International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 9, No.2 (Mar-2020)
http://dx.doi.org/10.12785/ijcds/090203

Framework for Developing Secure Converged Web and Mobile Applications

Devotha G. Nyambo[1], Zaipuna O. Yonah[2] and Charles N. Tarimo[3]

[1] *Information Communication Science and Engineering, Nelson Mandela African Institution of Science and Technology, Arusha, Tanzania*
[2]*College of Engineering and Technology, University of Dar es salaam, Dar es salaam, Tanzania*

Received 05 Jun. 2019, Revised 29 Oct. 2019, Accepted 31 Oct. 2019, Published 03 Mar. 2020

Abstract: The emerging need for web and mobile applications in service delivery information platforms has rapidly resulted in a bulk of applications in use with little concern about their security. Researchers in web and mobile applications security have proposed a number of solutions to security threats in these computing platforms such as 'in device' and 'in network' level security. However, little has been done in assisting developers of web and mobile applications build secure applications. This paper proposes SeC-WeMA framework which, is a holistic security framework for guiding the development of converged web and mobile applications. SeC-WeMA framework has four building blocks which provide guidance to application developers on conducting system threats modelling, identification of security requirements, conducting security controls assessment, and conducting system security testing. In addition, the paper presents SeC-WeMA framework validation results as subjected to developers of web and mobile applications.
Following our previous works on converged web and mobile applications, SeC-WeMA building blocks have been defined by using SmartDraw and ConceptDraw software. SeC-WeMA framework validation has engaged a quantitative empirical approach with three major assessment metrics which are: framework relevance, framework usability and framework flexibility. Preliminary results reveal acceptance of SeC-WeMA to web and mobile applications developers as a holistic security framework to guide them on development of secure applications.

Keywords: Holistic security framework, SeC-WeMA, Converged web and mobile applications

1. INTRODUCTION

The emerging need of web and mobile applications in service delivery information platforms has hastily resulted in a bulk of applications in use with little concern about their security. Web and mobile applications are converging to greatly support user mobility and preferences. It is clearly observed that, information systems developed to deliver certain services now include both web and mobile applications platforms. Examples of information systems delivering services through web and mobile applications in Africa include: iCow, rural eMarket and mFisheries in eAgriculture [1]. Not only that but also, in eHealth solutions exemplified by the remote health monitoring using mobile phone and web services in [2]. Many more information systems are being developed with web and mobile applications used together. For example, the Livestock Data Center (LDC) system used as a case study in our previous works [3], [4]. However, these improvements in the field of computing have left behind the design and creation of new or enhanced security solutions for the systems in place. Researchers in web and mobile applications security have stressed out a number of solutions to security threats in these computing platforms such as in device and in network level security [5], [6]. Developers of converged web and mobile applications are not yet equipped with standardized security frameworks or models that will guide them in building secured applications. The authors in [7] established that there is a need of having a holistic security framework to help developers build secure converged web and mobile applications.

This paper presents the SeC-WeMA (Secure Converged Web and Mobile Applications) framework, a holistic security framework for development of converged web and mobile applications. The design of Sec-WeMA follows a detailed study of existing security frameworks in web and mobile applications that, to the

E-mail: devotha.nyambo@nm-aist.ac.tz, engyonah@gmail.com, charles@udsm.ac.tz

best of our knowledge, are not focused on assisting the development of secure converged web and mobile applications [7]. Existing security frameworks are either for native web applications or native mobile applications. From these grounds, we present the design and validation of a holistic security framework that will guide developers of converged web and mobile applications towards development of secure applications.

Design of the SeC-WeMA framework has equally followed our previous work in identification of new security challenges in converged web and mobile applications [3] together with identification of suitable security controls for converged web and mobile applications [4]. Through these works, practical and theoretical approaches were combined to critically understand the converged web and mobile applications and its implication on clients' privacy, data and other information systems' resources. By using ConceptDraw, SmartDraw software and MS Office word, the building blocks are documented and pictorially presented. SeC-WeMA framework validation employed the use of questionnaire to collect developers' opinions on the framework's relevance, usability and flexibility.

SeC-WeMA framework is holistic because, its four main blocks cover the whole development process, that is, from system threats modelling to system testing phase. This paper ends with recommended future work of testing the framework by subjecting it to a live information system development process.

A. Problem Statement

While the converged web and mobile applications bring new security challenges, the existing approaches for securing such systems are inadequate in addressing the new security challenges [7]. Also, as pointed out earlier in this paper a defined/formal standard for secure web and mobile application development is lacking [8], [9].

Hence, in this paper an attempt is made to enhance the above situation of inadequacy by proposing a holistic security framework that can be used to guide the web and mobile applications developers in turning out secure applications. This guidance will be provided to the said developers during the applications development process from requirements engineering to system testing.

Remaining sections of this paper are organized as follows; Section 2: Background, Section 3: Methodology, Section 4: Data collection results and discussion, Section 5: SeC-WeMA framework building blocks, Section 6: SeC-WeMA framework validation, and Section 7: Conclusion and future works.

2. BACKGROUND

The increasing integration of services in the computing world is rapidly forcing service delivery enterprises to embrace the power of mobile applications in reaching clients. As reported by strategic analytics, current mobile phone usage is changing from voice as static communication to rich media data exchange. In strategic analytics, this is marked by 70% usage of average cell phone being voice while that of iPhone decreases to 45%, this is per research done in the United States by [10]. Coming back to Africa continent, research shows a tremendous year-on-year growth in mobile web browsing. The case has been exemplified by case studies in Côte d'Ivoire and Libya by hitting 744%- and 1,886,839%-page views by 2012 [11]. These statistics are communicating nothing else but the emerging power of mobile devices in reaching diversified customers.

In Africa, the power of mobile devices is evident in the way enterprises are focusing on development and deployment of various web and mobile based solutions for e-agriculture, e-health, e-government, e-learning and e-business. Regardless of the evident increasing power of mobile devices, traditional web applications cannot be abandoned due to existing challenges and limitations such as, browser capabilities, low device memory, and small screen sizes, on the use of mobile devices. Based on these grounds, the combined use of web and mobile applications is taking off requiring the two computing platforms to complement one another. That is, web and mobile applications usage has been combined to provide total support in user mobility as well as to reach a diversified number of clients. We call this a converged use of web and mobile applications. Developers of information systems, which make use of web and mobile applications are not equipped with formal standards, or frameworks for secure applications development [8] [9].

As reported in [3], available frameworks for web and mobile applications have not provided ways to guide developers in a holistic way towards secure applications. By a holistic way we mean, a step by step approach in secure applications development from requirements engineering stages to system testing. Moreover, it is reported that existing security frameworks for web and mobile applications have been designed in isolation. This isolation has made customization of the current frameworks to suit converged web and mobile applications development difficult. A review work by [3] pointed out the need for a new security framework that can guide developers of converged web and mobile applications to develop secure applications.

3. METHODOLOGY

A. *Data Collection on Use of Web and Mobile Applications Security Frameworks*

Data collection was focused on providing us with a real state of art in applications development. Selected areas for our survey were: enterprises, hubs and independent developers. The survey was done through use of questionnaire and interviews. Total number of respondents to the questionnaire was 54, and interview participants were 15. Collected data was analyzed by SPSS software, through which we were able to draw deductions based on analyzed data.

B. *Borrowed knowledge*

SeC-WeMA design took into account the results from our previous works in converged web and mobile applications security [7] [3] [4]. Design of the framework's building blocks borrowed knowledge created from these works.

Firstly, we conducted a detailed review of existing security frameworks used to secure web and mobile applications with the aim of finding out whether the existing security frameworks can address the new security challenges of the converged web and mobile applications. This was important since the existing security frameworks are either catered for native web applications or native mobile applications. The findings for this review are reported in [7]. The findings have shown that, existing security frameworks are inadequate in addressing the new security challenges in converged web and mobile applications.

Secondly, we steered a detailed study to find out whether the converged web and mobile applications bring about new security challenges. By using a case study (LDC system), we conducted a system threats modeling whose findings have been reported in [3]. It has been shown that there are new/prominent security challenges in converged web and mobile applications.

Thirdly, we devised a new approach that can deal with the prominent security challenges brought about by the convergence of web and mobile applications which, has been reported in [4]. At this stage, a model for security controls assessment was proposed together with a set of suitable security controls proposed for the converged web and mobile applications.

This paper is a culmination of research aimed at securing web and mobile applications in a converged web and mobile platforms. It integrates the outputs from the individual phases of the research these are: Review of Security Frameworks in the Converged Web and Mobile Applications, An Approach for Systematically Analyzing and Specifying Security Requirements for the Converged Web-Mobile Applications, and On the Identification of Required Security Controls Suitable for Converged Web and Mobile Applications. This integration is then referred to as SeC-WeMA: A Holistic Security Framework for Converged Web and Mobile Applications.

C. *Framework Design*

Design of SeC-WeMA framework employed the use of drawing software, ConceptDraw and SmartDraw to create visual representations of the processes and stages involved. Textual documentation was done by using Microsoft office word.

D. *Data Collection and Analysis Tools for SeC-WeMA Validation*

Preliminary SeC-WeMA framework validation engaged a quantitative empirical approach by involving a selected group of web and mobile application developers. Web and mobile applications developers were introduced to SeC-WeMA framework through face to face presentations. Questions and answers (Q&A) sessions were involved during the presentations in order to help respondents understand how the proposed models in the framework work. A questionnaire was then used for collecting data, which covered four major sections: respondents' profile, framework relevance, framework usability, and framework flexibility. Collected data were analyzed by using SPSS software.

4. DATA COLLECTION RESULTS AND DISCUSSION

The main objective of our survey was to find out if web and mobile applications developers consider and follow security procedures in application development. In addition, to assess the use of security frameworks in applications development, and to know exactly which frameworks are mostly used in web and mobile applications development. In the following paragraphs we summarize and discuss respondents' results in indicated categories.

1) Awareness to security risk assessment in web and mobile applications development: 63% of respondents indicated that they were unaware of security risks assessment in applications development. To our understanding, this finding indicate that many applications are sent to market with little concern on risks associated with their usage.

2) Use of security frameworks in applications development

Results show that 74% of applications developers do not use any security framework in their applications. This fact is highly contributed by lack of a tool or formal procedures to assist developers in observing and applying security practices in development stages. As a result, web and mobile applications are built under normal

development frameworks which have little contributions to application security.

3) New security challenges in web and mobile applications

Despite the fact that, web and mobile applications developers do not use formal security frameworks in applications development, 58% of the respondents indicated that they have encountered new challenges in working with web and mobile applications. Mentioned challenges include: client-side injection, phishing, disclosure of sensitive data, and use of passwords-based authentication. Others are: mobile devices do not limit internet connections, and devices which are older than two years do not receive security updates from manufacturers. To us these results call for a formal security framework to assist developers of web and mobile applications.

4) On mitigating the new challenges in web and mobile applications

Some respondents indicated approaches they already tried in addressing the said challenges in converged use of web and mobile applications. Among the given responses are: encryption of data stored on a mobile device, establishment of a mobile security policy, continual training on the use of updated anti-virus software, use of multilevel authentication, and biometric authentication.

Moreover, we discovered from our survey results that, only 37% of respondents use web and mobile applications frameworks/models. Indicated frameworks/models are shown in **Table 1**. However, these frameworks and models are not specific to security and hence the development process leaves behind loopholes for security attacks. Frameworks such as ASP.NET and PHP for web applications present some built-in security controls, but it is set clear that, guarantee to an application security lies entirely on the programmer based on the application context [12]. Another observation is that convergence of web and mobile applications expose and make vulnerable for attack trusted systems in mobile environments that are full of untrusted third-party applications and features incorporated in mobile devices [13] [14] [15]. Due to this fact, security in mobile applications becomes critical and therefore should be treated with attention when they are to work together with web applications.

5. SEC-WEMA FRAMEWORK BUILDING BLOCKS

Design of SeC-WeMA framework takes a holistic approach of a typical information system development process. As suggested by a number of researches, security practices are highly recommended to become part of information systems development [16] [17] [18] [19]. Through this approach, the cost of mitigating security flaws can highly be reduced.

TABLE 1. FRAMEWORKS/MODELS USED BY RESPONDENTS

Web	Mobile
Java, HTMl, Jsp	N/A
Netbeans	Netbeans
mvc-model-view-controller	mvc
Vaadin	Vaadin TouchKit
Macromedia Design Layout	N/A
web applications frameworks (ASP.NET framework, PHP framework, and Java framework)	mobile applications frameworks (Phone Gap,GWT mobile webkit + gwt mobile UI,)
Dreamweaver & Visual Studio	Sometimes NetBeans
web application framework (WAF)	multiple mobile web-based application framework
Codeigniter, Laravel and Yii	Android Studio, PhoneGap, XCode //Not sure there are frameworks here

Conceptually, we present four building blocks that will guide an information system developer of converged web and mobile applications in security practices to follow in four phases of an information system development. Information system development phases captured in SeC-WeMA framework are: system requirements engineering, system design, system implementation, and system testing. In addition, as an important process in information systems development life cycle, we include documentation on each block to make sure that all security practices have been documented. Figure 1 shows how the blocks are organized.

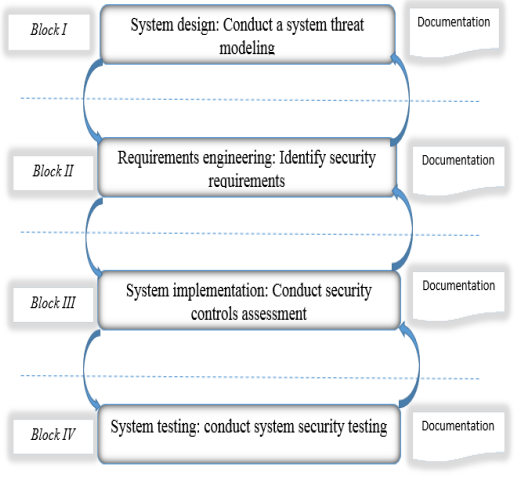

Figure 1. SeC-WeMA framework conceptual building blocks.

A. *Block I: System Threats Modeling*

Information system security threats modeling is hardly given a concern in applications development. This phenomenon results in development of web and mobile applications with no concern about most security threats which are likely to occur. SeC-WeMA presents an approach to threats modeling and specification of precise requirements during applications coding. Knowledge used here has been proved to provide specific/new security threats as tested in [3] using the Livestock Data Center (LDC) system. **Figure 2** presents a structure of a holistic system threats modeling recommended for SeC-WeMA framework.

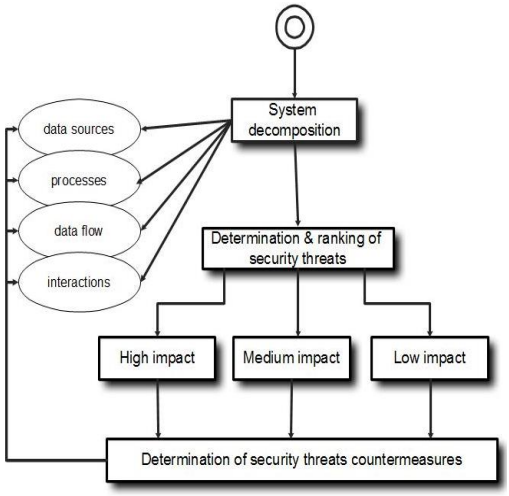

Figure 3. Systems threats modeling.

B. *Block II: Identification of Security Requirements*

Development of any information system to support either web or mobile applications usually starts with feasibility assessment and requirements identification. As much as this stage in applications development is important, we embed it with determination of system's security requirements which follows a successful threat modelling process. Development of security requirements at this stage is focused on assisting effective acceptance testing of an application (beta test). We break down the security requirements into three categories: 1) web application security requirements, 2) mobile application security requirements, and 3) intersecting web and mobile applications security requirements. One significant purpose of breaking down these security requirements is such that, we do not weaken the performance of mobile applications by feeding it with typical web applications security requirements and vice versa. This implies that, development teams should explicitly define three categories of security requirements depending on the nature of system being developed. Accomplishment of this block in web and mobile applications development is marked by documented set of initial security requirements. **Figure 3** represents a pictorial description of procedures for Block II.

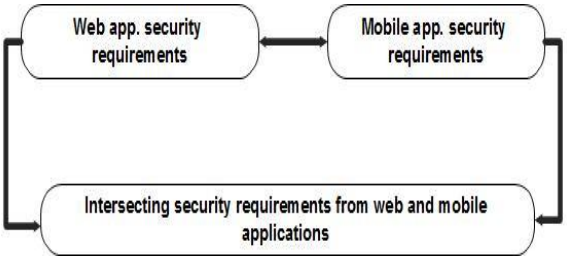

Figure 2. Security requirements categorization.

C. *Block III: Security Controls Assessment*

Block three recommends assessment of security threats countermeasures after a successful threats modeling and determination of specific security controls. Security countermeasures which are implemented at an application level needs to be assessed depending on a number of metrics including:

- type/nature of applications
- sensitivity of data involved
- nature and number of anticipated users

SeC-WeMA framework has a security controls assessment model embedded with suggested controls for converged web and mobile applications treated as an extension to assessment model reported in [4]. However, in SeC-WeMA framework we suggest a continual modification on the suggested security controls due to the fact that, applications requirements differ and might impact on the set security controls. Application development teams should, therefore, iterate the process of security controls assessment until a desirable level of vulnerability is attained. The white box and black box techniques in security controls assessment are deployed in SeC-WeMA framework to guide application development teams towards effective security controls assessment process. **Figure 4** presents the proposed security controls assessment model for converged web and mobile applications.

D. *Block IV: System Security Testing*

Testing follows a successful implementation, with an intent of finding out if the developed system conforms to user requirements. Likewise, from security point of view, one would test an application or system to make sure it conforms to the set security requirements. In the proposed SeC-WeMA framework we propose a testing approach to ensure that the developed web and mobile applications conform to the set security requirements as per Block one of this framework. Therefore, testing is done against the three categories of security requirements: web applications security requirements,

mobile applications security requirements and intersecting set of security requirements for web and mobile applications. **Figure 5** depicts the proposed system security testing in SeC-WeMA framework based on the three categories of security requirements. As any other block in SeC-WeMA framework, test scenarios should be documented.

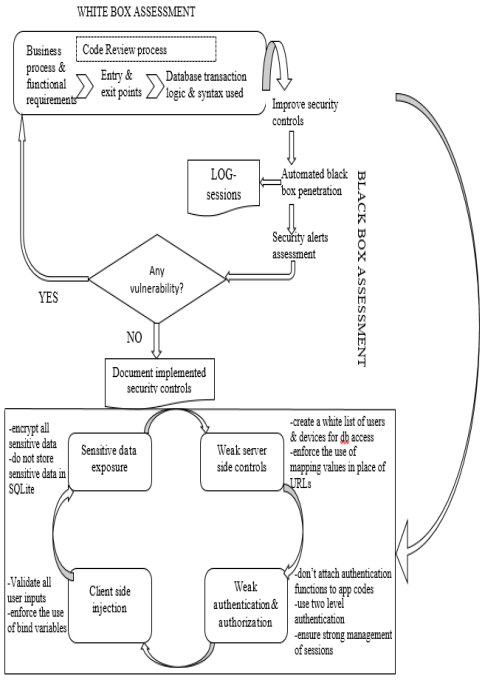

Figure 4. Security controls assessment.

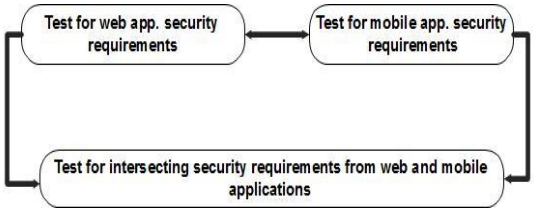

Figure 5. System security testing.

6. SEC-WEMA FRAMEWORK VALIDATION: A QUANTITATIVE EMPIRICAL APPROACH

A. Review on Existing approaches for Security Frameworks Validation

Security frameworks can be validated or tested under various metrics depending on the scope and purpose of a particular framework. To the best of our knowledge, security frameworks can be validated by using either of the following approaches, which may incorporate the use of qualitative or quantitative data analysis: -

- Using the framework to develop testing applications
- Implementing a framework to an existing system
- Using a working prototype
- Exploratory empirical studies

The following paragraphs summarize available security frameworks validation approaches and how they have been used by various researchers. In addition, we present the approach used for preliminary validation of SeC-WeMA framework.

Validation of a mobile applications development framework proposed by [20] engaged development of a mobile based application. The application called 'Eivom' a cinema guide, was developed by following the designed framework development methodologies and best practices. With major three evaluation metrics: originality, usability, and quality, the application 'Eivom' validated the designed framework in development of secure mobile and mobile web applications. Apart from developing testing applications, security frameworks can also be validated by subjecting them into an existing system. Security frameworks can be tested and consequently be compared to existing systems in order to identify their relevance as well as flexibility as justified by [21] [22].

Security framework validation using a prototype has also been demonstrated by various researchers. For example, validation of SecureSocial aware [23], security framework for Web 2.0 applications [24] and CENTRICLOUD: a framework for protecting Infrastructure as a service in cloud computing [25]. Validating a framework by a prototype entails the implementation of the design into a demonstrable software application. However, further performance metrics can be involved to validate and verify the prototype.

Exploratory empirical studies are also used in validating security frameworks as done by [26]. The authors proposed an approach to attack surface reduction that guide developers on how to reduce the attack surface of various information system from small scale to large scale. Explorative approaches allow testing of a framework before releasing to anticipated users, and can make use of qualitative or quantitative data sets. Empirical analysis in framework validation are highly based on reality and practicability of a proposed framework by engaging anticipated users. This kind of validation is used to communicate practicability, adaptability as well as relevance of the proposed approach from anticipated users.

TABLE 2. SURVEY STATISTICS ON VALIDATION OF SEC-WEMA FRAMEWORK

	focus in applications development	years of experience	develop applications for	SeC-WeMA relevance to your development process	water fall model	RAD	prototyping	spiral	SeC-WeMA is easy to follow	usability of models in SeC-WeMA	SeC-WeMA flexibility
Valid	54	54	54	54	54	54	54	54	54	54	54
Missing	0	0	0	0	0						

The proposed SeC-WeMA framework validation takes aboard a quantitative empirical approach, which involved web and mobile applications developers. The selection of this approach is focused on understanding the practicability of the proposed framework. We were very certain on involving applications developers in this validation because they are the anticipated users of the framework; so, their preliminary evaluation and suggestions has created a baseline for future developments in regard to SeC-WeMA framework. A total of 54 developers of web and mobile applications were involved in the survey which was run for two weeks involving developers from two academic institutions, one financial institution, and one government institution. As shown in **Table 2**, no any missing value was observed in all the questions.

a) Focus on applications development

Considering the focus of SeC-WeMA framework which is for converged web and mobile applications, the survey attracted developers from the two types of computing platforms. It was found that, 72.2% of respondents are engaged in both web and mobile applications development, while 14.8% and 13% engage in traditional mobile and web applications, respectively. As shown in Fig. 6, there is a high concentration of developers in the emerging mobile applications development than the traditional web applications. The implication here is that, developers are highly focusing on user mobility to satisfy the growing demand of data exchange.

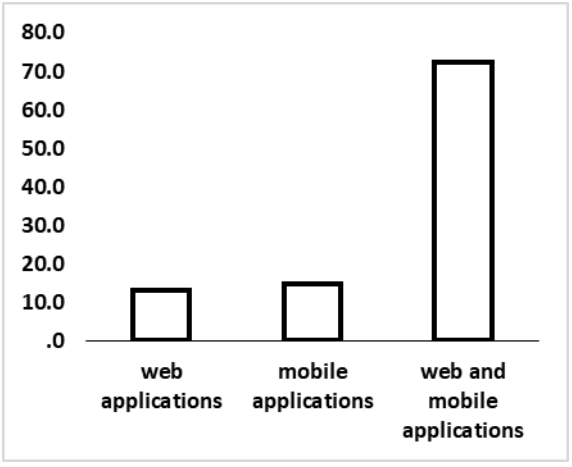

Figure 6. Respondents' focus in applications development.

b) Years of experience in applications development

Experience in applications development is highly related to knowledge in the field and how developers have experienced security challenges in the specific computing platform. Survey results showed that, majority of respondents (70.4%) have between 0-5 years of experience in the field. Comparing to the type of applications in which most are engaged with, this percent signifies a growing interest in mobile application than the traditional web applications. Further results indicate, 25.9% of respondents have 5-10 years of experience, while, only 3.7% have experience over 10 years and above. These statistics fall in line with the growing need for data exchange as described in the background section of this paper.

c) Develop applications for

The survey question was intended to confirm the fact that, web and mobile applications development ranges from personal use to enterprise contracts. Interestingly, 57.4% of respondents indicated that they develop applications for enterprises while, only 3.7% of respondents develop applications for personal uses. Connecting these results with part (a) and (b) on respondents' profile we can confidently say that, the improvement in the computing field is forcing young techno-preneurs to jump into contracts for web and

mobile applications with minimal consideration on security challenges. These data correlate very well to our survey results discussed in section 4 of this paper which states that 74% of developers (involved in the previous study) do not use any security framework during applications development. **Figure 7** shows more respondents' results on the use of applications developed.

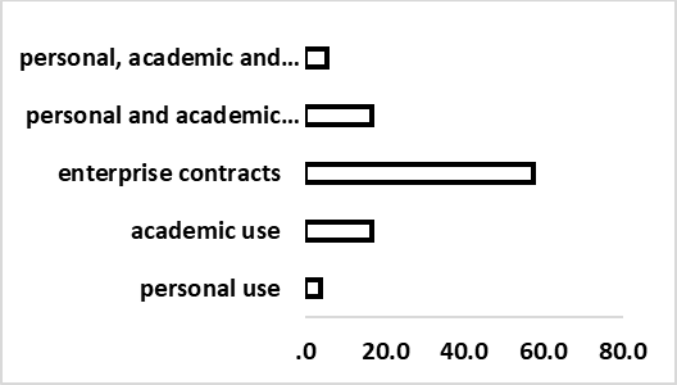

Figure 7. Respondents' results on the use of applications they develop.

2) SeC-WeMA Framework Relevance

a) How relevant is SeC-WeMA framework to your development activities?

Our survey results show SeC-WeMA framework has been stated to be very relevant to web and mobile applications development activities by 77.8% of respondents. The other 22.2% of respondents indicated that the framework is somehow relevant to their development activities, and there were no results indicating that the framework was not relevant at all. This significant result implies that the approach used in developing the framework followed a typical development approach from requirements engineering to testing phases. Moreover, the proposed framework being tested by using working applications and scenarios supports the results as given by respondents.

b) SeC-WeMA relevance to major phases in existing software development models

To understand the relevance of SeC-WeMA framework to existing Software Development Life Cycle (SDLC) models is to account for its holistic nature and provide room for modifications. The framework should be usable without considering the type of development model in use. By observing the results presented in **Fig. 8**, the respondents' agreement on the relevance of the framework to existing SDLC models depends highly on the complexity of the model. For example, water fall model is highly adopted for various categories of applications development due to its fewer number of phases and simplicity to follow. On the other hand, spiral model has multiple stages even in one phase. From these grounds, majority of respondents (77.8%) indicated that the framework is relevant to the water fall model while, 55.6% and 43.6% agrees on its relevance to RAD and spiral models, respectively. On prototyping model, majority of respondents had no opinion on the relevance because the model involves unlimited number of iterations. Very encouragingly, only 7.4% of respondents indicated that the framework is not relevant to any of the SDLC models. One key reason of having this result might be that, the respondents could not link the proposed security practices to the SDLC models they use. However, by allowing more time to learn how the framework can be used is likely to reduce or completely eradicate this variation.

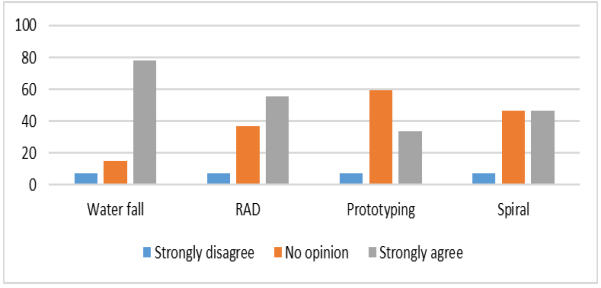

Figure 9. Respondents' results on relevance of SeC-WeMA to major phases in SDLC models.

3) SeC-WeMA Framework Usability

SeC-WeMA framework is easy to follow, from requirement engineering to system testing. Our survey results show that 83.3% of respondents indicated that SeC-WeMA framework is easy to follow from requirements engineering to system testing. However, 14.8% of respondents had no opinion on this question. Majority of respondents have appreciated that the framework is easy and adoptable for their development practices because the design effectively considered the common phases in application development. This also includes having instructions that are practical and can easily be embedded in the development process. A very small proportion of respondents indicated that the framework is not easy to follow as shown in **Fig. 9**.

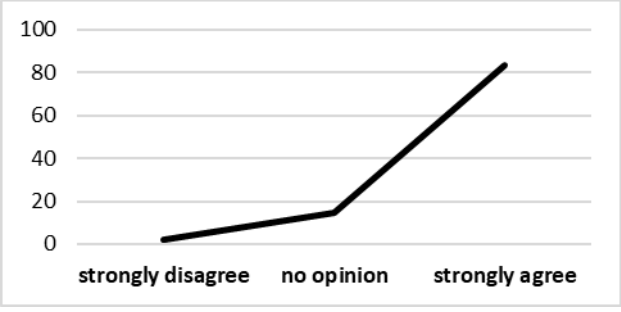

Figure 8. Respondents' results on whether SeC-WeMA is easy to follow.

4) Usability of the models presented in SeC-WeMA building blocks

The framework has been termed practical by 64.8% of respondents who indicated that all the models in the framework are practical; 33.3% of respondents indicated that only some of the models are practical. Generally, the framework can be regarded as practical. Because only 1.9% of respondents indicated that none of the models presented is practical.

5) SeC-WeMA Framework Flexibility

a) How flexible is SeC-WeMA framework?

The question on flexibility of the framework was designed to obtain from respondents their opinion on whether they think it is possible to adjust and add or remove some features as per their development context. As shown in **Fig. 10**, majority of respondents (57.4%) indicated that the framework is very flexible. However, 42.6% of respondents indicated that the framework was somehow flexible in regard to some models. None of the respondents indicated that the framework is not flexible.

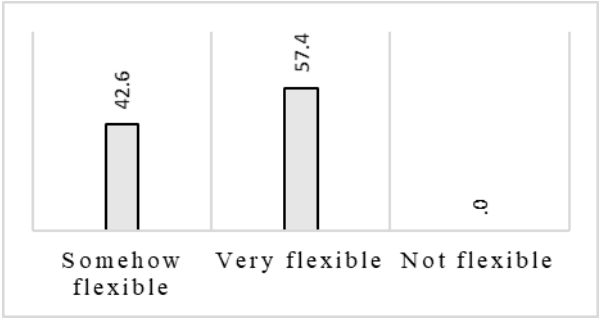

Figure 10. Respondents' results on SeC-WeMA flexibility

b) General comments on SeC-WeMA flexibility

Some respondents did express their opinion on the issue of modifying the framework for it to be more flexible. Among key comments on this aspect included:

- Extending the framework to specifically guide security practice is various mobile applications development platforms such as, iOS.
- The framework does not allow some stages to be bypassed when rolling back. A developer should be able to roll back to any phase without affecting intermediate phases.
- The framework should reconsider SDLC models such as Rapid Applications Development and prototyping. The stages in some models are complicated and time consuming, this will not favor the development of applications under models such as RAD and prototyping.

7. CONCLUSION AND FUTURE WORK

SeC-WeMA is a holistic framework because it has covered all major development stages of web and mobile applications. The framework includes the best security practices in all the stages of web and mobile applications development. Our focus has been on converged web and mobile applications security since it has been demonstrated that the coming together of these two computing platforms has introduced new security challenges. To this end, we have proposed and validated the holistic security framework that will guide developers in the development of secure converged web and mobile applications.

Our preliminary validation results show that SeC-WeMA is relevant to development activities and shows promising results on use under various web and mobile applications development models. Apart from that, survey respondents have positively confirmed the SeC-WeMA practicability in this new era of intertwined features of web and mobile applications. Some of our survey respondents mentioned that there is a need to test the applicability of the framework on acquired information systems. Some companies do rely on acquired systems and can hardly customize the security features in these systems. So, there is a need of defining guidelines on how security features should be customized in acquired information systems, we strongly recommend this for future SeC-WeMA framework implementations.

Since our goal is to test SeC-WeMA in a live development process, our preliminary validation results support the future stage because anticipated users of the framework are certain on its relevance, usability and flexibility in developing converged web and mobile applications.

One significant contribution from this paper is the design of a holistic security framework that can guide developers of converged web and mobile applications build secured applications. Through this framework, developers can follow proposed security practices that should be done in specific development phases. Approach used in SeC-WeMA design has not been used in existing security frameworks as far as the authors are aware.

ACKNOWLEDGMENT

We sincerely appreciate the support on this work from the Nelson Mandela African Institution of Science and Technology (NM-AIST) through the school of Computation and Communication Science and Engineering (CoCSE).

REFERENCES

[1] I. Rodrig, "Top 10 applications for agriculture. E-agriculture", http://www.e-agriculture.org/news/top-10-applications-agriculture, 2013, Accessed on 25th June 2014.

[2] S. Agarwal, and C. T. Lau, "Remote health monitoring using mobile phones and Web services," Telemedicine and e-Health, Vol. 16, no. 5, 2010, pp603-607.

[3] D. Nyambo, Z. Yonah, and C. Tarimo, "An Approach for Systematically Analyzing and Specifying Security Requirements for the Converged Web-Mobile Applications," International Journal of Computing and Digital Systems, 2014, Vol. 3, no. 3, pp207-217.

[4] D. Nyambo, Z. Yonah, & C. Tarimo, "On the Identification of Required Security Controls Suitable for Converged Web and Mobile Applications," International Journal of Computing and Digital Systems, 2016, Vol. 5, no. 01.

[5] C. C. Ho, and C. Y. Ting, "A Conceptual Framework for Smart Mobile Honeypots," Academia, http://www.academia.edu/download/31058450/KasperskyConferencecchocyting.Pdf. 2014, Accessed on 17th July 2014.

[6] D. S. Kumar, and A. Amalanathan, "A Framework for Mobile Web Mashup's using Cloud Resources. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), 2014, Vol. 3, no. 6, pp338-348.

[7] D. Nyambo, Z. Yonah, and C. Tarimo, "Review of Security Frameworks in the Converged Web and Mobile Applications," International Journal of Computer and Information Technology, 2014, Vol. 3, no. 4, pp724-730.

[8] J. Lounsbury, "Application Security: From Web to Mobile: Different Vectors and New Attacks," Security in Knowledge, 2013, 30pp.

[9] K. Johnson, and J. Jardine, "2013 SANS Mobile Application Security Survey: A SANS White Paper," SANS Analyst Program, 2013, 14pp.

[10] C. Dodge, "Over Half of Consumers in the US Now Use Mobile Web," Strategic analytics, 2012, http://www.strategyanalytics.com/default.aspx?mod=reportabstractviewer&a0=7972. Accessed on 14th Aug 2014.

[11] T. Elliott. The Mobile Web Is (Perhaps) Taking Off in Africa," Strategic analytics, 2012, http://www.strategyanalytics.com/default.aspx?mod=reportabstractviewer&a0=7689. Accessed on 14th Aug 2014.

[12] D. Balzarotti, M. Cova, V. Felmetsger, N. Jovanovic, E. Kirda, Kruegel, and G. Vigna, "Saner: Composing static and dynamic analysis to validate sanitization in web applications," In Security and Privacy, 2008. SP 2008. IEEE Symposium on, May, 2008, pp 387-401.

[13] D. Chappel, "INTRODUCING ODATA: Data access for the web, the cloud, mobile devices, and more," White Paper, 2011, pp6-10.

[14] Ernest and Young, "Mobile Device Security: Understading Vulnerabilities and managing Risks, Insights on Governance, Risks and Compliance," 2012, 9pp.

[15] T. Wasserman, Software engineering issues for mobile application development. FoSER 2010, 2010, 15pp.

[16] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann, and P. Sommerlad, "Security Patterns: Integrating security and systems engineering," John Wiley & Sons, 2013, 20pp.

[17] N. Kaur, and P. Kaur, "Input Validation Vulnerabilities in Web Applications," Journal of Software Engineering, 2014, Vol. 8, no. 3, pp116-126.

[18] M. Busch, N. Koch, and M. Wirsing, "Evaluation of Engineering Approaches in the Secure Software Development Life Cycle," In Engineering Secure Future Internet Services and Systems, 2014, pp234-265. Springer International Publishing.

[19] J. Park, and Y. Suh, "A Development Framework for Software Security in Nuclear Safety Systems: Integrating Secure Development and System Security Activities," Nuclear Engineering and Technology, Vol. 46, no. 1, pp47-54.

[20] M.A. Serhani, B. Abdelghani, D. Rachida, and M. Rabeb, "Toward an Efficient Framework for Designing, Developing, and Using Secure Mobile Applications," International Journal of Human and Social Sciences Vol. 5, no. 4, pp272-278.

[21] B. Fabian, S. Gürses, M. Heisel, T. Santen, and H. Schmidt, A comparison of security requirements engineering methods. Requirements engineering, 2010, Vol. 15, no. 1, 2010, pp7-40.

[22] M. Almorsy, J. Grundy, and A. S. Ibrahim, Collaboration-based cloud computing security management framework, In: Cloud Computing (CLOUD), 2011 IEEE International Conference on, July, 2011, pp 364-371.

[23] A. Beach, M. Gartrell, B. Ray, and R. Han, "Secure socialaware: A security framework for mobile social networking applications," Department of Computer Science, University of Colorado at Boulder, Tech. Rep. Technical Report CU-CS-1054-09, 2009.

[24] L. Desmet, W. Joosen, F. Massacci, K. Naliuka, P. Philippaerts, F. Piessens, and D. Vanoverberghe, "A Security Architecture for Web 2.0 Applications," In Future Internet Assembly, 2009, pp 35-46.

[25] B. Bertholon, S. Varrette, and P. Bouvry, "Certicloud: a novel tpm-based approach to ensure cloud iaas security," In Cloud Computing (CLOUD), 2011 IEEE International Conference on, July, 2011, pp 121-130.

[26] P. K. Manadhata, and J. M. Wing, "An attack surface metric," Software Engineering, IEEE Transactions on, 2011, Vol. 37, no. 3, pp371-386.

Devotha G. Nyambo is a PhD candidate at the Nelson Mandela African Institution of Science and Technology in Arusha, Tanzania. She is interested in social systems for decision support especially in Agriculture.

Eng. Dr. Zaipuna O. Yonah is holds a B.Sc. Degree (with Honors - 1985) in Electrical Engineering from University of Dar es Salaam - Tanzania; and M.Sc. (1988) and PhD (1994) Degrees in Computer-Based Instrumentation and Control Engineering from the University of Saskatchewan, Saskatoon- Canada. In Tanzania, he is a registered Consulting Engineer in Telecom/ICTs associated with Applied Engineering & ByteWorks (T) Limited a consulting firm in ICTs/Telecoms, Nelson Mandela – African Institution of Science and Technology, and the IEEE Inc. He has over 33 years of practice spanning the academia, industry and policy-making in ICTs/Telecom Sectors – with assignments within Tanzania, East Africa and SADC economic communities.

Dr. Charles N. Tarimo is an active researcher on ICT security issues, with research interests focused on operational and practical issues with regard to aspects of security requirements development, designing, implementation, and management of different technical and non-technical ICT security controls within organizations/enterprises as well as research on similar issues at the national level. He has been collaboratively working with other researchers to carry out different research studies in the field of Information and Communication Security and published the research findings at various International Conferences. Dr. Tarimo is currently an employee of the University of Dar es Salaam, working at the College of Engineering and Technology, serving as the University's ICT Manager. But also he is involved in the teaching of related subjects in computer engineering, such as computer hardware and software engineering, computer and networks security, computer networking as well as artificial intelligence.