. This Social metrics were derived from a sample questionnaire comprising lecturers , practising technical staff and security staff JKUAT and MMUST public Universities. Master students in Software engineering and Information Technology with experience in the area of security were also looped in.

4.1 Survey preparation

Before conducting any experiments or survey it important that preparation be done to ensure that the correct data is collected. The subjects are people sampled for social metrics analysis.

4.1.1 Subjects Selection

The subjects were chosen the staff of Jomo KenyattaUniversity of Agriculture and Technology and Masinde Muliro University of science and technology. The criteria was that the subject should have at least a Master degree in Information technology or related field. However technical staffs who have registered for Master degree in the said Universities were considered on the basis that they are practicing and the issue of security is a daily occurrence. Some security personnel in said universities were also sampled. On the ground this is a security and they are trained in security matters.

4.1.2 Materials

The material required were printing paper, a computer, a printer, photocopier, modem or internet link, means communications, office and SPSS softwares.

4.2 Experimental Planning

Experimental planning means going through whole process mentally to determine requirements, sequence, resource required, time required and any challenges that may arise.

4.2.1 Experimental Context

The goal of experiment was to determine the type of relationship between the chosen attributes and attackability and thereof consider the possibility of modeling the individual or/and the combined relationship.

4.2.2 Variables – IVs, and DVs.

Table 3 shows variables involved in the experiments . Type of measurement is quantitative is a lab exercise was carried out and actual measurement carried out. The qualitative measurement are based on 5 point licker scale questionnaire.

Table 3 Variables Source (Author 2012)

Serial No	Independent Variable(IV)	Dependent variable	Type Measurement
1	Dishonesty	Attackability	Qualitative
2	Distraction	Attackability	Qualitative

3	Greed/need	Attackability	Qualitative
4	Kindness	Attackability	Qualitative
5	Timepressure	Attackability	Qualitative
6	Social compliance	Attackability	Qualitative
7	Herd mentality	Attackability	Qualitative

4.3.3 Hypothesis

The null hypothesis - Ho : The identified social traits do not strongly contribute to the social attackability of a computer based system.

4.3.4 Experimental Design

The same questionnaire was answered by different subjects this to ensure consistence of the output.

he question bias then does not arise.

4.3.5 Threats to Validity

Construct Validity. The measurements for social metrics are subjective and are based on the perception of the subjects. However since these are expert in area of security the measurement can be considered valid.

Internal Validity: The subject for survey, difference among subject like, experience , motivation fatigue among others [20] could arise. The subjects were given at least two weeks to answer the questions to allow them to answer when they are most comfortable.

External Validity The survey was limited to two public universities. There could be an issue of external validity in that this may not be replica of general public. However the selection of the two universities was an attempt to avoid studies being in single region.

4.4 Experimental Operation

In this section will describe how the experiments were operationalsed.

4.4.1 Experimental Process

The Social metrics measurement were derived pilot survey using ten members of MMUST in the month of October 2012.Analysis of the data and modification of questionnaire was done in November and the results of the finding presented in a PhD seminar held in November 2012. Request to conduct research within MMUST and JKUAT was made in November 2012.

Questionaire issued in January 2013. Data collected was cleaned and inputted in SPSS as data was received. By April 2013, 35 of the 60 questionnaires given out had been returned. Some questions were used to test the social engineering awareness by the subjects. Four of the 35 questionnaires returned scored poorly in answering these questions and the questionnaires were discarded.

5. RESULTS

This outlines the result generated after analysis of the data.

5.1 Questionnaire Data Validation

Validity of a tool seeks to identify whether the tool will collect the required data. To validate this question a pilot study was carried out on ten experts. To increase the reliability of tool the test –retest approach of the questionnaire development was adopted. Table 4 shows the results of the pilot study.

Table 4: Validating Questionnaire Tool source (Author)

Attributes/trait	Test	Retest	Deviation
Distration	37	44	+7
Social Compliance	27	38	+11
Herd Mentality	32	34	+2
Dishonesty	50	39	-11
Kindness	41	38	-3
Time Pressure	38	44	+6
Greedy/need	48	38	-10

A deviation +2 (+26 +-24 =+2) is not significant and this was corrected by rephrasing questions that had issues. The tool could then be considered valid and reliable. Cronbach apha is greater that 0.7 the recommended for a tool to be considered internal consistent[20].

5.2 Subjects Demographic Data

The Research set out to find some demographic information on subject taking part in survey shown in Tables 5 (a,b, &c)

The results indicate that 80% of the subjects were male while 20% were female. This generally reflects the state of affairs in the field of interest.

Table 5a Gender Source(Author)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	MALE	25	80.6	80.6	80.6
	FEMALE	6	19.4	16.1	96.8
					100.0
	Total	31	100.0	100.0	

Table 5b shows the result of the age distribution among the subjects. 6.5 % constitute the over 50 year's age bracket. This is also to be expected for most of the IT personnel are generally young in age.

Table 5b: AGE Source(Author)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	BTW 20-30 YRS	12	38.7	38.7	38.7
	BTW 30-40 YRS	10	32.3	32.3	71.0
	BTW 40-50 YRS	7	22.6	22.6	93.5
	ABOVE 50 YRS	2	6.5	6.5	100.0
	Total	31	100.0	100.0	

Table 5c shows the job category within the subjects. 68 % of subject were technical and academic staff.

Table 5c: JOBCAT Source(Author)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SECURITY	4	12.9	12.9	12.9
	ADMIN	4	12.9	12.9	25.8
	TECHNICAL	14	45.2	45.2	71.0
	ACADEMIC	7	22.6	22.6	93.5
	NON OF THE ABOVE	2	6.5	6.5	100.0
	Total	31	100.0	100.0	

5.3 Social Metric Results

This section presents and analysis the results of the social metrics. Table 6 shows the result of a each of seven personality traits as a measure of its contribution to social

Table 6 Social metrics measure for Personality traits Source (Author)

Atribute/trait	Test	Retest	Mean
Dish	0.884	0.819	0.85
Dist	0.6451	0.819	0.73
Socomp	0.839	0.826	0.83
Herd	0.748	0.8	0.77
Kind	0.703	0.78	0.76
Timep	0.729	0.806	0.77
Greed	0.832	0.69	0.76

The table show the result of test retest[22],[23] and the metric is the computed as mean. Each was derived as a result of descriptive analysis on SPSS software. The values were derived as shown as indicated below.

Dish=95+32+6+4=137/155=0.884 ,
Dish1=45+64+18=127/155=0.819 =0.85

Dist =35+42+15+8+2=100/155 =0.6451,

Dist1=55+56+9+6+1=127/155=0.819=AVERAGE = 0.73

Socomp=4*5+14*4+5*3+6*2+2*1=0.839,
Socomp2=65+18+1=128/155=0.826=0.83

Herd= 55+28+27+4+2=116/155=0.7483,
Herd1=60+40+21+2+1=124/155=0.8=0.77

Kind =35+56+6+8+4=109/155=0.703,
Kind1=90+32+9+2=133/155=0.858= 0.78

Timep=45+44+12+10+2=0.729,

Timep2= 65+44+12+2+2=125/155=0.806=0.77

Greed=80+44+2+3=129/155=0.832,
Greed1=60+42+3+2=107/155=0.69=0.76

5.4 Social Metrics Validation Results

After getting the result of social metric the author went ahead to validate the result by requesting five practicing security experts to rate in scale of 1 to 10 how a given trait affects social attackability of a system. Table 7a shows the organization and job title of security expert used in validation. The data from this group was entered into an Excel spreadsheet for each of the attribute and mean determined referred as ValMean. This mean was converted into a value between 0 and 1. These means were also entered into an Excel worksheet together with mean result from sample population(sampleMean).

Table 7(a): Social metrics Validation Experts Company and job title

S/N0	Company	Job Title
1	Ministry of Finance - Treasury	Risk Analyst
2	Safaricom,	IT Security manager
3	Price Water house coopers	Security Analyst
4	Techmax Solutions Limited	Network security Engineer
5	Techmax Solutions Limited	Security Accounts Manager

The deviation between ValMean and Sample Mean was determined for each with ValMean used as reference. A mean deviation was determined and used to generate a corrected mean from sampleMean. Table 7(b)

Table 7b: Social Metrics Validation results and Correction

Attribute	Sample Mean	Val Mean	Deviation	Corrected mean
Dish	0.85	0.64	-0.21	0.751
Dist	0.73	0.64	-0.09	0.631
Socomp	0.83	0.3	-0.53	0.731
Herd	0.77	0.94	0.17	0.671
kind	0.76	0.9	0.14	0.661
Timep	0.77	0.56	-0.21	0.671
Greed	0.76	0.8	0.04	0.661
Mean Deviation			-0.09857	

5.5 Discussion on the implication of the results

This implies that the social attackability can be realized as

SocAttack =aGreed +bTimep +cKind+dDISH+eHERD +fSOCOMP +hDIST

=0.751DISH+0.661GREED+0.661KIND+ 0.671TIMEP + 0.631DIST + 0.671HERD + 0.731SOCOMP,
6.16

Max=0.751+0.661+0.661+0.671+0.631+0.671+0.731=4.777

Min = 0

This implies could generate a metric within a range 4.777 and 0. The higher the value ,the more the need for further social engineering training or awareness.

For a predictive metric we assume that each of the traits is equally likely with a probability of 1/7

Predictive Soattack =1/7(0.751DISH+ 0.661GREED+ 0.661KIND +0.671TIMEP +0.631DIST +0.671HERD+0.731SOCOMP)

Predictive SocAttack Max = 4.777/7 =0.682

Predictive SocAttack Min = 0/7 =0.0

This falls within the range of expected probability of between 0 and 1. The metrics is therefore valid and implies it can be used in predicting the social attackability of the operator in software system implying attackability of the system.

5.5 Conclusion and Recommendation

Personality traits models do exist. Researchers have identified traits that make human beings susceptible to social engineering attacks and have extended this to system view. Researchers have also identified that the human being is the weakest link in system security. This paper extends these concepts by not only modeling the traits as applied to software systems but also introduces some metrics that are theoretically and empirically sound. This may go along way in a in providing managers with a tool to assess their vulnerability and take the appropriate action.

There is need to increase the sample population of subjects to improve on the accuracy of the tool. There is need for an algorithm to compute the metrics rather than manual computation. The traits measurement should be automated that a subject just answers a series of questions from which the metrics are collected and social attackability computed. Only the social model was considered in this paper, the technical aspect should validate and the two combined to generate the holistic attackability metrics.

REFERENCES

[1]. Wilson, F. S. (2011). Understanding Scam Victims:Seven Principles For system , Security. *Communication Of ACM, Vol 54,No3* .

[2]. Al, L. e. (2009). *The Psychology of Scams:Provoking and Commiting Errors Of , Judgement.* London: University of Exeter School of Psychology.

[3]. http://www.psycometric.com/personality tests accessed on 31/12/12

[4]. Consta PT and McCrae R(2005) ,Trait theories of personality . Advanced personality New york Plenum press

[5]. https://syllabus.byu.edu/uploads/FoAbwzFVg-oc.pdf accessed 28/12/12

[6]. Kibeom Lee, Michael C. Ashton, David L. Morrison, John Cordery and Patrick D. ,Dunlop (2008) HEXACO Model within industrial organization , environment, Journal of Occupational and Organizational , Psychology, 81, 147–167© 2008 The British Psychological Society

[7]. Gosling, S. D.; Rentfrow, P. J.; Swann Jr, W. B. (2003). "A very brief measure of the , Big-Five personality domains". *Journal of Research in Personality*

[8]. Cattell, H.E.P, and Mead, A.D. (2007). The 16 Personality Factor Questionnaire , (16PF). Accessed on 31/12/http://www.psycometric.com/personality tests 30/12/12

[9]. In G.J. Boyle, G. Matthews, and D.H. Saklofske (Eds.), *Handbook of personality , theory and testing: Vol. 2: Personality measurement and assessment.* London: Sage.

[10]. V.B. Scott, and, W.D. Mclntosh (1999) The development of a trait measure of , ruminative thought Elsevier Science Ltd.

[11]. Justin Leverton (2003) The Bubble Mania ,*The park place Economist volume X*

[12]. Kellogg, J. S., Hopko, D. R., & Ashcraft, M. H. (1999). The effect of time pressure, on arithmetic performance. *Journal of Anxiety Disorders, 13*(6), 591-600

[13]. Si Man Lam and Ching Teng(2011) Time pressure, nurse conscientiousness and , patient safety .*Chang Gung University Taiwan*

[14]. Jing Chen(2004) Effects of test anxiety, time pressure, ability and gender on , response aberrance. PhD dissertation, Ohio State University

[15]. Mbuguah S.M, Mwangi W., Song P.C,Muketha G.M (2012) A Conceptual , Model for a Holistic Predictive Attack Ability Metric for Secure Service ,Oriented Architecture Software *International Journal of Information and ,Communication Technology Research* Volume 2 No. 7,

[16]. www.stat.yale.edu/Courses/1997-98/101/probint.htm accesed on 2/3/2013

[17]. Fenton N. E.and Pfleeger S. L. (1997). *Software Metrics: A Rigorous and Practical ,Approach,* . Boston, MA, USA,: PWS Publishing Co.

[18]. Weyuker, E.J., Evaluating software complexity measures. IEEE Transactions on Software Eng., 1988. 14(9): p. 1357-1365.

[19]. Lionel Briand, Yong-Mi Kim, Walcélio Melo, Carolyn Seaman, Victor Basili - Q-Mopp of Journal of Software Maintenance

[20]. Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. , *Psychometrika*, , *16*,297-334.

[21]. Mugenda, O. M. and Mugenda A.G (2003). *Research Methods.* Nairobi: ACTS.

[22]. Kasomo , D.(2006). Research Methods in Humanities and Education. Egerton , University Press.