International Journal of Mobile Communications

ISSN online: 1741-5217 - ISSN print: 1470-949X
https://www.inderscience.com/ijmc

Requirements analysis of security and privacy of mobile payments - Indian context

Thiruvaazhi Uloli, G. Sudha Sadasivam, R. Arthi

DOI: 10.1504/IJMC.2022.10041532

Article History:

Received:	02 March 2020
Accepted:	12 May 2021
Published online:	04 October 2022

Requirements analysis of security and privacy of mobile payments – Indian context

Thiruvaazhi Uloli*

Department of Information Science and Engineering,
Kumaraguru College of Technology,
Coimbatore, Tamil Nadu, India
Email: thiruvaazhi@gmail.com
*Corresponding author

G. Sudha Sadasivam

Department of Computer Science and Engineering,
PSG College of Technology,
Coimbatore, Tamil Nadu, India
Email: sudhasadhasivam@yahoo.com

R. Arthi

Department of Computer Science and Engineering,
Kumaraguru College of Technology,
Coimbatore, Tamil Nadu, India
Email: arthi28894@gmail.com

Abstract: Mobile payments, while displaying improved adoption, are limited by security and privacy concerns. An appropriate treatment of these risks has the potential to further spur up the utility of the system. The essential step towards this is to systematically analyse the security and privacy requirements. This paper presents the outcome of a systematic risk analysis both from the perspective of reported attacks, as well as from the inherent vulnerabilities of the mobile application software. Attack probabilities, its impact, analysis of the code and permissions of the mobile payment app and its comparison with that of spyware designed to compromise privacy, have all been used in this process. Given that identity and authentication are necessary to derive the utility, and pure anonymity cannot be of help in this context, the need is to provide the necessary utility while addressing the security and privacy risks. The requirements towards security and privacy that need to be met, to design such a system has been arrived from this and presented for the mobile payment ecosystem, and the same has the potential to be used appropriately in related contexts.

Keywords: utility; security; privacy; digital payments; mobile payments; risk assessment.

Reference to this paper should be made as follows: Uloli, T., Sadasivam, G.S. and Arthi, R. (2022) 'Requirements analysis of security and privacy of mobile payments – Indian context', *Int. J. Mobile Communications*, Vol. 20, No. 6, pp.639–658.

Biographical notes: Thiruvaazhi Uloli is a researcher and a faculty at the Kumaraguru College of Technology, Coimbatore, India and currently heads the Information Science and Engineering Department with a Master's in Computer Science and Engineering and Bachelor's in Electrical and Electronics Engineering. He completed his Postgraduate Program in Data Science and Machine Learning (PGPDM) from the University of Chicago and is currently pursuing his PhD in Computer Science. His research interests are in understanding the relationships between utility, security and privacy of information and maximising them. He has been conferred Certified Information System Security Professional (CISSP) and Certified Secure Software Lifecycle Practitioner (CSSLP) certifications by International Information System Security Certification Consortium (ISC2). He is also a Certified Product Manager by Association of International Product Marketing and Management (AIPMM). He is a life member of Cryptology Research Society of India (CRSI), ISC2, Cyber Society of India, Institute of Product Leadership, and AIPMM.

G. Sudha Sadasivam is a Professor and the Head of Computer Science and Engineering at PSG College of Technology, Coimbatore, India.

R. Arthi is an alumnus of Kumaraguru College of Technology, Coimbatore, Tamil Nadu. She has completed her Master's in Computer Science and Engineering from there.

1 Introduction

Recent reports on surveillance through Pegasus delivered through popular applications like Whatsapp (ANI, 2019), phishing alerts from Google (Ajmal, 2019) over email with valid credentials both purportedly initiated by government agencies, and Microsoft alerts of raising spear phishing attacks (Microsoft, 2019), have thrown open the debate of security and privacy to a larger audience, though people in the security community have been aware of the debate since long. This does not mean that people should put an undue limit on using mobile applications and emails, since both have immense utility value that people very much need. Instead, we would like to maximise the utility, while addressing the security and privacy requirements of information systems that we use. This requires specifying the requirements of essential attributes of security and privacy based on a systematic analysis. Doing this will require us to narrow down the requirements to a specific domain of interest. Towards this we analyse in this paper, the requirements of security and privacy of digital payments domain, and more specifically that of mobile payments in India and arrive at the requirements specification.

1.1 Motivation

Given the context of increasing penetration of smart phones, the digital India initiative foundations laid, the migration to digital payments pushed initially by the demonetisation in India and further forced by the pandemic situation, a systematic analysis of risks in the system is warranted. This work is motivated at the following two levels:

a Specifically, to systematically analyse the security and privacy risks of using mobile payment applications which is demonstrating high impact utility.

b More generically, to precisely arrive at the security and privacy requirement specifications that has the potential to drive useful solutions across domains. This is the larger objective of this work.

1.2 Review of literature

Shin (2010) empirically evaluates the relationships of security, privacy, usefulness, and other attributes in acceptability of ubiquitous computing. Narrowing down to the domain of mobile commerce (Liu and Li, 2019) shows how user trust positively influences the purchase intention towards mobile commerce. There are number of works that explore the problems of smartphone security including Thiruvaazhi and Arthi (2018) and Taleby Ahvanooey et al. (2017).

Specifically on mobile payments, Tellez and Sherali (2014) and Wang et al. (2016) categorise mobile payment systems and further identify and discuss mobile payment security threats and challenges. Bosamia (2017) surveys popular mobile wallet applications in India and gives a high-level view of its security threats and vulnerabilities. Kang (2018) discusses trends of mobile fintech companies and introduces broad requirements and security challenges of mobile fintech payment services.

On privacy of mobile payments, Sahnoune et al. (2015) identify critical factors that impact privacy disclosure in mobile payments and discuss customer expectations. Yang et al. (2015) show perceived financial risk, privacy risk and performance risk as the sources that influence acceptance of mobile payments. Further, Johnson et al. (2018) show empirically that security and privacy concerns of users impact mobile payment adoption.

There has been some work done in the analysis of security and privacy of other domains. Papageorgiou et al. (2018) have analysed and reported that several apps have been found to violate data protection regulations compromising user privacy in addition to insecure programming practices. Patsakis et al. (2015) have analysed mobile dating applications and have found that simple interception attacks could reveal very sensitive user personal information. Chu et al. (2018) have analysed children's IoT-based toy applications and have discovered similar vulnerabilities that violate privacy policies as well as compromise critical IoT security.

While it is seen from the literature that there are perceived risks from the vulnerabilities, threats, attacks, and the impact it has caused, the analysis needs to be further deepened systematically to crystallise the specification of the security and privacy requirements.

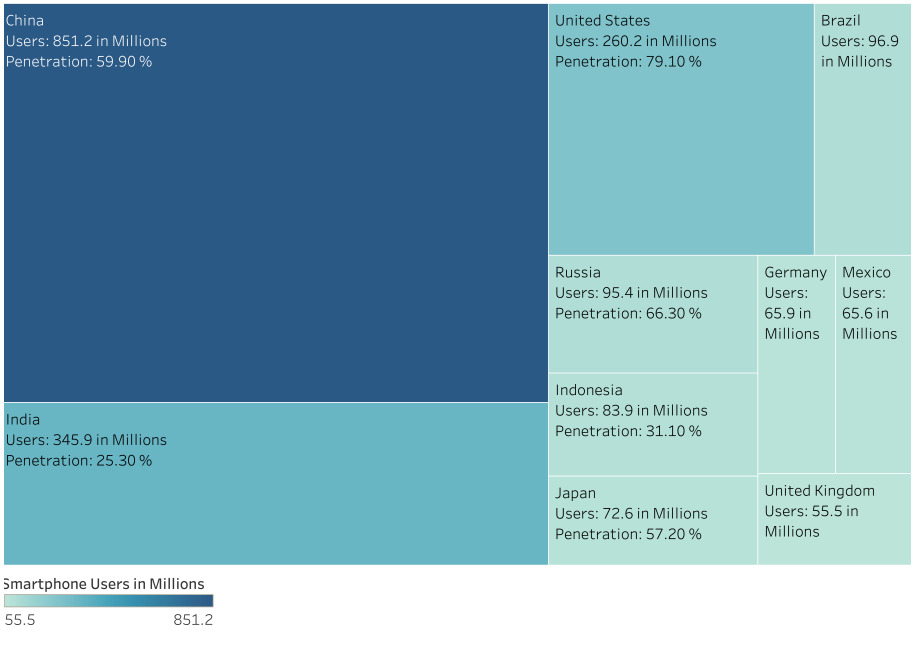
The rest of this paper is organised as follows to do and present that for the case of mobile payments. In Section 2, the rapidly growing significance and utility

of mobile payments are illustrated with data visualisations. Section 3 introduces the risk assessment approach used. Section 4 presents the security risk assessment of digital payments and the security requirement for mobile payments inferred from Section 4 is specified in Section 5. The context for analysis of security and privacy of mobile applications is presented in Section 6. Sections 7 and 8 present respectively the implications to security and privacy through the analysis of mobile applications. Section 9 concludes with precise requirement specifications for security and privacy of mobile applications. The last three sections discuss implications, limitations, and future scope of this work.

2 Utility of mobile payments

Newzoo's Global Mobile Market Report 2019 (Newzoo, 2019) has listed the top countries in terms of smartphone users. A tree map of top 10 countries is shown in Figure 1.

Figure 1 Smartphone users penetration % – top 10 countries (see online version for colours)



We can see that India has the second largest number of smartphone users in the world. Additionally, the smartphone penetration is just 25.3% with number of users at 345.9 million. Another joint study by Assocham-PwC (Assocham, 2019) reports that the number of smartphone users in India is growing at a compounded annual growth rate of 12.9%. These and other such reports (KPMG-Report, 2019) give us a clear perspective of the huge growth potential of businesses based on smartphone usage.

In this context it is pertinent to look at the India's payment system indicators released by Reserve Bank of India (RBI, 2019). The growth trends of total payment

systems, mobile payments and e-wallet payments both in terms of volume (number of transactions) and value is shown in the trend plots Figures 2 and 3.

Figure 2 India payment – volume indicators 2013–2019 (see online version for colours)

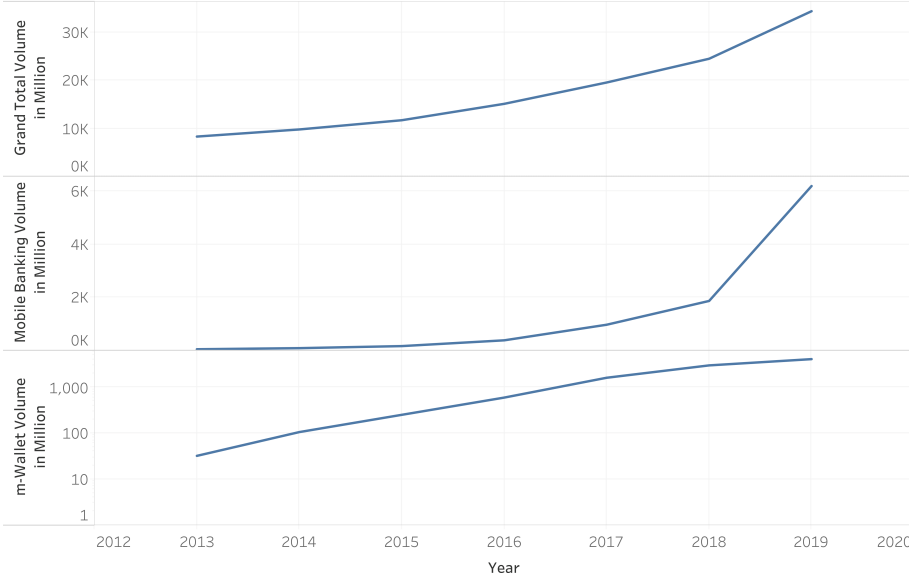
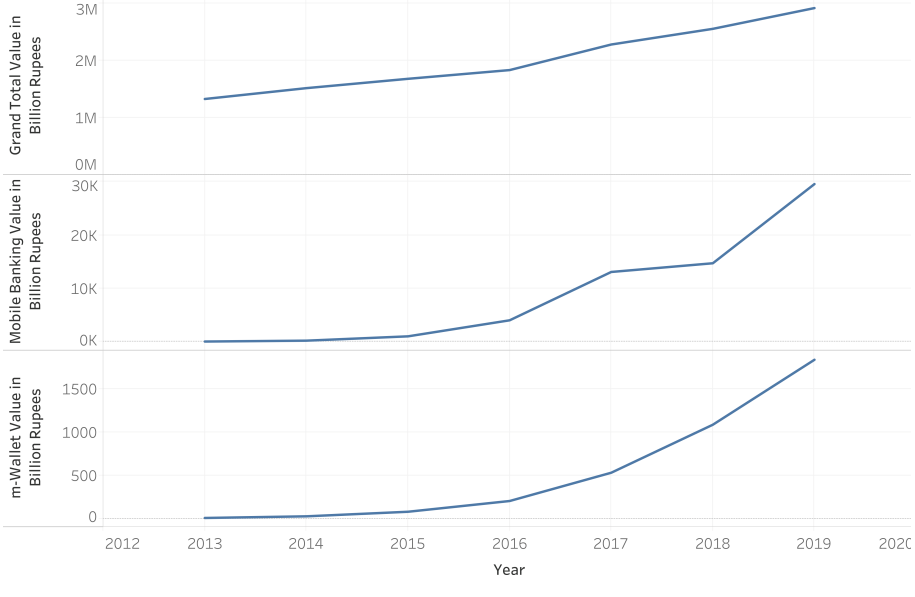


Figure 3 India payment – value indicators 2013–2019 (see online version for colours)



As seen in Figures 2 and 3, the growth of mobile payments and m-wallet payments have been showing an exponential growth ever since 2016 when demonetisation happened in India. Recent announcements by government on boosts for digital payments

(Financial Express, 2019) through waivers on merchant discount rate also give positive indications for such a growth momentum. Smartphone-based payments should continue this growth journey for years to come, given the context of similar trends exhibited in the smartphone users and the potential shown by the smartphone penetration percentage. The exponential growth trend of payments based on smartphone is a valid proof for the utility of mobile payments, without which such a growth could not have happened. The intents towards the use of mobile payments have been studied in other works (Liébana-Cabanillas et al., 2017; Madan and Yadav, 2016). Hence without further analysis of evident utility of the mobile payments, we shall move on to the analysis of its security and privacy.

3 Approach

While there are many methods of assessing risk in different contexts, we follow the ISO/IEC 27005 Information Security Risk Management Guidelines (ISO-IEC, 2018), for the process of assessing the security risks of digital payments. We identify key assets of the system, estimate the probabilities and impacts of possible attacks on it. We evaluate the risk based on the probabilities of occurrence of attacks and their impacts, prioritise them, from which we deduce the security requirements for the digital and mobile payment systems. Further to this we do static analysis of the popular mobile payment apps and from that we finalise the security and privacy requirements for mobile payment systems.

4 Security risk assessment of digital payments

Mcafee (Samani et al., 2019) reports that in 2017 there was a 77% increase in mobile Trojans which got further accelerated in 2018. Verizon's 2019 data breach investigations report (Verizon, 2019) states that 71% of breaches were financially motivated. In this environment it is essential to assess the risks of digital payments in general and move further specifically into that of mobile payments. The outcome of the risk assessment of digital payments in India has been captured in Table 1. Table 1 has been split into two pages for better readability. The process of arriving at the risk assessment is as shown in Table 1. We started with a detailed study of attack trends and its ranking from authentic security reports. Within that we shortlisted the attacks that targeted the financial sector and payment systems. For each of the attack vector we identified the key assets which could be the total bank balance, or mobile banking limit or credit limit or wallet balance, etc. as the case may be. The total bank balance would be the asset value that is being targeted by a phishing attack. We then evaluated the impact% of each of attack based on an assessment of how much of asset value will be exposed by the corresponding attack vector in the eventuality of a successful attack, which is specified in Table 2.

The eventuality must be quantified as the probability of occurrence of attack. We arrived at this from the assessment of vulnerability and the threat for each attack vector. It is this combination of weakness of the system (vulnerability) with the probable danger of attack (threat) that contributes to an actual attack which impacts the system with a loss of asset value.

Table 1 Risk assessment of digital payments

Attack vector	*Asset*	*Asset value description*	*Impact %*	*Authentication parameters*	*Vulnerability description*	*Vulnerability %*
Phishing attack on internet banking	Account balance	Bank account balance value	90	Username, password	Entering authentication credentials on phishing server	80
Mobile banking Trojans	Mobile phone, wallet balance	Mobile banking balance value or limit	80	MPIN, fingerprint	Malicious apps on the same mobile	80
Skimming of ATM/debit/credit card – PoS	ATM card, debit card, credit card	Card balance value or limit	70	PIN	Possible cloning	70
Computer malware attacks on internet banking	Account balance	Bank account balance value	90	Username, password	Authentication credentials lost	60
Social engineering attack on m-wallets	Phone, wallet account balance	m-wallet balance value or limit	40	MPIN	Weak authentication parameters based on data that can be mined from other sources	70
Device theft targeting mobile banking	Mobile phone, account balance	Mobile banking balance value or limit	80	MPIN, fingerprint	Easy access to Target Mobile	60
Credit/debit card theft through spam emails	Credit limit	Card balance value or limit	70	Card #, validity, cvv	Unverified receiver	50
Device theft targeting m-wallets	Card	m-wallet balance value or limit	40	MPIN	Mobile without adequate authentication	60
DDoS attack on internet banking	account balance, stock trade	Non-availability of funds, stock trading	30	Username, password	Non-availability of service	70

Table 1 Risk assessment of digital payments (continued)

Attack vector	*Threat*	*Threat details*	*Reference*	*Threat %*	*Probability of attack*	*Risk %*	*Risk classification*	*Current risk mitigation mechanisms*
Phishing attack on internet banking	Phishing	Phishing attacks continue to be on the rise	Akamai (2019)	50	0.4	36	High risk	• Awareness • Antiphishing services • Proper validation of ssl certificates
Mobile banking Trojans	Mobile Trojans, mobile ransomware	Fake apps and mobile Trojans are increasing in complexity and scope. Mobile ransomware increased by 33% in a year	McAfee (Samani et al., 2019), Symantec ISTR 2019 (Symantec, 2019)	45	0.36	28.8	High risk	• No rooting or jailbreaking mobile OS • Antivirus to detect and remove spy software • Granting least privilege to mobile apps
Skimming of ATM/debit/credit card – PoS	Skimming and spoofing	Combination of skimming and spoofing believed to be behind large-scale skimming attacks	Ladika (2019) and Knowles and Pistone (2019)	35	0.245	17.15	Medium risk	• Awareness • Further improvements like chip pin card and multi-factor authentication
Computer malware attacks on internet banking	Credential stuffing master lists	Akamai Financial Services Attack Economy Research Report 2019	Akamai (2019)	30	0.18	16.2	Medium risk	• Sandboxing using safe payment mechanisms • OS level and antivirus protection • Multi-factor authentication
Social engineering attack on m-wallets	Social engineering	Symentac 2016, identities stolen by Social engineering in 2016 is 64%. IDnow 2019 Report: in 2019 social engineering tops the list of most common fraud attempts	Symantec ISTR 2017 (Symantec, 2017), IDNow 2019 Security Report (IDnow, 2019)	40	0.28	11.2	Medium risk	• Awareness • Multifactor authentication
Device theft targeting mobile banking	Phone stealing and breaking in authentication	Symantec ISTR 2017 reported, loss or theft of device breach 31% of payment related data	Symantec ISTR 2017 (Symantec, 2017)	20	0.12	9.6	Low risk	• Lock • Find and erase • Encrypted storage
Credit/debit card theft through spam emails	Spam	Symantec reported by 2017 55% spam mail get increased	Symantec ISTR 2018 (Symantec, 2018)	20	0.1	7	Low risk	• Awareness • Spam filters • Antispam services
Device theft targeting m-wallets	Phone stealing and breaking in authentication	Symantec reported, loss or theft of device breach 31% of payment related data	Symantec ISTR 2017 (Symantec, 2017)	20	0.12	4.8	Low risk	• Lock • Find and erase • Encrypted storage
DDoS attack on internet banking	DDoS attack, disruptive and destructive malware	Ransomware, other malware with DDoS as smokescreen	Accenture (2019) and Akamai (2019)	20	0.14	4.2	Low risk	• DDoS resolution services by vendors

Table 2 Asset impact %

Asset value description	*Impact %*
Bank account balance value	90
Mobile banking balance value or limit	80
Card balance value or limit	70
m-Wallet balance value or limit	40
Non-availability of funds, stock trading	30

In order to arrive at the vulnerability of the system against each of the attack, we analyse the authentication mechanisms and the way these have been compromised by the reported attacks and evaluate the vulnerability. For example, Akamai (2019) reports phishing as the top attack on the banking system. It is very easy for the user to mistake the login page of a phishing site to be that of the bank site, unless the user is aware about the methods to verify the validity of the SSL certificate of the bank. In addition to that the user needs to be sure to know and use the authentic URL of the bank for login and not use the URLs from unauthentic sources like a generic web search. From this reasoning and the analysis of Akamai (2019) the vulnerability value has been assigned as 80% for phishing. The same process has been followed for assessing the vulnerability % against each attack vector.

Quantification of threat need to be based on projection of real incidents within an acceptable margin of error given the uncertainties involved in the context. Towards this we analysed inputs for such an assessment from variety of authentic threat reports released by variety of reputed agencies. We then shortlisted the top 10 threats and evaluated threat from them. For example, phishing threat has been assessed at 50% as it is a top threat according to several reports. We grouped attacks on assets with marginal difference in asset value, vulnerability and threat like that of skimming attacks on ATM/debit/credit cards.

Based on the outcomes of above computations, probability of occurrence of attack (attack probability) was computed by multiplying vulnerability and threat. Finally, risk was computed by multiplying attack probability and Impact. The resultant risk assessment table was then reordered in descending order of risk. Risk against each of the attack vectors was then categorised into one of high/medium/low risk as per Table 3.

Table 3 Risk category

Risk %	*Risk category %*
1 to 10	Low risk
10 to 19	Medium risk
19 to 29	High risk

Vulnerability and threat assessments were done not only based on reports, but the feasibility of the key attacks (phishing, spam, mobile Trojans, social engineering, stolen phone) were also ascertained through experimental validation by appropriate hacks in lab environment. We tested our own payment systems against each of these attack vectors and used the insights to tune and validate the quantifications that we present in Table 1. While this paper focuses on arriving at the requirement specification, a solution to which

could fix the underlying causes of these attacks for the long term, in this work we present the mechanisms that could be used meanwhile for current risk mitigation. The final risk assessment plot showing the risk classification and its relationship with attack probability and impact is in Figure 4.

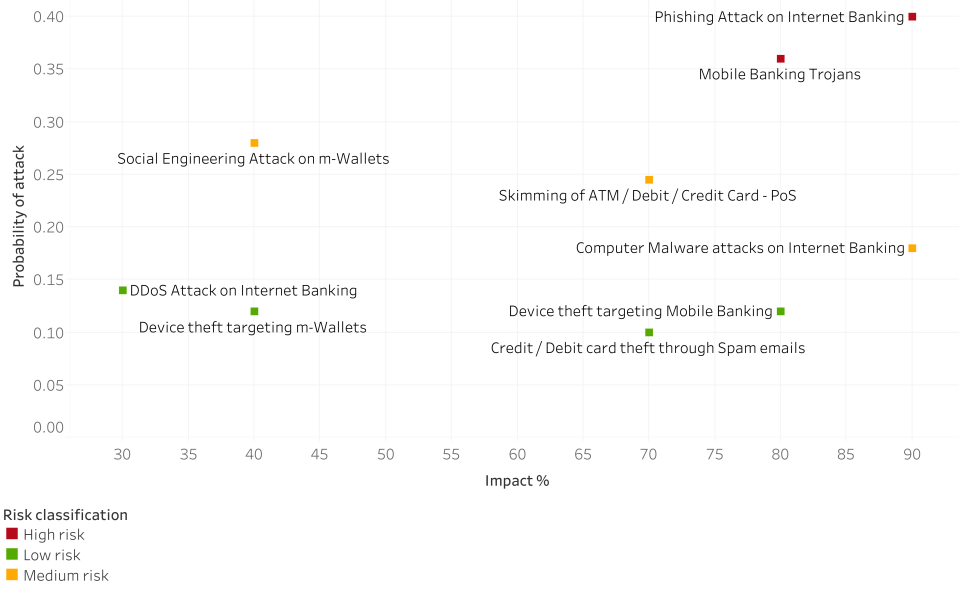
5 Inference of security requirement for mobile payment systems

The risk assessment of Figure 4 shows the following as the top high risks in terms of security of digital payment systems:

- phishing attacks on internet banking
- mobile banking Trojans.

Phishing attacks on internet banking is also applicable to mobile banking owing to the reported large-scale phishing attacks on mobile phones (Phishlabs, 2019) which includes SMS phishing or smishing.

Figure 4 Security risk assessment – digital payments (see online version for colours)



These two high risk threats apply completely to our narrowed down study on risks of mobile payments. Even if we extend the scope and consider all the top 10 threats on the digital payment systems, we see that essentially the goal of the attacker is to get the authentication credentials. Hence any solution that can be expected to comprehensively address the security requirements against such threats should have the following property:

- Prove authenticity of the transaction without explicitly sharing the knowledge of the authenticator.

Until this point, risk analysis from the attack probabilities based on reported threats and the impacts that they could have, has been presented. We shall now look at security and privacy risks to mobile payments through the vulnerabilities of the mobile payment application software.

6 Security and privacy of mobile payment applications

In order to understand the security and privacy of mobile payment applications in terms of software vulnerabilities, we picked up nine popular mobile payment apps and one known spyware (referred to with name SPY in this paper) for us to understand by comparison. The app names have been codified with names A to I without any particular mapping relationship, so as to not disclose their actual identities. The chosen spyware can pass on, to the corresponding cloud account, most information that the authorised user of the mobile device has access to by using the mobile phone. This includes contacts, call logs, messages, key stroke logs, all files on the phone including multimedia files. If the phone is rooted, it even has access to social networking messages (which goes out of the phone as encrypted text but remains as clear plain text in the end device). Further it can even access microphone and camera using which the environment surrounding the mobile phone can be captured and transmitted digitally on to the cloud account of the spyware. The account owner of the spyware configured on the smartphone can get to know all this information of the victim context from anywhere in the internet.

For analysing the mobile apps, we performed static analysis of them using the Mobile Security Framework (MobSF) (Abraham, 2019). For analysis of security we did code analysis of the apps and for analysing the implications for privacy we did permission analysis of the apps.

7 Assessing security of the mobile apps

Code analysis for security is based on the Open Web Application Security Project (OWASP) vulnerabilities list. OWASP periodically comes up with top mobile application security vulnerabilities, the latest being 'The Mobile Top 10 2016' (OWASP, 2019). Code analysis on each of the apps revealed vulnerabilities corresponding to common weakness enumeration (CWE) list (MITRE, 2019) and the category of the OWASP mobile top 10 vulnerability. Figure 5 is a summary of the comparison of top mobile application security vulnerabilities, with the number corresponding to CWE list/OWASP mobile top 10 ranking. Brief explanation of each issue has also been provided. For example, most of the apps analysed reads from and writes into the external storage, when the latter can also be accessed by any other app of the mobile device. This is a high severity risk corresponding to CWE number 276 and OWASP insecure data storage M2 ranking.

Similarly, we see many high severity application security issues listed in the figure, which could be potentially misused. Further the vulnerabilities for each of the mobile apps have been quantified using the geometric mean of the common vulnerability scoring system (CVSS, 2019) of each of the vulnerabilities detected and the results are presented in Table 4.

Figure 5 Mobile application security issues (see online version for colours)

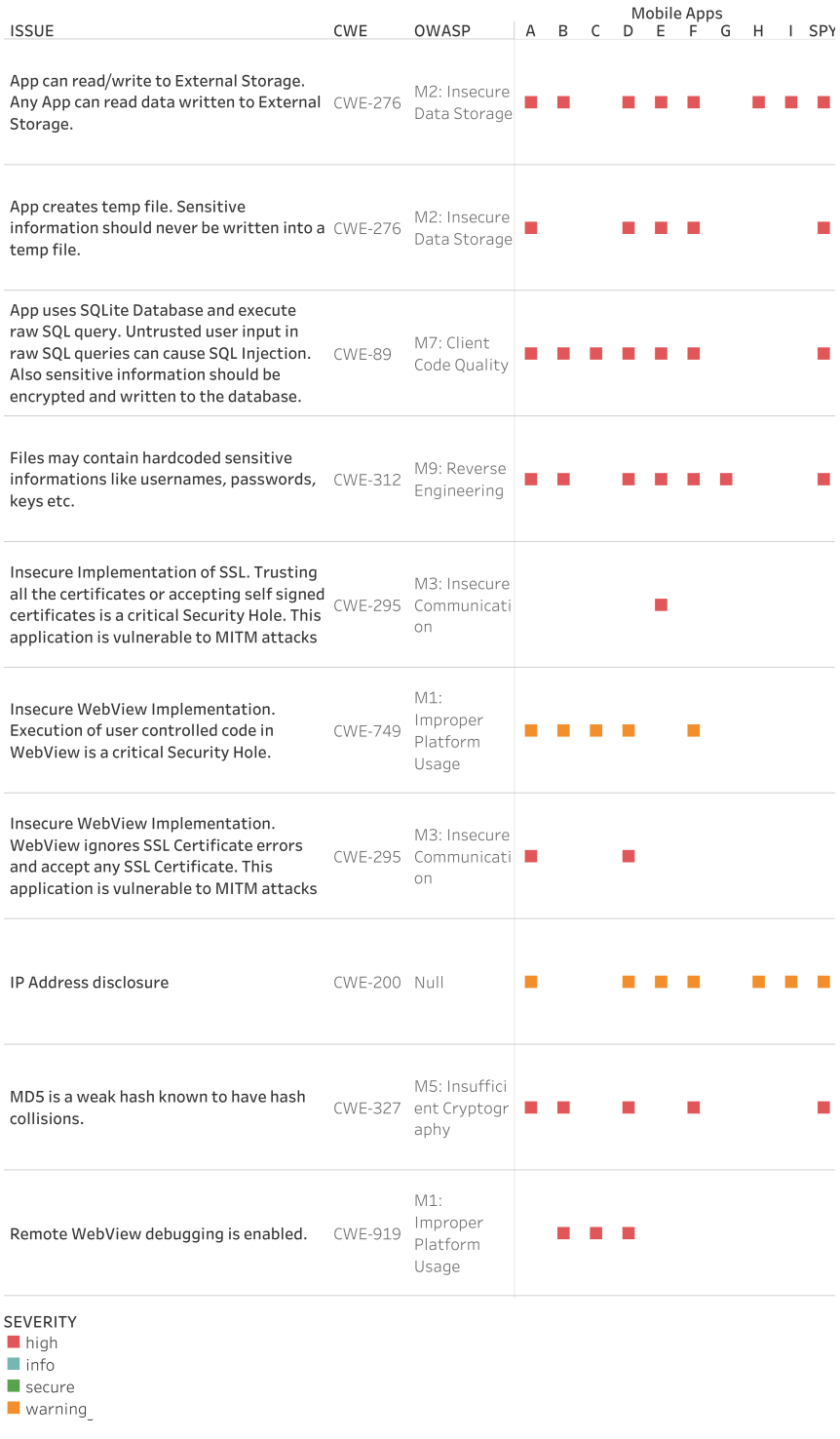
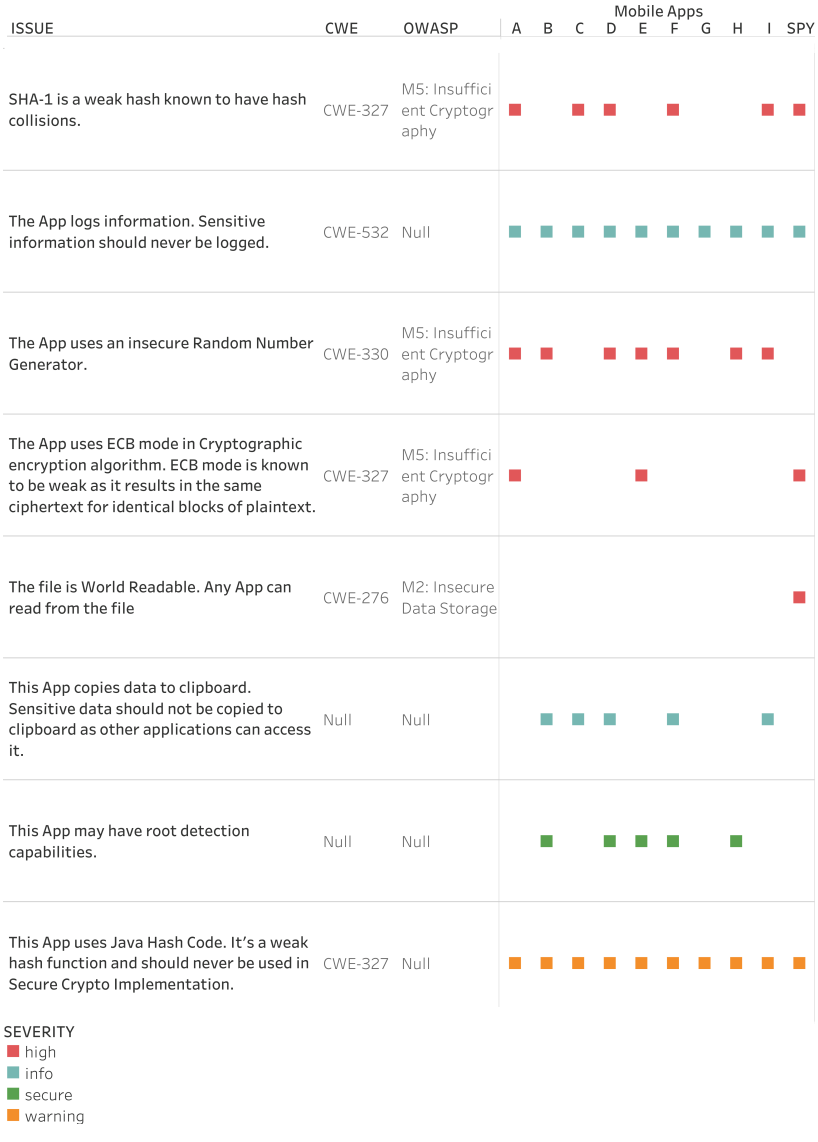


Figure 5 Mobile application security issues (continued) (see online version for colours)



Scores range from 0 to 10 with 10 being most severe vulnerability. We can see that the average CVSS score of all these apps fall in the medium risk category which range from 4 to 6.9 and cannot be accepted as such, without appropriate risk treatment. We should also note that there is no significant difference between the mobile payment apps amongst themselves as well as in comparison with spyware, as the issue here is about the security of the code against attacks from outside of these apps.

We have already captured the essence of the security requirement in our generic risk analysis from the threat perspective, and a solution to that will also mitigate the impact of a possible attack that exploits the mobile application security vulnerability. In addition to that, since the analysis points out to CWE-276/M2 – insecure data storage, wherein

the confidentiality of the data accessible to the mobile app including the authentication credentials is vulnerable, the following requirement needs to be added:

- The authentication credentials need to be stored in a confidential trusted vault and the credentials themselves cannot be moved out of it, excepting the processed responses which does not leak the knowledge of the authenticator enough to cause a successful attack.

Figure 6 Mobile apps – permissions comparison (see online version for colours)

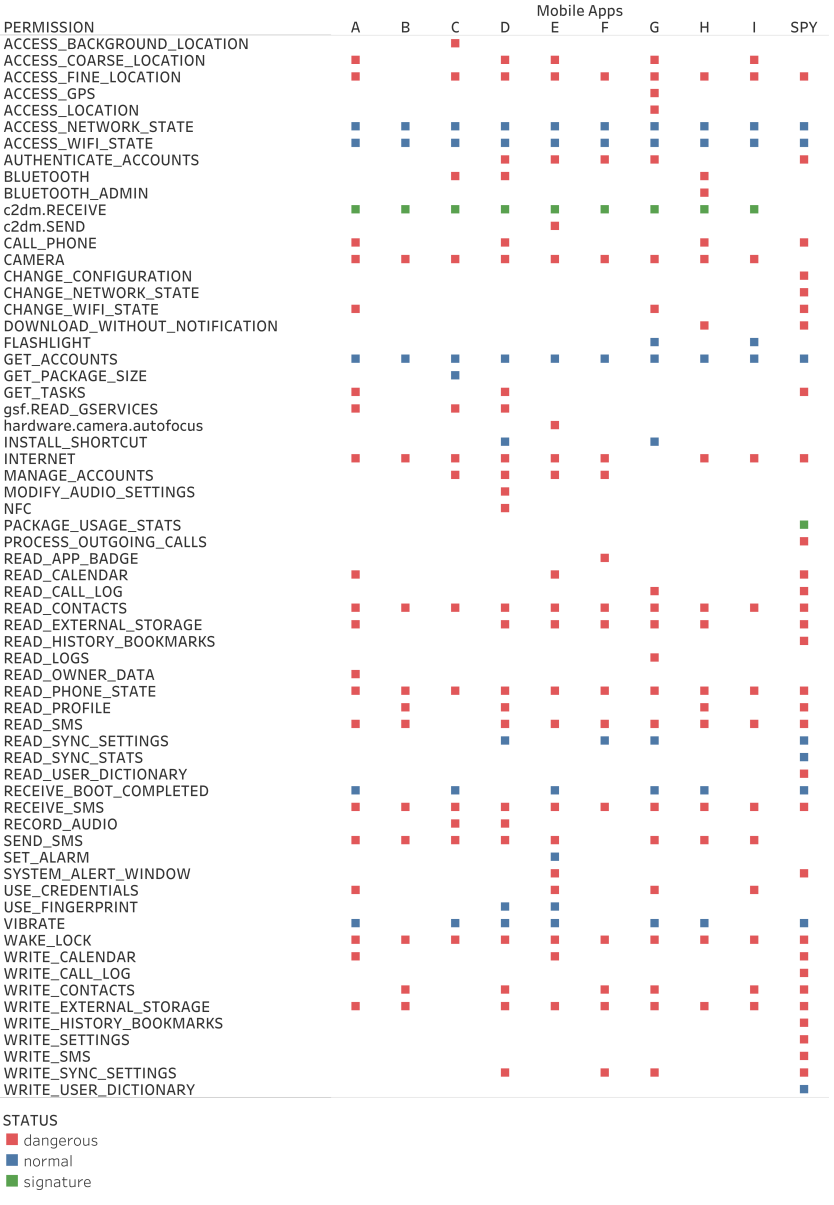


Table 4 Mobile apps CVSS score

Mobile apps	*Average CVSS score*
A	6.3
B	6.4
C	5.4
D	6.2
E	5
F	5.8
G	6
H	5.4
I	5.8
SPY	5.6

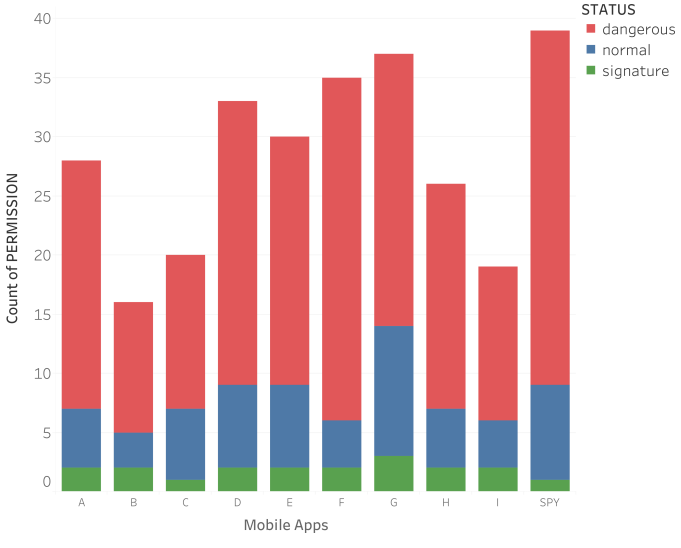
8 Implications to privacy by permission analysis of mobile apps

Cynthia Dwork's work on differential privacy (Dwork, 2006), and subsequent works in that direction, though focused on statistical databases, has made it clear that there will be no significant utility if we cannot even trade-off a small amount of privacy loss. Hence the focus is not on perfect privacy but to have some means for analysing and specifying the requirements for privacy, while satisfying the mandatory requirements for receiving the utility from the system. The task becomes more complex as the acceptable levels of trade-off between privacy loss and utility gains vary for different people at different contexts. Hence to have a valid analysis of the privacy requirements with a common comparative basis, we choose the analysis of the permissions sought by the mobile apps, as it can capture the attack surface of these apps on the privacy of the user and the same can be obtained for any given mobile app. Figure 6 shows the permissions sought and obtained by each mobile payment app during its installation and use, and the comparison of the same with that of the spyware.

The permission comparison shows that most of the mobile payment apps analysed, has got permission to access location, camera, contacts, read/write SMS, read/write external storage, etc. It can be argued that each of these permissions has a utility value in terms of a service to the user. But we need to compare with the privacy violations of the spyware with similar access permissions, to understand the risks to privacy. Figure 7 shows the aggregated count of dangerous, normal and signature permissions of each mobile payment app and the spyware.

We can infer from the comparisons in Figures 6 and 7, that with the permissions being provided, much of the privacy violating tasks such as that done by the spyware are potentially technically feasible through these mobile payment apps as well. This is not only because the mobile payment provider can potentially misuse. Even when the payment provider is assumed to protect privacy, since the mobile apps themselves are vulnerable to attacks from outside, some malicious third party can potentially compromise the system through the mobile application vulnerability and thereby access the mobile phone and compromise the privacy of the user.

Figure 7 Permission analysis of mobile payment apps – count of dangerous, normal and signature permissions (see online version for colours)



Given the above, the requirement therefore for privacy should be:

- The payment application should be given the least privilege necessary to provide the mobile payment utility

Though we have arrived at this from the analysis of permissions, providing the least amount of permissions necessary for the utility does not suffice for privacy. Even if the authenticator is not shared, the corresponding identity information is proven to the payment provider and is known to any entity who has enough privileges to access what the payment provider knows. The knowledge of the personally identifiable information, in itself, can be used to compromise privacy, by associating it with the person or his/her activities. There are different pseudo identities with differing levels of binding with the actual person like the person's name (strong binding), mobile number, etc. to an anonymous public key (weak binding).

Hence in addition to the above requirements the following should also be a requirement:

- The binding between the user credentials known to the payment provider and the actual personal identity should be as minimum as required to derive the mobile payment utility.

9 Conclusions

The data trends, policy initiatives and the potential market show a definite growth for the mobile payment industry. The increasing adoption of the same by people as reflected in the transaction data show the perceived utility of the mobile payment system. The concerns that remain to be addressed were the security of the system and the privacy of

the user. This paper analysed the risks to security and privacy through a systematic risk analysis; both from the attack probability and impact perspective, as well as from the mobile application vulnerability and permission perspective. Following is the summary of the security and privacy requirements from this analysis:

- *Security requirements*
  1 use an authentication mechanism that proves the identity without leaking the knowledge of the authenticator
  2 store and process the authenticator in a trusted vault.
- *Privacy requirements*
  3 the application should be designed to seek and use the least privilege necessary for providing the utility
  4 the binding between the utility application's user identity and the private personal identity should be the minimum necessary to provide the utility.

The above could be generalised to an appropriate extent to other applicable systems, where necessary.

10 Implications

If mobile payment systems are designed to meet the above requirements the following could be the key benefits. Addressing the requirement 1 ensures that even if the server entity and the client-server channel is compromised, no knowledge of the authenticator is compromised. For example, phishing attack will not be effective in such a case, as no information like password is shared by the user to the server yet satisfying the authentication requirements. Solution to requirement 2 would assure that the authenticator is safe when stored and processed at the client end. For example, mobile Trojans or spywares cannot access the authenticator stored in the trusted vault which assures confidentiality of the authenticator. A solution to these two requirements together will ensure that none of the attacks discussed above on using the vulnerabilities in the authentication mechanism could succeed.

Proper resolution of requirement 3 would assure that the permissions given is minimised thereby minimising the attack surface. A solution to requirement 4 would assure the minimum privacy trade-off for achieving the corresponding utility. An appropriate solution to requirements 3 and 4 together could ensure establishing bounds to assess possible privacy violations and issue suitable guarantees in terms of privacy for the corresponding utility value.

11 Limitations

The limitations of this work are the following:

a This work is focused on the domain of mobile payments. Extending this to other domains and generalising this across domains will require more work.

b Dynamic analysis involving real time analysis of execution and the data flow between the mobile app and the servers were not done. Personal identifiable information are mostly mandated to be shared with payment service providers by explicit consent by the user for getting the required service in this case of mobile payment apps. As such this does not amount to violation of privacy in India at the time of this work. Hence analysis of the same was not taken up for this work. But such an analysis would help to verify compliance to privacy laws, regulations and requirements especially involving sharing of personally identifiable information which is increasingly becoming necessary for privacy sensitive applications.

12 Future work

The four requirements stated in Section 9, capture the fundamental source of the risks to security and privacy of systems designed for utility, though this work focuses only on mobile payment systems. The clarity of the requirement arrived systematically and presented comprehensively, at least with respect to the current scope of security and privacy attack surface, paves the way for the design and implementation of solutions with bounded assurances for each of the key attributes of security and privacy of data utility systems. The latter would be the goal for future that this work calls for.

References

Abraham, A. (2019) *Mobile Security Framework (MOBSF)* [online] https://github.com/MobSF/Mobile-Security-Framework-MobSF (accessed 10 August 2019).

Accenture (2019) *Future Cyber Threats 2019 – Extreme But Plausible Threat Scenarios in Financial Services* [online] https://www.accenture.com/_acnmedia/pdf-100/accenture_fs_threat-report_approved.pdf (accessed 20 November 2019).

Ajmal, A. (2019) *Phishing – Google Alert* [online] https://m.timesofindia.com/india/500-indians-alerted-about-government-backed-phishing-google/amp_articleshow/72285551.cms (accessed 6 December 2019).

Akamai (2019) *Financial Services Attack Economy Research Report 2019*, Akamai – State of the Internet/Security, Vol. 5, No. 4 [online] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-attack-economy-report-2019.pdf (accessed 10 August 2019).

ANI (2019) *Pegasus Spyware Delivered via WhatsApp* [online] https://www.business-standard.com/article/news-ani/121-users-in-india-targeted-full-extent-of-pegasus-spyware-attack-may-never-be-known-whatsapp-told-govt-119112001779_1.html (accessed 7 December 2019).

Assocham (2019) *Assocham-PwC Report* [online] https://www.assocham.org/newsdetail-print.php?id=7099 (accessed 10 August 2019).

Bosamia, M.P. (2017) 'Mobile wallet payments recent potential threats and vulnerabilities with its possible security measures', *Proceedings of the 2017 International Conference on Soft Computing and its Engineering Applications (icSoftComp-2017), Changa, India*, pp.1–2.

Chu, G., Apthorpe, N. and Feamster, N. (2018) 'Security and privacy analyses of internet of things children's toys', *IEEE Internet of Things Journal*, Vol. 6, No. 1, pp.978–985.

CVSS (2019) *Common Vulnerability Scoring System (CVSS)* [online] https://www.first.org/cvss/ (accessed 18 January 2020).

Dwork, C. (2006) 'Differential privacy', *Proceedings of the 33rd International Conference on Automata, Languages and Programming – Volume Part II, ICALP'06*, pp.1–12, Springer-Verlag, Berlin, Heidelberg.

Financial Express (2019) *Boost for Digital Payments: Govt Waives off MDR Charges on RuPay, UPI Transactions* [online] https://www.financialexpress.com/industry/banking-finance/govt-waives-off-mdr-charges-on-rupay-upi-transactions-to-boost-digital-payments/1806281/ (accessed 7 December 2019).

IDnow (2019) *IDnow 2019 Security Report: Social Engineering Tops the List of Most Common Fraud Attempts* [online] https://www.idnow.io/news/idnow-2019-security-report-social-engineering-tops-list-common-fraud-attempts/ (accessed 10 November 2019).

ISO-IEC (2018) *Information Technology – Security Techniques – Information Security Risk Management* [online] https://www.iso.org/standard/75281.html (accessed 18 August 2019).

Johnson, V.L., Kiser, A., Washington, R. and Torres, R. (2018) 'Limitations to the rapid adoption of m-payment services: understanding the impact of privacy risk on m-payment services', *Computers in Human Behavior*, Vol. 79, No. 1, pp.111–122.

Kang, J. (2018) 'Mobile payment in fintech environment: trends, security challenges, and services', *Human-Centric Computing and Information Sciences*, Vol. 8, No. 1, pp.1–16.

Knowles, J. and Pistone, A. (2019) *Card Skimming Incidents on the Rise Report* [online] https://abc7chicago.com/card-skimming-incidents-on-the-rise-report/5391506/ (accessed 20 October 2019).

KPMG-Report (2019) *Fintech in India – Powering Mobile Payments* [online] https://assets.kpmg/content/dam/kpmg/in/pdf/2019/08/Fintech-in-India–Powering-mobile-payments.pdf (accessed 7 December 2019).

Ladika, S. (2019) *Scammers Splice Skimming with Spoofing to Steal Your Credit Card Information* [online] https://www.creditcards.com/credit-card-news/skimming-and-spoofing-card-fraud/ (accessed 20 October 2019).

Liébana-Cabanillas, F., de Luna, I.R. and Montoro-Ríos, F. (2017) 'Intention to use new mobile payment systems: a comparative analysis of SMS and NFC payments', *Economic Research-Ekonomska Istraživanja*, Vol. 30, No. 1, pp.892–910.

Liu, D. and Li, M. (2019) 'Exploring new factors affecting purchase intention of mobile commerce: trust and social benefit as mediators', *International Journal of Mobile Communications*, Vol. 17, No. 1, p.108.

Madan, K. and Yadav, R. (2016) 'Behavioural intention to adopt mobile wallet: a developing country perspective', *Journal of Indian Business Research*, Vol. 8, No. 3, pp.227–244.

Microsoft (2019) *Spear Phishing – Microsoft Alert* [online] https://www.bleepingcomputer.com/news/security/microsoft-warns-of-spear-phishing-attacks-shares-tips-to-dodge-them/ (accessed 5 December 2019).

MITRE (2019) *Common Weakness Enumeration (CWE)* [online] https://cwe.mitre.org/.

Newzoo (2019) *Top 25 Countries/Markets by Smartphone Users* [online] https://newzoo.com/insights/rankings/top-countries-by-smartphone-penetration-and-users/ (accessed 5 December 2019).

OWASP (2019) *OWASP Mobile Top Ten 2016* [online] https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10 (accessed 10 November 2019).

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A. and Patsakis, C. (2018) 'Security and privacy analysis of mobile health applications: the alarming state of practice', *IEEE Access*, Vol. 6, No. 1, pp.9390–9403.

Patsakis, C., Zigomitros, A. and Solanas, A. (2015) 'Analysis of privacy and security exposure in mobile dating applications', in *Selected Papers of the First International Conference on Mobile, Secure, and Programmable Networking*, Vol. 9395, No. 1, pp.151–162.

Phishlabs (2019) *2019 Phishing Trends and Intelligence Report – The Growing Social Engineering Threat* [online] https://info.phishlabs.com/hubfs/2019%20PTI%20Report/2019%20Phishing%20Trends%20and%20Intelligence%20Report.pdf (accessed 10 November 2019).

RBI (2019) *Reserve Bank of India Payment System Indicators, Handbook of Statistics on Indian Economy* [online] https://www.rbi.org.in/Scripts/AnnualPublications.aspx?head=Handbook%20of%20Statistics%20on%20Indian%20Economy (accessed 11 November 2019).

Sahnoune, Z., Aimeur, E., El-Haddad, G. and Sokoudjou, R. (2015) 'Watch your mobile payment: an empirical study of privacy disclosure', *IEEE Trustcom/BigDataSE/ISPA*, Vol. 1, No. 1, pp.934–941.

Samani, R., Davis, G. and Contributions from the McAfee Advanced Threat Research and Mobile Malware Research Team (2019) *McAfee Mobile Threat Report 2019* [online] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf (accessed 11 November 2019).

Shin, D.-H. (2010) 'Ubiquitous computing acceptance model: end user concern about security, privacy and risk', *International Journal of Mobile Communications*, Vol. 8, No. 2, pp.169–186.

Symantec (2017) *Symantec Internet Security Threat Report 2017* [online] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (accessed 15 April 2019).

Symantec (2018) *Symantec Internet Security Threat Report 2018* [online] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2018-en.pdf (accessed 15 April 2019).

Symantec (2019) *Symantec Internet Security Threat Report 2019* [online] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2019-en.pdf (accessed 20 November 2019).

Taleby Ahvanooey, M., Li, Q., Rabbani, M. and Rajput, A. (2017) 'A survey on smartphones security: software vulnerabilities, malware, and attacks', *International Journal of Advanced Computer Science and Applications*, Vol. 8, No. 1, p.30.

Tellez, J. and Sherali, Z. (2014) 'Secure mobile payment systems', *IT Professional*, Vol. 16, No. 1, pp.36–43.

Thiruvaazhi, U. and Arthi, R. (2018) 'Threats to mobile security and privacy', *International Journal of Recent Technology and Engineering*, Vol. 7, pp.407–412.

Verizon (2019) *Verizon 2019 Data Breach Investigations Report* [online] https://enterprise.verizon.com/resources/reports/dbir/ (accessed 7 December 2019).

Wang, Y., Hahn, C. and Sutrave, K. (2016) 'Mobile payment security, threats, and challenges', *2016 Second International Conference on Mobile and Secure Services (MobiSecServ)*, pp.1–5.

Yang, Y., Liu, Y., Li, H. and Yu, B. (2015) 'Understanding perceived risks in mobile payment acceptance', *Industrial Management & Data Systems*, Vol. 115, No. 2, pp.253–269.