IJCSN International Journal of Computer Science and Network, Volume 6, Issue 3, June 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Man – Mobile: Activity-based Cyber Security Analysis

[1] VSRao Sasipalli; [2] Hideaki Mukai; [3] KrishnamRaju Gottumukkala

[1] Center for Excellence in Computer Technology,
Hiroshima City, Hiroshima 7300048, Japan

[2] Fuji Soft Co. Ltd. Hiroshima City,
Hiroshima 7300029, Japan

[3] Center for Excellence in Computer Technology,
Visakhapatnam City, Andhra Pradesh 530013, India

Abstract – Mobile phones became main part of our daily life helping us accomplish many tasks or activities from anywhere anytime at fingertips. These activities involve information either receiving or passing over internet, which cause cybersecurity problems. Most of the activities handle sensitive data right from the identifying yourself to finish the activity. Cyber-threats increased with the increase in the number of Mobiles, People, Apps and Activities. This is forcing us to consider cybersecurity of Man - Mobile and Activity – Data/Apps concepts. In this paper, an analysis of these four main players is given in cybersecurity perspective by considering the relationships among these four players. Further driven-apps and their influence are also considered in the analysis graphically. Introduced a point scaling the effectiveness of analyzing the relationships which help understand the risk severity.

Keywords – *Man-Mobile, Data-Activity, Cybersecurity, Driven Apps, Point Scaling, t-tests and Analysis.*

1. Introduction

With the technology advancement, the relationship between Man (users) – Mobile (Mobile phones or Smartphones) became stronger than ever and more than any family, friendly or such other human relationship. No doubt Mobile provides extensive flexibility in daily life activities, and it brings in threats as well. Threats, also called cybersecurity problems, are being addressed continuously but new threats arise, it is an evergreen task and a hot research topic. Most researchers reported solutions to the cybersecurity problems on network side and some vendors like Norton, McAfee developed antivirus products to work on mobile devices. However, there is less focus given to the part that cover the Activities between Man and Mobile, and Data being transceived through Apps.

A professional hacker working for more than 15 years finds cybersecurity problems in technology to make that technology more secure stated that Cybersecurity problems are everywhere. The same problems are seen repeatedly. While we depend more and more on technology, technology is becoming more and more insecure [1]. Attackers use different methods to reach mobile devices, a simple scenario can be thought of as shown in Fig. 1.

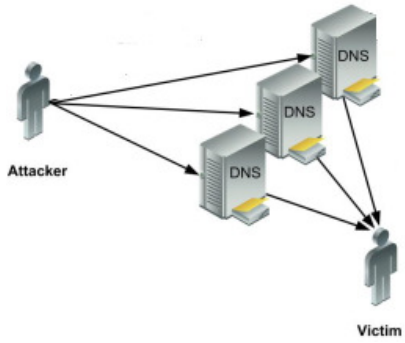

Fig. 1: Hacking: Attacker – Victim

Software solutions on network side, can control its interaction with connected components (by ways of taking logs, analytics, applying filters, etc), but not the Mobile itself, it is easy for hackers to take control of the mobile and some parts of network. Hence most security solutions addressed to work on network as network solutions work around Gateway, and not integrated with Mobile device. Fig. 2 depicts the architecture of network solutions and their locations [2].

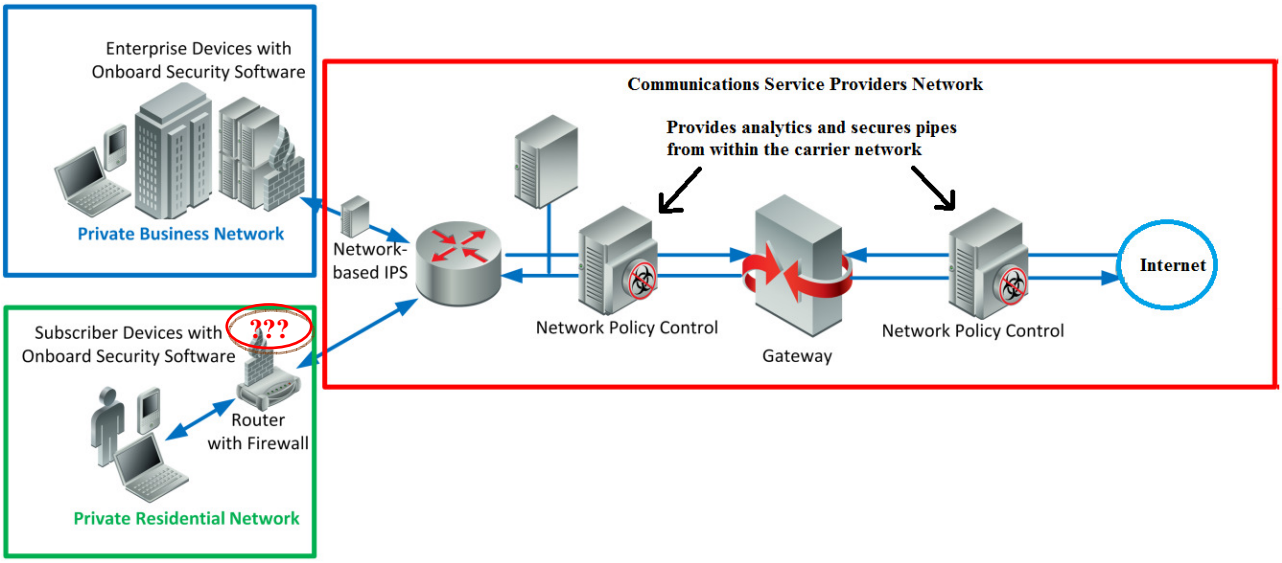

Fig. 2: General Scenario of Network Solutions Architecture

This general network solution architecture provides controls over network flow. However, this solution does not guarantee protections to all threats of security. For example, Activities between Man and Mobile and Data being passed through Apps.

Man and Mobile are bonded by Activities that involve Data flow. Some of the main daily activities are reported in [3] are shown in Fig. 3. Note that 78% of the total daily usage of smartphone by activity connects to internet. This dependence on internet by the activities make Mobile more vulnerable and prone to cybersecurity issues.

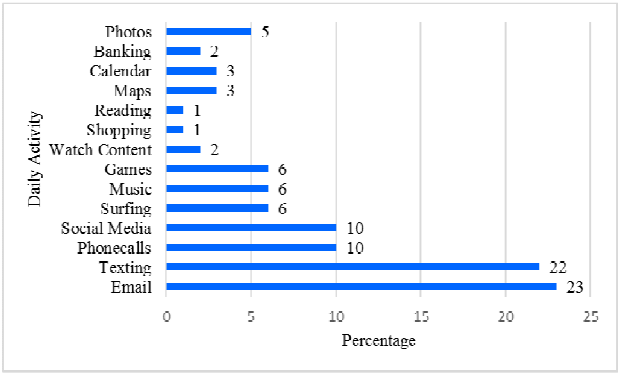

Fig. 3: Daily Usage Activity of Smartphone by Percentage

Most technology is vulnerable and can be hacked. Some examples of every day: Cars have been hacked, a popular U.S. smart home alarm system was hacked, implantable medical devices like pacemakers have been hacked, plane systems have been hacked, critical infrastructure like a power grid and a dam were hacked, mobile banking apps have been hacked, smart city technology has been hacked, and traffic systems are hacked. These are just a few examples; the list could go on. Every year, thousands of cybersecurity problems are identified in technologies from well-known vendors. Some of those vendors are among the best at cybersecurity, yet they still have hundreds of security problems each year. We attempt to address cybersecurity problems focusing on everyday Activities on Mobile by Man.

Though, all the story everywhere and anywhere revolves around Data transceived by triggering an action by man on mobile device, Activity between Man and Mobile is not focused for evaluating or analyzing the cybersecurity threats and techniques. We pose a question as shown in Fig. 4, and study the Man – Mobile relationships in terms of Activity and Data, by proposing null hypothesis. Null hypothesis here states that sample observations result purely from chance.

Fig. 4: Man – Mobile Relationship – Activity Scenario

In section 2, we consider commonly arizing cybersecurity threats and techniques, and in section 3 we develop Man – Mobile relationships, in section 4, we work on analyze the

sample data by introducing scaling points to derive sevirity of the scurity and hence the risk.

2. Cybersecurity Threats and Techniques

To improve the cyber security of mobile systems, we must understand the challenges and concerns that users currently have with performing sensitive operations on their smartphones and identify opportunities to improve the security of the device. If the device is connected to internet it is prone to cyber threats and one must care some security measures, without which the data cannot be keep safe and secure [4]. These measures cannot be centered at one point, need to scatter to different aspects, such as User side, Network side, Service Provider side, etc. Any loophole at any point can cause major threat to the data.

2.1 Cyber Security Threat and Risk (CTR)

Cyber security threats are common nowadays, however, severity pinches vulnerability of data transceive. All vendor and version of Mobile OS somehow allows the installation of malicious software through both authorized and unauthorized apps. Illegitimate apps are a big source for security issues. Even legitimate software can be exploited and attackers succeeded in eavesdrop, phone crash or conduct others. Some of the common security issues that arise in daily activity are considered for analysis:

A - CTR1: Data leakage: a stolen or lost phone with unprotected memory allows an attacker to access the data on it. This is directly accessing the mobile.
B - CTR2: Improper decommissioning: the phone is disposed of or transferred to another user without removing sensitive data, allowing an attacker to access the data on it.
C - CTR3: Unintentional data disclosure: most apps have privacy settings but many users are unaware (or do not recall) that the data is being transmitted, let alone know of the existence of the settings to prevent this.
D - CTR4: Phishing: an attacker collects user credentials (e.g. passwords, credit card numbers) using fake apps or (sms, email) messages that seem genuine.
E - CTR5: Spyware: the smartphone has spyware installed allowing an attacker to access or infer personal data. NB spyware includes any software requesting and abusing excessive privilege requests. It does not include targeted surveillance software.
F - CTR6: Network spoofing attacks: an attacker deploys a rogue network access point and users connect to it. The attacker subsequently intercepts the user communication to carry out further attacks such as phishing.
G - CTR7: Surveillance: spying on an individual with a targeted user's smartphone.
H - CTR8: Diallerware: an attacker steals money from the user by means of malware that makes hidden use of premium sms services or numbers.
I - CTR9: Financial malware: malware specifically designed for stealing credit card numbers, online banking credentials or subverting online banking or ecommerce transactions.
J - CTR-10: Remote Support Tool plug-ins: used by many handset makers. Attackers could exploit it by sneaking a bogus app onto a phone, which exploits the flaw in a way that elevates the attacker's permissions. From that point on, the attacker would have complete remote control over the smartphone. These remote support tools can't be removed by the end user and can only be patched by the network operator.
K - CTR-11: Stagefright: Attackers could exploit the issue by sending a malicious video message to almost any Android handset on the plant, which would execute automatically. Incredibly, no user interaction is needed and the message could even render itself invisible by deleting itself.
L - CTR-12: Forging Digital Certificate: offers a way for a malicious app to hijack the trusted status of a legitimate app through (by forging its digital certificate), effectively escaping any sandboxing security on the device. Though old versions are targeted.
M - CTR-13: An unusual kernel-level flaw affecting something called the futex subsystem. However, not long after it was incorporated into a tool designed to root
N - CTR-14: Third party apps: this offered a novel way of attackers to replace one installer (or APK file) with another one when using third-party app stores, in effect letting a malicious app replace a legitimate one without the user realizing it.
O - CTR15: Network congestion: network resource overload due to smartphone usage leading to network unavailability for the end-user.

2.2 Cyber Security Techniques

There are many ways network providers, device manufacturers, software providers adopt to tighten the security of Mobiles [5], at the same time, hackers also adopt new approaches. Some of the minimum necessary techniques (Tx) to protect the Mobile must be taken care.

T1: Network-based security configurations try to prevent bad packets from arriving the end devices such as Mobiles.
T2: Anti-virus software try to detect already installed malicious software, but damage already caused before detection.
T3: Firewalls filter traffic between untrusted networks and trusted side (user side), but these firewalls have several limitations.
T4: Intrusion Detection System (IDS) installed behind firewall, offline and is focused on detecting and logging security events that affect private networks.
T5: Security Information and Event Management (SIEM) Solutions is a visual dashboard to help analyze logs info from IDS.

We have several options such as Device Cyber Security Software, Firewalls, Intrusion Prevention Systems (IPS), Host-based IPS, Network-based IPS, Unified Threat Management, Scrubbing centers, etc. All these software solutions and strategies focus on out of the box (Man-Mobile) scenarios. This stresses the need to study the Relationships, Activities, Driven Apps that influence the security issues.

3. Structural Relationships

Almost all activities depend on some sort of applications and settings. Applications play an important role in users' experiences with their Mobiles. So, it is important to understand Man – Mobile activity through applications. Structural relationships bind the physical and abstract players and provide more information how the process takes place in the structures. Here, we introduce structural relationships among Man, Mobile, Activity and Data/Apps as shown in Fig. 5

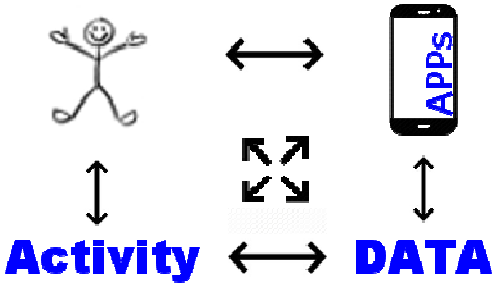

Fig. 5: Relationships among four players

3.1 Relationships

The relationships between Man and Mobile can be written as:

Relations due to Man,
R11: Man → Activity, R12: Man → Data/App, R13: Man → Mobile
Relations due to Mobile,
R21: Mobile → Man, R22: Mobile → Data/App, R23: Mobile → Activity
Relations due to Data/App,
R31: Data/App → Man, R32: Data/App → Mobile, R33: Data/App → Activity
Relations due to Activity,
R41: Activity → Mobile, R42: Activity → Man, R43: Activity → Data/App

If these relationships are omnidirectional then Man can expect control over other three entities, unfortunately, it is not. When it becomes multidirectional, problems increase with the broadcasting information in multi-direction. Besides personal and business need, what causes to trigger activities ? In what situations mobile is used extensively ?

Summary of Situational usage of Mobile in percentage [6] in Fig. 6, shows that more than 60% of Mobile usage is during Waiting, Boring or when Alone.

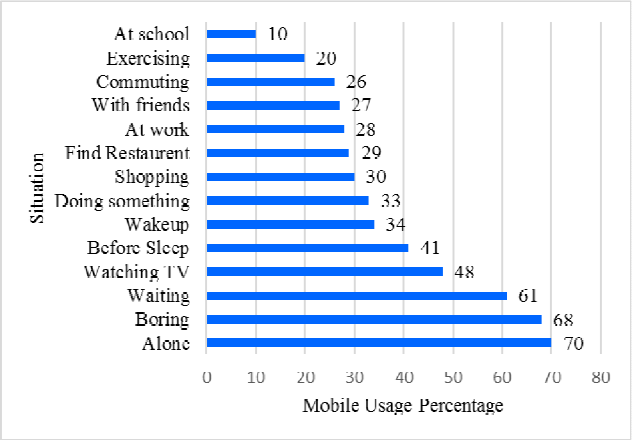

Fig. 6: Situation of Mobile Usage Percentage

Another set of data of that is considered is percent of people trigger applications as frequent activity [Relations due to Activity] in Fig. 7, to show the intensity of the activity and the heavily used applications. If we observe carefully, we will understand the Apps are driving the Activities and Man – Mobile relationship. Which ultimately creates the business need. In the following section, we will observe the popular apps that drive Man – Mobile relationships.

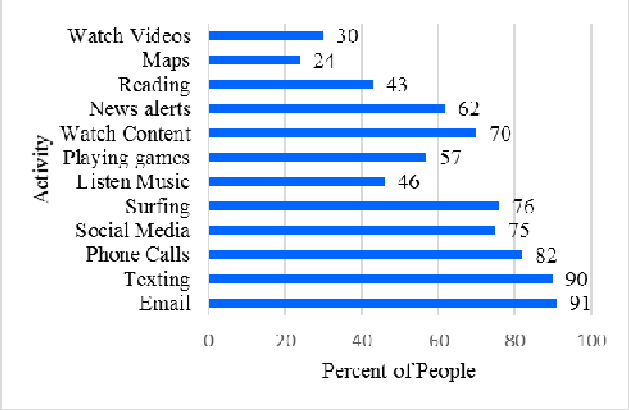

Fig. 7: Percent of people access as daily activity

3.2 Driven Apps

Driven apps are nowadays increasing with the increase of uploaded apps, irrespective of Android or iOS. Mainly these apps can be categorized into: Cost driven (Man), Model driven (Mobile), Activity driven and Data driven. Below figure shows number of people (in millions) use each app in one month (this number changes every month), below data is for May 2016 [7]. This summary shows [Relations due to Mobile] and [Relations due to Data].

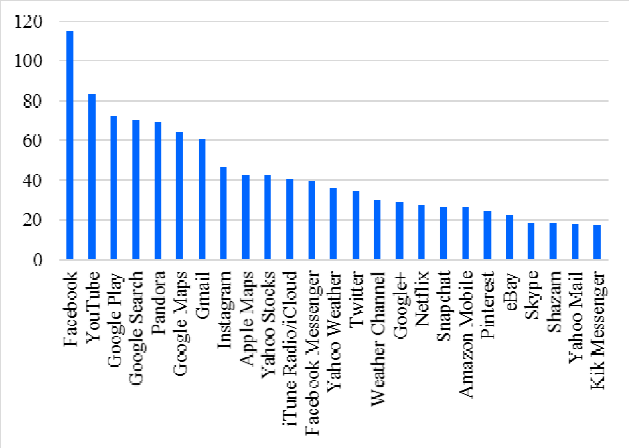

Fig. 8: Popular Apps that are Driving Man - Mobile

With the necessary information collected and described in the above sections, we will present a way of analyzing the information in Man – Mobile – Activity perspective. The information is dynamic and cannot be taken as specific case. Our presentation of risk assessment [8] and statistical analysis can be general and can be applied to any set of numbers.

4. Analysis of Relationships and Security

4.1 The Analysis

The relationship analysis utilizes the information that connects the four players Man, Activity, Data and Mobile. Since the driven apps exaggerate the situation, the block diagram depicted in Fig. 5 shall be modified as shown in below figure, making Data as a flow element among all 4 players. However, the relationships defined in section 3.1 shall be used as is assuming Apps in place of Data.

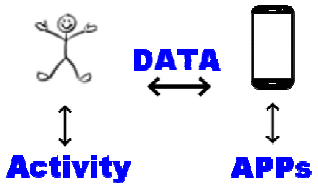

Fig. 9: Relationships Restructured

Our goal is to compute the total risk of each activity by analysis of activities triggered by man on, and analyze them to nullify the hypothesis. Let us now define the risk levels in a table as below.

Table 1: Risk Levels (L)

Risk Level	Points
No Risk	0
Low Risk	1
Medium Risk	2
High Risk	3
Very High Risk	4

Risk Assessment is done below for each Security Issue listed in section 2.1, horizontal are likelihoods and vertical are risk impact.

Very High 4			(I) (J)	(C) (D) (E)	(A) (B)
High 3		(M)	(K)	(F) (G) (H)	
Medium 2			(L) (N)		
Low 1			(O)		
Nil 0					
	Remote 0	Unlikely 1	Possible 2	Likely 3	Almost certain 4

Define Severity = Likelihood * Risk Impact, then we can compute severity in points for each security issue as below.

Table 2: Security issue and its Severity

CRT Issue	Severity
A - CRT1	16
B - CRT2	16
C - CRT3	12
D - CRT4	12
E - CRT5	12
F - CRT6	9
G - CRT7	9
H - CRT8	9
I - CRT9	8
J - CRT10	8
K - CRT11	6
L - CRT12	4
M - CRT13	3
N - CRT14	4
O - CRT15	2

Now we can compute severity in points for each Activity (shown in Fig. 3) as below.

Table 3: Activity and its CTR Severity

Category	Activity	CTRs	Severity Points
Communication	Texting	A+G+H+K+O	42
	Phone Calls	A+B+O	34
	Email	A+C+D+J+K+O	56
	Social Media	A+B+E+O	46
Entertainment	Web Surfing	A+C+F+J+O	47
	Music	A+C+M+O	33
	Games	A+C+M+O	33
	Watching Content	A+C+G+M+O	32
	Shopping	A+G+I+J+O	35
	Reading	A+J+O	26
Functional	Map	M+O	5
	Calendar	A+B+O	34
	Banking	A+B+I+J+L+O	54
Photos	Photos	A+C+O	30

Now let us calculate points due to the relationship among the depicted 4 players and their points. The points are assigned based on the data given Figures.6-7 and Fig. 9.

Table 4: Activity Relationship – Security Risk

Category	Activity	Relations	Scaled Points	CTR Risk
Communication	Texting	R1x, R22, R32, R41, R43	7	294
	Phone Calls	R1, R2, R4	3	102
	Email	R1x, R21, R22, R31, R32 R41, R43	8	448
	Social Media	R1x, R21, R22, R41, R43,	7	322
Entertainment	Web Surfing	R1x, R33, R41	5	235
	Music	R1x, R23, R41	5	165
	Games	R1x, R4x	6	198
	Watching Content	R11, R13, R2x, R41	6	192
	Shopping	R1x, R21, R22, R31, R41	7	245
	Reading	R1x, R23, R41	4	104
Functional	Map	R11, R13, R21, R41, R43	5	25
	Calendar	R1x, R3x, R22, R41, R442	9	306
	Banking	R1x, R2x, R3x, R4x	12	648
Photos	Photos	R1x, R23, R41	5	150

Scaled Points = number of relations involved (each relation carries 1 point).
CTR Risk = Scaled Points * CTR Severity (given in table 3)

4.2 Cyber Security Point Scale Analysis

Plotting the computed data (severity points) for Activity against Cybersecurity, we can identify the high measure of severity for some crucial activities in Email, Texting and Banking.

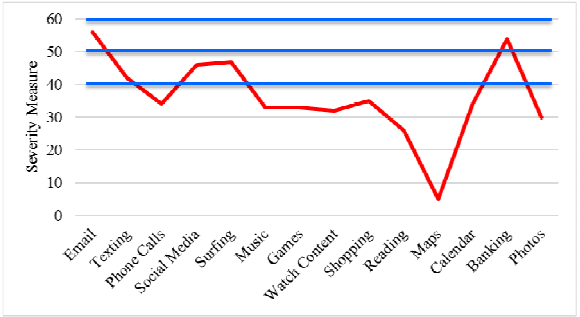

Fig. 10: Activity vs. Cybersecurity Severity

Plotting the computed points (scaled points) for each Activity, we observe that Banking received highest points followed by Email, Texting, Social Media and Shopping.

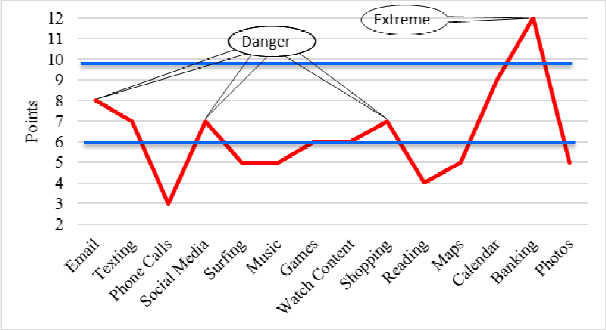

Fig. 11: Activity vs. Point Assessment

Apply Descriptive Statistical analysis to calculate confidence levels for the collected and computed data. Confidence levels for
Activity – Cybersecurity severity and
Activity – Point Assessment are observed respectively as
Confidence level (95.0%) = 7.37389047195695
Confidence level (95.0%) = 1.31287375789882

Since our focus is on activity items which are random selection of Activities, we do have variances of two normal distributions for Cybersecurity severity and Point Assessment, we apply t-test analysis in Two-Sample Assuming Unequal Variances.

t-Test: Two-Sample Assuming Unequal Variances		
	CTR Severity	Activity Points
Mean	36.2142857142857	6.35714285714286
Variance	163.104395604395	5.17032967032967
Observations	14	14
Hypothesized Mean Difference	0	
df	14	
t Stat	8.61197615827795	
P(T<=t) on-tail	2.8736292655E-07	
t Critical on-tail	0	
P(T<=t) two-tail	5.7472585310E-07	
t Critical two-tail	0.69241706957000 5	

From this result, P(T<=t) two-tail (5.747) gives us the probability that a value of the t-Stat (8.612) would be observed that is larger in absolute value than t-Critical two-tail. Since the p-value is larger than Alpha (0.05), we cannot reject the null hypothesis that there is no significant difference in the means of each sample.

4.3 Minimization of Risks and Recommendations

Risk is the expected loss resulting from a threat exploiting a vulnerability existing in Mobile or Smartphone. Risk management process is continuous with options of acceptance, avoidance, transference and mitigation.

Risk = Vulnerability * Threat * Impact Probability
If Loss = Vulnerability * Threat then
Risk = Impact Probability * Loss

In Table.4, CTR Risk is the risk quantified by the activities and relationships. If we can minimize Impact Probability or Loss by implementing some strategies, we can downsize the risk. We will skip this study here and continue in the next paper.

5. Conclusions

Cybersecurity is a Fuzzy network of security problems and solutions. Though several methodologies, approaches and solutions are proposed by various researchers, none of them focused on the Man – Mobile relationships to analyze the security issues. We proposed new methodology, studied and analyzed the Man – Mobile relationships, by statistical methods. These statistical methods usually are applied in population, or action – response observation, but we apply them for security problems.

By introducing the points concept, the severity of security for each activity is computed and it became easy to observe which activity attributes high risk. Considering a particular set of activities in this paper, we observed that Email, Texting, Social Media, Shopping and Banking are high risk activities. Since our methodology can be generalized by changing the set of activities of interest, one can compute the risks involved thereof.

By changing the CTRs in Table. 3 and Relations in Table. 4, we can derive new set of results in the given analysis method. This paper can be extended to study the risk minimization and mitigation strategies, do analysis, and can be generalized by changing the sets of activities.

Acknowledgments

The research was sponsored by R&D Grant from RAMTEJ Technologies Corp., Grant No. RDIT-01-2017. Authors express gratitude to the sponsors.

References

[1] Cesar Cerrudo "Why Cybersecurity Should Be The Biggest Concern Of 2017", Forbes Technology Council, Jan 2017.
[2] "Cyber Security: Considerations and Techniques for Network-Based Protection", an Industry Whitepaper, Sandvine Incorporated ULC, 2016.
[3] "Which Activities Do Smartphone Owners Prioritize on Their Devices?", Marketing Charts staff, Feb. 2016.
[4] Paul Ruggiero and Jon Foote, "Cyber Threats to Mobile Phones", US-CERT, Carnegie Mellon University, 2011.
[5] Robertas Damasevicius Rytis Maskeliunas, et. al., "Smartphone User Identity Verification Using Gait Characteristics", MDPI, pp.1-20, Vol.8, Symmetry 2016.
[6] "Situational Usage of Mobile Applications?", Marketing Charts staff, Nov. 2016.
[7] Fox Van Allen "Top 25 Smartphone Apps Revealed", Techlicious, Technical Report, Aug 2016.
[8] David Frei, "Conducting a Risk Assessment for Mobile Devices" Information Systems Security Asso., May 2012.

First Author Rao received bachelors and masters in Mathematics from Andhra University, advanced masters from Technical University of Kaiserslautern and Doctorate from Hiroshima University. He worked as Lecturer, Engineer and coordinator for companies and Universities both in India and Japan. His main research interests focus on applications of technology to society. Other interests include developing strategies for technology development. He is a life member in many professional organizations. He published paper in interdisciplinary areas of Mathematics, Computer Science, Electronics and Sociology. He received best faculty award from SITAM Engineering College, India. He is currently focusing on Cybersecurity problems.

Second Author Mukai received bachelors and masters from Hiroshima City University. He has been with Fuji Soft Co. Ltd., as Manager of Software Division. His research interests include development of good smartphones and manage technical human resources. He is currently focusing on business development strategies in smartphone arena.

Third Author Gottumukkala is a retired professor of engineering mathematics. His served Andhra University for 45 years and now research advisor. His research interests focus on engineering applications for society. He is currently focusing on developing methodologies for social change through technology.