Review of Security Frameworks in the Converged Web and Mobile Applications

Devotha Nyambo
School of Computation and Communication Science and Engineering
Nelson Mandela African Institution of Science and Technology
Arusha, Tanzania
Email: Nyambod {at} nm-aist.ac.tz

Zaipuna O. Yonah
School of Computation and Communication Science and Engineering
Nelson Mandela African Institution of Science and Technology
Arusha, Tanzania

Charles Tarimo
College of Engineering and Technology
Univesrity of Dar es Salaam
Dar es Salaam, Tanzania

Abstract - **As the Internet access is becoming pervasive there is an increasing number of mobile applications users. Enterprises are now reaching a diversified number of customers through the use of Web and mobile applications. However, this improvement in the accessibility means to computing resources does not move in same pace with the improvement of security controls to protect data and services offered through Web and mobile applications.**

This review paper is focused on identification of both practical and theoretical security frameworks for Web and mobile applications in use, with an intent of assessing the capability of the frameworks to assist developers build secure mobile Web applications.

A discussion follows the review by highlighting main characteristics of the frameworks with their merits and demerits. The analysis establishes that, available security frameworks are not adequate for the growing convergence of Web and mobile applications, in that there are some security gaps and therefore suggest a need of developing a new security framework for the converged Web and mobile applications.

Keywords - Web and mobile applications; security frameworks.

I. INTRODUCTION

Web applications refer to software applications that are coded in a browser supported programming language and depends on a common Web browser to provide the intended service. Mobile applications refer to lightweight piece of software that can be deployed into a phone remotely over the Web or offered remotely as a service. As the Internet access over mobile phones becomes pervasive, there is an increasing number of mobile application users, which in turn is rapidly changing the mode of service delivery from traditional Web applications to lightweight mobile applications [1]. This change does not mean abandonment of the traditional mode since clients can now access same applications from their mobile phones as they do with computers and tablets. From this perspective, enterprises are progressing on the use of Web and mobile applications platforms for their services to reach as many clients as possible. However, the observed increased use of Web and mobile applications by enterprises is not taking place along with an increased security level for the associated Web and mobile applications. As highlighted by [2], enterprises are experiencing different types of application security attacks with application authentication and attack on sensitive information having 27% and 25% of total attacks, respectively.

The increase in the variety of security attacks is partly due to the emerging number of sophisticated tools for attack penetration in both Web and mobile applications. The availability of sophisticated attack tools is a single factor that makes it so hard to secure these computing platforms. Examples of sophisticated tools includes, WS-Attacker, Nmap, Hydra, Cain&Abel, and Metasploits [3], [4].On the other hand, the other factors affecting the security on these platforms include: lack of developers who know about security aspects especially mobile applications' platforms security [5], and also there is lack of development standards, frameworks and languages [6], [7]. All these factors taken together have opened up a vast new targeted threat landscape and already are causing loss of enterprises assets, integrity and confidentiality.

As technology advances at a fast pace, Web and mobile applications are no longer used as separate resources but are used as two in one. Same applications offered through Web are customized and then offered as mobile applications, which can either be downloaded into the device or be used remotely as a service. The resulting convergence is of great significance but raise concerns on the level of security offered to users by the applications. The use of mobile applications to access sensitive information is indispensable, but their standards cannot be trusted since they can easily be put under control of attackers [5].

References [6] and [7] mentioned that lack of development standards, frameworks and languages have been mentioned as one among the factors contributing to insecure applications. Therefore, in this paper a review of seven selected security frameworks for Web and mobile applications is presented in the light of: their suitability for the converged Web and mobile applications services; and identification of security gaps if any.

The methodology used to conduct the review is as follows: Security frameworks to be reviewed were selected from both Web and mobile applications, respectively. Only a few (seven) of the available security frameworks for Web and mobile applications have been considered in the review. The selection criteria were to include specific frameworks that existed since 2000 until recently including a security framework for Web 2.0 technology. The frameworks include both practical and theoretical frameworks as regards to usage. The idea behind is to capture the trend in security advancement of the computing technology during this period of increased Web and mobile usage. After obtaining the candidate frameworks based on the selection criteria, the main characteristics of the selected frameworks were discerned and then their merits and demerits established as a part of the review. This analysis and comparison was ultimately used to discern security gaps in the existing security frameworks for mobile and Web applications.

Security frameworks for Web applications included in this review are; authorization framework for Web applications [8], analysis framework for Web applications [9], security framework for Web 2.0 applications [10], and GuardRails: Data centric Web security framework [11].

Security frameworks for mobile applications included in this review are; Secure SocialAware [12], Framework for Designing, Developing, and Using Secure Mobile Applications [13], and Mobile applications security framework [14].

In addition to the above frameworks assessment, the paper also tried to generally look at what has been done so far to help developers implement secure enterprise applications given the said convergence; and future directions towards secure applications development.

The remained sections of this paper are arranged as follows; Section II: security frameworks for Web and mobile applications, Section III: analysis and discussion, section IV: conclusion and recommendation.

II. SECURITY FRAMEWORKS FOR WEB AND MOBILE APPLICATIONS

A. Security Frameworks for Web Applications

Available Web applications frameworks such as Vaadin, Flight and Django do not provide enough assistance to enable Web application developers build secure applications without a great effort but rather help developers build quality applications [15]. They are general with less focus on security aspects of the applications. To remedy these challenges some frameworks have been developed to carter for the most important security flaws on the Web.

The whole work started with the Web based applications before the coming and evolving of mobile applications, so known frameworks are either targeted to Web or mobile applications, individually. The new shape of service delivery through Web and mobile applications, is making neither of the known security frameworks applicable for secure application development.

The work done by [8], discusses security issues that Web applications must face and thereby proposed an authorization framework. A challenge that triggered this development was the inability of Web servers to provide authorization services for sensitive Web applications such as electronic commerce. Due to this, developers implemented authorization systems together with the applications. Authorization of users into an application is crucial since a malicious user may override privileges and then exploit systems' vulnerable components.

In [8] the lack of controls on parameters and their contents in a Web request has been presented as one among the issues that cause majority of Web specific security difficulties from the server's perspective. This is basically an input related problem. The authorization framework presented in [8] categorizes the responsibility for managing in a role based manner; developers, policy administrators, system administrators, and end users. In the framework, security enforcement out of the application is what gave it the strength even to stand out of other frameworks that came later. From that perspective, the framework then required that, implementation of security controls be a responsibility of all Web application stakeholders.

The work of [9] contributed to the field by developing a framework for addressing input related problems particularly the SQL command injection in the context of Web applications. The authors focused on addressing only the class of SQL injection attacks based on previous works towards dealing with that category of attacks.

One issue with Web applications concerning user inputs validation is the assumption that user will enter valid inputs as the programmer intended. And on the other hand, the backend program may be set up with an assumption that the application will only send authorized input queries. The fact is, all input violations must be cached at the application level. Unlike other frameworks and techniques to address the problem of input validation, such as AppShield [16], InterDo [17], and Perl's [18], analysis framework presented in [9] considered the syntactic structure of generated queries to conclude them

as bad or unsafe queries. The analysis framework presented operated directly on the source codes of an application.

In the era of Web 2.0 applications, the problem of input related security threats had been worked on by various techniques, some mentioned on previous paragraphs. The emerging challenge in Web 2.0 applications concerns the support of secure execution of potentially malicious third party applications. Reference [10] described a security architecture for Web 2.0 applications that can support the integration of different technologies and applications for secure execution. As discussed in [10] there are potential harms caused by the execution of untrusted codes and consequently they defined solutions in the architecture provided.

Among issues in third party applications (untrusted) is the problem of permissions that can easily be exploited. Giving certain permissions to third party applications such as to create new connections has failed to put enough control over the potential harms of such applications; this is due to the fact that permissions once assigned do not give control to the user on how they are used. The only obvious solutions is, to sandbox the applications or allow them and let them do everything they are designed for. The defined architecture integrated policy enforcement technologies such as proof-carring code and inlined reference monitors, together with a defined support for applications contracts and the security by contract paradigm.

The whole work presented in [10] was carried under the assumptions that, all individual compliance modules and certification technology services are secure. This is a pitfall. Such unreliable implementation can validate an application that does not comply with the platform policy. However, the work presented in [10] described future work towards effectiveness of the architecture including an extensive evaluation and end-to-end threat analysis for the proposed architecture.

Reference [11] added on the work towards secure Web applications development by developing GuardRails, a data centric Web applications security framework. GuardRails adds on previous framework the capability to prevent other types of security challenges including cross site scripting attacks and access control violations while assuring a large degree of flexibility to support a range of policies and development styles.

GuardRails is a source to source tool for Ruby on Rails that was developed to assist application developers build secure Web applications. The framework was aimed at helping developers prevent the effects of security challenges other than input related ones. Main categories of threats dealt with the framework includes, cross site scripting (XSS) and access control. Moreover, the framework supports flexible application development under various policies and development styles.

An important contribution made by the GuardRails framework is the fact that security policies are attached to data objects and hence provide assistance to developers towards implementing secure applications without a great deal of effort. However, an issue with GuardRails is that, it has been tested and validated under two types of vulnerabilities; access control and injection attacks. This fact leaves a loophole in other vulnerable system components that cannot be covered by this framework.

B. Security Frameworks for Mobile Applications

Mobile applications have a number of requirements depending on their functionalities and users' contexts. For instance, a social networking application would have some different requirements from a common service provisioning application such as user privacy and availability. But generally security concerns for confidentiality (user and data privacy), data integrity and availability needs to be enforced for all kinds of mobile based applications.

The work presented in [12] describes a security framework for mobile social networking applications called Secure SociaAware (SSA). The framework was to remedy the consequences caused by the exchange of social network information such as users' position and preferences. Through SSA users of a social networking mobile application can exchange information without compromising their privacy. An issue about this framework is that it is limited to a small scope of mobile applications security concerns, and focused on user's security concerns only. Reference [12] discuss SocialAware [19], Whozthat [20] and Serendipity [21] frameworks for mobile social networking applications. As the work of [12] build on these three frameworks, Secure SocialAware is aimed at protecting data on transit to secure against attack through Bluetooth devices and eavesdropping.

On developing secure mobile applications and Web services there are number of issues to consider as described in [13]. The work described by these authors focuses on all issues to consider during design and implementation of mobile applications, together with a proposed framework to assist developers implement secure applications. The work of [13] describes the challenges of mobile applications, among them being variability of development platforms and the fact that each platform is independent of the others.

Reference [13] tried to remedy the challenges left by previous frameworks for mobile applications security such as Secure SocialAware [12], which are not only specific to mobile applications but also focused only on user's privacy. In applications security, different issues are dependent and have an impact on each other. Dealing with a single aspect at a time will not only leave a weak security level in the system but also unreliability of the set measures since mechanisms for one security flaw can easily be breached. The framework

described in [13] is of two major participants: the mobile client and the backend server.

Eivom Cinema guide mobile application was used to test the framework. However, the authors have not described extensively the implementation of the features/components of the framework. For instance, how they enforced security aspects in the secure layer interface component (part of the framework). Moreover, from the highlights given by the authors security enforcement have been made on the mobile client environment. The fact makes application codes attached to security procedures. On developing mobile applications this is a pitfall since security procedures can easily be studied through attacking the application codes on a mobile device [5]. Irrespective of the said drawback, the developed framework is practical to the current state of the computing world since it has integrated the mobile applications and mobile Web services (which is the convergence of Web and mobile applications).

Reference [14] stated that, new business opportunities lead to an emerging number of significant security threats for both enterprises and respective customers. A major security challenge defined by [14] in the new mobile era is that, apart from existing models/frameworks (defined as static) for mobile applications security, there is a need of defining a dynamic threat detection and protection model. According to the analysis done by IT Best Practices Network World (2013), at least 80% of mobile applications have security and privacy issues that still put enterprises at high risk.

The framework presented by [14] focuses on identifying unique security challenges in mobile applications, together with defining guidelines to overcome them. The framework is architecturally extensive in the sense that it has covered most of the issues with mobile application security including data protection, device management, application testing, and mobile application security.

Fig. 1 shows part of the security framework which describes an authentication model called a *zero trust pattern* which assess security parameters dynamically to allow a user or device access the needed system's data.

Another feature defined for systems' data security is called *device fingerprinting* that determine the characteristics needed to authenticate a device. This feature is very essential considering the fact that mobile devices can easily be put under attack or stolen. Therefore, all accesses from a device to databases or other systems must be authenticated even before the user is authenticated. Factors defined for device fingerprinting includes, Media Access Control (MAC) address, Operating System (OS) details, Wi-Fi profile, and location through GPS services. The framework also provides a guide to application developers on mobile device risk profiling. Therefore, the device fingerprinting for device authentication is to be accompanied by device risk profiling for dynamic authentication.

III. ANALYSIS AND DISCUSSION

A. Overview

Frameworks presented in above sections are those focused on addressing security challenges in Web and mobile applications development. Every work has contributed in part towards solving the existing security threat but the main challenge that is still encountered is the inability of the frameworks to adopt new techniques and diversified tools for avoiding security breach. However, most of these frameworks are focused on either Web or mobile applications separately. This fact results into inability of the set mechanisms to perform as expected when the system is expanded or some features are added to make it usable in both Web and mobile applications platforms. One reason for that can be the lack of standard for mobile applications development and the fact that each platform is specific in terms of coding, testing and deployment of mobile applications.

As discussed in previous sections, all frameworks presented possess some unique and identifiable merits towards solving some Web and mobile applications threats. Merits and demerits of each framework are highlighted in **Table 1.** From the highlights we show the need of developing a new framework that will help bridge the existing gap between Web and mobile applications security frameworks.

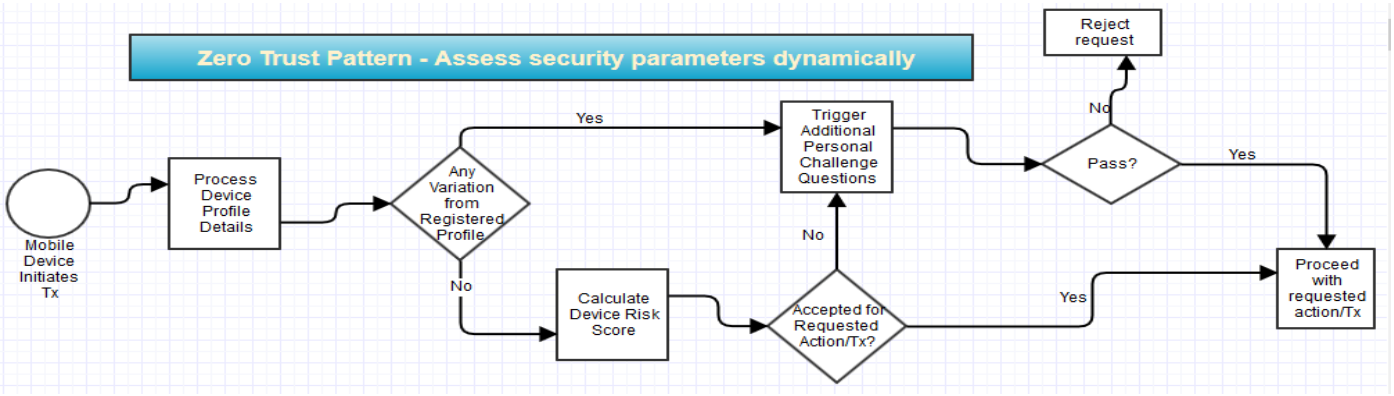

Figure 1. Dynamic assessment of security parameters
Source: Yadav & Mishra (2013)

TABLE 1
OVERVIEW OF DISCUSSED SECURITY FRAMEWORKS FOR WEB AND MOBILE APPLICATIONS

Framework	Context	Merits	Demerits
Authorization framework [8]	Web applications	The framework defined roles for each stakeholder of an application towards ensuring that security measures are enforced. Therefore security measures are enforced out of the application context.	The framework cannot be adopted for mobile applications and basically could help mitigate input related problems only.
nalysis framework[9]	Web applications	The framework uses syntactic structure of generated queries (user input) to determine if they are safe or unsafe. Other frameworks addressing input related problems did not have this feature	The analysis framework operates directly on source codes of an application. Due to this fact, the framework cannot be adopted for mobile applications since the source codes can be studied and lead to compromising the security functions.
Security framework for Web 2.0 applications [10]	Web applications	The framework presented is flexible since it has pluggable compliance modules. This feature supported by extensive evaluation can be adopted for mobile applications security.	The framework assumes that all individual compliance modules and certification technologies are secure.
GuardRails: Data centric Web security framework [11]	Web applications	Security policies are attached to data objects hence provide assistance to developers to implement secure applications. Security policies defined can be adopted for mobile applications but this depends on the development platform	The framework has been tested under two types of vulnerabilities; access control and injection attacks (XSS) only. This fact makes in less supportive to mobile applications since mobile applications have another wide range of security threats which have not been studied for this
Secure SocialAware (SSA) [12]	Mobile applications	The framework aimed at keeping user's privacy by giving location information of where the user is not currently available rather than where the user is currently available.	This framework is focused on social networking applications and user privacy only; this fact makes the frameworks not customizable for other types of applications having to access sensitive information from central databases and systems.
Framework for Designing, Developing, and Using Secure Mobile Applications [13]	Web and Mobile applications	Framework is applicable to the current state of the art since it has integrated mobile applications and Web services (the convergence of Web and mobile applications)	Security enforcement have been made on the mobile client environment, making security procedures be attached to the application code.
Mobile applications security framework [14]	Mobile applications	The framework ensures protection of data which is accessed by a mobile device by including a feature called device fingerprinting. Authentication here is done to the device and then to a user. This framework is dynamically designed to remedy the challenge left by other frameworks in that only static features are tested for application and data security.	The framework has not stressed the Web applications part. Since it is very dynamic and flexible the context can be extended by testing its validity on Web applications

B. On Going Challenges in Convergence of Web and Mobile Applications

The convergence of Web and mobile applications is evident in this era of computing as enterprises explore more opportunities and come closer to customers. This issue is less sensitive when someone just needs to have an application run on android devices (as a native mobile application) to access data and services offered remotely; or say just a Web application (native Web application) to offer the same service. The challenge lies on the fact that, Web and mobile applications have come together to allow users with various platforms to access same data. This phenomenon is unlike the use of native Web or mobile applications. With this improvement in the computing world, data is put more at risk in both the server side and mobile client side (since it is not a good idea to keep all data at the server for mobile applications due to some parameters like connection availability). The convergence of Web and mobile applications is due to a number of advantages of the combination, such as: cross platform compatibility in mobile applications, no need of developing applications for each platform like Android™, iOS™, Windows™, etc.; mobile applications are cheap, easy and fast to build and allow a large number of clients to be reached through minimal efforts.

The number one challenge that is still encountered in the field is lack of a security framework/model that is focused on mitigating the risks produced by the convergence of Web and mobile applications. Apart from that other challenges include:

- Mobile browsers still have low capabilities compared to desktop browsers resulting in inadequate check and track of security features such as session and cookies, and certificates.
- Mobile device users hardly have security software installed on their devices, this makes systems accessed through the devices prone to security attack.
- Applications developers hardly assess the security architecture and features in mobile browsers and operating system features before applications development.
- Mobile application users need training on secure use of applications and smart browsing for enterprise data and systems' security.

IV. CONCLUSION AND RECOMMENDATION

This review paper is focused on analysis of available security frameworks that help Web and mobile application developers implement secure systems. On top of that, a critical analysis has been done on the convergence of Web and mobile applications and the consequences on the security frameworks that are on use. It is shown that, most of the frameworks are focused on either native mobile applications or native Web applications. Hence the existing frameworks leave behind security gaps in the converged Web and mobile applications. The security gaps are on customizing the Web applications security frameworks to be used for mobile applications, attachment of security procedures on application codes, and the frameworks being validated by using few security threats (mainly are the input related problems). These security gaps are due to the fact that, existing security frameworks were designed for traditional Web or mobile applications. From the analysis and evaluation, it is clearly established that there is a need for a new security framework/model that is more encompassing and thus able to address the existing challenges/gaps towards secure mobile and Web applications.

ACKNOWLEDGMENT

We sincerely appreciate the Nelson Mandela African Institution of Science and Technology (NM-AIST) through the school of Computation and Communication Science and Engineering (CoCSE) for supporting this work to completion.

REFERENCES

[1] P. Ruggiero, and J. Foote, "Cyber Threats to Mobile Phones," United States Computer Emergency Readiness Team, pp1-6, 2011.

[2] J. Oltsik, "Enterprises Are Experiencing a Wide Variety of Web Application Attacks," Available: http://www.esg-global.com/blogs/enterprises-are-experiencing-a-wide-variety-of-Web-application-attacks. Last accessed 23/10/2013.

[3] P. Asadoorian, L.Pesce, and Strand, J. "Best of Network Penetration Testing Tools," PaulDotCom Enterprises, LLC. pp1-51, 2009.

[4] Mainka, J. Somorovsky, and J. Schwenk, "Penetration Testing Tool for Web Services Security," Horst Gortz Institute for IT Security, pp1-8, 2011.

[5] B. Prince, "Mobile Application Developers Face Security Challenges," eWEEK, 2010.

[6] J. Lounsbury, "Application Security: From Web to Mobile. Different Vectors and New Attacks," Security in Knowledge, pp2-30, 2013.

[7] K. Johnson, and J. Jardine, "2013 SANS Mobile Application Security Survey: A SANS White Paper," SANS Analyst Program, pp1-14, 2013.

[8] D. Jacobs, "An Authorization Framework for Web-based Applications," MITRE Corporation, pp1-14, 2000.

[9] G. Wassermann, and Z. Su, "An Analysis Framework for Security in Web Applications," INPROCEEDINGS, P1-9, 2004.

[10] 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, pp35-46, 2009.

[11] J. Burket, P. Mutchler, M. Weaver, M. Zaveri and, D. Evans, "GuardRails: a data-centric web application security framework," In Proceedings of the 2nd USENIX conference on Web application development, pp. 1-1 USENIX Association, June 2011.

[12] M. Beach, 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.

[13] 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, 2010.

[14] K. P. Yadav, and R. Mishra, "Mobile Application Security Framework, " IT Best Practices Alert, Network World. pp1-5, 2013.

[15] Grönroos, Marko. Book of Vaadin. Vaadin Limited, 2011.

[16] S. Inc. (2002). Appshield 4.0 whitepaper. 2002. Available: http://www.sanctuminc.com. Last accessed: 5/12/2013

[17] I. Kavado, InterDo Vers. 3.0, 2003.

[18] L. Wall, T. Christiansen, and R. L. Schwartz, *Programming Perl*, 3rd Ed. O'Reilly, 2000, pp23-45.

[19] C. M. Gartrell, "Socialaware: Context-aware multimedia presentation via mobile social networks," ProQuest, 2008.

[20] M. Beach, Gartrell, S. Akkala, J. Elston, J. Kelley, K. Nishimoto, and R. Han, "Whozthat? Evolving an ecosystem for context-aware mobile social networks," Network, IEEE, Vol. 22, no. 4, pp50-55, 2008.

[21] N. Eagle, and A. Pentland, "Social serendipity: Mobilizing social software," Pervasive Computing IEEE, Vol. 4, no. 2, pp28-34, 2005.