International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:2, 2015

# Secure Mobile E-Business Applications

Hala A. Alrumaih

***Abstract*—**It is widely believed that mobile device is a promising technology for lending the opportunity for the third wave of electronic commerce. Mobile devices have changed the way companies do business. Many applications are under development or being incorporated into business processes. In this day, mobile applications are a vital component of any industry strategy. One of the greatest benefits of selling merchandise and providing services on a mobile application is that it widens a company's customer base significantly. Mobile applications are accessible to interested customers across regional and international borders in different electronic business (e-business) area. But there is a dark side to this success story. The security risks associated with mobile devices and applications are very significant. This paper introduces a broad risk analysis for the various threats, vulnerabilities, and risks in mobile e-business applications and presents some important risk mitigation approaches. It reviews and compares two different frameworks for security assurance in mobile e-business applications. Based on the comparison, the paper suggests some recommendations for applications developers and business owners in mobile e-business application development process.

***Keywords*—**E-business, Mobile Applications, Risk mitigations, Security assurance.

## I. Introduction

DURING the first and the second wave of electronic commerce (e-commerce), World Wide Web (WWW) and Internet technology had an important role in e-commerce growing. A website became an important business tool that promotes and provides a place where customers can get services and products they need at once. Smart phone technology and tablet computer accentuated the beginning of the third wave of e-commerce. The number of mobile users is continuing to rise daily. Mobile users find that applications are easy to access and are more user-friendly than searching the Internet on a mobile browser. The International Data Corporation (IDC) market research company predicts [1] that "the market for mobile applications will continue to accelerate as the number of downloaded applications is expected to increase from 10.9 billion worldwide in 2010 to 76.9 billion in 2014".

Just as many global businesses are beginning to feel comfortable doing business over the Internet, smartphones and tablets, applications is opening up a whole new avenue to interact with customers. As a result, smart business owners will be developing and launching mobile applications that allow their customers to get helpful information including directions, recipes, ratings, reminders, phone numbers, photos and more. For example, E-Bay's mobile application has already been downloaded by more than 50 million people worldwide, representing 190 countries and eight languages.

On the other hand, as users download applications to their mobile phones, security becomes a critical issue. Mobile applications face an array of threats that take advantage of numerous vulnerabilities found in such applications and devices. These vulnerabilities can be the result of inadequate technical controls and the poor security practices.

Since applications can originate from third party providers, they present an opportunity for introduction of malicious exploits. Apart from utilizing computing power provided by mobile devices, the attackers are starting to target the data. This is due to the fact that the smart-phones are becoming storage units for personal information through use of various social networking applications, personal organizers and e-mail clients. The U.S. Government Accountability Office (GAO) stated [2] that the number of variants of malicious software aimed at mobile devices has reportedly risen from about 14,000 to 40,000 or about 185% in less than a year between July 2011 and May 2012 as can be seen in Fig. 1.

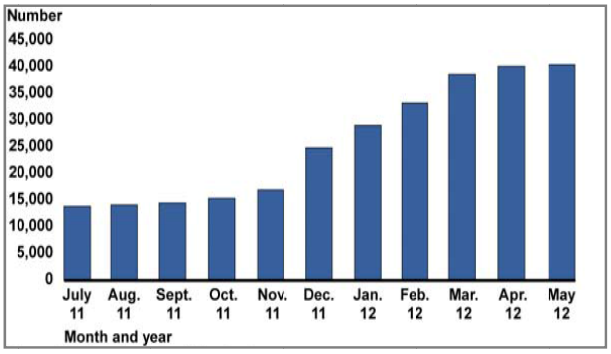


Fig. 1 Number of malicious software [2]

This paper introduces a broad risk analysis for the various threats, vulnerabilities, and risks in mobile e-business applications and presents some important risk mitigation approaches. It reviews and compares two different frameworks for security assurance in mobile e-business applications. Based on the comparison, the paper suggests some recommendations for applications developers and business owners in mobile e-business application development process.

The reminder of this paper is organized as follows: Section II sheds light on mobile application, its classifications, and the benefits of mobile e-business applications for customers and business owners. In Sections III and IV, the paper explains the need for mobile e-business applications security and introduces the various security requirements in mobile e-

Hala A. Alrumaih is with the Information Systems Department, Al Imam Mohammad Ibn Saud Islamic University, Riyadh, Saudi Arabia (corresponding author phone: +966505496409; fax: +966114915527; e-mail: hala.alrumaih@ccis.imamu.edu.sa).

business applications. Section V presents a broad risk analysis for the various threats, vulnerabilities, and risks in mobile e-business applications. In addition, Section VI offers some approaches for risk mitigations in mobile e-business applications. Section VII reviews and compares two different frameworks for security assurance of mobile e-business applications. Finally, Section VIII sheds light on two different case studies in secure mobile e-business applications. The first one is a secure mobile banking application in Australia and the second one is a secure mobile health application in Portugal.

## II. Background of Mobile Application

In fact, mobile phone is very smart due to having the vast range of applications that are already built into the phone. Moreover, the larger range of applications that are available from external application markets also be a reason. Mobile applications allow the user to do almost everything that used to be done via a desktop or laptop computer remotely and "on the go" from their mobile device [3].

Beji and Kadhi in [3] have defined mobile application (app) as a program that can be found in low power handheld devices such as a smartphone or tablet. It is an effective mode of marketing products and introducing services to a wider audience. Mobile app is currently available in various forms in business environment. These forms range in bank and insurance services, education and academic services, commodity exchange, weather services, governments services, etc.

### *A. Classification of Mobile Applications*

The capabilities of mobile apps continue to grow and expand. While there are a variety of different apps, from games to fully integrated business apps, also not all mobile apps are created equal and not all mobile apps are all the same. This section shows the main structural differences of how apps are developed. There are three main classifications of mobile apps based on the technology used to create them [4], [5]:

- *Native Apps:* They stored on the device and are accessed through icons on the device home screen. They are developed specifically for one platform and installed through an application store such as Apple's App Store. They provide fast performance and a high degree of reliability. It is expensive to develop this type of apps because it is tied to one type of operating system, forcing the business owner that creates the app to make duplicate versions that work on other platforms. Most video games are native mobile apps.
- *Mobile Web Apps:* They are not real applications. They are really websites that look like native applications, but are not implemented as such. They are typically written in HTML5, stored on a remote server and delivered over the Internet through a browser. This means that they are not separate programs that get stored on the user's mobile device but they're delivered via the Internet.
- *Hybrid apps:* They are part native apps, part web apps. They are like native apps, run on the device, and are written with web technologies (HTML5, CSS and JavaScript). Business owners build hybrid apps as wrappers for an existing web page because they hope to get a presence in the app store, without spending significant effort for developing a different app. Hybrid apps are also popular because they allow cross-platform development and thus significantly reduce development costs. The same HTML code components can be reused on different mobile operating systems. Skype, Facebook, Twitter are hybrid mobile apps.

### *B. Benefits of Mobile E-Business Applications*

By using mobile apps and internet services, people can make sure they are connected at all times, allowing them to collaborate and communicate in real time without any lag. Users can attend meetings, prepare reports, and share them with anyone in the world and stay connected with family and friends using the social media applications. At the business process side, both customers and business owners benefit from mobile apps. The following is summarization of mobile apps benefits for business owners [6]-[8]: build relationships and loyalty; reinforce brand appearance, increase visibility, accessibility and sell-through. Moreover, mobile apps connect business owners with on-the-go consumers, enhance their social networking strategies and gain competitive advantage. For the customers' side [6]-[8], they have an easy access to transaction information record, notifications and reminders of special events, one-touch access to contact information, directions to their location from wherever business are, embedded QR Code Scanner and free one-on-one chat.

## III. The Need for Mobile E-Business Applications Security

Many industry experts now recommend mandatory security developing and remediation of all e-business mobile applications, including internally developed and third party applications. Even if mobile apps developers are not malicious, they may have unintentionally incorporated components and libraries that violate security policies. As mobile devices become an important component in the daily work, work-related apps are important tools and critical in terms of security. That is make developing e-business mobile apps must be part of an overarching enterprise security plan. The following reasons are calling for a secure mobile e-business application [9]-[11]:

- *Storage and Processing of Sensitive Data:* If mobile apps developed insecurely, these applications could potentially disclose sensitive information. This results because mobile apps store and transmit a lot of sensitive personal and corporate information, such as login credentials, credit card details, private contact entries, invoices, location, and purchase orders through a range of services, from social networking, banking, ticketing, and shopping to corporate applications such as email, calendar and address book applications.
- *Nontransparent Use of Mobile Devices:* The boundary between corporate and personal devices used to be distinctive. Conversely, the line currently is being

increasingly blurred. Firstly, no one purchases two different mobile devices or tablets for work and personal use. Different statistics state that employees' personal devices are being used for working needs as well, storing critical data including corporate information on personal mobile devices. Using personal phones for corporate purposes makes it difficult to enforce corporate policies and restrictions on these devices. Also, an attacker can more easily compromise personal devices than corporate devices.

- *Regulatory Requirements:* There are different regulatory requirements for business owners in countries around the world that store and process sensitive and confidential customer data. Business owners develop mobile apps that deal with such confidential information must ensure adherence to security measures mandated by these regulations. Violation of regulatory requirements could lead to hefty fines or lawsuits against business owners.
- *Mobile Platforms:* Hackers and attacker are shifting their attention toward the mobile environment. This results because mobile apps store and transmit a lot of sensitive personal and corporate information. A vulnerable mobile app can become an easy target for a determined attacker.
- *New Technologies:* Newer technologies open up newer attack goals for hackers and attacker such as Quick Response (QR) codes that redirect customers to malicious websites that host viruses, worms, etc.

## IV. Security Requirements in Mobile E-Business Applications

In order to achieve a trust transaction in mobile e-business apps the following security functions must be performed [12], [13]:

- *Authentication:* Each party needs to make sure that the counterpart is the one he claimed to be.
- *Authorization:* Assigning access rights to different customers and controllers.
- *Availability:* Mobile app is always available for authorized use.
- *Integrity:* Each party needs to make sure that the received messages are not altered by other than the counterpart.
- *Confidentiality:* Each party wants to protect the content of the communication secret.
- *Non-repudiation:* Each party wants to prevent that the counterpart later on denies the agreements that he has approved earlier.

All of these security functions could be performed through insurance of possible protection means to the following main components [14]:

- *Device Control*: Ensuring that the physical mobile device is protected from any unauthorized access through stealing.
- *System Protection*: Ensuring that the system inside the mobile device supports a set of appropriate security mechanisms to protect it from running malicious software.
- *Application Protection*: Ensuring that an application currently running is not influenced or modified by other applications.
- *Transmission Security*: Ensuring that data is keeping from unauthorized access during transmission over the network and it has not been modified in transit.

## V. Risk Analysis in Mobile E-Business Applications

Mobile apps face an array of threats that take advantage of numerous vulnerabilities found in such applications and devices. These vulnerabilities can be the result of poor security practices that lead to risk impact for both customers and business owners. In this section, a risk analysis process is made on mobile apps environment. It allows business owner and customers identifying all currently vulnerability, threat and risk concerns.

### *A. Vulnerabilities in Mobile E-Business Applications*

Similar to a traditional PC environment, mobile devices expose to multiple threats that can affect the functioning of applications and devices and can cause misuse of sensitive personal data due to multiple vulnerabilities that have. These vulnerabilities are presented in the following points [15], [16]:

1. *The app code:* It is the primary source of most mobile app vulnerabilities because the rate of apps developers using routines that contain known malware remains high. To eschew this vulnerability, apps developers have to take care for the following: all parameters are initialized upon app startup, app code must never include references to external resources and apps must not call functions that are vulnerable to buffer overflows. Race conditions must also be avoided due to the probability becomes a bug when events do not happen in the order the programmer intended.
2. *Input handling:* It is a key distinguishing feature of apps relative to traditional desktop applications. This is because the input in traditional applications usually consists of standard keyboard characters. However, user input in mobile apps may also consist of swiping or tapping fingers on the display. To eschew this vulnerability, apps developers have to take care for the following: the input character set must be defined and constrained, the input field must be designed to not be vulnerable to XML and SQL injection attacks that allow an attacker to inject code into a program can read or modify data. Format string forms vulnerability to mobile apps in cases to lead to information disclosure and also be used to execute arbitrary code.
3. *Initialization:* When the app fails to initialize, the app must shut down, reset, or perform some safeguard action if a security module or function is unavailable in case that the app relies on external security functions such as software modules that encrypt data.
4. *Termination:* Securing the app to its initial level of security in the event the app crashes or terminates will mitigate the threat of an unauthorized user taking control of the device and accessing the app and stored data. To eschew this vulnerability, apps developers have to take

care for the following upon app termination: removes all temporary files and tracking cookies it created during the session and clear any memory blocks that were used to store and process sensitive data to completely prevent any trace of that data.

5. *External code:* Apps must validate the signature of any external code. If no signature is present or the signature could not be verified, then app must not execute it.
6. *Poor authorization and authentication:* Authorization and authentication schemes that are relying on device identifiers for security are a recipe for failure.
7. *Network communications:* The communication channel that is used during an app's operation is the same used by a malicious user. This results that a device is most vulnerable when using network communicating. To eschew this vulnerability, apps developers have to take care for the following: the app must close any opened network ports at the end of the app session or after a period of inactivity as defined by the business owner.
8. *Operating system (OS) vulnerabilities:* There is a need to prevent the app from assuming OS-level privileges when managing files because locking a file or preventing it from being backed up can cause a denial of service that prevents access to the file or its loss. Also, any app using GPS services must not forward the user's location to an external resource unless the user explicitly acknowledges that this is taking place and knows where the data is going because the user may be physically targeted. In addition, the app must not share memory with other apps, nor must it read from OS resources unless necessary to perform app functions.
9. *Cryptography concerns:* Improper use of cryptography can create exploitable vulnerabilities in mobile devices and apps. To eschew this vulnerability, apps developers have to take care for the following: Networks and apps have to use such as Class 3 certificates to prevent from a variety of malicious attacks and assures authentication, message, data and content integrity, and confidentiality encryption. In addition, digital signatures are of prime importance in discerning between malicious code and which originated from a trusted source.

### *B. Threats in Mobile E-Business Applications*

Like viruses and spyware that can infect PC, there are a variety of security threats that can affect mobile apps. These threats [17] could be divided into several categories: application-based threats, mobile-based threats, network-based threats and physical threats.

1. *Application-based Threats:* Malicious apps may look fine on a download site, but they are specifically designed to commit fraud. Mobile Malware generally fit into one or more of the following categories:

- Trojan horse is an application that usually performs some useful functionality while running malicious activities in the background.
- Botnet is a set of compromised devices that can be controlled and coordinated remotely. It is used to utilize the computing power of compromised devices in order to commit various activities.
- Worm is a self-replicating malicious application designed to spread autonomously to uninfected systems.
- Rootkit is a malicious application that gained rights to run in a privileged mode. Such malicious applications usually mask their presence from the user by modifying standard operating system functionalities.

2. *Mobile-based Threats:* Mobile platforms provide multiple attack vectors for delivery of malicious content:

- Cellular service can be used as attack vectors for mobile devices. It provides opportunities for phishing attacks. Phishing is an attack strategy in which the attacker gains sensitive information from the user by presenting itself as a trustworthy entity. Two basic phishing attacks over mobile networks exist: smishing uses SMS and vishing uses voice calls.
- Bluetooth attacks are a method used for device-to-device malware spreading.
- USB and Other peripherals in commonly used to synchronize the mobile device with a personal computer.

3. *Network-based Threats:* Mobile devices can access the Internet using Wi-Fi networks or 3G/4G services provided by mobile network operators. Prolonged connection to the Internet increases the chances of a successful malicious attack.
4. *Physical Threats:* Mobile devices are often lost or stolen, providing malicious users greater accessibility to private user data and critical application credentials.

### *C. Risks in Mobile E-Business Applications*

Insecure mobile apps can cause serious security risks and data privacy issues and can have severe repercussions on users and business owners alike. Mobile apps risks are categorized as covert or harmful risks. Covert risks disrupt the operation of the device while performing activities useful to the attacker. On the other hand, harmful risks are aimed at disrupting the normal operation of a mobile device. These risks are presented in the following points [17], [18]:

1. *Collect Private Data:* Since mobile device is becoming storage units for personal data, it is an attractive target for breaching user's privacy. The attackers target both the confidentiality and integrity of stored information.
2. *Utilize Computing Resources:* Increasing in computing resources make mobile devices into focus for malicious attacks. Attackers aim to exploit the raw computing power in combination with broadband network access. They can intercept or send fake SMS, forward e-mails to alternative inboxes. The attacker can also turn the infected mobile phone into a listening device by utilizing the voice recording hardware. In addition, accessing the camera provides an opportunity to take photos or record video of the user's surroundings.
3. *Harmful Malicious Actions*: Harmful malicious actions are aimed at generating device user's discomfort rather on performing useful operations for the attacker. Attacks can range from data loss to draining the devices battery and

other resources, like generating huge network traffic. Attackers could disable the device permanently.

## VI. Approaches for Risk Mitigation in Mobile E-Business Applications

The objective of risk mitigation is to explore risk response strategies for the high-risk items identified in the previous risk analysis. In addition to the suggested behaviors to eschew vulnerabilities that presented previously, there are some important strategies that also help in risk mitigation [19]:

1. *Don't Store Sensitive Data Locally:* Apps developers have to keep all sensitive information on the system's back end, and securely transmit and display only what customers need and only for as long as they need it. Also, developers have to turn off all caching of information in apps when handling sensitive data to ensure such data isn't left in memory. There is also need to use the strongest encryption libraries if application must store sensitive information locally.
2. *Close Down Idle Sessions:* As a convenience to mobile app customer, mobile apps leave sessions active longer than web applications do. They don't have to re-authenticate to continually use an application. It results to more likely an attacker can perform a malicious action such as stealing a session ID and becoming a legitimate user. To mitigate this risk no idle session should be allowed to go longer than five minutes before it shuts down.
3. *Don't Trust Clients:* Apps developers have to make apps validate all input received from the customer, disable verbose errors and messages, return the minimum server response at all times, change all default directories for where information is maintained and give a standard response to invalid user name or password requests.
4. *Don't Forget about Native Code:* Most mobile platforms support the creation of native code applications. This is letting code be written in languages that are vulnerable to traditional attacks, such as stack buffer overflows, memory corruptions, heap overflows, and race conditions. Apps developers should use some technologies such as code revenue, code scanning and sandboxing to identify code-level vulnerabilities and eradicate them before using them.
5. *Understand App Platform:* It is important to apps developers to understand of how the mobile platforms operate. There is need to understand:

- What vulnerabilities have been identified for platform in the past and make sure having the latest version of the operating system installed.
- How data is stored, how it's protected from access.
- The default configurations for applications, the mobile browser and application communication permissions.
- When information is cached, keyboard keys are logged, and screenshots are saved.

In addition apps developers have to specify application white listing, predefined interactions between the mobile application and the operating system.

## VII. Security Assurance in Mobile E-Business Applications

There are many frameworks that apps developers can use to build an application satisfies the security requirements. Most of them use existing information on vulnerabilities, coding guidelines and security standards in the validation process. Repositories like the Common Weakness Enumeration (CWE) [20] or the joint work with the SANS top 25 [21] provide a set of identified vulnerabilities in mobile apps. They also discuss mitigation strategies. There are also language specific guidelines. For example the CERT Oracle Secure Coding standard has been published for Java [22]. These can be further specialized for specific platforms. Standard such as NASA-STD- 8739.8 [23] is more relevant in mobile apps. This standard specifies the software assurance requirements for software developed. It maintained by the National Aeronautics and Space Administration (NASA) and for open source software, Government off-the-shelf (GOTS) software, modified off-the-shelf (MOTS) software, and commercial off-the-shelf (COTS) software when included in a NASA system. This section reviews some of the relevant security assurance frameworks.

Comprehensive, Lightweight Application Security Process (CLASP) [24] describes a process where the various security resources are identified. It addresses all the phases of the software development life cycle (SDLC): planning, analysis, design, implementation and maintenance. It is a framework focusing security concerns at early stages of development lifecycle. Twenty-four security-related activities have been defined, and each individual activity is integrated into software development processes. It is designed to be both easy to adopt and effective. It takes a prescriptive approach, documenting activities that organizations should be doing. And, it provides an extensive wealth of security resources that make implementing those activities reasonable. CLASP is an important project, which developed by the Open Web Application Security Project (OWASP). Software Assurance Maturity Model (SAMM) [25] is an open framework to help organizations formulate and implement a strategy for software security. Four business functions constitute SAMM framework: governance, construction, verification, and deployment. SAMM was established and maintained by OWASP. Advantages of this public security framework are: it is flexible enough to encompass best practices available in public domains and it is continually updated released based on a free- license policy.

This paper makes a comparison between the presented frameworks, CLASP and SAMM, based on three criteria. First, the most important feature is security awareness. Second, applicability of frameworks that explain how easily to integrate the frameworks into existing development processes. Third, it is also important to see how the framework constitutes its structures by terms of techniques, tools, and standards that the framework may have been influenced or interacted with. CLASP suggests software engineers to establish security policy at early stage of development, and all the activities later on should be considered within the range of

security policy. However, SAMM is particularly focused on vulnerability identification and attack surfaces on the resource at planning stages only. Both frameworks are difficult applied in the area of government-driven sectors. They are market driven approaches. They have week-defined steps of conformation and certification. Methodological flexibility is high for CLASP but it is medium for SAMM. CLASP and SAMM do not confine particular tools at specific phases of SDLC. CLASP interacts with Rational unified process (RUP) standard. On the other hand, SAMM does not influenced by any standards.

After reviewing and comparison two of the relevant security assurance frameworks, apps developers have to define and implement processes to manage security risk for mobile app development. Apps developers in collaboration with business owners should choose framework that interact with specific security risk management policies and standards that are suitable with their IT policies and standards to protect the confidentiality, integrity, and availability of the developed mobile app. Also, the chosen framework has to have more narrow view for security targets, and more strict criteria on quality issues. In addition, it is good to have a secure development guides that provide clear objectives, and target users, well defined set of tool support, verification guideline and methodological flexibility and good SDLC coverage.

## VIII. Case Studies in Secure Mobile E-Business Applications

Mobile banking applications give customers fast access to account information and ability to use device's built-in functions to provide a better banking experience. It considered to be one of the most important mobile e-business applications currently available. It is important to secure the transmission of the financial data between the financial business owners' server and the mobile device used by customers. In Australia, the security of sensitive financial data is one of the main concerns in acceptance of these applications. As a result, Elkhodr et al. [26] proposed a security approach and a prototype solution that aims to secure the transmission and access to personal and financial data over different networks through mobile devices anywhere and at any time. This approach authenticates the requester, the device in use, and secures the communication channel. It substitutes and enhances the SMS two-factor authentication method by automating the authentication process. It adds extra protection features to the authentication mechanism. It also improves the user experience by minimizing the users' inputs. The proposed approach is implemented as a mobile application. It demonstrates that the developed application is easy to use and integrated with other apps in mobile environments.

Mobile health applications play an important role for patients and health workers. Health apps also aim to help health care professionals improve and facilitate patient care. Patients or normal customers can use mobile health apps to manage their own health and wellness, such as to monitor their caloric intake for healthy weight maintenance. Some mobile health apps can diagnose cancer or function as the central command for a glucose meter used by an insulin-dependent diabetic patient. Mobile health apps need to security architecture to avoid errors in medication intake such as a misinterpretation in dosage, drug name and time. Goncalves et al. [27] defined a basic security architecture based on a study carried out in Portugal. This architecture is easily deployable on mobile devices, which would allow establishing and managing a medication prescription service in mobility context making use of electronic Personal Health Records (ePHR). This security architecture is aimed to be used with a mobile e-health application supported by Radio frequency identification (RFID) technology. This architecture enables an easy deployment of mobile health applications. It keeps a secure and auditable log record of all significant events and interactions with the patient's ePHR, so that any health caregiver may be implied in the process, even if the patient is at home.

## IX. Conclusion

While Mobile apps have changed the way companies do business; the requirement for security is becoming ever more pervasive and intensive, it is affecting every avenue of life. Security is a continuing journey, not a final destination. The attackers are not about to disappear. There are numerous attack surfaces on a smartphone or tablet. These attack surfaces appear in the form of the high volume of widely used apps. Each app represents a plethora of vulnerabilities not only for the device and all data on it but also for the networks to which the device is attached. This paper introduces a broad risk analysis for the various threats, vulnerabilities, and risks in mobile e-business applications and presents some important risk mitigation approaches. It reviews and compares two different frameworks for security assurance in mobile e-business applications. Based on the comparison, the paper suggests some recommendations for apps developers and business owners in mobile e-business application development process.

## References

[1] "IDC Forecasts Worldwide Mobile Applications Revenues to Experience More Than 60% Compound Annual Growth Through 2014," www.idc.com. (Online). Available: http://www.idc.com/getdoc.jsp?containerId=prUS22617910. (Accessed: 20-Apr-2014).
[2] "Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged." (Online). Available: http://www.gao.gov/products/GAO-12-757. (Accessed: 20-Apr-2014).
[3] S. Beji and N. E. Kadhi, "Security Ontology Proposal for Mobile Applications," 2009, pp. 580–587.
[4] V. L. Uskov, "Mobile software engineering in mobile computing curriculum," in Interdisciplinary Engineering Design Education Conference (IEDEC), 2013 3rd, 2013, pp. 93–99.
[5] Compuware Corporation, "Mobile Apps: What Consumers Really Need and Want." 2012.
[6] Compuware Corporation, "Mobile Computing." 2011.
[7] K. Burden, "Business Benefits of Industry-Specific Mobile Applications." Oct-2005.
[8] M. Gunnarsson, "The business benefits of enterprise mobile solutions." 2012.
[9] A. K. Jain and D. Shanbhag, "Addressing security and privacy risks in mobile applications," IT Prof., vol. 14, no. 5, pp. 0028–33, 2012.
[10] C. Gates, N. Li, H. Peng, B. Sarma, Y. Qi, R. Potharaju, C. Nita-Rotaru, and I. Molloy, "Generating Summary Risk Scores for Mobile

Applications," IEEE Trans. Dependable Secure Comput., vol. 11, no. 3, pp. 238–251, May 2014.
[11] S. Moran, "Security for mobile ATE applications," in AUTOTESTCON, 2012 IEEE, 2012, pp. 204–208.
[12] J. Swartz, "Security systems for a mobile world," Technol. Soc., vol. 25, no. 1, pp. 5–25, Jan. 2003.
[13] S. Motahari, S. Ziavras, M. Naaman, M. Ismail, and Q. Jones, "Social Inference Risk Modeling in Mobile and Social Applications," 2009, pp. 125–132.
[14] J. Jang-Jaccard, J. Li, S. Nepal, and L. Alem, "Security analysis of mobile applications: A case study of a collaboration tool in healthcare," in Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on, 2013, pp. 553–562.
[15] S. M. Dye and K. Scarfone, "A standard for developing secure mobile applications," Comput. Stand. Interfaces, vol. 36, no. 3, pp. 524–530, Mar. 2014.
[16] S. Wankhade, "Ensuring Mobile Application Security." Enterprise Mobility group at Dell Services, 2013.
[17] G. Delac, M. Silic, and J. Krolo, "Emerging security threats for mobile platforms," in MIPRO, 2011 Proceedings of the 34th International Convention, 2011, pp. 1468–1473.
[18] C. Jianmin, "Research on Behavior-based Detection Method for Mobile Application Security," 2012, pp. 240–243.
[19] J. Payne, "Secure mobile application development," IT Prof., vol. 15, no. 3, pp. 0006–9, 2013.
[20] "Common Weakness Enumeration." (Online). Available: http://cwe.mitre.org. (Accessed: 05-May-2014).
[21] "SANS Information, Network, Computer Security Training, Research, Resources." (Online). Available: http://www.sans.org. (Accessed: 05-May-2014).
[22] "The CERT ORACLE Secure Coding Standard for Java." (Online). Available: https://www.securecoding.cert.org/confluence/display/java/The+CERT+Oracle+Secure+Coding+Standard+for+Java. (Accessed: 05-May-2014).
[23] "NASA Office of Safety and Mission Assurance (OSMA)." (Online). Available: http://www.hq.nasa.gov/office/codeq/doctree/. (Accessed: 02-May-2014).
[24] "CLASP (Comprehensive, Lightweight Application Security Process)." (Online). Available: https://buildsecurityin.us-cert.gov/resources/websites/clasp. (Accessed: 10-May-2014).
[25] "Software Assurance Maturity Model (SAMM): A guide to building security into software development." (Online). Available: http://www.opensamm.org/. (Accessed: 10-May-2014).
[26] M. Elkhodr, S. Shahrestani, and K. Kourouche, "A proposal to improve the security of mobile banking applications," in ICT and Knowledge Engineering (ICT & Knowledge Engineering), 2012 10th International Conference on, 2012, pp. 260–265.
[27] F. Goncalves, J. Macedo, M. J. Nicolau, and A. Santos, "Security architecture for mobile e-health applications in medication control," in Software, Telecommunications and Computer Networks (SoftCOM), 2013 21st International Conference on, 2013, pp. 1–8.